

Child safety online

PROTECTING AND EMPOWERING
MINORS IN A DIGITAL WORLD

REPORT BY THE CO-CHAIRS OF THE SPECIAL
PANEL ON CHILD SAFETY ONLINE

Prof. Dr. Jörg M. Fegert and Dr. Maria Melchior



This document should not be considered as representative of the European Commission's official position.

Luxembourg: Publications Office of the European Union, 2026

© European Union, 2026



The Commission's reuse policy is implemented under Commission Decision 2011/833/EU of 12 December 2011 on the reuse of Commission documents (OJ L 330, 14.12.2011, p. 39, ELI: <http://data.europa.eu/eli/dec/2011/833/oj>). Unless otherwise noted, the reuse of this document is authorised under the Creative Commons Attribution 4.0 International (CC BY 4.0) licence (<https://creativecommons.org/licenses/by/4.0/>). This means that reuse is allowed, provided appropriate credit is given and any changes are indicated.

For any use or reproduction of elements that are not owned by the European Union, permission may need to be sought directly from the respective rightholders.

Content

FOREWORD

→ 04

PREFACE

Growing up safely in the social media+ world

→ 07

CHAPTER 01

A developmental approach to child safety online

→ 28

CHAPTER 02

Evidence on risks minors face online

→ 52

CHAPTER 03

Protecting minors in a rapidly changing social media+ environment

→ 76

CHAPTER 04

Empowering minors to safely navigate the digital world

→ 114

ACKNOWLEDGEMENTS

→ 137

Foreword

In March 2026, European Commission President Ursula von der Leyen tasked two Special Advisers – Prof. Dr. Jörg M. Fegert and Dr. Maria Melchior – with co-chairing the Special Panel on child safety online and potential age restrictions for social media. The Co-Chairs were tasked to write a report on the outcomes of the panel and to advise on the best approach for Europe to make the online world safer for children.

First announced in the 2025 State of the Union address by the Commission President, the panel brought together high-level academics, practitioners, youth and parent representatives and other specialists from diverse fields across Europe to assess the impact of social media on minors.

The Special Panel met three times and involved varied specialists on each occasion. The first Special Panel took place on 5 March 2026 and examined the existing scientific evidence concerning the impact of social media, and more broadly the digital environment, on children and adolescents.

The second Special Panel took place on 16 April 2026 and discussed existing EU legislation and tools, and national policy approaches to address child safety online.

The third Special Panel met on 16 June 2026 and focused on national policy approaches and potential recommendations to protect and empower children and adolescents in the digital world.

“And in all of this work we will be guided by the need to empower parents and build a safer Europe for our children. Because when it comes to our kids’ safety online, Europe believes in parents, not profits.”

— EUROPEAN COMMISSION
PRESIDENT URSULA VON DER LEYEN,
STATE OF THE UNION ADDRESS, 2025

KEY TOPICS DISCUSSED DURING THE PANELS INCLUDED:

- // The positives and negatives of introducing specific age restrictions for social media and other digital services;
- // Tailored approaches to protect and empower minors based on age groups, socioeconomic background and age-specific risks;
- // Safety by design/default and the responsibility of social media and other digital services providers;
- // Educational and awareness measures to promote responsible online use among children and adolescents, parents and caregivers, teachers and educators;
- // Ways to support parents and educators, and to empower children and adolescents to seize the opportunities of the digital world.

The analysis and recommendations of this report are informed by crucial contributions from a diverse group of specialists invited for each panel meeting and numerous additional meetings with representatives of Member States, especially those hosted by the Irish Presidency of the Council of the EU and Luxembourg (D9+ Ministerial meeting), third countries (including Australia and Brazil), the European Parliament and its Members, especially of the Intergroup on Children's Rights; industry, civil society, think tanks, and other organisations, including the UN OHCHR and the European Data Protection Board (EDPB).

Following these interactions and based on the collected evidence, the Co-Chairs developed their recommendations. While the responsibility for the recommendations lies solely with the Co-Chairs, their work owes a great deal to the input of other renowned experts, parents' and youth representatives, and to expertise provided by the European Commission.

The report is intended to inform future actions to be proposed by the European Commission and EU Member States to reinforce child safety online. This independent analytical assessment provides recommendations and inspiration for children and adolescents, parents and caregivers, teachers and educators, and social media and other digital services providers on how to better protect and empower minors online.

SCOPE AND TERMINOLOGY

The main task, as prescribed by President von der Leyen, was for the Special Panel to discuss child safety online and potential age restrictions for social media. While the scope of this report adheres to this tasking, the evolving discussions during the Special Panel meetings and other political developments (for instance, the G7 Leaders' Call on a safer digital space for minors of 17 June 2026) underscore the need for the Co-Chairs to precise the terminology used in this report.

Without prejudice to any international, EU or national legal acts, the following terms and corresponding definitions are used throughout this report:

Social media and other digital services (in short, social media+)

Within the scope of this report, the terms 'social media+' and 'social media and other digital services', are used to broadly define services that may be available to minors and contain age-inappropriate and/or risky features (for example, addictive and harmful features, among which infinite scroll, autoplay, recommendation algorithms and persistent notifications) and/or content. Social media and other digital services providers include online platforms serving as intermediaries of content from third parties, such as social media, as well as app stores. AI systems posing risks to minors' safety and development, including AI companions, video games exposing children to harmful commercial practices or dangerous contacts, and video-sharing platforms enabling age-inappropriate access to minors are also included.

Minors, children and adolescents

Without prejudice to the legally defined use of the term 'children' (for example, in the United Nations Convention on the Rights of the Child), this report argues for the need for a developmental approach to protecting minors online, which addresses the specific risks and vulnerabilities they are exposed to at different ages. For the purpose of this analysis, the authors use the term 'minors' to refer to all children and adolescents under the age of 18 (the age of majority). The term 'adolescents' applies to all minors from 13 to 18. The term 'children' refers to all minors under the age of 13. This report uses the term 'children's rights' to refer to the rights of all children under the age of 18, as defined in legal texts. The term 'child safety online', as stated in the mandate of the Special Panel process, is used as an umbrella term for the protection and empowerment of minors in the digital world.

PREFACE

Growing up safely in the social media+ world

The rapid advancement of digital technologies has radically changed the way children and adolescents grow up, interact with their peers, parents, teachers and the world around them. At the same time, activities in the offline world remain crucial for learning, fostering meaningful relationships and experiences that shape minors' development.

The social media+ world offers many opportunities for children and adolescents to learn, connect, participate and create. Yet, minors need to be educated and empowered to seize these opportunities to reach their full potential.

Despite this, **social media+ spaces also present a number of risks** to minors' healthy development and well-being. This includes risks of excessive use due to addictive features, the substitution of developmentally favourable activities, exposure to harmful content and inappropriate contacts online. These risks are amplified by the emergence of new technologies and require bold, but careful choices to protect children and adolescents online.

The wide adoption of social media and other digital services has made **policymakers and parents extremely worried about the threats children and adolescents face online**. While age restrictions for access to social media and other digital services have been met with criticism, **they may be a necessary precautionary step** until social media+ spaces are shown to be safe to be accessed by children and adolescents or until safe alternatives emerge.

Age restrictions are not about making parents and caregivers or children and adolescents themselves primarily responsible for minors' safety online. Neither are they about letting providers 'off the hook'. **Social media and other digital services providers retain primary responsibility for the safety of the services they develop and provide.**

The burden of proof needs to be on providers, not regulators, parents and children. **Until they demonstrate that their services are safe by design, social media and other digital services providers should have restricted access to children under the age of 13 in the EU.** In addition to EU-wide restrictions, further precautionary age restrictions may be introduced by Member States for adolescents older than 13.

Precautionary age restrictions are immediate measures to achieve the long-term goal of ensuring social media+ spaces are safe for minors by promoting cultural change. Early results from countries that have introduced blanket age bans to access social media show that most minors find a way to circumvent these policies. At the same time, some minors have withdrawn from risky social media and other digital services and now have more time for offline activities (such as sport and face-to-face social interactions). This demonstrates that progressive change surrounding the norms of social media+ use by minors is possible and must be recognised.

Yet, change takes time. As an example, societal attitudes with respect to the legislative prohibition of corporal punishment in education evolved over more than a generation (for instance, in Germany and Sweden). The prohibition of corporal punishment clarified expectations for parents, caregivers, teachers and educators, and enhanced bystander engagement to ensure the non-violent upbringing of minors. The success of this measure has been proven with the positive trends and by constant evaluation since its introduction.

The efficacy of age restrictions would also require societal attitude change. Continuous evaluation and long-term monitoring can help policymakers to understand if the habits of minors and their parents, caregivers, and educators will change over time.

Growing up in today's social media+ world, children and adolescents must be enabled to lead healthy and fulfilling lives, and to take advantage of the opportunities provided by social media and other digital services. **Children's rights apply online just as they do offline** – from the right to be safe and protected from economic exploitation and crime in all forms (in particular, sexual violence), to the right to access information, education, and leisure.

Children have the right to grow up in an environment that is safe and favours their development, both online and offline. While supporting minors offline should continue, we also need to recognise that online environments have become an increasingly important part of minors' daily lives. This is why protection must be ensured by default throughout all social media and other digital services.

Children's rights must underpin online child safety measures. Potential age restrictions must be in full respect of children's rights, proportionate and balanced against children's best interests. The means used to achieve this must keep pace with technological developments.

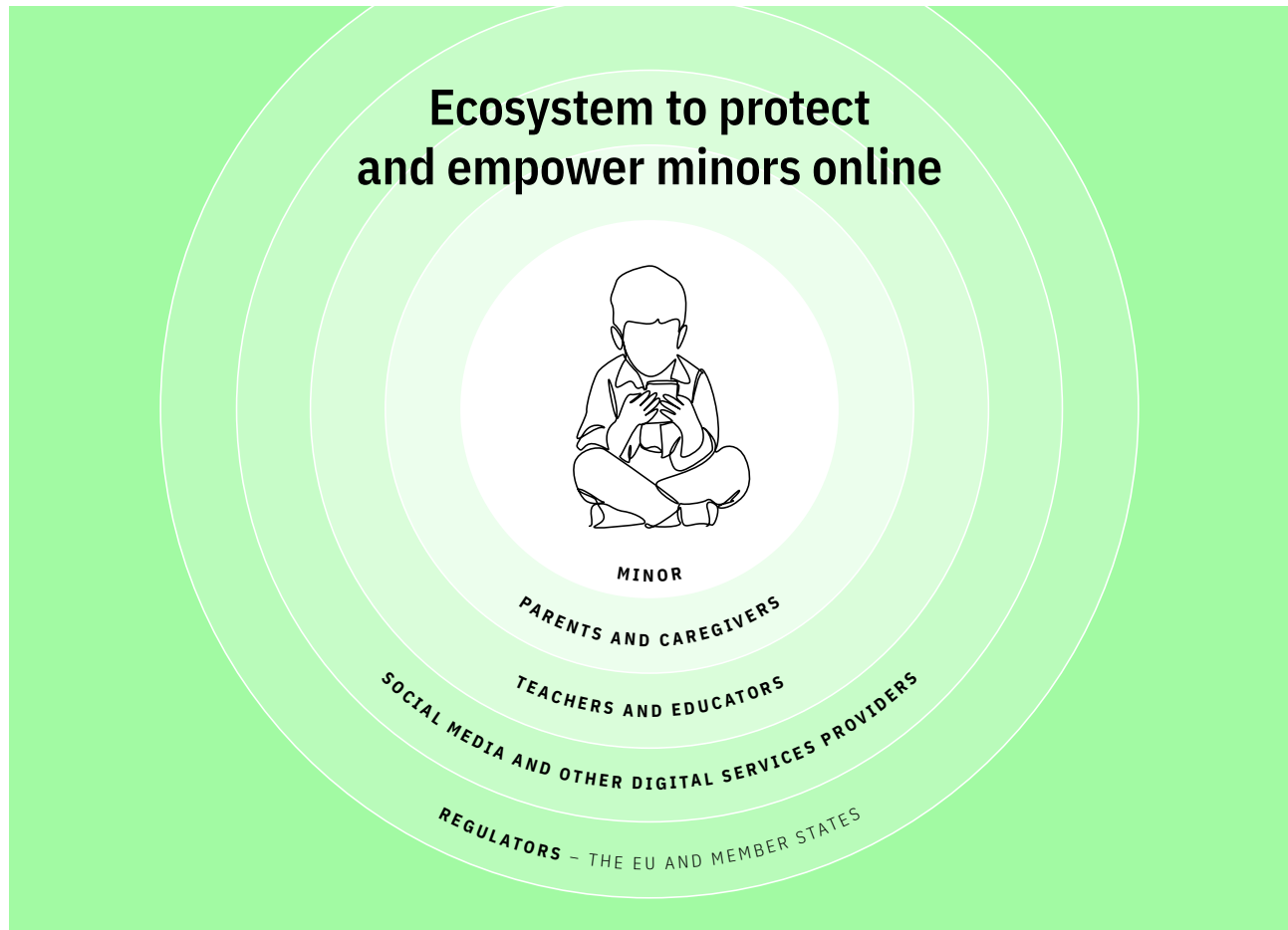
While social media and other digital services providers retain primary responsibility for the safety of their services, especially for minors, an **ecosystem of actors is needed to protect and empower children and adolescents in the social media+ environment.** From regulators who need to put in place necessary measures, to providers which offer safe and age-appropriate services, to parents, caregivers, teachers and educators who play a key role in supervising and guiding minors' online use. As minors mature and

“For decades, we have made the real world safer for children and we must do the same in the digital world. The positive opportunities that technology offers cannot come at the cost of their safety, health or happiness.”

— EUROPEAN COMMISSION PRESIDENT
URSULA VON DER LEYEN

social media+ environments change rapidly, **the success of the ecosystem depends on the interconnected actions of all actors** sharing the same vision: children and adolescents growing up safely in a digital world.

Figure 1: Ecosystem to protect and empower minors online



Increasing political momentum to strengthen child safety online

The past months have shown that child safety online is becoming a political priority around the world. The **introduction, implementation and continuous evaluation of a ‘social media delay’ by Australia have offered key lessons to the rest of the world.** Other countries, such as the United Kingdom and Canada have followed suit with planned legislative proposals, while Indonesia has already adopted a ban.

A recent report suggests that 92% of Europeans think that strengthening the protection of children and young people online should be a priority for the EU^a.

a. European Commission (2026). [Digital decade – Eurobarometer report – February – March 2026](#).

European leaders have also started addressing the issue. The Jutland Declaration^b in September 2025 and the European Parliament resolution calling for an EUwide digital minimum age^c, the establishment by President von der Leyen of the Special Panel on child safety online, and the recent conclusions by the European Council^d are clear signs that there is increasing political momentum to take concrete steps to address the growing risks children face online.

In June 2026, for the first time, the G7 – including Canada, France, Germany, Italy, Japan, the United Kingdom, the United States and the European Union – agreed at the highest political level on common principles to protect minors from digital services that pose risks^e.

Moreover, **several EU Member States are legislating to establish a minimum age to access social media and other digital services** that may expose children and adolescents to harm. For example, France is currently proposing a limit at 15 years, based on a blacklist of restricted services. Greece is envisaging a limit of 15 years for online social networking services. Denmark is considering a limit for minors under 16, with an option to lower the age with parental consent. Sweden envisages a limit based on the year the child turns 15, with several types of services exempted. Many others, from Portugal and Spain to Germany and Poland, are considering legislating on this topic.

Against this backdrop, the fragmentation of the European Single Market for digital services is a real risk. In view of this, many Member States are calling for the matter to be addressed at the EU level. It should be recognised that Member States have different cultural and national contexts concerning education, digital literacy and the protection of minors. Fragmentation could lead to minors enjoying different levels of protection across the EU. This would also mean regulators could be confronted with practical complexities regarding enforcement and providers with higher compliance costs. This could have knock-on effects on the development of safer social media and other digital services and the effectiveness of online safety laws.

The EU has already taken concrete action to protect minors. Recent decisions taken by the European Commission have only underscored the necessity to address the threats children and adolescents face online with concrete evidence. The preliminary findings against Meta and TikTok for allegedly failing to meet the high standards to protect minors online required under the Digital Services Act (DSA) and failure to provide easily accessible mechanisms to flag child sexual abuse content are clear examples. Moreover, recent landmark decisions by US courts have marked a historic turning point in the debate on platform liability.

A short history of protecting minors online

Efforts to protect children and adolescents online are as old as the internet and originate from a time before social media, smartphones and AI. The foundations of today's rules to protect minors online were laid in the 1990s and early 2000s, with laws designed to enable services and businesses to operate and exchange information across borders. Although these rules were not designed for the sole purpose of

b. Danish Presidency, Council of the European Union (2026). [The Jutland Declaration: Shaping a Safe Online World for Minors](#).

c. European Parliament (2025). [Protection of minors online – European Parliament resolution of 26 November 2025 on the protection of minors online \(2025/2060\(INI\)\)](#).

d. European Council (2026). [European Council conclusions](#), 19 March 2026.

e. G7 (2026). [Leaders' call on a safer digital space for minors](#).

protecting children and adolescents online, they established many of the principles that continue to underpin current legislation in three areas.

First, the regulation of media and digital services in the internal market introduced common rules for television services across Europe, including safeguards against content that could be harmful to minors. The first harmonised framework for online or ‘Information Society Services’ (under the e-commerce Directive) also supported the development of cross-border online services within the EU.

The second area is data protection and privacy rules, starting with the 1995 Data Protection Directive’s common standards for the collection and use of personal information across Member States.

Third and finally, consumer protection. Common EU rules tackle misleading and aggressive commercial practices. These rules recognise that vulnerable consumers need additional protection, a significant principle in the digital environment. This includes where children and adolescents are exposed to commercial practices that may affect them differently to adults.

As digital technologies became deeply embedded in everyday life, the EU has continued to update these legal frameworks to respond to new challenges. The General Data Protection Regulation (GDPR) introduced specific protections to safeguard children’s personal data and consent online. The Audiovisual Media Services Directive was expanded to cover new forms of audiovisual content and video-sharing platforms. Finally, the Digital Services Act established rules for online intermediary services, including for the specific purpose of protecting minors.

This evolution reflects a broader trend: digital technologies no longer fit neatly into a single regulatory or legal category. Social media and other digital services combine elements of media, communication, commerce and data processing, often within the same platform. As a result, an effective approach to protecting minors online must be holistic, drawing on instruments in several areas of EU law, including platform regulation, data protection, consumer protection, and audiovisual media regulation.

With the rapid development and roll-out of AI, the risks to minors online are being supercharged. This is coupled with the continuous evolution of social media and other digital services to capture and retain users’ engagement in today’s ‘attention economy’. The need for regulators to step in to strengthen the protection of minors and to empower them to navigate the social media+ world safely is greater than ever.

The evidence on the risks and opportunities minors face online

Rapid technological change has brought extraordinary opportunities for children to exchange with peers, to express their creativity, and to access knowledge and support. However, children are not adults, and the social media+ environment exposes them to diverse risks for their physical and mental health and development at different ages. Socioeconomic and individual factors, such as family background and gender, as well as the design of social media and other digital services, also have determining influences.

Robust evidence on how risks and harms relate to social media and other digital services is crucial to inform appropriate actions to protect and empower minors online. Specific features, functionalities or formats implemented in social media+ may be harmful to a different extent, depending on a child’s or adolescent’s social and personal circumstances. Minors belonging to racial, ethnic and religious minority groups, members of the LGBTIQ+ community, those with special educational needs or pre-existing

mental health conditions may be particularly vulnerable to harm online. This vulnerability is, of course, magnified by social media and other digital services with harmful, manipulative or addictive content or designs. As these features evolve, so should research and evidence gathering.

The physical and mental health risks social media and other digital services pose to minors are extensive. In terms of physical health, excessive screen time replaces outdoor play and sport and can impact children's health, fitness and sleep. Using social media+ and devices at an early age displaces hands-on exploration and in-person social interactions. This may affect socio-emotional development and susceptibility to mental health issues. Prolonged device use can also provoke problems, such as musculoskeletal issues and digital eye strain.

The mental health risks posed by using social media and other digital services to children are significant. The risks of the social media+ environment directly harming children's mental health intersect with their potential to exacerbate pre-existing mental health issues, including depression and anxiety. Here too, social and individual factors determine children's and adolescents' exposure to risks.

In general, high social media and other digital services use among children and adolescents is associated with sleep and concentration problems, and increased rates of depression and anxiety. Addictive design features amplify these effects by encouraging compulsive checking, 'fear of missing out' (FOMO) and heightened social comparison. This can erode minors' self-esteem and heighten stress. Algorithmic amplification and recommender systems have the potential to enhance disinformation and hate speech. Strong harm from these effects is experienced in particular by vulnerable groups online.

The risks that minors are exposed to criminal and illegal content online are considerable. Both adults and minors purposefully exploit social media and other digital services, including gaming platforms, to engage with children and adolescents. Risks include exposure to child sexual abuse (material), grooming, cyberbullying, radicalisation and incitement to commit illegal, violent or terrorist acts. The widespread use of AI tools poses serious threats to children and adolescents from the production of synthetic child sexual abuse material (for example, deepfakes). These misuses have drastic effects on minors' development, their mental and physical health, and – in the most serious cases – may cost their lives.

Social media and other digital services providers retain primary responsibility for keeping minors safe on their services. In addition, parents and caregivers have important roles in supervising children's and adolescents' time online, and in guiding minors in addressing the risks they face in social media+ environments together. Ensuring adequate offline activities and in-person interactions is crucial at every age.

Despite multiple potential harms, **the social media+ world offers children and adolescents many opportunities.** When minors are empowered to interact safely online and have solid digital skills, the use of social media and other digital services can benefit well-being, social connectedness, provide supportive peer networks, opportunities for self-expression, civic engagement and independent learning. Targeted digital skills initiatives — such as the EU's Better Internet for Kids, Safer Internet Centres, and the embedding of media literacy into national education and training curricula — have demonstrated their ability to improve critical thinking, resilience to disinformation, and minors' ability to navigate safely online.

Social media and other digital services that are 'safe by design' could contribute to children's and adolescents' empowerment and participation online by supporting the acquisition of digital skills and media literacy. Age-appropriate digital education delivered by schools with the support of parents and caregivers could also equip minors to seize the opportunities of the online world and to manage possible risks and harms.

The need to address age-specific risks

As children grow up and become more independent, parents' ability to supervise children's online activities decreases. The role of peer influence grows. During adolescence, as they reach majority, minors become increasingly autonomous in their online use and better be able to understand and tackle the risks they are exposed to online. A 3 year-old and a 16 year-old naturally have different needs. This underscores the **importance of a developmentally sensitive approach to child safety online** as we applied it in this report, **by differentiating between various age groups**:

Under the age of 3, children primarily suffer from relational risks and 'technoference'^f as passive online users. Risks largely stem from caregivers substituting direct interaction with screen time to 'calm' or distract small children. This may impact children's attention span, language acquisition, and socio-emotional development.

Between 3 and 5, children as emerging independent users with supervision, are increasingly vulnerable to the risks present in online environments and related to higher screen exposure. Social media and other digital services that are optimised for immediate gratification, repetitive reward and continuous external stimulation are fundamentally mismatched with children's developing capacities and can harm their long-term development.

Between 6 and 9, children's use of social media and other digital services expands significantly. Externalised feedback from the online world (for example, likes, scores and leaderboards) intersects with emerging self-esteem based on developing competencies in the real world. This may amplify anxiety about performance and peer comparison, increasing vulnerability to cyberbullying, hate speech, and harassment by peers.

Between 10 and 12, children's access to social media+ spaces becomes a central prerequisite for social participation. At this age, children are confronted with the most acute convergence of developmental sensitivities and platform-driven amplification. Algorithmic recommendation systems intensify social comparison, exposure to harmful or illegal content (including child sexual abuse material, extremist propaganda, and disinformation) and to addictive design patterns that heighten symptoms of depression and anxiety. Recent prospective research suggests that acquiring a smartphone for the first time at 12 (rather than 13) may be linked to a higher risk of depression and other mental health issues after one year^g. This example highlights that, in general, children are especially vulnerable under the age of 13.

Between 13 and 15, adolescents transition from supervised to evolving autonomous use of social media and other digital services. At this age, traditional forms of supervision by caregivers and educators at school become increasingly ineffective. Risks are increasingly shaped by the structures of social media and other digital services, rather than individual behaviour alone. A key challenge lies in addressing algorithmic systems that structure exposure and influence behaviour, while operating with limited transparency.

The transition to autonomy is a normal part of growing up in today's online world, as it is offline. The question therefore is not how to hold adolescents back in their transition to autonomy, but how to limit their exposure to harm during a stage of peak developmental vulnerability. Effective protection requires a developmentally informed, multi-layered approach combining social media and other digital services regulation, educational interventions, and support for self-regulation and critical media use.

^f. The interruption of parent-child interactions by technology.

^g. Children's Hospital of Philadelphia (2026). [Age Limits Alone Won't Fix Smartphone Risks, Suggests Children's Hospital of Philadelphia Study](#). Accessed on 12 July 2026.

Finally, **between 16 and 18**, adolescents experience a stage of increasing identity consolidation and growing autonomy. Adolescents' evolving capacities better equip them to understand and handle the risks they confront online. However, neurobiological development is far from complete, and risks of addiction, anxiety and mental health issues are exacerbated by social media and other digital services use. Adolescents at this age need to acquire the necessary skills (for instance, critical thinking and evaluation) to successfully and safely navigate the digital world, and to seize its full potential.

Six Guiding Principles to protect and empower minors online

The presence of both risks and opportunities for children and adolescents in the social media+ environment calls for a comprehensive policy framework that both protects and empowers minors online. The following **Six Guiding Principles developed by the Co-Chairs steered the work of the Special Panel** and are reflected in the structure of this report. Measures should be built on robust evidence and analysis of the challenges and opportunities children face online. Effective implementation and evaluation are key to ensure results.

PRINCIPLE 1

Developmental approach (see chapter 1)

Ensure age-appropriate regulation and differentiated guidance. Children's and adolescents' staged development calls for the design and deployment of protection measures that address the risks they face at specific ages. Where possible, these measures should take into account children's personal and social circumstances, which may have compounding effects on their exposure to risk.

PRINCIPLE 2

Equality and diversity (see chapter 2)

Recognise inequalities in risks and exposure to online harms for different ages and socioeconomic groups. Gender, sexuality, racial, ethnic and religious backgrounds, special educational needs and pre-existing mental health issues all determine minors' vulnerability to online harms. These factors also influence the resources and capacities parents and caregivers have to support children and adolescents along their road to autonomy.

PRINCIPLE 3

Protection of minors (see chapter 3)

Children and adolescents must be able to benefit from safe social media+ spaces. The protection of minors against harmful content, addictive features, digital neglect^h and crimes online (for example, sexual abuse) should be implemented in the design of social media and other digital services. Any harmful content or features should be easily reportable by minors. Such reports should be prioritised and harmful content or features promptly removed by providers.

h. A caregiver's repeated failure to provide developmentally appropriate attention, responsiveness, supervision, or protection because digital technologies interfere with, replace, or undermine essential caregiving functions.

PRINCIPLE 4**Accountability of digital services and consumer rights (see chapter 3)**

Social media and other digital services providers must take primary responsibility for ensuring online spaces are safe for minors to access and use. Incentivise ‘safety by design’ measures by digital services and rapidly enforce content-based regulation. The burden of proof should be on social media and other digital services providers to prove the features of their services are not harmful before they can access children and adolescents.

PRINCIPLE 5**Empowerment and media education (see chapter 4)**

Enable parents and caregivers, teachers and educators to support children’s and adolescents’ gradual transition to safe and autonomous online use. Offer sufficient opportunities (for example, digital and media literacy training) and adequate infrastructure to enable parents to reflect on their own activities and to guide minors’ online interactions. Measures must be tailored to caregivers’ and educators’ roles, which evolve as children and adolescents mature.

PRINCIPLE 6**Children’s rights and participation (see chapter 4)**

Safeguard children’s right to safe participation, interaction and co-creation, online and offline. Children’s rights, as understood under relevant international frameworks,ⁱ should always underpin child protection measures. Age restrictions must respect the rights of the child online, be proportionate, time-limited and balanced against children’s best interests. This also underscores the need to invest in and to promote offline activities for minors at all ages.

Special Advisers to the President and Co-Chairs of the Special Panel on child safety online



Prof. Dr. Jörg M. Fegert

*Medical Director of the Department
of Child and Adolescent Psychiatry,
Psychosomatics and Psychotherapy
at the Ulm University Hospital*



Dr. Maria Melchior

*Research Director at the French
National Institute of Health and
Medical Research (INSERM)*

i. Notably, the United Nations Convention on the Rights of the Child and the general comments of the Committee on the Rights of the Child, the Charter of Fundamental Rights of the European Union, and the EU Strategy on the Rights of the Child.

SIX GUIDING PRINCIPLES

To protect and empower minors online

CHILD SAFETY ONLINE

ANALYSIS OF THE SITUATION

DEVELOPMENTAL APPROACH

Ensure age-appropriate regulation and differentiated guidance

EQUALITY AND DIVERSITY

Recognise inequalities in risks, exposure, and digital harms across all groups

PROTECTION OF MINORS

Protect against harmful content, addictive design, digital neglect, crimes (e.g. sexual abuse, bullying)

ACCOUNTABILITY OF DIGITAL SERVICES AND CONSUMER RIGHTS

Enforce safety by design and content-based regulation

EMPOWERMENT AND MEDIA EDUCATION

Enable parents and caregivers to support minors' digital skills and media literacy for responsible use

CHILDREN'S RIGHTS AND PARTICIPATION

Safeguard the right to safe participation and co-creation online

MEASURES

EVALUATION

Key recommendations to protect and empower minors online

The overarching objective of the recommendations of this report, building on the developmentally sensitive approach and reflecting the Six Guiding Principles, are to balance the necessity to protect children and adolescents online with their rights to participate in and seize the opportunities of the social media+ world.

Recommendations on age-appropriate use of social media and other digital services

0 TO 2 YEARS OLD

Avoid screens and social media+

Avoiding extensive screen exposure during early childhood does not mean an outright ban. Instead, it recognises children's developmental needs concerning attachment, sensory development and early language acquisition. Parents and caregivers should prioritise face-to-face interactions and be mindful of their own use of digital devices to offer a positive role model and avoid 'technoference'. This approach is in line with recommendations of the World Health Organization to prevent disruptions to children's neurobiological and cognitive development, emotional attachment formation and physical problems (for example, affecting vision).

3 TO 12 YEARS OLD

Supervised use of age-appropriate social media+ and devices

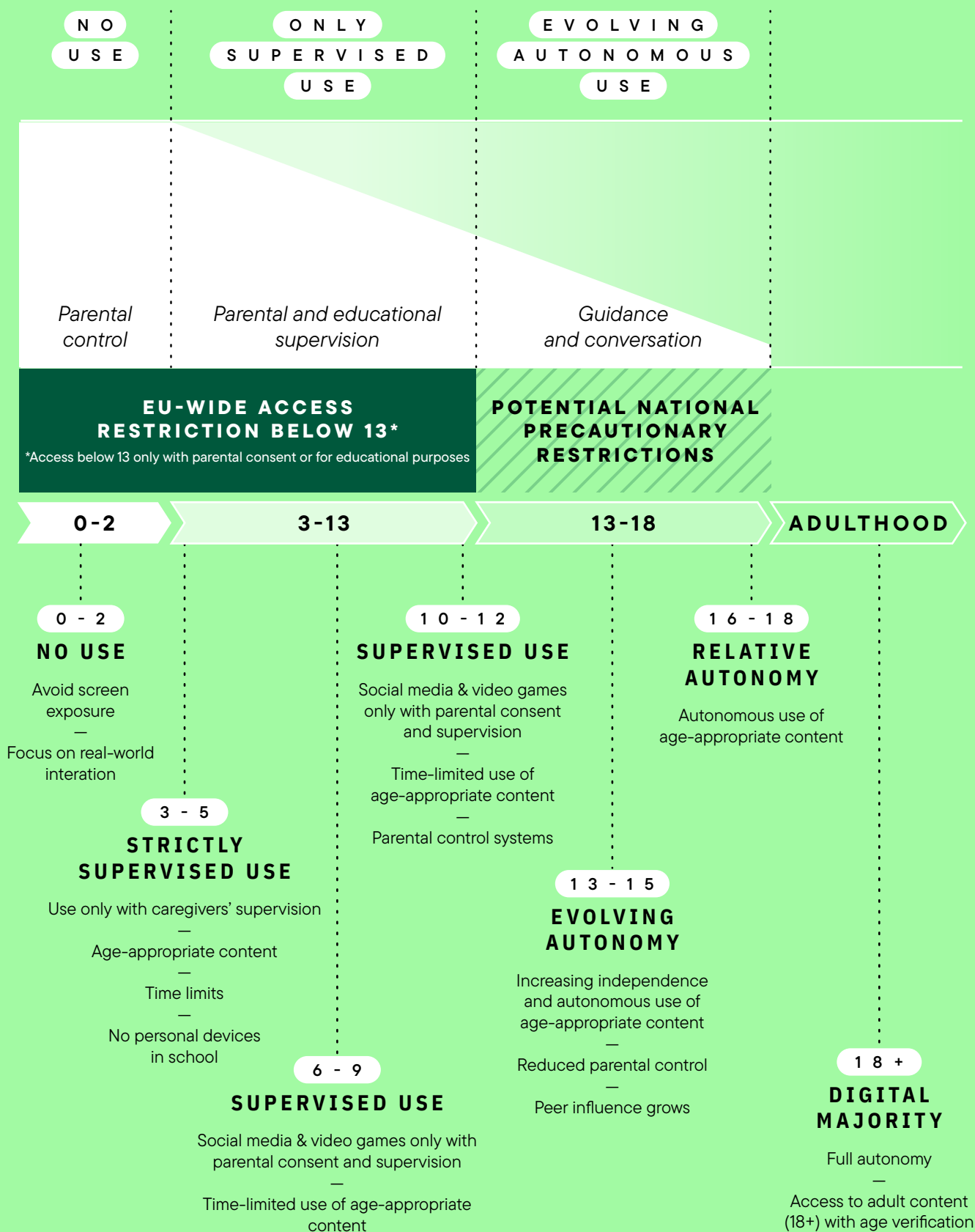
Children should not be allowed unsupervised use of internet-enabled devices. Schools should provide the facilities for supervised and limited use of devices for educational purposes supporting digital and media literacy, emotional resilience, and critical reflection on risks. Parents and caregivers should supervise and support digital autonomy gradually with age-appropriate social media and other digital services. They should also have regular conversations with children on the potential benefits and risks of minors' interactions online. Both caregivers and educators should continue to encourage children at this age to take part in offline activities.

13 TO 18 YEARS OLD

Evolving autonomous use of age-appropriate social media+

From 13 to 18, adolescents should only have access to age-appropriate and 'safe by default' social media and other digital services that have actively introduced key safety features (for instance, limits to infinite scroll and recommender systems). Until these 'safe by default' social media and other digital services are developed, individual age-appropriate parental control and supervision remain essential. Additional precautionary measures by regulators might be considered. As adolescents above 16 move towards greater digital autonomy, the risks related to exposure to harmful content online remain. As such, parents and caregivers should continue conversations with minors about their online experiences. Adolescents should have privileged access to support services and complaint systems, while benefitting from peer support networks promoting the responsible use of social media and other digital services.

Age-appropriate use of social media+ by minors



Recommendations to protect children and adolescents online

// **Propose a harmonised EU-wide access restriction to social media and other digital services for children under 13.**

A harmonised EU-wide access restriction to social media and other digital services, including AI companions, for children under 13 is necessary. A harmonised access restriction would facilitate the implementation of proportionate and rights-respecting age assurance and encourage safety by design requirements for social media and other digital services providers. Under the age of 13, children should have time-limited access to age-appropriate social media+ environments only with parental authorisation and supervision or in educational contexts. From the age of 13, adolescents should benefit from evolving autonomous use of age-appropriate and safe social media and other digital services.

Harmonised rules on an EU-wide minimum age of 13 would contribute to the proper functioning of the Single Market by ensuring a single compliance framework for providers. Harmonised rules would facilitate enforcement and supervision by regulators at both the national and EU levels. It would also ensure an equal level of protection for all minors online across the EU, regardless of socio-economic, cultural and national contexts.

// **Introduce effective age-assurance systems to check age and underpin safety-by-design and age-appropriate approaches to protect and empower minors online.**

Age-assurance methods – both age verification or age estimation – must be proportionate and uphold minimum requirements, notably concerning the fundamental rights of users, including children's rights and related safeguards. Any method employed to check age should uphold the highest privacy and data protection standards, and should not lead to the processing of identity documents and biometric data for the purpose of age estimation. Technical standards such as 'Zero Knowledge Proof' should be implemented to ensure that both the platform required to assess the age and the age verification provider do not receive any information that can lead to the tracking or identification of the user.

Age-assurance methods should be accurate in determining the age or age groups required and easy and reliable to use in practice, in real-life conditions. Methods should be robust to avoid circumvention and cybersecurity threats, inclusive (and non-discriminatory), and available equally to all who need to use them. Social media and other digital services providers must uphold their obligation to prevent minors from being exposed to risky services or users impersonating children and adolescents.

// **Extend and harmonise rules on key safety features in the design of social media and other digital services.**

Clear safety by design and age-appropriate safeguards (for example, potential limits on infinite scrolling, autoplay, push notifications, and problematic personalised recommendation engines) should be embedded into social media and other digital services. To tackle addictive design, dark patterns, unsolicited contact and rabbit holes, protective default settings should be an integral part of social media and other digital services. Extending and harmonising rules on key safety features would ensure certainty and uniformity across the social media+ environment. Due to the rapid development of technology, any rules on key safety features should be adaptable to continuously address new harmful design features.

// Shift the burden of proof to social media and other digital services providers to demonstrate that their products and services are safe for minors.

Specific age restrictions should apply until key safety design features protecting children and adolescents are introduced by social media and other digital services providers. Until providers have demonstrated safe and age-appropriate features, therefore complying with EU and national measures, they should not have access to minors. Where there is a 'safe by default' version, age-inappropriate features (features for adults) should only be activated following effective age assurances.

// Strengthen enforcement and evaluation capacities.

Given the multiple rules now applying to child safety online (the DSA, GDPR, AI Act, etc.), supervisory authorities should intensify cooperation and exchange information across legal frameworks. This is key to avoid inconsistencies and to ensure a coherent, predictable and effective legal environment grounded in the protection of fundamental rights. The European Commission should explore mechanisms enabling seamless cooperation between supervisory authorities to leverage existing enforcement structures. Moreover, there is a need to assess whether additional resources and restructuring are needed for regulators responsible for enforcement and evaluation. Actions should be considered to strengthen the role of civil society in enforcement and their contribution to enforcement capacity, including through existing structures. Enforcement should be complimentary and avoid conflicting actions.

// Swiftly adopt measures to ensure social media and other digital services providers have clear obligations to prevent, detect, report and block child sexual abuse online, including in interpersonal communication.

The child safety gap that currently exists due to the expiration of the Interim Regulation laying down rules to prevent and combat child sexual abuse (CSA Interim Regulation) must be quickly filled. EU co-legislators should swiftly adopt the proposed long-term Regulation to prevent and combat child sexual abuse. More than 80% of child sexual abuse investigations start from reports submitted by social media and other digital services providers. Children are often too afraid to report abuse. Detecting child sexual abuse material, including in interpersonal communication, is often the only way to stop it.

// Member States can introduce additional precautionary access restrictions to social media and other digital services as of 13.

Additional precautionary access restrictions should be complimentary to the EU-wide access restriction to social media and other digital services under 13. Adolescents can have access only to a social media+ environment that is safe, with respect to content and design features, age-appropriate and designed with their rights and needs in mind. Member States have varied historical and national contexts and may prefer to adopt a higher age threshold than 13. All additional precautionary national access restrictions should be subject to continuous evaluation, and possibly reassessed, once social media and other digital services have been made safe by default for children and adolescents.

// Strengthen the enforcement of rules on researchers' access to and scrutiny of data.

Article 40 of the Digital Services Act (DSA) delegated act of July 2025 has opened, in principle, a new pathway for vetted researchers to access online platform data. This data can be used to conduct research contributing to the detection, identification and understanding of systemic risks, and to the assessment of risk mitigation measures promoting child safety online.

Whether this pathway delivers on its promise depends on social media and other digital services providers' compliance and regulators' effective enforcement. It also relies on the breadth of services covered, and the quality and continuity of the data provided. The Commission should evaluate the operational performance of Article 40 data access and scrutiny requirements after initial researcher experience under the delegated act. This is key to ensure online platforms follow up on requests for access to data for compliance, risk assessment and research purposes.

Data access obligations are not only a key element of the transparency toolbox of the DSA, they are also a part of social media and other digital services providers' broader risk mitigation responsibilities. Smaller platforms should also be encouraged to allow researchers access to data, considering the risks these platforms pose to minors and the role of independent scrutiny in addressing these risks. The use of the FAIR Guiding^j Principles for scientific data management and stewardship should be the standard in the implementation of Article 40.

Recommendations to empower children and adolescents online

// Expand safe opportunities for minors to actively participate in shaping the social media+ environment.

Children and adolescents should have meaningful opportunities to actively shape legislation, policies, and educational initiatives promoting child safety and empowerment online. The use of the child and youth participation tools to inform this work should be expanded. More specifically, children should be included in the co-design of safety policies, training programmes, evaluations and guidelines. Measures should be continuously monitored and evaluated to assess their impact on children's safety and rights.

Participation processes should ensure that children receive clear information, understand how their contributions will be used, and receive feedback on outcomes. Special efforts should be made to include children from disadvantaged, marginalised, and vulnerable groups. Appropriate safeguarding measures should accompany all participation activities involving children.

// Strengthen complaint mechanisms and consumer rights for children and adolescents.

Reports and complaints by children and adolescents should be treated as a priority in content moderation procedures by social media and other digital services providers. Providers' obligations under existing frameworks need to be strengthened to appropriately fund helplines and complaint mechanisms. These mechanisms must be age-appropriate, user-friendly, accessible, privacy-preserving, and effective.

j. The FAIR Guiding Principles for scientific data management and stewardship were introduced in 2016 in a publication in the journal *Scientific Data*. The principles intend to improve the infrastructure supporting the reuse of scholarly data by enhancing the ability of machines and individuals to find and use data. See: Wilkinson, M.D., et al. (2016). [The FAIR Guiding Principles for scientific data management and stewardship](#). *Scientific Data*, 3.

// Mainstream digital education and literacy actions for minors, parents and caregivers, teachers and educators.

Digital education and literacy should be embedded at all levels of education as a key basic skill for minors, parents and teachers. Digital well-being should be integrated into digital education for all.

Education should enable children and adolescents to critically evaluate online information and sources, and to recognise manipulation techniques, including disinformation, deepfakes and targeted advertising. It should also build an understanding among minors, parents and teachers of how digital content is created and shared, and how algorithms shape what users see and experience in the social media+ world.

Structured online safety education should build practical skills in protecting personal data, managing privacy settings, maintaining secure digital identities, and identifying risks on social media, messaging and gaming environments in particular. These skills should be developed progressively, beginning with basic safety habits and advancing to more complex understanding of digital footprints, consent, and platform risks. Healthy screen use should be addressed through guidance on balance, attention management, and recognising excessive or harmful patterns of use.

// Create more opportunities and adequate infrastructure to support offline activities.

Member States and local authorities should maintain and expand access to affordable sport, arts, youth clubs, libraries, and community spaces to encourage healthy offline engagement and create attractive alternatives to excessive screen use among minors. This should include investment in safe, inclusive and age-appropriate environments where minors can connect, learn, play and build positive relationships within their communities.

// Promote the co-creation of Guidelines for Parents.

Together with Parents' Associations, the EU and Member States should promote the development of Guidelines for Parents. The Guidelines could provide clear, accessible advice to empower parents and caregivers in supporting minors' safe, responsible and positive engagement with social media+ environments. The Guidelines should provide practical advice on key areas, including online safety and privacy, digital well-being, ethical and responsible use, and access to support.

// Ensure sufficient public funding and common standards for civil society organisations and peer counselling.

The EU and Member States should ensure that the Safer Internet Centres and comparable civil society organisations continue to receive sufficient financial resources and that their work is based on common standards, developed by experts. This is vital to maintain and further develop their activities, including awareness-raising, training and support services. Public funding is crucial to guarantee independence and cohesion.

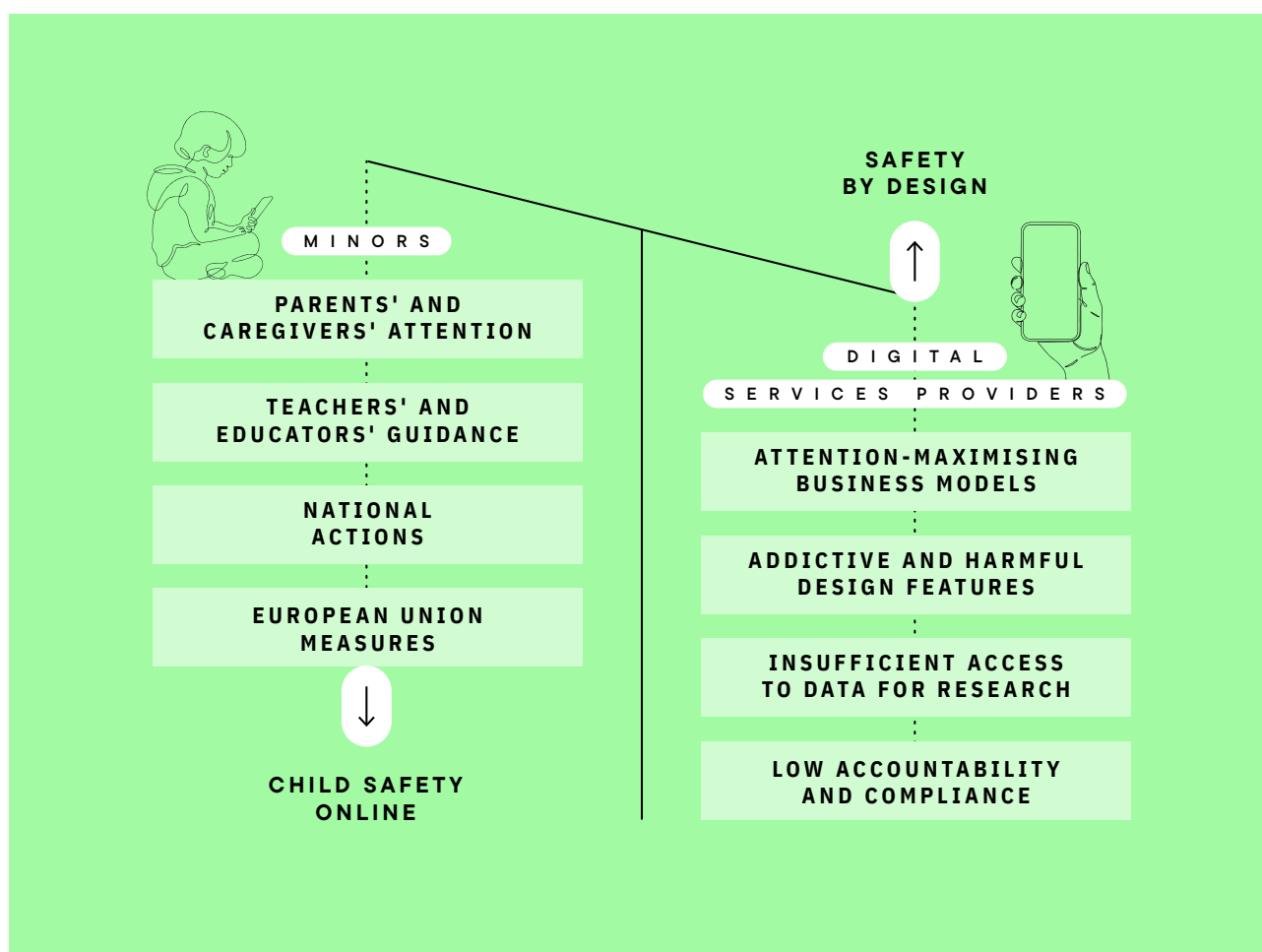
Funding should also support the further development of peer counselling, helplines, hotlines, educational resources, awareness-raising campaigns and capacity-building activities. Additional investment should be directed to increase the visibility, accessibility and reach of these facilities, including among vulnerable minors, and to support initiatives promoting safer social media+ environments.

// Make available long-term funding for European large-scale longitudinal research and continue supporting randomised control trials.

Examples, such as the North American Adolescent Brain Cognitive Development (ABCD) Study^k, could inspire European large-scale longitudinal research related to child safety online. The availability of European large-scale longitudinal evidence (covering a ten-year period or longer) is important to support a developmental and neurobiological approach to child safety online. This would help to address gaps in largely correlative findings in the European context concerning the impact of the use of social media and other digital services on minors' development, physical and mental health, and their exposure to harm online.

Randomised control trials (RCTs) are also key to strengthen the evidence base for policy. Research funding should explicitly support developmental and psychopathology approaches investigating minors' susceptibility to online risks, influenced by social and individual factors across childhood and adolescence.

Figure 2: Balancing the ecosystem: safety by design in social media+ environments



- k.** The ABCD Study is the largest long-term study of brain development and child health in the United States. The study follows the behavioural development of more than 11,000 children aged 9 to 10 through adolescence into young adulthood. The data gathered will enable the creation of baseline standards for adolescent brain development, and examines the influences of sex, gender, sleep, physical activity and screen time on adolescents' development. Its findings will also help to understand the development of mental health issues during adolescence and their relationship with substance abuse.

Online safety

TIPS FOR CHILDREN AND TEENS



Know your rights – remember that you have the right to be safe and respected online.



Be kind to others online – social media and gaming should be a positive experience for everyone. Treat others with the respect you would like to be treated with.



Think before you post – photos, videos and comments can stay online forever. Share now only what you would be comfortable with others seeing years later.



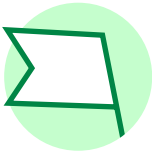
Protect your personal information – do not share private details such as your full name, address, school, phone number, passwords, or live location online.



Remember that AI is a tool, not a real person – AI can make mistakes and create false information, fake images, videos, voices and messages.



Check before you trust or share – not everything online is true. Always question information, especially surprising stories, videos, or messages, and check reliable sources before sharing.



Recognise danger – stop and think about strange requests from 'friends of friends', 'too good to be true' offers, or messages trying to pressure you into a decision.



Do not accept photos or chat requests from strangers – if you doubt someone's age or identity, ask an adult to check who it is (or tell them that 'your dad/mum is next to you' and see the reaction).



Use privacy and security settings – keep your accounts private, use strong passwords, and turn on extra security features whenever possible.



Do not share private images – never share intimate photos or videos, even if someone pressures you (especially if you're under 18). Once shared, they're out of your control.



Block, report and save evidence – if someone online is bullying, scamming, threatening, or making you feel uncomfortable, report and block them, and keep screenshots or messages.



Tell an adult you trust if something feels wrong – you are not being silly and you are not in trouble for asking for help.



Help make the internet a safer place – learn how apps, games, websites, algorithms and AI work, and help others to stay safe too.



Use your voice – get involved and shape the future of the digital world.



Online safety

TIPS FOR PARENTS AND CAREGIVERS



Help your child build healthy screen habits – limit screen time, from no screen use at all for children from 0 to 2, to age-appropriate time limits for children up to 10 to 12 years-old, under your supervision. For adolescents from 13 to 18, limits on screen time should still be discussed, so they have enough time to study and meet friends in person.



Check that apps and games are age-appropriate for your child.



For younger children (up to 12), **consoles and devices should be used only in the presence of an adult.**



Do not allow devices in the bathroom, in the bedroom or at meal times.



Pay attention to the tone of their conversations online and while gaming. Look out for red flags.



Spend time together online – ask your child to watch their favourite content with you.



Do not criticise 'their stuff' – help your child to develop their own judgement (you will also get an idea of what their algorithm is suggesting).



Encourage your child to talk to you if they are worried about something online – reassure them that you will help, not blame, punish, or take the device away.



Continue conversations about online safety as your child gets older, including from 16 to 18 and beyond.



Avoid sharenting – think carefully before sharing photos or videos of your children or teens online. Strangers and AI can use that information in many ways.



Set an example – don't be glued to your device when your children are around. Give them the attention they deserve and don't miss important moments and conversations with your child.



List of all recommendations from the Co-Chairs by chapter

CHAPTER 1

A developmental approach to child safety online

- // Design and deploy age-appropriate online child protection measures
- // Ensure safe online spaces for minors
- // Empower minors and their supporting circles
- // (0 to 2 years old) - Increase caregivers' awareness of the developmental importance of direct, human interaction, starting in early childhood
- // (0 to 2 years old) - Avoid the use of social media and other digital services and ensure minimal screen exposure, specifically for children under 3
- // (0 to 2 years old) - Limit the dissemination of children's data by social media profiles
- // (3 to 12 years old) - Ensure structured, supervised use for children online
- // (3 to 12 years old) - Offer children and their supporting circles quality digital and well-being education
- // (13 to 18 years old) - Ensure evolving autonomous use for adolescents online

CHAPTER 2

Evidence on risks minors face online

- // Build on evidence in understudied areas to strengthen evidence-based policymaking
- // Social media and other digital services should actively involve independent academic expertise in the design of risk mitigation strategies and tools
- // Make available long-term funding for European large-scale longitudinal research and continue supporting randomised controlled trials
- // Invest in secure, shared European research infrastructure to allow safe access to minors' data
- // Strengthen enforcement of rules on researchers' access to and scrutiny of data

CHAPTER 3

Protecting minors in a rapidly changing social media+ environment

- // Propose a harmonised EU-wide access restriction to social media and other digital services for minors under 13
- // Introduce effective age-assurance systems to check age and underpin safety-by-design and age-appropriate approaches to protect and empower minors online
- // Extend and harmonise rules on key safety features in the design of social media and other digital services

- // Shift the burden of proof to social media and other digital services providers to demonstrate that their products and services are safe for minors
- // Strengthen enforcement and evaluation capacities
- // Swiftly adopt measures to ensure social media and other digital services providers have clear obligations to prevent, detect, report and block child sexual abuse online, including in interpersonal communication
- // Member States can introduce additional precautionary access restrictions to social media and other digital services as of 13
- // Strengthen consumer protection policies to protect minors online
- // Continuously monitor and evaluate the impact of measures being implemented
- // When processing children's data under the GDPR, social media and other digital services should ensure children's best interests are a primary consideration
- // Ensure effective implementation of the Product Liability Directive
- // Mainstream digital education and literacy actions for minors, parents and caregivers, teachers and educators
- // Create more opportunities and adequate infrastructure to support offline activities
- // Promote the co-creation of Guidelines for Parents
- // Ensure parents and carers are continuously supported by state-of-the art and up-to-date control and supervision tools
- // Ensure sufficient public funding and common standards for civil society organisations and peer counselling
- // Enable the health system to diagnose and treat addictions and other mental health disorders related to the use of social media and other digital services
- // Support teachers' training to include digital and media literacy and involve parents
- // Promote AI literacy as an integral part of digital education
- // Schools should provide structured opportunities to improve mental health and digital well-being

CHAPTER 4

Empowering minors to safely navigate the digital world

- // Expand safe opportunities for minors to actively participate in shaping the social media+ environment.
- // Strengthen complaint mechanisms and consumer rights for children and adolescents
- // Fund and promote the establishment and use of EU-values-based social media and other digital services where minors can safely interact with each other
- // Invest in secure, preventive, robust and trusted educational digital infrastructure

01

A developmental approach to child safety online

Childhood as a distinct, protected life phase

The recognition of childhood as a distinct life phase is a relatively recent development. Throughout much of history, children were not considered as being fundamentally different to adults.

In premodern and early industrial societies, this view was closely tied to material conditions, especially the ‘economic necessity’ of child labour. Children’s characterisation as ‘small adults’⁰¹ masked their distinct needs and vulnerabilities, hindering the emergence of child protection frameworks.

With the rise of modern scientific disciplines, such as developmental medicine and psychology, a paradigm shift occurred. Evidence demonstrated that children’s cognitive, emotional, and social development follow distinct trajectories. These advances helped to redefine childhood as a distinct and vulnerable life phase⁰².

This idea was reinforced by insights from child and adolescent psychiatry, which highlighted the long-term consequences of adversity experienced in early life. Gradually, the notion of childhood and adolescence as distinct life phases requiring protection and support⁰³ took hold.

Children’s development in stages

Over the course of the 20th century, this growing awareness laid the foundations for modern child and youth protection frameworks. Initially, these frameworks focused on safeguarding children in the physical world.

The United Nations Convention on the Rights of the Child is one key example. Under the Convention, children below the age of 18^a are treated as a homogenous group.

Despite the rapid development of digital technologies and services, such as social media and other digital services, and the ways they have transformed children’s lives, many approaches to child protection still rely implicitly – or explicitly – on the idea of ‘children’ as a homogeneous group.

a. Under the Convention, a child is defined as ‘every human below the age of eighteen years’, unless majority is attained earlier under applicable law. See: United Nations (1989). [Convention on the Rights of the Child](#). Part 1, Article 1.

This assumption is misleading. Developmental science proves that children's development unfolds across qualitatively distinct stages, each characterised by unique cognitive, emotional and social capacities. These capacities shape how children perceive, engage with, and communicate in their environments, including online.

The need for age-appropriate protection

Children's exposure to the social media+ world begins early in life and increases steadily throughout childhood in intensity, complexity and personalisation⁰⁴. One study shows that children under the age of 2 use screens for an average of 49 minutes a day. By 8, this has more than tripled to around 3 hours a day⁰⁵. Evidence shows that digital technologies have a pervasive and structuring effect on children's development, and form part of the complex environment in which children and adolescents learn, form a sense of self and relate to others.

Simply put, children's development both influences and is *influenced by* their interactions online. As such, the digital world cannot be considered external to, but rather a key part of children's development, especially during later stages⁰⁶. This two-way interaction underscores the need for age-appropriate measures to protect and empower children to navigate safely and confidently online.

“Developmentally appropriate protection acknowledges that children's cognitive control, emotional regulation, and risk awareness are still maturing.”

— PROF. DR. EVA MÖHLER
CHAIR AND MEDICAL DIRECTOR OF CHILD
AND ADOLESCENT PSYCHIATRY, SAARLAND
UNIVERSITY HOSPITAL

Main challenges for age-appropriate protection

THE TENDENCY TO ADDRESS 'CHILDREN' AS A SINGLE GROUP

Existing approaches to child safety online often rely on the idea of children as a single group with uniform needs. This idea needs bringing up to date. It is today understood that children's development occurs in stages, which shape how children (from 0 to 12) and adolescents (from 13 to 18) engage with the online world and their vulnerabilities to diverse risks.

Social factors, gender and sexuality, socioeconomic background, racial and ethnic origin, religion, migration backgrounds and special educational needs, also have an important impact on children's and adolescents' interactions and vulnerabilities online⁰⁷.

THE MISMATCH BETWEEN MINORS' CAPACITIES AND SOCIAL MEDIA+

Digital services, including social media, deliver a rapid and constant flow of information using highly optimised engagement architectures, including algorithmic recommendation systems and infinite scrolling. These features are specifically designed to maximise user attention⁰⁸.

Children's and adolescents' capacities meanwhile develop gradually, remaining incomplete well into adolescence⁹⁹. As a result, minors are increasingly exposed to social media+ environments and content that they are not equipped to engage with and may cause serious harm.

MINORS' EVOLVING AUTONOMY AS ONLINE USERS

As alluded to above and explored more extensively in the following sections, children's and adolescents' evolving capacities throughout their development determine (in part) how well they are equipped to navigate safely and confidently online at different ages.

As children get older, they shift from being entirely dependent on parents and caregivers, to partially autonomous, and fully autonomous adults. Social media and other digital services design has an increasing influence on minors' development. As children grow up and become more independent, their supporting network (parents and caregivers, teachers and educators) capacities to protect, supervise and guide minors online become more limited.

RECOMMENDATIONS

Design and deploy age-appropriate online child protection measures

Children's and adolescents' staged development calls for the design and deployment of protection measures that are suitable for their evolving capacities and address the risks they are exposed to at different ages. These measures should take into account minors' personal and social circumstances, where possible.

Ensure safe online spaces for minors

Social media and other digital services providers have primary responsibility to ensure that their services are safe for all children and adolescents. This includes by deploying safe design features. Providers must take primary responsibility for ensuring that their services are safe for minors to access and use.

Empower minors and their supporting circles

To be effective, actions designed to protect and empower children and adolescents online must take into account their evolving needs and capacities. Measures must also be tailored to support the changing role of parents and caregivers, teachers and educators (supporting circles) to protect minors, and to supervise and guide their use of social media and other digital services as they grow up.

Age-specific challenges

The previous section explored three main challenges and accompanying recommendations intended to steer the design and deployment of a developmental approach to child safety online.

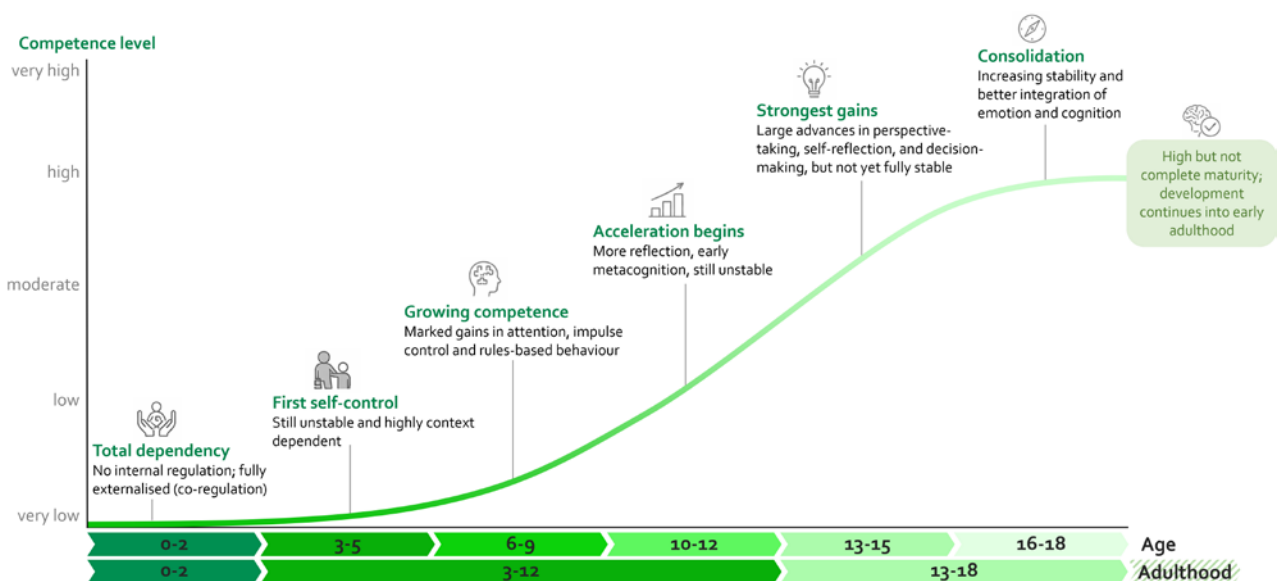
On this basis, the following sections explore the various characteristics and vulnerabilities that define minors' development during three primary developmental stages: 0-2 years (early childhood); 3-12 years (childhood); and 13-18 years (adolescence).

These primary stages encompass both minors' evolving capacities and their supporting circles' changing role in protecting and empowering children and adolescents online:

- // **0-2 years:** early childhood as a specially protected stage of development;
- // **3-12 years:** childhood as a supervised stage of development;
- // **13-18 years:** adolescence as the stage of evolving autonomy.

Figure 1 – The staged development of core competencies

Self-regulation, judgement and critical thinking



This report examines the risks for minors online and presents recommendations to address these risks according to these three primary developmental stages, defined for the purpose of this analysis as early childhood, childhood and adolescence.

This first chapter outlines the first of Six Guiding Principles proposed by the authors to steer actions designed to protect and empower children and adolescents in the digital world: the need for a developmental approach to child safety online.

“All persons under 18 years have specific rights to protection and enjoyment of age-appropriate experiences.”

— MIE OEHLenschLAGER,
INDEPENDENT RESEARCHER ON AI,
ETHICS AND PUBLIC POLICY

To ensure a comprehensive examination of the characteristics and unique vulnerabilities for minors at different stages of their development, the primary stages of their development are broken down into secondary stages (0–2 years, 3–5 years, 6–9 years, 10–12 years, 13–15 years, and 16–18 years), explored in depth in this chapter.

Some of the recommendations presented for each primary stage are not exclusive to the stage where they are situated, but apply across stages as specified.

0-2 years: Early childhood as a specially protected stage of development

Early childhood, in particular from 0 to 2 years, represents a stage of maximal dependency and foundational developmental significance. During this period, the basic building blocks of emotional security, social relatedness, language acquisition, and self-regulation are established.

Core processes, such as attachment formation, co-regulation, and the differentiation between the self and a child’s environment, emerge through repeated interactions with responsive caregivers. Self-regulation is not yet internally established, but develops gradually through co-regulation.

In this sense, early co-regulation also forms the developmental basis for later autonomy and self-determined functioning. The gradual internalisation of emotional regulation, communication, and social interaction emerges through repeated relational experiences, rather than isolated exposure to digital stimuli.

Development during this stage is fundamentally relational. Self-regulatory capacities, emotional stability, and early cognitive structures are externally scaffolded before being internalised.

AGE-SPECIFIC CHALLENGES

The need for direct, human interaction

A central challenge in this stage is to ensure that small children receive sufficient direct human interaction. Reductions in interactional quality may affect attachment processes, impair early language development and foundational communicative capacities, directly affecting developmental trajectories.

Ensuring the availability of consistent, emotionally attuned interaction represents a core condition for safe development in increasingly digitalised environments. During this stage, small children are almost entirely dependent on external regulation.

Neurophysiological systems involved in stress regulation, arousal modulation, and sleep-wake cycles are still immature and highly sensitive to environmental input. This creates a heightened vulnerability to overstimulation and disruptions in sleep and stress regulation.

Learning in this stage is interaction-based, rather than content-based. Small children acquire meaning through embodied, reciprocal engagement with parents and caregivers, not through passive exposure to screen-based representations.

Early language acquisition and communication development depend fundamentally on repeated contingent interaction with parents and caregivers. Responsive verbal engagement, shared attention, and emotionally attuned communication constitute essential developmental conditions during this stage.

Risks of screen exposure

At this age, evidence links increased screen exposure to shorter sleep duration, dysregulated stress patterns, and lower levels of caregiver-child interaction and linguistic input¹⁰. These vulnerabilities can be differentiated across biological, psychological, and developmental dimensions.

Biologically, small children are highly susceptible to overstimulation due to immature self-regulation systems¹¹. Psychologically, development depends on consistent and responsive interaction, making small children sensitive to disruptions in attention and communication. Developmentally, risks relate to attachment formation and the emergence of self-regulation.

During this stage, higher screen exposure has been associated with socioemotional difficulties, behavioural problems, and delays in self-regulation development¹². These relationships are often two-way, as small children with self-regulatory difficulties may also engage in higher levels of screen use.

Caregiver-mediated digital exposure

From 0 to 2 years, social media+ exposure is entirely caregiver-mediated. Small children do not in principle control access, duration or content. Social media and other digital services use is mainly shaped by parents' and caregivers' practices, routines and situational needs, such as calming or distraction¹³.

During early childhood, digital risks arise in theory less from direct interaction with content, but rather from the ways social media and other digital services restructure caregiving environments. A central concept is 'technoference'^b. At this age, even brief shifts in caregiver attention can reduce responsiveness, joint attention and verbal engagement¹⁴.

Caregiver screen use with small children has been associated with less favourable developmental outcomes. This is not primarily because of content, but because of the restructuring of interactional space¹⁵. In this sense, digital risk in early childhood is often relational before it is individual.

Research on commercial family influencing highlights that small children may increasingly become objects of visibility, monetisation, and data extraction long before they can understand or influence these processes themselves. This reinforces the need for strong external protective frameworks during early childhood.

b. 'Technoference' is defined as the interruption of parent-child interactions by technology. See: Zhang et al (2025). [Parental Technoference and Child Problematic Media Use: Meta-Analysis](#).

The digitalisation of early childhood

An emerging and increasingly relevant dimension concerns the digitalisation of early childhood environments beyond traditional screen-based interactions. A growing number of toys, including dolls and interactive play objects, are being augmented with digital features and increasingly artificial intelligence (AI).

This development of a social media+ environment is particularly relevant because AI-enabled toys and voice-based devices may appear to children not merely as objects, but as responsive social partners. During early childhood, attachment, co-regulation, language acquisition and symbolic play depend on contingent human interaction.

These systems raise specific developmental concerns. AI-enabled toys and voice-based devices may simulate responsiveness without providing the genuine reciprocity, emotional attunement, or relational accountability that characterise human relationships.

AI-enabled toys also often integrate microphones, cameras, speech processing or app-based personalisation. This introduces privacy and data protection risks at an age when children have no capacity to understand, consent to, or contest data processing.

Displacement of direct human interaction

Children's interactions with the digital world raise concerns about potential displacement or distortion of interactional learning processes, as well as new forms of dependency and overstimulation. These dependencies are not yet adequately addressed in existing research or regulatory frameworks.

Parents' and caregivers' social media and other digital services use may reduce time dedicated to face-to-face interaction with children, free play, physical activity, and sleep – all essential for early development¹⁶. In its most serious forms, the displacement of caregiver interactions may equate to 'digital neglect'¹⁵.

Issues related to the displacement of face-to-face caregiver-child interactions extend beyond immediate overstimulation or distraction to potential long-term effects on autonomy development, imaginative play, communication, and the emergence of internally guided social and emotional capacities.

A very restrictive approach to digital exposure

Despite these challenges, not all forms of social media and other digital services use at during early childhood are inherently harmful. Under specific conditions – especially when parents and caregivers ensure content is age-appropriate (low-stimulation, slow-paced, etc.) and embedded in active caregiver mediation – social media+ spaces may support aspects of early learning.

Evidence shows that joint engagement with social media and other digital services (co-use) can facilitate learning, especially when accompanied by verbal interaction and scaffolding¹⁷. However, these effects appear limited and context-dependent.

- c. Building on established forms of emotional and supervisory neglect, (Dubowitz et al., 1993; Hildyard & Wolfe, 2002) digital neglect extends these constructs into digital environments. When parents use screens extensively in the presence of their children, interactions decrease and parental responsiveness diminishes. Children's language development may be impaired. This displacement may also generate feelings of rejection and emotional distance in children, increasing their risk of depression, anxiety, and aggression.

The preservation of relational interaction with small children is not only relevant for preventing harm, but also for enabling healthy socioemotional, linguistic and cognitive development. Secure attachment, responsive communication and caregiver modelling constitute central protective factors in increasingly digitalised early childhood environments.

Taken together, these findings support a very restrictive approach to the use of social media and other digital services in early childhood, consistent with guidance from major paediatric health authorities¹⁸. While such recommendations may not be universally adhered to, they provide important normative guidance aligned with the developmental needs of this age group.

Caregiver-centred online interactions

Child safety online during early childhood must be fundamentally caregiver-centred. Since small children are not autonomous users, responsibility for their exposure to digital environments lies primarily with parents and caregivers.

Parental mediation capacity is unevenly distributed. Socioeconomic status, parental mental health, and parents' own social media+ use significantly influence children's exposure patterns [as discussed in more detail in chapter 2]. Higher parental stress and screen use are associated with longer and less structured digital services use in very small children¹⁹. As such, screen use is strongly discouraged for this age group.

CONCLUSIONS

Online safety during early childhood is not primarily about regulating small children's behaviour, but about structuring caregiving environments and interactional contexts. Protection depends on preserving the conditions necessary for attachment, co-regulation, and the development of self-regulation. These conditions form the foundation for later developmental stages.

Insights from established age classification systems (for example, film and game ratings) may provide orientation. If content is designed for this age group, it should be strictly limited to low-stimulation, slow-paced and non-narrative formats that support joint engagement with caregivers. This includes simple visual or auditory stimuli embedded in co-use contexts.

Fast-paced, highly stimulating or emotionally arousing content – including rapid scene changes, intense audiovisual effects, or emotionally charged narratives – should be considered developmentally inappropriate. Exposure to any form of violent, frightening, or complex narrative content is clearly unsuitable at this age.

RECOMMENDATIONS (0-2 YEARS)

Increase caregivers' awareness of the developmental importance of direct human interaction, starting in early childhood

Empower parents and caregivers using educational campaigns and parenting support programmes on the importance of early childhood for children's development. Inform caregivers about the risks for small children associated with 'technoference', for example caregivers' own use of social media and other digital services. Encourage caregivers to reflect on the direct and indirect effects of their online interactions on minors of all ages, especially small children.

The risks of 'digital neglect' should be recognised within child protection frameworks. Parents, schools and social services should be informed how to detect the signs of digital neglect in children and adolescents, starting in early childhood.

Avoid screens and social media+ for children under 3

During the first 1,000 days of life, children's developmental needs are primarily related to attachment, co-regulation, sensory development and early language acquisition. However, avoiding exposure to social media and other digital services and screens during early childhood does not imply an absolute prohibition.

Under specific conditions, social media and other digital services may be used in a limited relational way with small children, for example as part of shared activities (e.g. viewing family photos or communicating with relatives over video calls). However, the use of screens as tools for 'calming' or occupying small children over extended periods should be strictly avoided.

As a general principle, parents and caregivers should prioritise face-to-face interactions with children and adolescents (starting in early childhood) to support minors' healthy cognitive, physical and emotional development.

Limit the dissemination of children's data by social media profiles

Regulatory frameworks must address the systematic documentation and public dissemination of children's data (including images and videos), especially concerning children under the age of 3, by social media profiles (for example, through 'sharenting' and 'family influencing'). Children at this age have no capacity to consent to their digital representation or to understand the commercial contexts where their data is used and the future implications.

Social media and other digital services providers must not incentivise the creation or dissemination of content featuring children through monetisation structures, algorithmic amplification or engagement-driven design features. Enforceable social media and other digital services obligations should be deployed, rather than relying on voluntary caregiver responsibility alone. Caregivers should receive clear guidance on the long-term implications of early digital visibility for children's privacy, dignity and right to informational self-determination.

3-12 years: Childhood as a supervised stage of development

3-5 YEARS: THE STAGE OF STRICTLY SUPERVISED DEVELOPMENT

Between the ages of 3 and 5, children enter a developmental stage characterised by intentional activities under continued external structuring. Children begin to develop intentional action, symbolic thinking and a more coherent sense of self.

Neurodevelopmentally, this stage is marked by the ongoing maturation of systems involved in attention, executive functioning and emotional regulation, which remain incomplete and sensitive to external stimulation²⁰. Reward-related systems, however, are already active. Children increasingly develop intrinsic motivation, curiosity-driven exploration, and early forms of autonomous goal-directed behaviour.

Development during this stage depends strongly on opportunities for imaginative play, self-initiated activity, and relational experiences that support the development of competencies. This includes the formation of a narrative self, expressed for example through language and roleplay.

Children at this age can sustain activities for limited periods, but their capacity to regulate attention, impulses and emotions still relies heavily on external support in the form of language, imitation and caregiver guidance. This stage can therefore be understood as a transition from co-regulation to guided self-regulation.

AGE-SPECIFIC CHALLENGES

Vulnerability to instant gratification

This gap between the ongoing maturation of children's systems involved in attention, executive functioning and emotional regulation, and already active reward systems creates an imbalance. Children at this age are highly responsive to salient stimuli and immediate rewards, but have limited inhibitory control and tolerance for delay.

This makes children from 3 to 5 years particularly vulnerable to social media+ environments optimised for immediate gratification, repetitive reward, and continuous external stimulation. Experimental evidence suggests that digital environments may interfere with the development of frustration tolerance, persistence and internally guided motivation²¹.

This developmental configuration creates a distinct vulnerability profile. The conditioning of reward systems through rapid feedback, repetition and intermittent reinforcement by children's online interactions may shape expectations of immediate gratification and contribute to habitual usage patterns²².

Excessive reliance on external reward structures may also affect the development of intrinsic motivation. Children's use of digital technologies defined by characteristics, including continuous reinforcement and instant feedback, risk shifting behaviour towards externally regulated engagement patterns, rather than internally motivated exploration and learning.

This is particularly relevant during developmental stages when autonomy and competence are still emerging. Research indicates that these vulnerabilities are strongly influenced by contextual factors, such as family environment, parental mediation and socioeconomic conditions²³.

Risks of screen exposure

Higher levels of screen exposure at this stage are associated with lower self-regulation, particularly in children's attention and impulse control²⁴. As explored above, social media and other digital services use may displace developmentally critical activities, such as free play, physical activity, sleep, and face-to-face interaction²⁵.

However, these effects are context-dependent and moderated by content quality, co-use, timing and social environment, rather than metrics such as screen time alone²⁶. Evidence suggests that online interactions at this age may support learning when content is interactive, age-appropriate and embedded in active caregiver mediation²⁷.

The availability of safe offline alternatives

Child safety online cannot be fully understood without considering the broader ecology of children's everyday lives. In contexts where educational, recreational and social opportunities for children are limited, especially in rural or underserved areas, social media+ environments may become default spaces of engagement.

This may expose children to harm and negatively impact their development. To limit the potential harmful effects of social media and other digital services use on children's development, parents and caregivers should provide safe, offline alternatives starting in early childhood. Beyond caregivers, structural and environmental conditions outside the digital sphere shape exposure patterns and associated risks. These include access to safe public spaces, extracurricular activities, and supportive social infrastructures.

Caregivers' reduced mediation capacity

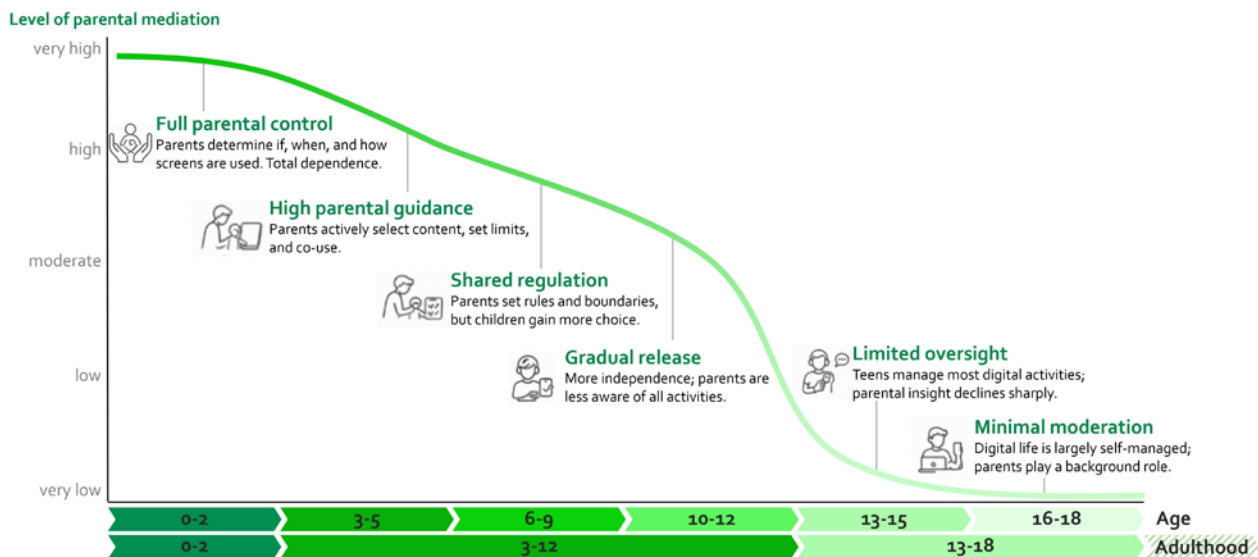
From the ages of 3 to 5 years, caregiver mediation remains a central regulatory mechanism, but undergoes a qualitative shift. Parents and caregivers move from direct control towards supervised mediation, co-use, and interpretive support.

Children's increasingly self-initiated activities reduce the effectiveness of purely external control, as parental influence competes with highly engaging digital systems. Existing parental control tools often fail to adequately support this shift, for example due to fragmentation across social media+ spaces and lacking usability²⁸.

Active mediation – discussing content, structuring use, and providing explanations – has been shown to support learning and to mitigate risks. Purely restrictive strategies may prove less effective without such engagement²⁹. Caregiver mediation is also constrained by factors, such as digital literacy, socioeconomic resources, parental stress, and caregivers' own digital services use³⁰.

Figure 2 – The decline of parental mediation throughout development

As children grow, direct parental oversight naturally decreases, together with children's digital dependence



CONCLUSIONS

This stage represents a critical transition for child safety online. Children are no longer passive recipients of exposure, but increasingly active participants in the digital world, while still lacking stable self-regulation. Exposure expands, while internal regulation remains incomplete.

Meanwhile, responsibility begins to shift from purely parental control to a more distributed system involving families and educational institutions. From a policy perspective, this implies a reduced but nonetheless important role for parental supervision. The main challenge at this age is not simply limiting exposure, but preventing the consolidation of harmful patterns of use at an early age.

Online child protection measures for this age group must include structured environmental and institutional support. This includes age-appropriate design of apps and digital content intended for young children, addressing in particular reward-based and attention-capturing mechanisms.

Given children's slowly increasing self-initiated activities starting at this age, digital education should be integrated into early childhood education. In light of caregivers' continued supervisory role, parental guidance and co-use practices should be strengthened, especially in vulnerable contexts.

Current regulatory frameworks often overlook this developmental stage, focusing either on very small children or adolescents. As a result, the specific vulnerabilities of children from 3 to 5 remain insufficiently addressed. Child safety online at this age must focus on designing environments that support, rather than undermine children's developing self-regulation and empower caregivers in supervising children's use.

6-9 YEARS: THE STAGE OF SUPERVISED DEVELOPMENT

Between the ages of 6 and 9, children enter a developmental stage characterised by increasing cognitive competence, structured goal-directed behaviour, and the emergence of competence-based self-evaluation. Children are now able to engage more consistently in rules-based activities, sustain attention over longer periods, and pursue defined goals.

A central developmental task is the formation of a competence-based sense of self, in which self-worth becomes increasingly linked to performance and feedback. During this stage, the development of competence and self-efficacy becomes increasingly important for healthy psychological development. Children develop more stable self-regulation, gradually learn to tolerate frustration, and persist in challenging tasks.

Children also begin to derive satisfaction from mastery and internally experienced competence, rather than immediate external rewards alone. With school entry, structured evaluation systems and peer comparison become central, shaping how children interpret their abilities in relation to external standards.

Neurobiologically, this stage is marked by increasing efficiency and specialisation of brain networks, particularly in regions associated with executive functioning. Reward and stress systems remain sensitive though, creating a configuration in which children are more capable of self-regulation, but are still responsive to external reinforcement.

AGE-SPECIFIC CHALLENGES

Increased sensitivity to external evaluation

Social Media+ environments intersect directly with these processes. Social media and other digital services that provide quantifiable feedback, including scores, rankings and achievements, align closely with competence-based self-evaluation.

This can shape motivation and self-perception by imposing externalised standards of success³¹ in place of internally experienced mastery, curiosity and learning processes. At this age, attentional systems remain sensitive to highly stimulating environments, which can compete with the sustained attention required for learning³².

Risk of early addiction

From 6 to 9, children's habits stabilise, as patterns of social media+ use, attention and motivation become more consistent over time. At this age, reward-based reinforcement, especially in gaming, can contribute to the formation of habitual usage patterns³³. These vulnerabilities are shaped by contextual factors, such as family environment, parental mediation, and socioeconomic conditions³⁴.

During these years, children's access to social media and other digital services expands significantly. With school entry and increasing peer interaction, children gain more frequent and less supervised access to social media+ spaces. This expansion is accompanied by a gradual decline in direct parental control, although caregiver supervision remains vital.

At this age, parental mediation shifts increasingly towards rule-setting, monitoring and guidance. However, its effectiveness decreases as children's independent access and social media and other digital services' complexity rise³⁵. Responsibility for shaping children's digital environments becomes more distributed between social media and other digital services providers, caregivers and educators.

Risks of screen exposure

As in earlier stages, children's online use risks displacing developmentally crucial activities in the 'real world', including physical activity, sleep and face-to-face interactions³⁶. One frequently discussed example is the phone-free primary school as a deliberate counterbalance to children's increasingly digital lives. Research suggests that restricting smartphone use during the school day can improve not only children's concentration and academic performance, but also strengthen social interaction.

Research reviews indicate that smartphone-free environments can enhance social well-being and reduce conflicts, such as cyberbullying³⁷. Evidence from system-level interventions, for example in countries such as the Netherlands, also suggests that restricting smartphone use contributes to a calmer and more conducive learning environment³⁸. Studies consistently show that smartphones carry significant distraction potential in classroom settings and can impair children's attention³⁹.

Under appropriate conditions, however, online use at this age can support children's learning and cognitive engagement, especially when it is structured and developmentally aligned⁴⁰. Adaptive tutoring systems and educational apps may support individualised learning pathways, provide explanations and reduce dependency on caregiver support. This may contribute to educational inclusion.

CONCLUSIONS

Child safety online during this stage requires a multi-layered approach. This implies the need for clear standards for the age-appropriate design of social media and other digital services, especially regarding external feedback systems and reward mechanisms that interact with children's developing self-concepts, self-regulation and intrinsic motivation. Reinforcement loops and monetisation features that affect attention and intrinsic motivation require particular attention.

Children's digital education should be strengthened within school systems, focusing not only on technical skills, but also on attention, self-regulation and critical engagement. Structured frameworks for online use are needed that balance digital engagement with offline activities.

The phone-free primary school can be understood as a developmentally appropriate protective and learning arrangement. This creates spaces in which children can develop essential social skills, such as face-to-face communication, conflict resolution and cooperative interaction. These competencies form the foundation for more reflective, responsible online use during later stages.

Such measures should not be conceived as a prohibition of digital technologies, but as pedagogically embedded and supervised online use that strengthens children's analogue experiences, while gradually preparing children for media literacy in social media+ environments. These measures do not replace the role of parents or caregivers, whose informed mediation remains a central component of effective protection.

10-12 YEARS: THE STAGE OF DECREASINGLY SUPERVISED DEVELOPMENT

The ages of 10 to 12 represent a critical stage in children's development characterised by the reorganisation of the self in relation to others. Self-concept becomes more differentiated, but also more unstable as children increasingly construct their identity through peer comparison, social positioning and perceived acceptance. In parallel, external feedback becomes a central organising principle of self-evaluation.

Peer relationships gain substantial importance. Peers increasingly function as central reference points for norms, values and behaviours. Processes of social influence, such as conformity pressure, social comparison and implicit group norms, significantly shape children's self-perception and behaviour.

Peer networks fulfil important supportive functions. They provide emotional validation, social orientation, and opportunities for coping together with developmental challenges. Peer support can act both as a source of resilience and as an amplifier of risk dynamics, depending on the context and prevailing group norms.

AGE-SPECIFIC CHALLENGES

Continuous online access

With age, these peer processes increasingly shift into digital environments. Social media and other digital services enable continuous, low-threshold and often boundaryless interaction for children with their peers. This allows social connectedness and belonging to be established and maintained beyond physical contexts.

For many children at this age, access to social media and other digital services already becomes a prerequisite for social participation. As with previous stage, social media+ use may displace crucial developmental activities, such as physical activity, sleep, and offline interaction⁴¹.

Intensified social comparison

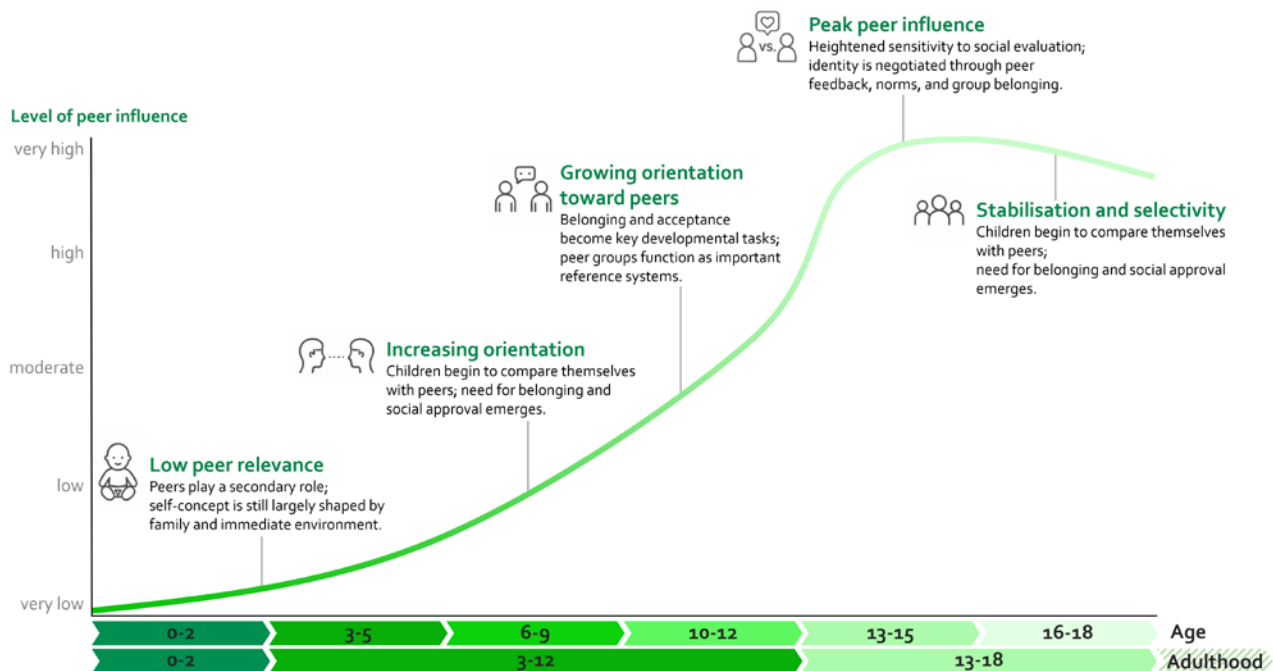
The structural features of social media and other digital services, especially the persistence, visibility and scalability of interactions, intensify the effects of peer influence. Algorithmically structured environments may also amplify these dynamics by continuously prioritising emotionally salient, socially rewarding or highly engaging content.

At this age, children increasingly evaluate themselves across domains, such as appearance, popularity and social competence. They also begin to engage in intentional self-presentation and identity experimentation, especially in digital environments.

Another mechanism involves the internalisation of norms and behaviours. Exposure to content depicting risky behaviours or harmful norms can increase the likelihood of imitation, particularly during a stage where normative frameworks are still forming⁴². More severe risks, such as coercion or exploitation, are less frequent but potentially more harmful.

Figure 3 – The rise of peer influence throughout development

As children grow, peer influence increases, reaching a peak during adolescence as belonging, social evaluation and identity expression become central



Algorithmic influence on identity formation

In a developmental stage marked by emerging identity formation and heightened peer orientation, algorithmic amplification may also contribute to shaping opinion formation, social orientation and self-evaluation in ways that children cannot yet fully recognise or resist.

Social media+ platforms provide tools for curating identity and managing impressions⁴³. Online identity is not only experienced, but continuously displayed and evaluated, creating a new developmental context. For children at this age, social media visibility becomes a meaningful dimension of peer status⁴⁴.

Children increasingly interact with personalised information environments where content is selected according to predicted engagement, rather than developmental appropriateness. This can reinforce existing interests and vulnerabilities while narrowing exposure diversity, creating feedback loops of attention and reinforcement⁴⁵.

At the same time, identity formation remains unstable. This makes children at this age particularly susceptible to external influences, such as idealised representations and appearance-based norms, especially in visual social media+ contexts.

Mental health risks

As sensitivity to social evaluation sharply increases, children's self-esteem and emotional well-being fluctuate. This stage marks the emergence of online interpersonal risks, including cyberbullying, exclusion and negative peer interactions. Due to heightened sensitivity to social evaluation and the persistence of digital communication, such experiences can have strong emotional effects.

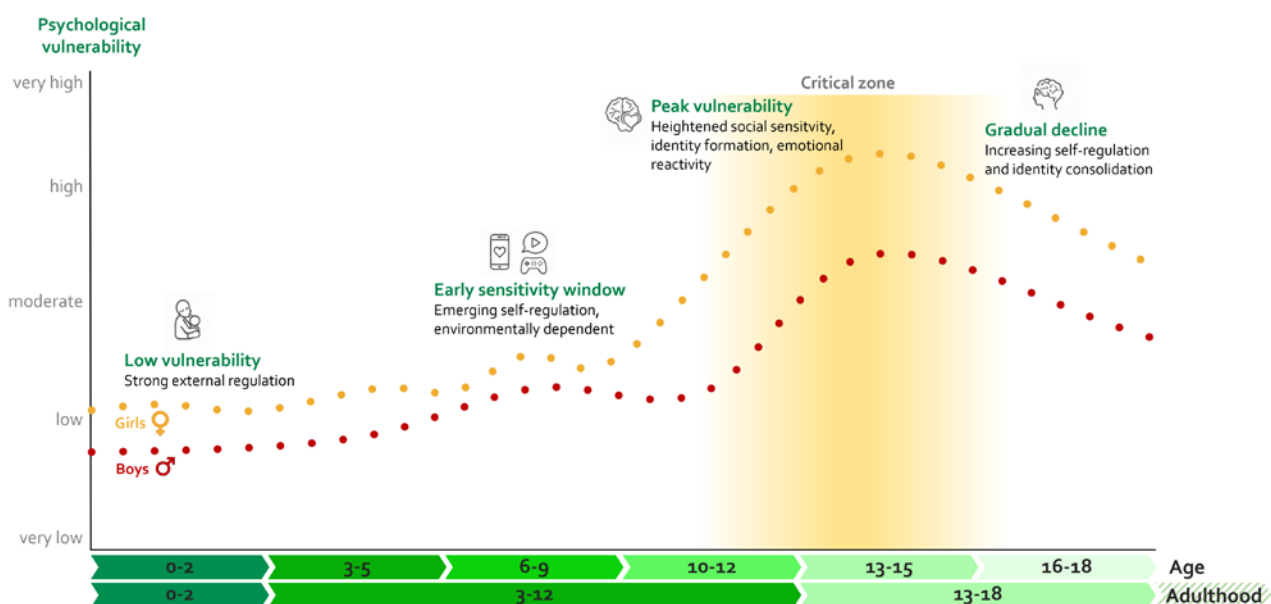
Concerning smartphone use, prospective longitudinal research indicates that for children aged 12, acquiring a smartphone may be linked to mental health issues and insufficient sleep at 13. Evidence suggests that acquiring a smartphone at 13, on the other hand, is not statistically associated with depression at 14. These results are also impacted by duration of use. The suggestion is that children at 13 are more emotionally ready to acquire a smartphone, to use social media and other digital services, and to handle potentially negative effects for their mental health⁴⁶.

For many children, the period of 10 to 12 marks an early stage in the development of internalising problems, such as anxiety and depressive symptoms. These issues are often influenced bidirectionally by social media and other digital services use⁴⁷. Dynamics are not equally distributed. Evidence suggests that girls are particularly vulnerable to appearance-based comparison and platform-mediated social evaluation.

Social media and other digital service-specific architectures further shape risk exposure. In particular, exposure to idealised and appearance-focused content has been linked to body dissatisfaction and negative self-perception, especially among girls⁴⁸. At this age, individual vulnerabilities, such as ADHD, anxiety or social difficulties, interact with social media+ environments in more complex ways, often reinforcing problematic patterns of use⁴⁹. The impact of social media+ environments on children's mental and physical health, and social and individual risk factors are explored in more detail in chapter 2.

Figure 4 – Psychological vulnerability throughout development

Sensitivity to mental health difficulties and digital risks



CONCLUSIONS

10 to 12 years represents a critical stage in which developmental sensitivity, decreasing supervision and digital services use converge. Digital risks arise from the interaction between these factors, rather than from individual use alone. As such, this stage marks a key inflection point for child safety online. The main challenge is the convergence of developmental sensitivity and amplification mechanisms, which increase the risk of self-esteem instability and problematic use.

This requires a transition from parent-centred approaches towards structurally oriented and developmentally adaptive regulation. Access to digital devices at this stage should be carefully regulated. Use should primarily occur either with parental consent and supervision or within structured educational contexts (for example, using guided school-based learning applications), rather than through unrestricted personal ownership of devices. This approach helps to balance early digital engagement with the establishment of necessary protective boundaries.

Institutional responses, especially in schools, should support digital skills and literacy, emotional resilience and critical engagement. Caregiver supervision remains essential, especially in the context of leisure use. However, its effectiveness is increasingly limited by children's emerging autonomy and the complexity of social media and other digital services.

RECOMMENDATIONS (3-12 YEARS)

Ensure supervised use of age-appropriate social media+ and devices

From the age of 3 onwards, children's online interactions should be limited and supervised and gradually adapted to children's evolving capacities in a structured manner. Device use should be avoided without parental authorisation and supervision. Caregivers should continue to privilege face-to-face interactions, offline activities, and ensure children benefit from sufficient sleep. In educational settings, children and adolescents' use of school-provided devices should be with a defined educational purpose. Primary schools should be largely device-free to protect children's development, social interactions and learning.

Offer children and their supporting circles quality digital and well-being education

Children and adolescents should have access to high-quality digital and media literacy (including AI literacy) education throughout schooling, starting at an early age. Minors could be consulted on the design of digital and media literacy education. Education should equip children and adolescents with the knowledge and skills they need to understand the risks and to navigate safely online.

Self-regulation skills should be highlighted as a priority from the very first years of life, not just for children of school age. Schools should ensure children and adolescents receive information about well-being and quality mental health education. Relevant resources and professionals should be made available to support children, and caregivers and educators (supporting circles) in their supervisory roles. Supporting circles must be able to recognise early signs of digital neglect, harmful use and abuse online, and know where they can receive support.

13-18: Adolescence as the stage of evolving autonomy

13-15 YEARS: THE FIRST STAGE OF EVOLVING AUTONOMY

Adolescence between the ages of 13 and 15 represents the central stage of minors' identity formation, characterised by heightened exploration, instability and the search for coherence across social contexts. Peer relationships become the primary reference point for self-evaluation and belonging. Cognitive capacities expand, enabling more advanced abstract thinking, perspective-taking and self-reflection.

Decision-making and self-regulation also improve, but remain context-dependent, in particular, in emotionally or socially charged situations. Identity development increasingly unfolds within digitally mediated environments, where self-presentation, feedback, and social evaluation are continuous, visible and scalable⁵⁰.

Neurobiologically, adolescence is marked by an imbalance between highly active emotional and reward systems and developing cognitive control systems. While limbic processes^d heighten emotional reactivity and sensitivity to social feedback, the prefrontal cortex (responsible for impulse control and self-regulation) matures more gradually. Hormonal changes further intensify emotional experience.

This results in a developmental configuration in which adolescents are more reactive, more sensitive to social evaluation and more prone to risk-taking, especially in peer contexts. Although self-regulatory capacities improve, they are often outpaced by the intensity of socio-emotional processing⁵¹.

Psychologically, this stage is defined by intensified shaping of identity work, emotional variability, and reliance on external validation. Self-esteem becomes unstable and contingent on social feedback, while adolescents increasingly engage in intentional self-presentation. Social media+ environments provide affordances, such as editability, visibility and quantifiable feedback, which facilitate these processes⁵².

AGE-SPECIFIC CHALLENGES

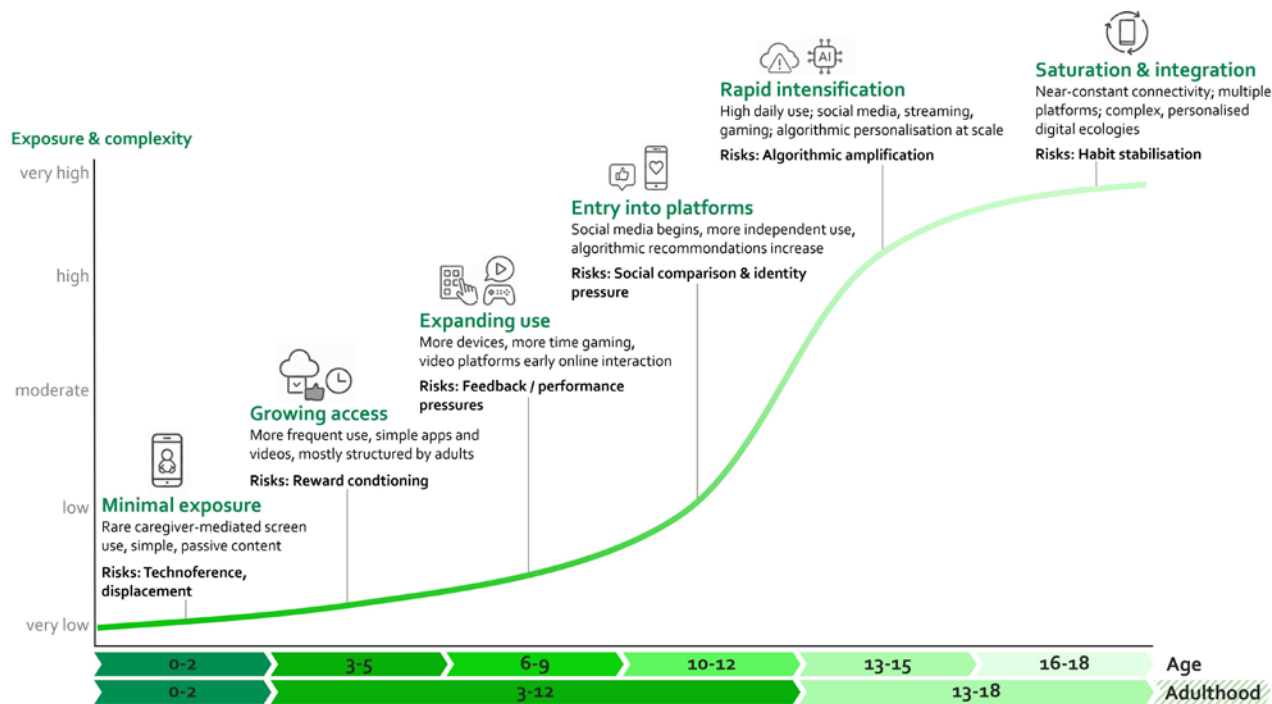
Mental health risks

During this stage, social media and other digital services are used for emotion regulation and coping, which may offer short-term benefits, but can reinforce dependence on external regulation⁵³. The use of social media+ by adolescents as a mood-regulation strategy may be associated with higher instances of depression⁵⁴.

Adolescence from 13 to 15 represents the peak of vulnerability to mental health problems, driven by the interaction of developmental changes and environmental influences. This stage is associated with increased rates of internalising disorders, such as depression and anxiety⁵⁵. Heightened sensitivity to social comparison, feedback and exclusion creates specific pathways of vulnerability in social media+ environments. Pressures related to self-presentation and identity instability may contribute to reduced self-concept clarity.

Risk-taking behaviour peaks and is strongly shaped by peer dynamics. This can be amplified through digital visibility and feedback. Individual and contextual factors, such as pre-existing mental health conditions and family stress, interact with social media+ environments, often reinforcing vulnerabilities over time⁵⁶. Longitudinal evidence suggests that these risks are not uniform. Particularly strong and persistent negative effects are observed among adolescent girls.

d. The limbic system is a set of brain structures involved in emotional processing, motivation and reward.

Figure 5 – Digital exposure and complexity throughout development*Access, the intensity and complexity of social media+ environments increase*

Risks related to AI and social media and other digital services

Digital risks in adolescence are intensified by the convergence of autonomous use, developmental sensitivity, and algorithmically structured environments. An especially important AI-specific risk in this stage concerns conversational agents and so-called ‘AI companions’. Adolescents may use such systems not only for entertainment or information seeking, but also for personal, emotional or crisis-related conversations.

These interactions are often designed to be affirming, low-conflict, and permanently available. While this may provide a form of low-threshold support, it also creates risks of one-sided attachment and emotional dependency. This can be met with reduced exposure to the ambiguity, disagreement and mutual responsibility characterising human relationships.

Where such systems are accessible without reliable age verification or adequate safeguards, additional risks arise in relation to sexualised communication, manipulation, grooming and crisis-related content. AI companions represent not merely another form of digital content, but a new type of socio-emotional environment which requires specific developmental and regulatory attention.

A central mechanism is algorithmic amplification. Recommendation systems prioritise content that maximises engagement, often reinforcing emotionally salient and identity-relevant material. This can shape perception and behaviour over time by strengthening existing vulnerabilities⁵⁷. Many social media and other digital services promote continuous social evaluation, exposing adolescents to persistent feedback and comparison. This can increase emotional volatility and dependence on external validation.

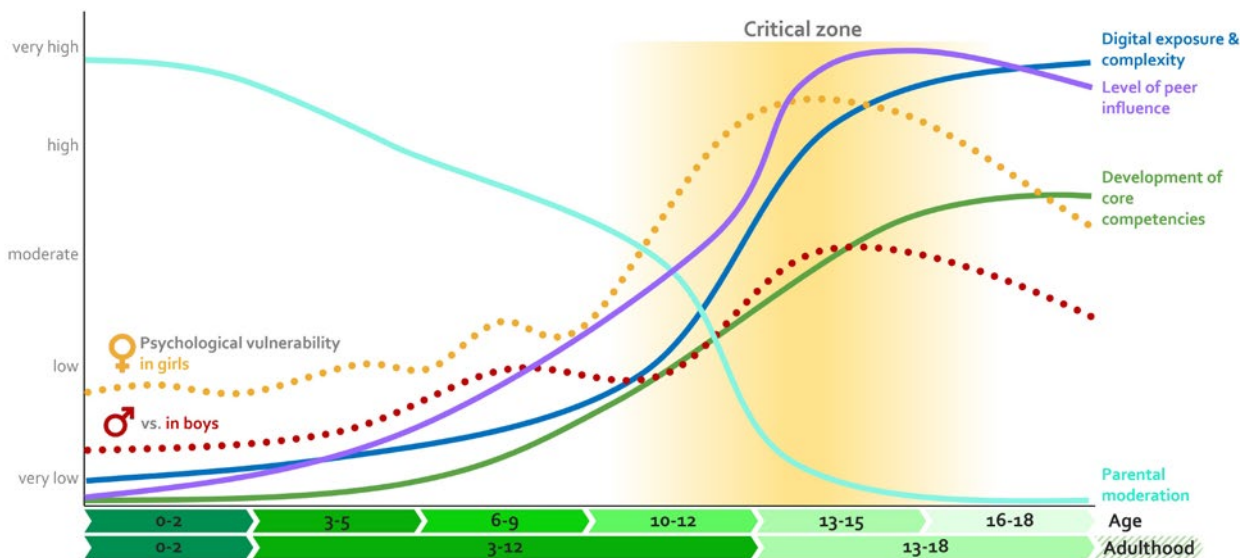
Risks of addiction

Design features such as variable rewards, infinite scrolling and constant availability contribute to problematic or compulsive use, interacting with adolescents' heightened reward sensitivity⁵⁸. Social media and other digital services use is also associated with sleep disruption, reduced well-being and emotional distress, although effects are generally small and moderated by context⁵⁹.

Importantly, these risks are not uniform in all services or deterministic. They emerge from the interaction between developmental vulnerabilities and digital features, highlighting the need to move beyond simplified models of the impact of digital services⁶⁰.

Figure 6 – A developmental mismatch between digital exposure, vulnerability and regulatory capacity

The combined trajectories illustrate that digital exposure increases rapidly, while parental mediation declines and regulatory competencies develop more slowly. This trend coincides with a peak in psychological vulnerability during adolescence.



CONCLUSIONS

From the age of 13, adolescents transition from supervised to guided online use. Adolescents have greater freedom to explore the opportunities presented by the online world to connect, learn and explore their creativity. Social media and other digital services offer adolescents the chance to develop their passions and interests, and to share them with others.

The transition to autonomy is a normal part of growing up in today's online world, as it is offline. The question is not how to hold adolescents back in this transition, but to limit their exposure to potential harm during a stage of peak developmental vulnerability. This vulnerability is characterised by the convergence of identity formation, heightened socio-emotional sensitivity and algorithmically structured environments.

Digital risks arise not from exposure alone, but in its intensity and structure within social media+ designed to maximise engagement at an age of increased vulnerability. These factors make adolescence a central stage for both research and regulation.

At this age, traditional forms of supervision by caregivers and educators become increasingly ineffective and difficult to implement. Risks are increasingly shaped by social media and other digital service structures, rather than individual behaviour alone. A key challenge lies in addressing algorithmic systems that structure exposure and influence behaviour, while operating with limited transparency.

Regulatory approaches must balance protection with adolescents' need for online autonomy and participation. Effective protection requires a developmentally informed, multi-layered approach combining social media+ regulation, educational interventions and support for self-regulation and critical digital services use.

Recent research indicates that blanket bans on social media+ use may be less effective than often assumed. While such measures aim to reduce exposure and associated risks, the evidence for their effectiveness is currently limited, in particular, for adolescents. Overly restrictive approaches may be circumvented or shift risks to less regulated environments.

Against this background, an age-tiered model of regulated participation – combining privacy-preserving age verification, safety by design, and media education – has been proposed as a more developmentally sensitive alternative. This approach aligns protection measures with children's evolving capacities, balancing safety, participation and children's rights within an integrated framework for child safety online.

16-18 YEARS: THE SECOND STAGE OF EVOLVING AUTONOMY

Late adolescence marks a stage of increasing identity consolidation and growing autonomy. Previously explored roles, values and self-concepts begin to stabilise, resulting in more coherent and internally integrated self-representations. Meanwhile, cognitive capacities reach a higher level of sophistication. This includes abstract reasoning, long-term planning and reflective decision-making.

These developments support more autonomous participation in social, educational and economic systems. Social media and other digital services are no longer exploratory spaces, but fully embedded in everyday life, shaping communication, participation and self-expression⁶¹. Neurobiologically, the brain approaches functional maturity, especially in the prefrontal cortex. This leads to improved self-control, planning and decision-making.

Emotional and cognitive systems become more integrated, enabling more stable emotional regulation and better anticipation of long-term consequences. However, development is not yet complete, with maturation continuing into early adulthood⁶². This results in a profile of increased stability combined with continued sensitivity to highly stimulating environments.

AGE-SPECIFIC CHALLENGES

Path dependency

Despite increasing maturity during this age, vulnerabilities remain. Mental health difficulties that emerged earlier may persist, especially when underlying mechanisms remain unaddressed⁶³. This emphasises the need to protect minors from potential harm not only during adolescence, but starting at the earliest age.

Self-regulation while improved remains context-dependent and can be challenged by highly engaging digital environments. Moreover, the consolidation of behavioural patterns introduces path dependency, making established habits more resistant to change. Digital risks at this age relate less to emergence and more to stabilisation and reinforcement.

Risks of problematic use

Established usage patterns, including problematic and excessive use or addiction, are maintained and strengthened by features in social media and other digital services (for example, personalised recommendations, continuous content streams and reward-based engagement)⁶⁴. Algorithmic systems continue to shape exposure and behaviour, often subconsciously⁶⁵. Finally, vulnerabilities continue to be shaped by structural inequalities, such as family environment and access to resources⁶⁶.

Social media+ use remain associated with outcomes, such as sleep disruption, emotional stress, and social comparison. However, effects are increasingly driven by long-term patterns, rather than acute developmental sensitivity⁶⁷. Risks related to data exploitation, commercial influence and participation in digital economies become more relevant as adolescents engage more actively with social media+.

CONCLUSIONS

Late adolescence presents a challenge for child safety online, marking the transition from protected minor to adult majority. The main challenge at this age is reconciling adolescents' increasing autonomy with persisting developmental vulnerabilities.

Another important issue is the emergence of a discrepancy. Individuals aged 16 to 18 are often treated as fully autonomous users, despite still ongoing developmental processes. This highlights the need for regulatory approaches moving beyond rigid age thresholds and accounting for gradual developmental transitions.

Effective protection in this stage must not only address access and content, but also the structural conditions shaping long-term behaviour, including the design of social media and other digital services, algorithmic systems and data practices. Adolescents should be supported in developing sustainable and reflective practices concerning the use of social media+, including self-regulation and critical awareness of digital environments, during this stage of evolving autonomy.

Risks are increasingly cumulative, shaped by established habits and structural influences, rather than immediate developmental sensitivity. Child safety online must therefore extend into this stage to address the transition to autonomous participation, in parallel to persisting developmental vulnerabilities. Measures should promote the development of sustainable engagement practices that guide adolescents into adulthood.

RECOMMENDATIONS (13-18 YEARS)

Ensure evolving autonomous use of age-appropriate social media+

From the age of 13, adolescents may begin to transition from supervised to autonomous social media+ use. Parents and caregivers, teachers and educators maintain an important role in guiding adolescents' online interactions. Adolescents' supporting circles should continue to promote face-to-face interactions and activities offline, including sufficient sleep. In educational settings, device use should be with a defined educational purpose.

Conclusion

This chapter has explored the defining features and the risks associated with children's online use at three primary stages of their development: early childhood (0-2 years), childhood (3-12 years), and adolescence (13-18 years). Overarching recommendations were presented to guide social media and other digital services providers, regulators, caregivers and educators in delivering an age-appropriate approach to child safety online, in accordance with their respective powers and responsibilities.

Grounded in an analysis of the available evidence concerning the risks to minors' health and well-being throughout these developmental stages, a staged approach steering children's and adolescents' interactions online was outlined in three primary stages:

- // 0-2 years: early childhood as a specially protected stage of development;
- // 3-12 years: childhood as a supervised stage of development;
- // 13-18 years: adolescence as the stage of evolving autonomy.

Existing online child protection frameworks and instruments are explored in more detail in chapter 3. Measures designed to empower minors online and their supportive circles in guiding children's and adolescents' social media+ use are presented in chapter 4. The next chapter examines in greater detail the risks for children online at different stages of their development, including in relation to various social and individual factors.

02

Evidence on risks minors face online

As alluded to in chapter 1, child safety online cannot be conceptualised from a developmental perspective alone. Factors, such as socioeconomic background and gender have an important influence on children's and adolescents' patterns of online use and susceptibility to associated risks⁶⁸. Sexuality, racial and ethnic origin, religion, migration backgrounds, and special educational needs also impact minors' exposure to harm.

This chapter explores the second of the Six Guiding Principles proposed by the Co-Chairs as a framework to steer action: equality and diversity. It outlines how inequalities in risks and exposure to online harms for different ages and socioeconomic groups intersect with minors' needs throughout their development. It also assesses minors' exposure to various risks online (for example, illegal content and harmful design features of social media and other digital services) that have an impact on their physical and mental health.

Currently, **there is substantially more evidence (for example, focusing on cyberbullying and harmful content) for a potential negative association between social media and mental health** than there is regarding its positive effects. Much of the evidence concerning social media's potential to harm minors' health and well-being is correlational, allowing no causal conclusions. However, it nonetheless offers sufficient indications to warrant actions to protect minors online.

Despite the availability of evidence in certain areas, some data gaps hinder a comprehensive analysis that can incorporate social and individual risk factors from a developmental perspective. More generally, a lack of transparency and access to social media data hinder research on the positive and negative effects of minors' social media use⁶⁹.

More longitudinal studies and European-wide data sets could help to better understand in detail the consequences of the risks children and adolescents face across different social media+. Any detailed examinations on minors require care in terms of research ethics⁷⁰.

Some of the collected evidence has also led to a few misconceptions in public debate. One example is claims of 'brain rot' caused by social media, with some reports suggesting excessive social media use may reduce grey matter in the human brain⁷¹. Such statements are overly reductive and are not based on medical evidence.

This chapter serves to present and reinforce the current evidence base. **Robust evidence on how risks and harms relate to different digital services, and not just social media, is crucial to inform appropriate actions** to protect and empower minors online. Opportunities for children and adolescents in the digital world are explored in chapter 4.

Social and individual risk factors

GENDER AND SEXUALITY

Risks for girls and boys

Young women and girls are particularly exposed to a number of gender-specific harms online. This includes bullying of a sexist and misogynist nature and disproportionate exposure to sexual harms⁷², such as the non-consensual sharing of intimate images and sexually explicit deepfakes online⁷³.

More generally, research suggests that girls are more likely to experience cyberbullying than boys⁷⁴. One study showed that as many as 63% of girls in Europe have reported experiencing some form of online harassment on social media⁷⁵.

There is some evidence that the **harms young women and girls are exposed to online evolve with age**. Girls aged 13 to 15 may be more likely to experience exclusion from group chats, body shaming, gossip and public humiliation⁷⁶. Young women aged 11 to 18, meanwhile might be more likely to experience abuse of a sexualised or controlling nature, including coercion, deepfakes and grooming. While girls of this age are particularly at risk, boys are also exposed to these dangers.

The growing pervasiveness of artificial intelligence (AI) and its integration in online applications and services augments risks⁷⁷. As an example, deepfakes can be used maliciously to cyberbully others⁷⁸. Since their emergence, the creation of deepfakes has been on the rise and may be used to perpetrate sexual abuse online⁷⁹. Deepfakes have introduced a new dimension of harm that not only damage a person's reputation, but like other cyberbullying acts could also potentially lead to psychological trauma.

Girls may be more exposed to harms related to social comparison online and have a higher chance of developing a negative image of their own body⁸⁰. Research suggests that peer pressure concerning body image ideals may be compounded by online use⁸¹.

As such, girls may be more likely to adhere or promote online communities encouraging eating disorders⁸². Evidence indicates a link between adolescent girls' online interactions for self-presentation, including social media use, and negative effects for mental health, including depression and anxiety⁸³. Girls between the age of 10 and 12 may be at particular risk.

As a general pattern, girls spend more time on social media and using online chat features than boys⁸⁴. Some studies have associated moderate or heavy digital services use among girls with a higher prevalence of mental health issues and lower well-being⁸⁵.

Boys, meanwhile, are more likely to spend time online gaming. A number of studies have demonstrated that online gaming is associated with mental health issues, such as depression and anxiety. However, there may be a stronger association between social media use and mental health issues than with gaming⁸⁶. The risk of online sexual transgressions online is higher for boys than in real-world settings. Their vulnerability in these settings is often underestimated⁸⁷.

Finally, girls and boys may cope with online harms in different ways. In the case of cyberbullying, young men might be more likely to use avoidance coping techniques due to norms that encourage young men to self-manage problems, rather than seeking help from their supporting circles⁸⁸. For both girls and boys, studies link higher social media use with poorer mental health and well-being⁸⁹.

LGBTIQ+ communities

Sexually diverse children and adolescents are more likely to experience hate⁹⁰ and violence online, including cyberbullying⁹¹ and sexual harassment⁹². Digital services may also amplify young LGBTIQ+ users' experiences of grooming, sexual assault, and the risk of being 'outed' without their consent⁹³.

At the population level, among people belonging to LGBTIQ+ communities, 63% report having encountered violent online content and disinformation targeting LGBTIQ+ communities⁹⁴. Evidence suggests that adolescents belonging to LGBTIQ+ communities may be more likely to use online spaces to explore their sexuality and identity online, to search for sexual health information, or to seek peer support and connection without exposing themselves to 'in-person' risks⁹⁵.

This may increase LGBTIQ+ children's and adolescents' exposure to risks and harm online. Despite many arguments in favour of online spaces' potential to offer sexually diverse children and adolescents the chance to connect and receive peer support, evidence suggests that in-person interactions may remain more effective in offering support than interactions online⁹⁶.

SOCIOECONOMIC BACKGROUND

Adolescents from disadvantaged socioeconomic backgrounds are more likely to have negative experiences online, including cyberbullying⁹⁷, excessive device use, social media addiction⁹⁸ and problematic use⁹⁹. Socioeconomic factors, including lower family income, may also increase the prevalence of harmful online experiences among children and adolescents¹⁰⁰.

Family background has an important influence on minors' exposure to harm online. Children and adolescents whose parents have low online digital literacy may be exposed to greater harm online¹⁰¹. Evidence suggests that minors from less advantaged socioeconomic backgrounds tend to have lower levels of digital literacy enabling them to navigate safely online and may take part in more risky behaviour online¹⁰².

More privileged families, on the other hand, may be better equipped and benefit from more resources to guide their children's and adolescents' interaction with digital technologies in positive ways¹⁰³ and to address negative impacts. In this way, problematic use of digital services, including social media, may reinforce existing inequalities in adolescents' and young adults' health, academic involvement and achievement.

While living in an urban or rural area may not directly influence minors' exposure harm online, children and adolescents living in rural areas might be more likely to deploy avoidance coping mechanisms, which are more closely associated with negative mental health outcomes. This highlights the need to develop programmes that address social inequalities, including in rural and underserved areas, to reduce the likelihood of minors experiencing harm online¹⁰⁴.

RACIAL AND ETHNIC ORIGIN, RELIGION AND MIGRATION

BACKGROUNDS

Adolescents belonging to racial minorities are more likely to experience online harm, such as cyberbullying, racial discrimination and harassment¹⁰⁵. Evidence from Europe indicates that online hate speech frequently targets people because of their racial or ethnic origin, religion, nationality or migration background, with Black people, Roma, Jews and Muslims among the groups most commonly targeted¹⁰⁶. Moreover, racism, religious hate, sexual orientation hate, and sexism are some of the most prevalent forms of hate speech found online¹⁰⁷.

Evidence from the European Union further suggests that these online experiences reflect broader patterns of discrimination affecting minority communities. According to the European Union Agency for Fundamental Rights (FRA), nearly half (47%) of Muslims surveyed across 13 EU Member States reported experiencing racial discrimination during the previous five years. This includes harassment and discrimination in education, employment and public spaces. Many also reported exposure to anti-Muslim hostility online¹⁰⁸. Similarly, FRA's survey of people of African descent found that almost half of respondents had experienced racial discrimination, with online environments identified as an important setting in which racist abuse occurs¹⁰⁹.

There appears to be a growing normalisation and trivialisation of online hate speech. The Council of Europe's European Commission against Racism and Intolerance (ECRI) has highlighted increasing levels of hate speech across Europe. It notes that ethnic origin and religion are among the most common risk factors for online hate, and warns that xenophobic, anti-Muslim, antisemitic and anti-Black rhetoric has become increasingly normalised in digital spaces¹¹⁰.

Moreover, at the population level, evidence suggests that people from minority backgrounds may be disproportionately affected by restrictions and removal measures in content moderation systems, as a result of biases in algorithms used in these systems¹¹¹. This reflects broader concerns regarding ethnic and gender biases in speech detection and prediction models used by digital services providers to automatically scan for harmful content online¹¹².

CHILDREN WITH SPECIAL EDUCATIONAL NEEDS

Evidence suggests that young people with special educational needs and disabilities are more likely to experience harms¹¹³, such as hate speech, cyberbullying, cyberthreats, harassment, exposure to sexual content and grooming online¹¹⁴.

Factors, such as communication barriers and emotional literacy, may exacerbate existing vulnerabilities for children and adolescents with disabilities in online spaces¹¹⁵. Social isolation and feelings of vulnerability experienced by minors with disabilities significantly increase the risk of victimisation¹¹⁶.

Evidence suggests that children and adolescents with disabilities may feel more comfortable to express themselves in online spaces¹¹⁷. Furthermore, minors with disabilities engage online to a greater extent to share their interests and hobbies, to play games with others, and search for health information and emotional support, despite experiencing higher exposure to harm online¹¹⁸.

Similarly, research suggests that children and adolescents with neurodevelopmental conditions, including attention-deficit/hyperactivity disorder (ADHD) are more exposed to problematic online use¹¹⁹. In addition, minors with characteristics of Autism Spectrum Disorder, Intellectual and Developmental Disorders are

increasingly likely to be targeted by bullying online¹²⁰. Extended screen time may also be associated with increased ADHD symptoms¹²¹.

It is important to note that social and individual risk factors for children and adolescents online intersect. For example, minors with disabilities may be more likely to experience hate speech online attacking their gender, sexuality, race or religion¹²². This demonstrates the need to consider the interplay between diverse social and individual factors and how they exacerbate the exposure of particular social groups to harm when designing measures promoting child safety online.

RISKS FOR MENTAL HEALTH

According to data from the World Health Organization, one in seven 10 to 19 year-olds worldwide experiences a mental health issue¹²³. At the European level, the 2023 Eurobarometer survey on mental health showed that 59% of young people had experienced an emotional or psychosocial problem, such as feeling depressed or anxious¹²⁴.

Among adolescents, depression, anxiety and behavioural disorders are among the leading causes of illness¹²⁵. Globally, suicide is a leading cause of death among young people¹²⁶ (see below: Deliberate self-harm and suicidality). At the population level, vulnerable groups including people belonging to LGBTIQ+ communities and those with migration or refugee backgrounds are most at risk¹²⁷.

Evidence suggests that girls are particularly vulnerable, for example to appearance-based comparison and platform-mediated social evaluation. For many minors, the ages of 10 to 12 mark an early stage in the development of internalising problems, such as anxiety and depressive symptoms. Mental health issues may continue into adolescence, which represents the peak of vulnerability, if the underlying mechanisms remain unaddressed.

Mental health issues not only have serious direct consequences for children's and adolescents' well-being and development. They also impact minors' attendance and performance at school and in later life their employability¹²⁸. Data suggests broad effects of digital services use, in particular social media, on children's and adolescent's health and development.

One study indicated that excessive social media use of more than three hours per day may be associated with negative mental health outcomes, especially depression and anxiety¹²⁹. Similarly, the results of the 2022 PISA Assessment covering 22 EU Member States showed that the estimated probability of 15 year-olds experiencing poor mental health rises with the time they spend online¹³⁰.

EVIDENCE OF A BIDIRECTIONAL RELATIONSHIP BETWEEN MENTAL HEALTH ISSUES AND DIGITAL SERVICES USE

The relationship between children's and adolescents' interaction with the social media+ world and mental health issues is complex. Concerning social media, evidence points to a bidirectional relationship between minors' online interactions and the prevalence of mental health issues¹³¹. This is to say that children's and adolescents' interactions with online spaces may cause, but also reinforce existing mental health issues, including depression¹³².

Existing evidence supports the notion that negative online experiences are highly prevalent in adolescents already struggling with mental health issues¹³³. Adolescents experiencing social anxiety may be

particularly inclined to spend more time on social media or to develop problematic usage patterns¹³⁴. Socially anxious individuals sometimes turn to social media to build positive online relationships, alleviating anxiety from face-to-face interactions, but fostering avoidant behaviours.

Similarly, minors' exposure to content that is inappropriate for their age, including content depicting or encouraging physical self-harm, eating disorders and suicide, is likely to exacerbate pre-existing conditions.

For adolescents on social media, the quality of offline networks and personality traits, including introversion or extroversion, may act as protective or risk factors. Research suggests that the use of social media by extroverted adolescents with good self-esteem and high-quality offline friendships may reinforce offline relationships and increase support online.

Introverted adolescents with low self-esteem and weaker social networks offline on the other hand may be more inclined to seek new friends online. This may increase potential risks of exposure to unwanted contact or content¹³⁵.

"Take a broader and closer view at the various technologies involved. [...] Focusing only on social media is much too narrow as other technologies, such as GenAI, pose comparable if not higher risks for minors."

— JUDITH SIMON,
PROFESSOR FOR ETHICS IN INFORMATION
TECHNOLOGIES, UNIVERSITY OF HAMBURG

AI TOOLS AND COMPANIONS IN SOCIAL MEDIA+

Recent technological advances have accelerated the use of generative AI, large language model chatbots and 'AI companions' by children and adolescents. This shift has been accompanied by growing concern regarding the implications of these technologies for minors' mental health and well-being. This is why the Co-Chairs have opted for the broad term social media+ in this report.

Unlike earlier digital mental health tools, including apps and virtual reality, which struggled to sustain use, AI chatbots are already being used by millions of children and adolescents to seek information (including on mental health issues), interaction and emotional support. Some early evidence suggests benefits, such as the potential of AI conversational agents to help reduce symptoms of depression¹³⁶.

Research also indicates potential benefits of AI-driven interfaces for inclusive education among students with visual, physical and cognitive disabilities¹³⁷. However, the impact of AI tools on minors' education and skills development needs to be more extensively analysed to understand potential benefits and risks¹³⁸.

Concerning signals are emerging in media reporting and in early research of the possibilities of AI-associated ‘psychotic’ symptoms, parasocial attachment, patterns of dependence¹³⁹ and incitement to suicide¹⁴⁰. Evidence suggests that minors often perceive ‘AI companions’ as human-like¹⁴¹. However, they may not provide genuine empathic support and can pose risks to minors’ mental health¹⁴².

Young children may be particularly susceptible to becoming emotionally attached to AI companions, which they might understand to be responsive social partners. Adolescents who use these tools for personal and emotional exchanges are also exposed to risks of attachment and dependency.

A recent European study showed that more than 86% of Irish, French, German and Swedish teenagers use AI tools. Among them, more than half use AI tools to discuss intimate topics and solve personal issues¹⁴³. This study indicated that adolescents who use AI tools are more likely to suffer from symptoms of anxiety.

AI systems may exploit minors’ vulnerabilities by abusing their natural curiosity, desire for rewards, susceptibility to pressure and inclination towards instant gratification. They may also exacerbate the impact of manipulative design techniques, such as behavioural ‘nudging’¹⁴⁴.

Algorithmic and societal biases embedded in AI training data can also foster disinformation, misinformation and stereotypes that minors may internalise from an early age¹⁴⁵. The consequences of AI-enabled exploitation can be severe and long-lasting for children and adolescents, including addictive behaviour, reduced concentration and cognitive capacities, poor academic performance and social difficulties.

Children from 6 to 12 may be especially exposed to developing early addictive behaviours, which may continue into early adolescence and beyond. Further research is needed, not only into the opportunities AI tools offer children and adolescents, but also to understand how to detect harm and ensure human oversight remains a key part of AI-mediated support.

Moreover, AI-powered features (for example, within gaming environments, including AI-driven characters, personalised content generation, and in-game chatbots) are not fully addressed by existing legislation framework to adequately protect minors online.¹⁴⁶

LONELINESS AS A CAUSE OR EFFECT OF SOCIAL MEDIA USE

For children and adolescents, loneliness may be a cause or effect of social media use¹⁴⁷. In cases where loneliness can be considered a cause, feelings of isolation may encourage increased social media use¹⁴⁸ to form new friendships. Loneliness offline may also motivate behaviours, such as unrealistic presentations of the self online, which may in turn exacerbate feelings of loneliness¹⁴⁹.

More generally, experiencing harm online can encourage minors to withdraw from social activities and school, to lose trust in others, and become more reluctant to join online activities promoting well-being (such as connecting with friends or services)¹⁵⁰. It is important to recognise that online harms, including cyberbullying, frequently overlap with harms in the physical world.

PASSIVE VERSUS ACTIVE USE

The design of social media+ is another important factor in how these services impact children's and adolescents' mental health. Automated pathways, optimised for commercial goals, can lead to minors being fed a seemingly endless supply of harmful content, from graphic images of self-harm, eating disorders and sexual images¹⁵¹.

Research indicates that how children and adolescents engage with social media influences the effects it can have on their mental health and well-being. Passive use, such as browsing and scrolling, may be associated with higher levels of depressive symptoms, loneliness, and stress¹⁵².

Meanwhile, active use such as posting, commenting, messaging and liking tends to correlate with higher well-being, life satisfaction (especially among girls) and heightened perception of social support. However, some findings show mixed results concerning active and passive use and the frequency of depression¹⁵³.

BODY IMAGE CONCERNS AND EATING BEHAVIOURS

Social media platforms open access to children and adolescents to a wide array of content related to eating behaviours, encompassing both healthy and unhealthy practices. Channels promoting eating disorders pose significant concerns and have the potential to foster dysfunctional eating behaviours hindering recovery¹⁵⁴.

Such channels may use evolving hashtags to evade detection and blocking by social media platforms, promoting thinness, low self-evaluation and perfectionism. These behaviours are associated with eating disturbances affecting teenage girls¹⁵⁵ in particular, starting at 10 years of age.

The widespread dissemination and normalisation of 'perfect body posts' and 'thin-ideal' imagery, often through photo-centric activities on social media, may further contribute to children's and adolescents' body image dissatisfaction and body shame.

This exposure can lead to heightened self-objectification, body image concerns and even a desire for cosmetic surgery. Adolescents, especially teenage girls, are at special risk of developing negative body image perceptions perpetuated by social media's portrayal of idealised body standards¹⁵⁶.

DISINFORMATION AND MISINFORMATION

Minors tend to prefer social media and online platforms as sources of news and information over traditional media outlets¹⁵⁷. This use exposes them to a wide array of disinformation and misinformation online.

By the age of 8, about half of children report encountering misinformation on a weekly basis¹⁵⁸. The older children are, the more frequently they report experiencing misinformation¹⁵⁹. One survey in the United States indicated that over a third of teens have been misled by fake content online¹⁶⁰.

Children and adolescents may not even be familiar with the concepts of misinformation and disinformation, leading to underreporting and a lack of awareness of related risks. This highlights the gap between children's cognitive and emotional capacities, and the risks they are exposed to online. While around 70% of young people in the EU reported they could confidently recognise disinformation online¹⁶¹, their responses are influenced by their understanding of what constitutes disinformation and other factors (i.e. gender, socio-economic background etc.).

With the emergence of increasingly sophisticated technologies capable of creating and disseminating misinformation and disinformation, including AI tools¹⁶², it is becoming more and more difficult for users, in particular minors, to distinguish unreliable from reliable information.

Minors may not only be directly harmed by misinformation and disinformation, but also disseminate it among their peers¹⁶³, for example to gain popularity or confirmation¹⁶⁴. A particularly concerning trend is adolescents' increasing use of social media to search for information about personal and (mental) health-related issues, despite the widespread prevalence of misinformation online on these topics¹⁶⁵.

One media investigation in 2021 showed that in the first 35 minutes on one social media platform, nearly 90% of users were shown misinformation specific to COVID-19 vaccines¹⁶⁶. These findings highlight the need for protective measures to limit the spread of misinformation and disinformation online.

In Very Large Online Platforms' (VLOPs) and Very Large Online Search Engines' (VLOSEs) risk assessment and mitigation cycles under the EU Digital Services Act, both providers and civil society noted systemic risks to public health stemming from the large-scale dissemination of medical disinformation and misinformation. Providers of online marketplaces equally noted systemic risks stemming from the sale of legal but harmful substances, illegal, non-compliant or unregulated medical products on their marketplaces. Content related to self-harm, eating disorders and risky health practices is another area for concern.

This underscores the importance of equipping children and adolescents, but also caregivers and educators, with digital skills and literacy from an early age. Public services, including health services, should reflect on how to make accurate and age-appropriate information and guidance on mental, physical, sexual and other health-related issues accessible¹⁶⁷ to children, adolescents and caregivers online.

DELIBERATE SELF-HARM AND SUICIDALITY

The prevalence of deliberate self-harm among adolescents is challenging to ascertain due to limited hospital attendance data, yet evidence suggests an increase in its occurrence¹⁶⁸. The World Health Organization (WHO) lists suicide as the third leading cause of death among 15 to 29-year-olds globally in 2021, with women in this age group being particularly vulnerable¹⁶⁹.

Social media+ use to access and share deliberate self-harm content is a societal issue. Such activities contribute to the normalisation and desensitisation to self-harming behaviours. Research indicates that exposure to self-harm or suicide-related content on social media may lead to so-called ‘contagion’ or ‘Werther’ effects¹⁷⁰. Engaging with suicide and self-harm related content on social media may also increase the likelihood of seeing related content in the future through algorithmic amplification¹⁷¹.

Adolescents may post self-harm content on social media to feel a sense of belonging, or to seek validation or support. However, the feedback received can be difficult to manage. While it might offer positive support, it may also inadvertently reinforce self-harming or suicidal behaviours¹⁷². The relationship between social media influence and suicidality is complex, involving indirect and multifaceted associations [see the box on the ‘White Tiger’ case].

Online victimisation, including cyberbullying, and its potential to enhance children’s and adolescents’ sense of isolation have been linked to an increased prevalence of deliberate self-harm and suicidal ideation¹⁷³. The role of social media+ in these contexts requires careful consideration to mitigate negative impacts and to support vulnerable children, adolescents and their supporting circles effectively.

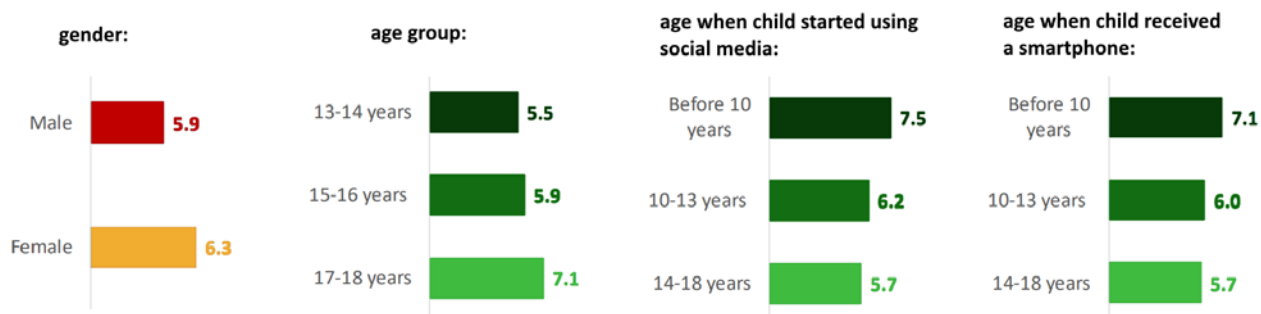
Risks to physical health

Most physical health effects of social media and other digital services are associated with minors’ screen use in general, rather than specific types of use, such as social media. Similar to social media, screen time does not necessarily only involve negative effects, but depends strongly on the specific activity performed. Main research topics in this area include the impact of screen time on children’s and adolescents’ vision, brain development, alcohol use and sleep¹⁷⁴.

Eurobarometer data on the impact of excessive screen time and social media on young people’s mental health indicates that 13 to 18 year-olds spend on average 4.5 hours on screens on a typical school day. At the weekend, this rises to an average of 6.1 hours a day, with almost half of adolescents (46%) exceeding 6 hours. During weekends, 14% of adolescents exceed 10 hours daily.

Figure 1: Adolescents' increased screen use over the weekend

Question: How much time do you spend on screens (smartphone, computer, tablet, TV, gaming console) in total?^a



Source: European Commission (2026). *Impact of excessive screen time and social media on young people's mental health* – June 2026 – Eurobarometer survey.

SIGHT AND PHYSICAL HEALTH

Prolonged screen use is recognised to increase the risk of back pain, headaches¹⁷⁵ and digital eye-strain (also called computer vision syndrome). The risk of suffering these symptoms increases with long screen time, uncorrected vision, small text, low resolution, poor screen height or distance, and inadequate lighting¹⁷⁶.

Children are especially vulnerable to sight issues caused by prolonged screen time because many have undiagnosed visual disorders or receive low-quality eye examinations¹⁷⁷.

Spending an excessive amount of time on social media+ may also lead to an opportunity cost, where children and adolescents are unable to engage in offline activities, including physical activity and offline play, that are critical for their development and health.

“Most of the risks discussed during the Special Panel on child safety online, including excessive screen time and the use of AI companion apps, are relevant not only for children and young people, but for people of all ages.”

— ALBERTO MONGE ROFFARELLO,
ASSISTANT PROFESSOR ON DIGITAL
WELLBEING & ETHICAL AI DESIGN,
POLITECNICO DI TORINO

a. Note: Figures represent mean hours of screen use per day (during the weekend).

SLEEP

Other common physical health risks to social media use include decreased physical activity, time spent outdoors, and sleep reduction¹⁷⁸. Adequate sleep is vital for children’s and adolescents’ development, emotional regulation, memory consolidation, brain maturation and growth hormone release¹⁷⁹. Despite this, a large proportion of adolescents fail to meet sleep recommendations for their age¹⁸⁰.

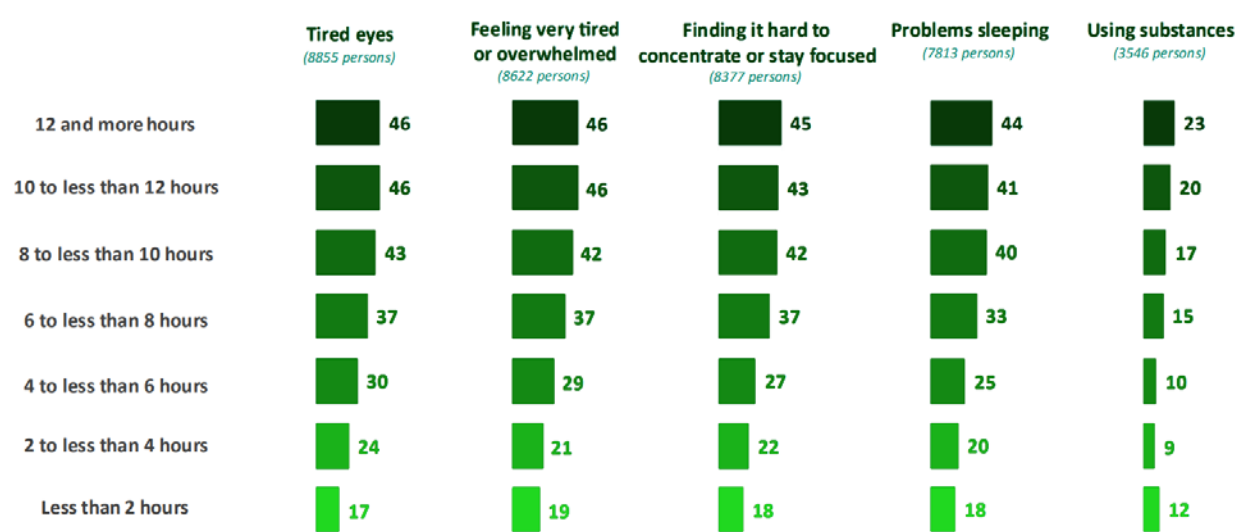
Evidence suggests that screen use by children and adolescents may contribute to reduced and poorer quality sleep, displacing sleep, providing psychological stimulation, and suppressing melatonin production (especially through blue light emission)¹⁸¹. Screen time may also replace time outdoors, having a negative effect on sleep¹⁸² and minors’ overall physical and mental health.

Surveys show high nighttime engagement among adolescents. Age-specific patterns reveal that children under 5 are largely protected by parental control. 6 to 12 year-olds meanwhile experience longer sleep latency and poorer quality, while 13 to 15 year-olds report sleep onset delays, reduced sleep quality and pre-sleep cognitive arousal¹⁸³.

General interventions to cut screen time (for example, reducing screen use before bedtime, after 21:00) have demonstrated a positive effect in sleep duration¹⁸⁴ and next-day vigilance¹⁸⁵. Research exploring the effects of high screen exposure on minors’ brain development is largely correlational and cannot establish causation.

Figure 2: Adolescents’ increasing symptoms by time spent on screens

Question: Which of the following situations, if any, have happened to you in the past 30 days?^b



Source: European Commission (2026). Impact of excessive screen time and social media on young people’s mental health – June 2026 – Eurobarometer survey.

b. Note: Figures represent the percentage (%) of respondents reporting issues by time spent on screens (during the weekend).

ADDICTIVE DESIGN AND ‘DARK PATTERNS’

According to evidence from the WHO, over a third of adolescents reported being in constant contact with friends online. One in ten adolescents shows signs of problematic social media behaviour, characterised by addiction-like symptoms¹⁸⁶.

Recently, research on addiction medicine has shifted its focus from individual factors that lead to or characterise addictive behaviours online to also examine the design of social media and other digital services that encourage these behaviours. Children between 6 and 12 may be at particular risk of developing early addictive behaviours from their use of social media+. These risks continue, especially into early adolescence.

Addictive design techniques and ‘dark patterns’¹⁸⁷ available in some social media+ (intentionally or unintentionally) distort or impair users’ ability to make autonomous and informed choices or decisions. Addictive features include autoplay content, infinite scrolling, gamification, and ‘pull-to-refresh’ features. Dark patterns include fake countdown timers, web interfaces designed to lead consumers to purchases, subscriptions or other choices, and hidden information¹⁸⁸.

Research indicates that other features, including the ‘like’ mechanism and ‘push notifications’, can also encourage compulsive behaviours¹⁸⁹. Studies have also suggested that engagement-maximising platforms have predominantly negative effects for adolescents¹⁹⁰. Adolescents, due to their developmental characteristics and the importance of peer acceptance in identity formation, are particularly susceptible to these persuasive designs¹⁹¹. Young adults and adults with pre-existing well-being issues are also especially vulnerable¹⁹².

The European Commission’s 2024 Digital Fairness Fitness Check¹⁹³ found that features, such as dark patterns, are very frequently encountered by people online. Up to 97% of the most popular websites and apps used by EU consumers were found to deploy at least one dark pattern. It also found that 31% of consumers spent more time and money online due to addictive designs.

Achieving systemic change requires shifting the focus from individual responsibility to addressing the broader impact of social media+ design strategies. Researchers are examining the data-driven business models of social media platforms, which prioritise engagement for profit, and are discussing alternative models that emphasise ethical design¹⁹⁴.

This is met, more broadly, with calls for children’s best interests to be the primary consideration in the design and management of digital environments¹⁹⁵ to support their digital well-being.

ALCOHOL AND SUBSTANCE ABUSE

Over the last decade, research has identified and studied the link between social media use and alcohol consumption among adolescents¹⁹⁶. Alcohol is very present on social media, but important differences exist across digital services concerning its prevalence and portrayal¹⁹⁷. Positive portrayals of alcohol on social media shape attitudes and perceived norms¹⁹⁸. Exposure to and sharing of alcohol-related content is associated with higher drinking, creating a bidirectional reinforcement loop¹⁹⁹.

Individual differences, such as dispositional traits, social context and developmental stage, moderate this relationship. Family environments can buffer these effects, with negative parental and peer alcohol social-

isation attenuating the influence of online alcohol content²⁰⁰. Future research priorities include expanding studies beyond WEIRD^c samples, clarifying temporal dynamics and examining how varied content types (positive depictions, advertising and prevention messages) interact with adolescent drinking behaviour.

Concerning substance abuse, evidence indicates that content promoting engagement with substance use or actively depicting their use is widely available on social media. This may influence attitudes, behaviours and risk perceptions concerning substance use, especially among children and adolescents²⁰¹. Similarly to alcohol, research suggests that social media content related to drugs is associated with higher chances of cannabis and multiple substance use²⁰².

EXPOSURE TO CRIME AND ILLEGAL CONTENT ONLINE

According to Europol, children and adolescents are exposed to a number of crimes, including grooming, child sexual abuse, radicalisation or recruitment for violent acts and terrorism online²⁰³. These risks are increased with minors' engagement with online spaces²⁰⁴, as well as exposure to harmful or abusive content, including access to pornography from a very young age²⁰⁵.

Evidence in the German context indicates that online child sexual solicitation and abuse is significantly more frequent among recent young generations. This may be due to increased exposure to digital environments, together with the proliferation of social media in recent decades. These findings highlight the need for urgent, targeted prevention to address online risks to children and adolescents online²⁰⁶.

CHILD SEXUAL ABUSE MATERIAL

Over the last decades, social media+ spaces have become central to the proliferation of child sexual abuse material, as well as its production, dissemination and consumption. In 2025, 63% of all child sexual abuse webpages found by the Internet Watch Foundation were hosted in EU Member States.

According to 2025 data from the United States' National Centre for Missing and Exploited Children (NC-MEC), online grooming is expanding at an alarming rate, with reports increasing by 158% over the past three years. Offenders systematically use social media, messaging applications, and gaming platforms to establish contact with minors and to engage in grooming activities. These online interactions often translate into offline exploitation, demonstrating a strong link between online grooming and the perpetration of related crimes offline.

Technological developments, including generative AI, are amplifying risks and accelerating the scale of possible abuse. The proliferation of AI has led to an exponential increase in AI-generated child sexual abuse material, with reports surging from 5,000 instances in 2023 to 1.3 million in 2025²⁰⁷.

Between 2024 and 2025 alone, AI-generated child sexual abuse videos increased by more than 26-fold. 65% was regarded as Category A material, the most severe form of abuse. This evidence highlights the threat social media+ environments and generative AI pose in enabling the rapid proliferation of child sexual abuse material.

The consumption of realistic synthetic material may reinforce existing sexual interests. According to a 2021 survey carried out by Protect Children Finland, 44% of 5,171 respondents said that viewing child sexual abuse material made them think about seeking contact with minors, with 37% reported having sought contact²⁰⁸.

^{c.} Western, Educated, Industrialized, Rich, and Democratic (WEIRD) sample demographic.

Girls may be particularly exposed to harm. In 2025, 97% of AI-generated child sexual abuse images identified by the Internet Watch Foundation depicted girls²⁰⁹. Adolescent girls between 12 and 18 may be particularly vulnerable.

Online sexual exploitation is also closely linked to trafficking. Digital services may facilitate the recruitment, control and monetisation of victims, including in large-scale operations involving live-streamed abuse. This form of exploitation is one of the fastest-growing globally, enabled by anonymity. Harm to victims is severe and long-lasting.

Victims report long-term psychological consequences, including anxiety, shame and persistent fear of being recognised²¹⁰. The continued circulation of material online prolongs victimisation indefinitely, meaning that harm does not cease once the initial abuse ends.

An internal study by the European Commission's Joint Research Centre (JRC) found that while social media platforms are not the primary hosts of child sexual abuse material, they can be used to disseminate it, often through links to external sites or encrypted channels.

Algorithmic systems integrated into social media platforms can amplify content related to child sexual abuse material, making it more discoverable and accessible to users, including perpetrators and minors.

Other content depicting minors present on social media platforms, while not necessarily child sexual abuse material, can be exploited by offenders and reinforce risks to children and adolescents. Risks for minors caused by exposure to child sexual abuse material include emotional and psychological harm, anxiety, depression and trauma.

For children and adolescents who have already experienced sexual abuse, online environments may contribute to the risk of revictimisation²¹¹. The continued availability and circulation of child sexual abuse material means that the abuse can be repeatedly re-experienced long after the initial offence has ended²¹². Unlike many forms of offline victimisation, digital material can be copied, redistributed and accessed indefinitely, creating an ongoing source of distress and uncertainty for victims who often remain aware that images or videos of their abuse continue to circulate.

Evidence further suggests that survivors of childhood sexual abuse may be particularly vulnerable to harmful online experiences²¹³. Childhood sexual abuse has been associated with increased engagement in high-risk online behaviours, greater exposure to sexual content online, higher rates of cyberbullying victimisation, and an elevated risk of internet-initiated revictimisation²¹⁴. These vulnerabilities may reflect the long-term impact of trauma on psychosocial development and sexual self-concept, rather than individual behaviour alone²¹⁵.

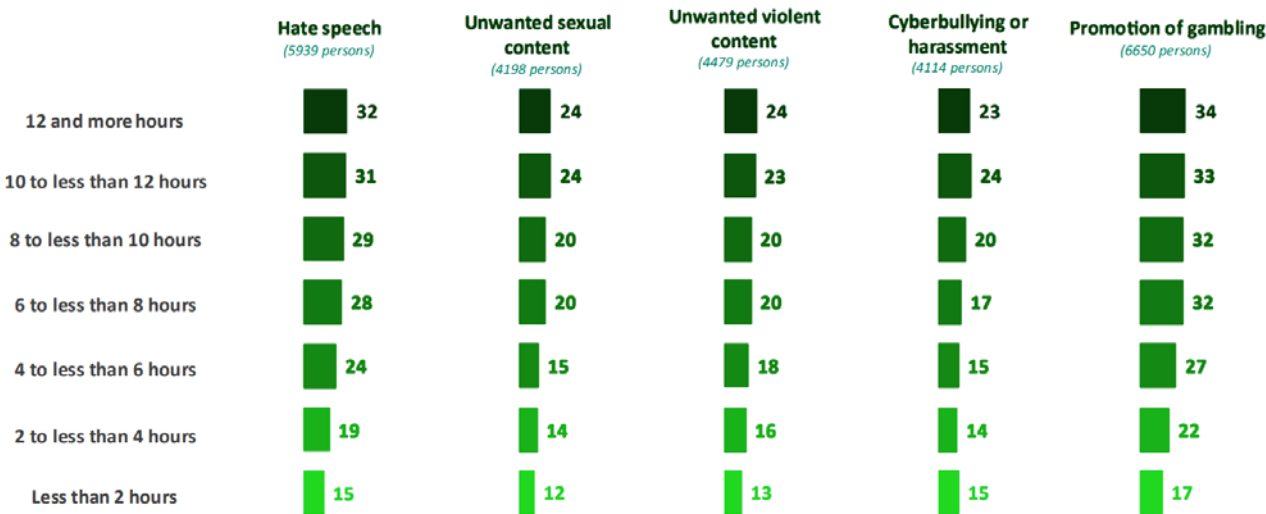
Repeated online exposure to sexualised or exploitative material may therefore reinforce trauma-related symptoms, interfere with recovery and increase the likelihood of further victimisation. At the same time, exposure to child sexual abuse material may contribute to the normalisation of exploitative sexual behaviours among minors, increasing the risk that vulnerable children become targets of further abuse or coercion. Preventing the dissemination of child sexual abuse material is not only essential to stop ongoing abuse, but also to reduce the risk of repeated victimisation and to support the long-term recovery of affected children and adolescents²¹⁶.

Minors who are exposed to this material or groomed on social media+ are at a higher risk of being exploited or abused themselves. Repeated exposure to child sexual abuse material can desensitise minors to its harmful effects, potentially leading to the normalisation of exploitative behaviours.

Children and adolescents who have previously experienced sexual abuse are at a heightened risk of on-line revictimisation. Evidence indicates that a history of child sexual abuse is associated with increased vulnerability to technology-assisted sexual solicitation and abuse, underscoring the need for targeted protective measures for this group²¹⁷.

Figure 3: Adolescents encounter an increasing amount of unwanted and illegal content the more time they spend on screens

Question: *In the past 3 months, have you seen or experienced any of the following when using social media?*^d



Source: European Commission (2026). *Impact of excessive screen time and social media on young people's mental health – June 2026 – Eurobarometer survey.*

RADICALISATION AND RECRUITMENT FOR VIOLENT

ACTS AND TERRORISM

Social media+ environments play a significant role in radicalising and recruiting minors to commit acts of terrorism and violent extremism. Social media, encrypted messaging services, and online communities are used to disseminate propaganda, to create networks and engage directly with minors.

The 2025 EU Terrorism Situation and Trend Report demonstrates that nearly one third of suspects arrested in the EU in 2024 for terrorism-related offences were minors or young adults²¹⁸. Of the 133 young suspects reported, 70 were under 18. Most young suspects were linked to jihadist terrorism, followed by right-wing terrorism, and violent extremism.

Recruitment can begin at a very young age, with documented cases involving children as young as 8 or 9 years old. Children and adolescents are particularly vulnerable to online recruitment strategies adopted by organised crime and terrorist groups, who often employ gaming environments and online fora to lure minors into these activities.

^d. Note: Figures represent the percentage (%) of respondents reporting risks by time spent on screens (during the weekend).

Evidence shows that minors convicted of terrorist offences in the EU may undergo a process of self-radicalisation online, with algorithm-driven content playing a key role in the reinforcement of radical ideas. Regular exposure to violent content online may lead to a dangerous normalisation and general desensitisation to human harm and suffering²¹⁹.

The ‘White Tiger’ case [see box below] illustrates how online platforms can enable criminal networks and individuals to lure minors into online abuse networks, facilitating exploitation, grooming and psychological abuse.

THE ‘WHITE TIGER’ CASE

The ‘White Tiger’ case focuses on a suspect arrested in Germany in the summer of 2025 and allegedly identified as a prominent figure within the online violent nihilist extremist group ‘764’. Acting under the pseudonym ‘White Tiger’, the suspect is charged with over 200 offences against more than 30 children and adolescents^e. The suspect was 16 and 19 years old, respectively, when he perpetrated the alleged offences.

Suspected offences include the incitement to suicide of a 13 year-old boy from the United States, broadcasted live online in 2022. Other cases include the grooming of 11 to 15-year-olds to self-harm online in front of viewers, and the production of child sexual abuse material. Victims have been identified across multiple countries, primarily Germany, the United States, the United Kingdom, and Canada. The suspect is accused of having deliberately scouted for vulnerable, isolated or emotionally distressed children and adolescents online, including individuals exploring their LGBTIQ+ identity.

Through rapid grooming techniques, the suspect allegedly established intense emotional dependencies, gradually cutting the victims off from their real-world support systems. Once isolated, the grooming transitioned into a malicious form of radicalisation to violent extremist ideologies and psychological torture. The trial against the suspect started in Germany in 2026. The prosecution faces difficulties due to the transnational and virtual dimensions of the case.

The 764 network utilises severe extortion, dox threats, and gaslighting to erode victims’ sense of agency. The perpetrators systematically weaponised mainstream digital services popular among minors. Teens were also coerced into executing increasingly dangerous commands, filming degrading acts, and adopting the group’s nihilistic ideology as a twisted form of validation.

A key characteristic is that victims are often blackmailed into becoming perpetrators themselves, forced by the network to target, groom and exploit other minors. This dynamic illustrates the overlap between child victimisation and child offending, where coerced minors are used to commit crimes against other children or to encourage them to self-harm. The ideological fluidity, mixing of online harms, and the gradual intensity of self-harm and violence, linked with private online spaces hinder efforts to detect and bring to justice online violent extremist networks.

- e. This trial is ongoing. The offences presented are alleged and do not in any way prejudge the outcome of the legal proceedings.

THE (MIS)USE OF MINORS' DATA

Children and adolescents face several risks when using social media⁺ concerning how their personal data is collected and used. A key concern is the profiling of minors. The behaviour of users on social media and other digital services is typically tracked for a variety of purposes by cookies and similar tracking technologies. The most privacy-intrusive of the purposes of such tracking is cross-site tracking for personalised advertisement. Many social media platforms collect personal data not only via on-device cookies, but also via the use of their servers, on a scale that may intrude minors' privacy. In certain instances, digital services providers and advertisers may collect data from multiple different sources^f.

Such practices allow providers to build a comprehensive picture of a minors' behaviour, preferences, interests, movements and online activities^g. They may also reveal private aspects of a child's or adolescent's lifestyle or beliefs, even if minors did not directly provide this information. Pervasive data gathering may reduce minors' control over their data and expose them to unforeseen risks, including pressure to make in-app purchases or to buy additional services.

While children can rely on the unconditional right to be forgotten under the GDPR²²⁰, this right must be invoked by the minor after the processing has already taken place. Naturally, this also requires children to be able to understand this right and how to invoke it.

Linked to this, minors face risks from their use of social media and digital services, which may integrate recommender systems and algorithms. These systems often rely on behavioural data and search activity to generate personalised content feeds and advertisements. They may also direct minors to harmful or inappropriate content designed to encourage prolonged engagement. These practices enhance children's and adolescents' exposure to risk and the possibility of developing compulsive or addictive behaviours.

In both instances, minors may not understand that their personal data is being collected, the scale of the collection, and what their data is being used for. Such practices make it more difficult to determine whether children's consent was 'freely given', a core tenet of what constitutes consent under the GDPR.

Another concern is the use of minors' geolocation data which can be recorded by common, everyday applications like mobility and weather apps, and is frequently traded by global data brokers. If a child's or adolescents' location can be tracked or identified, there is a risk that their personal data could be misused, with potential negative effects for their physical safety and well-being both online and offline. While the use of geolocation data is typically subject to consent^h, minors can consent unsupervised, for instance when setting up an app downloaded on their phone, without their consent being made valid by the verification of their age.

Finally, data breaches can have a range of adverse effects on minors, which can result in physical, material or non-material harm²²¹. This may include children's loss of control of their personal data, the limitation of their rights, discrimination, identity theft or fraud, financial loss, and the unauthorised reversal of pseudonymisation. It may also include other significant economic or social disadvantages.

f. See, for example, *Meta Platforms Inc v Bundeskartellamt* (C252/21).

g. *Meta Platforms Inc v Bundeskartellamt* (C252/21).

h. For geolocation data generated in the context of traditional telephony services (the place from which a mobile phone call was taken or SMS sent), this follows from Article 9 of the ePrivacy Directive. For geolocation data obtained through a different means (typically the GPS location function of the mobile device), this would be subject to the GDPR and could be based on different legal bases. However, considering the privacy-intrusive nature of geolocation data, the former Article 29 Data Protection Working Party and the EDPB regard consent to be necessary.

VIDEO GAMES

Video games not only offer children and adolescents entertainment, but social spaces where they can connect and communicate with others online. Some evidence suggests that video games can bring benefits in the form of prosocial behaviour²²², community building, and escapism²²³. It is currently estimated that 80% of minors (between 2 and 18) spend 30% of their entertainment time gaming²²⁴.

Video games take very different forms, presenting diverse risks to minors. Several of the most-played games offer platform-like features. Open communication using these services may expose minors to risks, including cyberbullying, grooming and radicalisation²²⁵, as well as access to harmful or age-inappropriate content. So-called 'intermediary video games', for instance, enable users to play and create their own content or games. User-generated content increases the risk of minors being exposed to age-inappropriate content.

Certain platforms also distribute games. Both video games and such platforms may deploy commercial practices, including loot boxes, pay-to-advance, in-app purchases and virtual currencies, that may be manipulative, cause unwanted spending, compulsive or addictive behaviours²²⁶. In 2018, gaming disorderⁱ was included in the 11th Revision of the International Classification of Diseases (ICD-11). It appears to be most prevalent among adolescents and young men between 12 and 20.

One survey indicated that 12% of adolescents were classified as being at risk of problematic gaming²²⁷. This evidence also suggests that boys between 11 and 15 face increased risk of problematic use compared to girls. Among adolescents, gaming disorder has been associated with elevated levels of externalising (such as antisocial behaviour and anger issues) and internalising (for instance, emotional distress and lower self-esteem). Adolescents suffering from gaming disorder may be at higher risk of academic underachievement, early school leaving, psychosocial and sleep-related issues.

In June 2026, the Pan-European system for the age classification of video games, PEGI, added new categories to its classification criteria to address online interaction risks in video games. Newly submitted games are now classified with broader criteria addressing both content and functionalities. This includes purchases of in-game content, paid random items, communication features and those incentivising continuous gameplay. Some of these features are now tied to specific age categories, which can be used to assess whether a video game needs a higher age rating.

According to a representative of the German 'Unterhaltungssoftware Selbstkontrolle' (USK), at least one of the new USK criteria has been applied to around 30% of all games that were submitted since the system was updated. Of these, approximately one in three has received a higher age rating as a result²²⁸.

- i. Gaming disorder is defined as a pattern of gaming behaviour characterised by 'impaired control over gaming, increasing priority given to gaming over other activities to the extent that gaming takes precedence over other interests and daily activities, and continuation or escalation of gaming despite the occurrence of negative consequences'. See: World Health Organization (2020). Addictive behaviours: Gaming disorder.

COMMON FEATURES OF SOCIAL MEDIA+ AND THE RISKS

Social media and other digital services differ widely, but share a set of common features. The OECD²²⁹ and researchers have been developing different classifications of the risks children and adolescents may be exposed to online. The 5-C classification aids providers of social media and other digital services, academia and policymakers to better understand and assess the risks to minors online²³⁰.

The 5-C classification contains five categories:

- // Conduct risks: risks for minors to participate, witness or be a victim of harmful conduct;
- // Contact risks: risks for minors of encountering or being targeted by malicious actors online;
- // Content risks: risks of encountering harmful content;
- // Contract risks: risks for minors to enter into a potentially harmful contract;
- // Cross-cutting risks (abbreviated by 'CC' in the table below): risks to minors' health, privacy and fair treatment (non-discrimination).

The European Centre for Algorithmic Transparency (ECAT)²³¹ has connected common features to risks from the 5-C classification in an Online Minor Protection Matrix, outlined in the table below. It is important to note that minors of different ages are exposed to different levels of risk by these features.²³²

COMMON ONLINE FEATURES AND ASSOCIATED 5-C RISKS

Features	Description	5-C Risks
Advertisement	Promotional content displayed to users, often to promote products or services.	Content, Conduct, Contract, CC-Health, CC-Privacy, CC-Discrimination
Age assurance / verification	Methods used to confirm the age of users to ensure they meet the platform's age requirements.	Content, CC-Health, CC-Privacy, CC-Discrimination
AI Chatbots	Automated systems that simulate conversation with users using artificial intelligence.	Content, CC-Health
Beauty filters	Tools that enhance or alter a user's appearance in photos or videos.	CC-Health
Comments / Opinions	Feedback or expressions of thought on content or posts.	Content, Conduct, Contract, CC-Health, CC-Privacy
Commercial practices	Strategies and activities used by social media+ to promote and sell products or services.	Conduct
Contact recommendations	Suggestions for users to connect with other users on social media+.	Contact, CC-Health, CC-Privacy
Content recommendations	Suggestions provided to users.	Content, CC-Health, CC-Privacy, CC-Discrimination
Default settings	Initial configurations of social media+ that are in place when a user first accesses it.	Content, CC-Privacy
Editorial content	Content created by professional writers or editors for an online platform.	Content
GenAI	Generative artificial intelligence that creates new content or data.	Conduct, Content, CC-Health, CC-Privacy
Geolocalisation	Use of data to determine the physical location of a user.	CC-Health, CC-Privacy
Loot boxes	Virtual items that contain random rewards, often purchased with real money.	Conduct, CC-Health
Marketplaces	Social media+ where users can buy and sell goods or services.	Content, Conduct, Contract, CC-Health
Notifications	Alerts or messages that inform users about activities or updates on the platform.	CC-Health
Online design interface	Layout and features of social media+.	CC-Health
Parental controls	Tools for guardians to monitor and manage minors' online activities.	CC-Health, CC-Privacy
Private messages	Individual communications between users that are not publicly visible.	Contact, Contract
Reporting and redress	Mechanisms for users to flag and rectify harmful issues on a platform.	Conduct, Content, CC-Privacy, CC-Discrimination
Terms and Conditions	-	Contract
User-generated content	Any form of content—such as text, videos, images, reviews, or comments—that is created and shared by users on social media+.	Conduct, Content, CC-Health, CC-Privacy

Source: MANOLIOS, S., *Online Minor Protection Matrix*, CHAUDRON, S., SALA, A. and GOMEZ, E. (editors), Publications Office of the European Union, Luxembourg, 2026, JRC147657.

Recommendations

Despite the challenges involved, policies promoting child safety online must be designed in a needs-oriented and developmentally appropriate way, which addresses children's and adolescents' complex and heterogeneous social and individual situations and backgrounds. In an increasingly digitalised world, whether or not minors are considered 'active users', they are often passively exposed to social media+ by primary caregivers during the very first days of life.

The challenge for policymakers is to reflect this complexity in targeted policies, while ensuring effective implementation and evaluation. Robust evidence on how risks and harms relate to different social media and other digital services is crucial to inform appropriate actions to protect and empower minors online. Specific features, functionalities or formats implemented on social media+ may be harmful to a different extent, depending on a child's or an adolescent's social and personal circumstances.

Minors belonging to racial, ethnic and religious minority groups, with migrant backgrounds, members of the LGBTIQ+ community, those with special educational needs and disabilities, or pre-existing mental health conditions may be particularly exposed to harm online. This exposure is magnified by digital services integrating harmful, manipulative or addictive content or designs. As these features evolve, so should research and evidence gathering.

For this research to materialise, one ingredient is key: reliable data, coming directly from the source – the providers themselves. Only by accessing relevant data can researchers, educators, and policymakers understand systemic risks, monitor emerging threats and design appropriate safeguards.

The EU has taken substantial steps to ensure research is facilitated via meaningful, proportionate and effective access to data from online platforms, notably under the Digital Services Act, which facilitates both access to public and non-public data to study systemic risks affecting minors online. Building on this existing framework, and on actions that providers should take [\[see also the recommendations in chapter 4\]](#), the following recommendations could be considered:

RECOMMENDATION 1

Build on evidence in understudied areas to strengthen evidence-based policymaking

Researchers should further build on evidence concerning the risks and opportunities related to children's and adolescents' use of social media+ in understudied areas. Key areas to strengthen include the heterogeneous impacts of minors' use of social media+ throughout development, minors' use of money online (including on online marketplaces), AI tools (including AI companions), and ethical social media+

“Recommendations on children's and adolescents' use of social media should be evidence-based and grounded in the best available scientific studies.”

— PROF. CHRISTOPH PIEH,
HEAD OF DEPARTMENT FOR
PSYCHOSOMATIC MEDICINE AND
PSYCHOTHERAPY, UNIVERSITY FOR
CONTINUING EDUCATION KREMS

design. Controlled user studies in specific social media and digital services are important to investigate the impact of certain or a group of design features. To clarify causal effects of certain features, randomised controlled trials (RCTs) should be founded. Providers have an important responsibility in facilitating such studies by giving access to independent researchers.

The potential positive effects of social media+ use for example in structured caregiver or educational settings, is another area that should be further explored. Social and individual factors influencing the impact of social media+ use on minors' development, and the interplay between these factors, should also be further examined. These insights are needed to inform and strengthen evidence-based policymaking promoting child safety and empowerment online.

RECOMMENDATION 2

Providers should actively involve independent academic expertise in the design of risk mitigation strategies and tools

Beyond compliance with applicable rules, social media and other digital services providers should actively involve independent experts and minors in the design of their risk mitigation strategies and tools, as well as when developing specific features and services for minors online. Expertise from a wide range of disciplines and using diverse methodologies should be represented to ensure robust and well-founded insights.

RECOMMENDATION 3

Make available long-term funding for European large-scale longitudinal research and continue supporting randomised controlled trials

Examples, such as the North American Adolescent Brain Cognitive Development (ABCD) Study, could inspire European large-scale longitudinal research related to child safety online. The availability of European large-scale longitudinal evidence (covering a ten-year period or longer) is important to support a developmental and neurobiological approach to child safety online. This would help to address gaps in largely correlative findings in the European context concerning the impact of social media+ use on minors' development, physical and mental health, and their exposure to harm online.

Randomised controlled trials (RCTs) are also key to strengthen the evidence base for policy. Research funding should explicitly support developmental and psychopathology approaches investigating minors' susceptibility to online risks, influenced by social and individual factors across childhood and adolescence.

RECOMMENDATION 4

Invest in secure, shared European research infrastructure to allow safe access to minors' data

The European Union and its Member States should invest in secure, shared European research infrastructure based on the FAIR Guiding Principles [\[see below\]](#) enabling researchers and policymakers to also access sensitive, non-public data on the protection of minors online, in full respect of applicable privacy and data protection laws.

Shared infrastructure should integrate the FAIR (Findability, Accessibility, Interoperability, and Reusability) Guiding Principles^j for scientific data management and stewardship to ensure the robustness, reliability and reusability of data and research. Collaborate with the research community to ensure continuous improvement and availability of data, and the use of methodological innovations.

Social media and other digital services providers should be encouraged to contribute to the development of shared research infrastructure to strengthen the evidence base for measures protecting minors online.

RECOMMENDATION 5

Strengthen enforcement of rules on researchers' access to and scrutiny of data

Article 40 of the Digital Services Act (DSA) delegated act of July 2025 has opened, in principle, a new pathway for vetted researchers to access online platform data. This data can be used to conduct research contributing to the detection, identification and understanding of systemic risks, and to the assessment of risk mitigation measures promoting child safety online.

Whether this pathway delivers on its promise depends on social media and other digital services providers' compliance and regulators' effective enforcement. It also relies on the breadth of services covered, and the quality and continuity of the data provided. The Commission should evaluate the operational performance of Article 40 data access and scrutiny requirements after initial researcher experience under the delegated act. This is key to ensure online platforms follow up on requests for access to data for compliance, risk assessment and research purposes.

Data access obligations are not only a key element of the transparency toolbox of the DSA, they are also a part of social media and other digital services providers' broader risk mitigation responsibilities. Smaller platforms should also be encouraged to allow researchers access to data, considering the risks these platforms pose to minors, and the role of independent scrutiny in addressing these risks. The use of the FAIR Guiding Principles for scientific data management and stewardship should be the standard in the implementation of Article 40.

j. The FAIR Guiding Principles for scientific data management and stewardship were introduced in 2016 in a publication in the journal *Scientific Data*. The principles intend to improve the infrastructure supporting the reuse of scholarly data by enhancing the ability of machines and individuals to find and use data. See: Wilkinson, M.D., et al. (2016). [The FAIR Guiding Principles for scientific data management and stewardship](#). *Scientific Data*, 3.

03

Protecting minors in a rapidly changing social media+ environment

The previous chapter explored the diverse risks children and adolescents are exposed to through their use of social media and other digital services for their mental and physical health and well-being, and how these risks intersect with social and individual factors to enhance minors' exposure to harm.

This chapter examines how existing legislation and tools currently available to the EU and its Member States address these risks and strengthen child safety online.

This analysis builds on pillars three and four of the Six Guiding Principles presented by the Co-Chairs to steer efforts to enhance child safety online: child protection, and social media and other digital services providers' accountability and consumer rights. This chapter begins by examining the main legislative instruments and tools available to the EU and Member States, highlighting examples of their successful enforcement to date.

The EU's main legislative instruments in the field of child safety online were one of the key starting points for the Co-Chairs' reflection on how to strengthen the protection of minors online. Grasping the content and scope of the most powerful tools at the EU level and identifying gaps in legislation and/or enforcement were also among the main topics discussed at the Special Panel meetings.

It is widely recognised that the EU has set up a powerful legislative framework – but technologies develop fast, business models adapt, new features evolve, and regulators have to adapt accordingly, be it in enforcing existing rules or filling gaps. Protecting minors in a rapidly changing social media+ environment needs constant evaluation and attention to keep pace.

In the section 'Unfinished business', several areas are identified where existing instruments and tools need to be strengthened. The chapter concludes by presenting a series of recommendations on how to reinforce enforcement of these existing instruments and how to better address harmful practices, and features and functionalities deployed by social media and other digital services to bolster child protection online.

The need for age-appropriate child protection online

As explored in chapter 1, an effective approach to child safety online must be based on an understanding that children's and adolescents' development occur in stages. At different moments along their path to adulthood, minors are particularly exposed to specific risks. Children's and adolescents' evolving capacities determine, in part, the extent to which they are equipped to address these risks.

This analysis takes as a starting point the respective international and EU frameworks on the rights of the child^a. Measures promoting child safety online must be based on the recognition of children's rights. Caregivers' and educators' changing roles in supervising minors' use of social media and other digital services must also be better reflected in child protection instruments.

The growing political momentum to restrict children's and adolescents' access to and use of potentially harmful social media and other digital services, is a step in the right direction towards shaping a more developmentally sensitive approach to child safety online. Early results from countries that have introduced blanket age bans to access social media (for instance, Australia) show that most minors find a way to circumvent these policies²³³.

At the same time, some minors have withdrawn from risky social media+ and now have more time for offline activities (including sport and face-to-face social interactions). This demonstrates that progressive change surrounding the norms of social media and other digital services use by minors is possible and must be recognised.

However, several challenges remain to successfully deploy age restrictions to strengthen the protection of minors online and to allow them to seize the opportunities offered by the digital world. These challenges are explored later in this chapter as part of the section on 'Unfinished business'.

Ensure safe design features online

There is a growing body of evidence demonstrating the potentially harmful effects of minors' use of social media and other digital services, as explored in chapter 2. The risks children and adolescents face in social media+ environments are not incidental. In many cases, they are the result of deliberate choices of providers of social media and other digital services that are designed to maximise users' engagement, including for minors who can easily access them. The continuous evolution of social media+ to capture and retain users' engagement has become part of many providers' core business models.

There are increasing calls for regulators to apply a risk-based approach and to address inherent risks, including addictive or compulsive use, that certain features and functionalities pose to children and adolescents to ensure social media and other digital services are 'safe by design'. Despite many examples of successful enforcement to tackle such issues, regulators often find themselves 'on the back foot'.

^a. Notably, the United Nations Convention on the Rights of the Child and the general comments of the Committee on the Rights of the Child, the Charter of Fundamental Rights of the European Union, and the EU Strategy on the Rights of the Child.

Currently, regulators typically have to prove that specific features and functionalities are harmful after they have been deployed on the Single Market and potentially used by millions of children and adolescents. Social media and other digital services providers should have more responsibility to ensure and demonstrate that features in their services are not harmful before making them available to minors.

It could therefore become the rule that social media and other digital services providers launching, operating or updating services that may pose risks to children and adolescents must demonstrate that their services or new functionalities are safe for minors to use before market deployment. The protection of children and adolescents should be an integral part of the architecture of social media+ and should be a key standard at the very beginning of its development and design.

“No toy, medicine, or vehicle reaches children without independent pre-market assessment; digital products are the conspicuous exception, scrutinised only after harm is already visible.”

— ALEX COONEY,
CEO & CO-FOUNDER, CYBERSAFEKIDS

Strengthen enforcement and evaluation

Last but not least, enforcement at the EU and national levels of existing legislation must be strengthened. The EU has one of the most cutting-edge legislative toolboxes in the world which it can use to ensure minors can navigate the online world safely and in confidence. However, the effectiveness of these rules is determined by their enforcement. Gaps in existing legislation must be filled and cooperation between regulators at the EU and national levels reinforced.

Additional resources may be needed to enhance enforcement capacity. The evaluation of existing instruments is essential to ensure legislation and enforcement deliver results. Civil society and researchers have important contributions to make in this regard. Their role should be strengthened to ensure legislation is designed and deployed effectively to achieve the goal of allowing children and adolescents to grow up safely online.

Existing EU legislation

The following section examines existing EU legislation and tools available to the EU and Member States to protect minors^b online. This analysis focuses on EU legislation that the Co-Chairs of the Special Panel consider needs further strengthening or enhanced enforcement. Of course, there are many important instruments that are not explored in detail in this chapter, but form an essential part of existing EU policy.

Notably, these include the 2008 Framework Decision on combating racism and xenophobia, the Directive on combating violence against women and domestic violence, the Directive on procedural safeguards

b. Note: in the following sections of this chapter, the terms ‘children’ and ‘minors’ appear as they are used in specific legislative instruments.

for children who are suspected or accused in criminal proceedings, the Victims' Rights Directive, and the Commission Recommendation on integrated child protection systems.

Preventive policies, such as digital education and literacy (including AI literacy), well-being education, and support for minors, caregivers and educators, are examined in chapter 4 which focuses on children's and adolescents' empowerment online.

DIGITAL SERVICES ACT (DSA) AND THE GUIDELINES

ON THE PROTECTION OF MINORS

The Digital Services Act (DSA) lays down fully harmonised rules for the provision of intermediary services to create a safe, predictable and trusted online environment that respects users' rights, in particular for minors. The DSA was adopted in 2022 and became fully applicable to Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs)^c on 25 August 2023. The DSA became applicable to all other services in its scope on 17 February 2024.

Amidst the rise of digital services, which have become an important part of our daily lives in the digital era, the DSA develops the fundamental principles enshrined in the e-Commerce Directive since 2000 to address new risks and challenges for minors today online and to promote responsible behaviour by digital services providers.

Ultimately, the DSA seeks to create an online environment where everyone can enjoy their fundamental rights. This includes by imposing obligations on online platforms to ensure a high level of privacy, safety and security for minors online²³⁴.

Scope

Specifically, the DSA regulates providers of intermediary services. These are digital services that facilitate the hosting of third-party content and interactions online. The definition of intermediary services spans providers merely transmitting information (for example, internet service providers), services 'caching' (transmitting information with temporary storage), including network operators; and hosting data at the request of users (for instance, cloud providers and online platforms).

As examples, intermediary services include all online platforms, such as online marketplaces, social media, online games or video games where users can play and create their own content (unless these features are just minor 'add-ons' to an existing video game), app stores, video-sharing and streaming sites, and online platforms where users can view, post and share content.

The DSA does not apply to private or direct (interpersonal) messaging services or features, or to digital services without an intermediary function^d. To ensure proportionality, some of the obligations the DSA imposes on online platforms do not apply to providers of online platforms which qualify as micro or small enterprises due to their revenue and number of staff. This exception does not apply if these services are designated as VLOPs in view of the number of their users.

- c. Under the DSA, VLOPs and VLOSEs are defined as services with over 45 million monthly active users in the EU.
- d. An 'intermediary function' refers to services that facilitate third-party content between different recipients of that service. Examples of non-intermediary services would include online retailers, many video games without third party interactions or content creation, or individual websites or apps.

Enforcement

The DSA empowers the Commission to open formal investigations against the largest platforms based on a wide range of risks to minors, while maintaining flexibility to react to new risks and technological developments. Investigations must at all times comply with due process and all other necessary legal safeguards for companies.

Given the DSA's fully harmonised rules, which is a directly applicable Regulation, EU Member States cannot adopt or maintain national legislation duplicating the DSA or imposing obligations on intermediary service providers. This includes imposing age verification obligations on online platforms.

This would affect the direct and uniform application of the rules across the Single Market. National law, in compliance with Union law, can however prescribe a minimum age to access certain products or services, as also indicated in the Commission guidelines on the protection of minors.

The DSA's enforcement is based on a system of shared supervisory and enforcement powers between the national and EU levels. For VLOPs and VLOSEs (see below), the Commission has exclusive powers to supervise these providers.

VLOPs and VLOSEs

Under the DSA, additional obligations apply to Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs)^e given their extensive reach and influence. These obligations address concerns about the widespread risks these services have the potential to cause, which is matched by the highest standard of due diligence.

Under the DSA²³⁵, VLOPs and VLOSEs must proactively identify, assess and mitigate real and foreseeable systemic risks stemming from the provision of their services, including risks affecting minors. For platforms with less than 45 million monthly users, national authorities in the EU Member State where the company has its establishment are responsible for enforcing the DSA.

VLOPs and VLOSEs must put in place reasonable, proportionate and effective measures to mitigate identified risks. This may include adapting the design, features and functioning of their services, as well as adapting algorithmic systems deployed as part of their services. VLOPs and VLOSEs must provide at least one option for each of their recommender systems to users that is not based on profiling.

Given the need to ensure verification by independent experts, providers of VLOPs and VLOSEs are accountable through independent auditing for their compliance with the obligations under the DSA.

e. For the full list of designated VLOPs and VLOSEs, see: European Commission (2026). [Supervision of the designated very large online platforms and search engines under DSA](#).

DSA guidelines on the protection of minors

The DSA guidelines on the protection of minors set the enforcement benchmark to ensure all online platforms accessible to minors have a high-level of privacy, safety and security for minors using their services.

The guidelines' main recommended measures include:

- // Set minors' accounts to the highest level of privacy, safety and security by default, such as geolocation and recommendations of other accounts.
- // Set up age verification where certain products or services pose a high risk to minors (for example, access to pornographic content) and where those risks cannot be mitigated by less restrictive measures. Clearly define what the platform considers as content and behaviour that is harmful for minors. This includes any content and behaviour that is illegal under EU or national law. Communicate information concerning these standards and expectations. Establish moderation policies and procedures that set out how content and behaviour are detected and moderated to limit minors' exposure to it.
- // Prevent unknown accounts from contacting minors and hide their personal information, data and social media content from accounts they are not connected with. As an example, two designated VLOPs have automatically set the profiles of users under the age of 16 to private. This means that the videos they upload can only be viewed by the people they approve.
- // Prohibit accounts from downloading or taking screenshots of content posted by minors to prevent sexual extortion.
- // Modify recommender systems to lower the risk of minors encountering harmful content or getting stuck in so-called 'rabbit hole' effects, in which minors are exposed to prolonged chains of content related to eating disorders, self-harm or suicide.
- // Put safeguards around AI chatbots integrated into online platforms. Warn minors that interactions with an AI feature are different from human interactions and that information provided by such features may be factually inaccurate or misleading.
- // Introduce measures to improve moderation tools. Ensure that user reporting, feedback and complaint mechanisms are effective, visible, child-friendly and easily accessible. Ensure such mechanisms allow reporting and feedback on all relevant elements of minors' experience on the platform.

"Make the Article 28 Guidelines of the Digital Services Act mandatory for digital providers. This would be effective, legitimate, consistent with existing law and regulation, and most importantly, a crucial means of respecting children's rights in the digital environment."

— SONIA LIVINGSTONE,
PROFESSOR AT LONDON SCHOOL
OF ECONOMICS AND POLITICAL
SCIENCE, AND MEMBER OF THE EU
KIDS ONLINE NETWORK

- // Set minimum requirements for parental control tools. These tools should be age-appropriate, easy to use, access and activate. They should also be interoperable, effective and not disproportionately restrict minors' rights to privacy or access to services.
- // Introduce user support tools. This includes directly visible warning messages, links to relevant support lines or other sources when minors search for, upload, generate, share and receive content that is potentially illegal. Options could also be deployed to retain control of minors' experience by restricting interactions and contacts.
- // Ensure minors are protected against economically exploitative practices. Minors must not be exposed to practices and techniques that can cause excessive or unwanted spending or addictive behaviours (for example, paid 'loot boxes').
- // Establish governance practices, including internal policies, processes, roles and responsibilities to foster a culture of safety for minors on their service.
- // Ensure that all information, warnings and any other communication are child-friendly, age-appropriate, easy to understand and accessible for all minors, as well as presented clearly and at the relevant point of use. More generally, under the DSA all users including minors are protected by minimum requirements (for instance, online platforms must make their terms and conditions understandable in the local EU language, so that users, including minors, are aware of the terms and conditions they are accepting).

A risk-based approach

The DSA guidelines adopt a risk-based approach, as different online platforms may pose different types or levels of risks for minors. The guidelines recognise that these risks may vary depending on the size, reach and type of platform, its nature, intended or current use, features and user base, its impact on children's rights, and other rights and freedoms. Platforms should consider these factors when applying the guidelines.

In line with this risk-based approach, the guidelines set out how providers should meet obligations to provide a high level of privacy, safety and security for minors in a proportionate and appropriate manner. Providers should consider the impact of the protective measures they take on children's rights and other rights and freedoms, grounding such measures on the highest available standards, the perspective and rights of children. In this context, the precautionary principle should be applied when there is indication that a practice, feature or design choice poses risks to children, until there is evidence that they are not harmful.

Specific prohibitions under the DSA

Concerning advertising, the DSA prohibits providers of online platforms from presenting advertisements based on profiling using the personal data of minors when they are aware with reasonable certainty that the recipient of the service is a minor.

The DSA also prohibits 'dark patterns'. This refers to the way online interfaces are designed to persuade or manipulate users into making certain choices against their interests. The prohibition of dark patterns applies in situations not already covered by consumer law (the Unfair Commercial Practices Directive (UCPD)) and data protection rules (the General Data Protection Regulation (GDPR)).

Trusted flaggers

The DSA also facilitates the reporting of illegal content (such as illegal hate speech and child sexual abuse material) and goods by users by mandating user-friendly flagging systems, including for minors. Civil society organisations, which are experts in detecting certain types of illegal content online, can be granted the status of ‘trusted flagger’.

Trusted flaggers’ notices of illegal content to platforms are treated with priority. Currently, more than 70 organisations have been designated as trusted flaggers by Digital Services Coordinators, representing areas of expertise from the protection of minors online, scams and fraud, to the fight against counterfeited products.

GENERAL DATA PROTECTION REGULATION (GDPR)

The General Data Protection Regulation (GDPR) takes a risk-based approach to the processing of personal data. The greater the risk that processing personal data poses to the rights and freedoms of individuals, the more stringent the obligations imposed on data controllers and the stronger the safeguards that must be put in place.

The GDPR specifically provides that children merit specific protection. Where an online service is accessed by children, there is a requirement to ensure that specific data protection measures are in place to ensure an appropriate level of protection against the risks posed by their use of the service. The Regulation recognises that children may not be fully aware of the risks and consequences of how their personal data will be used.

Relevant data protection principles

Organisations processing data are required to adhere to data protection principles, which are very relevant for protecting children online. For example, the data minimisation principle requires organisations to minimise the amount of children’s data collected and its subsequent use.

The principle of purpose limitation requires that when children’s data is collected for one purpose it should not be used by the organisation for any other purpose. The integrity and confidentiality principle requires that the organisation should take appropriate security measures to protect the child’s data from unlawful or unauthorised use.

Another important measure is the obligation for organisations that collect and use personal data is to comply with the data protection by design and default obligation²³⁶. This requires data protection measures to be built into the service from their design and that the highest privacy settings are used by default.

These requirements also demand that the organisation takes appropriate technical and organisational measures to protect minors. Compliance with this principle may require different measures, depending on the service offered and the risk to the data subject. Measures could include:

- // ensuring children’s personal data is not systematically shared with third parties;
- // ensuring children’s identity or contact information is not made available to others without parental consent;

- // turning off geolocation by default;
- // avoiding ‘nudging’ techniques that encourage or incentivise children to provide unnecessary information.

The GDPR also sets down specific transparency requirements for children. It requires that, where children use a product or service that processes their personal data (for example, if they have an account with a particular service), it must provide easily accessible explanations in clear and plain language of how the child’s personal data will be used.

This is particularly important as some children are not aware of what is meant by their personal data (for example, photographs and video) and that their data may be used for purposes, such as tailoring targeted advertisements and in-app experiences.

Legal basis

A core safety feature of the GDPR is that the organisation processing personal data (the data controller) must have a legal basis to do so. It must rely on one of the six legal bases established under the GDPR²³⁷. There is no hierarchy when it comes to the six legal bases provided. Data controllers should choose the most appropriate ground, taking into account the requirements of each of the different legal bases.

One of these legal bases is consent. Consent must be freely given, specific, informed, and unambiguous, expressed through a clear affirmative action, and individuals must be able to withdraw it as easily as they gave it²³⁸. Consent cannot be freely given if children have no real choice or feel compelled to consent. For consent to be informed, the controller must explain in clear and plain language accessible for children how it intends to process the data it collects²³⁹.

When consent is relied upon as the legal basis by an ‘Information Society Service’^f (such as social media platforms and video games), children can provide their consent to process their personal data starting at 16 years of age.

The GDPR provides the option for Member States to lower this age anywhere between 13 and 16. Where the child is below 16, the processing is lawful if consent is given or authorised by the holder of parental responsibility.

Member States have established different age ranges when consent is relied upon by Information Society Services. As of figures available at the end of 2025, 7 Member States have set 13 as the minimum age for consent, 6 Member States at 14, 5 Member States at 15, and 9 Member States at 16.

In accordance with the principle of accountability, a data controller needs to be able to demonstrate that they have complied with the GDPR. This includes by ensuring that the consent they have obtained is valid. Nevertheless, in practice, it can be difficult for a controller to ensure that the consent obtained by the holder of parental responsibility, where applicable, is valid. It may be difficult to validate that the individual providing consent for the child has the legal authority to do so.

f. Most online services are considered an Information Society Service. This includes apps, search engines, social media platforms, online messaging or internet-based voice telephony services, online marketplaces, content streaming services (for example, video, music or gaming services), news or educational websites, and any websites offering other goods or services to users over the internet. See: Article 4(25) GDPR.

Furthermore, in accordance with the principle of data minimisation, a controller should only process the data necessary for this purpose and should avoid processing sensitive personal data (such as documents indicating sensitive care arrangements) to adequately demonstrate valid consent.

However, the requirement to obtain the consent of the holder of parental responsibility does not apply when data are processed under another legal basis, such as contract or legitimate interest (see below). This means that when a social media company relies on one of these grounds to process children's data (for example, to set up their account to access the service and their interactions on the service), the additional safeguards that come with processing children's data based on consent do not apply.

When an organisation processes personal data based on a contract, it is for each Member State to fix the age when a child can enter a contract.

Another ground that online services rely on is legitimate interest. This refers to the processing of a child's personal data for the purposes of the legitimate interests of the controller or of a third party, except where those interests are overridden by the interests or fundamental rights and freedoms of the individual. Legitimate interest is not a 'default' legal ground for processing.

When controllers rely on legitimate interest to process children's personal data under the GDPR, in accordance with the accountability principle, they must ensure that they meet all the requirements of Article 6(1)(f) of the GDPR before carrying out the processing^g. One of these requirements is that the controller's legitimate interests must not be overridden by the child's interests or fundamental rights and freedoms²⁴⁰.

The CJEU has noted that, when a controller is carrying out such an assessment, it is necessary to pay particular attention to the situation where the data subject is a child. It noted, in accordance with recital 38 of the GDPR, children merit special protection. In addition, the CJEU has stated that such specific protection should apply to the processing of children's personal data for marketing purposes or creating personality or user profiles, or offering services aimed directly at children²⁴¹.

Controllers should also consider the extent and intensity of any interference with the child's rights and freedoms. They should be able to demonstrate that the children's best interests were taken into account as a primary consideration and that appropriate safeguards have been implemented²⁴². The best interests of the child should be a primary consideration when balancing any competing interests.

Controllers should also consider a child's reasonable expectations as to how their personal data will be used. The expectations of the child may also vary depending on the age of the child²⁴³. Depending on the complexity of the processing, a child's limited ability to understand data processing increases the risk of unexpected or disproportionate consequences of the processing.

It is noted that the European Data Protection Board (EDPB) considers that certain types of data processing operations, such as extensive profiling and targeted advertising activities²⁴⁴, subject to certain limited exceptions, will generally not align with the obligation to ensure the specific protection of children²⁴⁵.

Where a controller's legitimate interests conflict with a child's interests or fundamental rights and freedoms, the child's interests and rights should generally take precedence. Where this is not possible, a controller should rely on another legal basis to process the data or cease processing the data.

g. As confirmed by the CJEU, Article 6(1)(f) GDPR imposes three cumulative conditions, for the processing to be lawful: "first, the pursuit of a legitimate interest by the data controller or by a third party; second, the need to process personal data for the purposes of the legitimate interests pursued; and third, that the interests or fundamental freedoms and rights of [the data subject] do not take precedence". See: Case C-252/21, *Meta v. Bundeskartellamt* (ECLI:EU:C:2023:537), paragraph 106.

Other relevant provisions

The GDPR also provides increased protection for children regarding the right to erasure, taking into account that the child may not have been fully aware of the risks involved in the processing and later wants to delete this data²⁴⁶. It also provides that children should not be subject to profiling or automated decision-making²⁴⁷, and provides specific protections for children when marketing to them²⁴⁸.

The European Data Protection Board (EDPB) has held that “organisations should, in general, avoid profiling children for marketing purposes [...] and that such profiling should be permitted in very limited circumstances such as where it is necessary to protect the welfare/well-being of the child”²⁴⁹.

The GDPR also sets down the circumstances under which a Data Protection Impact Assessment (DPIA) is required. This requires organisations to assess the risks associated with the proposed processing of users’ personal data, and where necessary, to reduce the risk posed to users including children. The risk assessments should consider the varying ages and developmental needs of child users.

Risk assessments for children should also consider risks arising from the processing of children’s personal data to their general well-being. This includes any physical, mental or financial harm they may face as a result of the processing. The principle of the best interests of the child must be one of the main primary risk evaluation tools when carrying out a DPIA concerning the processing of children’s personal data.

Where the risk is still high after the proposed measures are put in place, the organisation is required to consult their Data Protection Authority (DPA). The DPA is required to provide written advice, and can also utilise any of its powers, including issuing a ban on processing where the risks are too high and cannot be adequately mitigated²⁵⁰.

ARTIFICIAL INTELLIGENCE ACT (AI ACT)

In addition to the DSA, the Artificial Intelligence Act (AI Act) lays down a comprehensive legal framework for the regulation of artificial intelligence (AI) in the EU. The AI Act has an important role in strengthening the protection of children’s rights by imposing safeguards to protect health, safety and fundamental rights when developing and deploying AI. The AI Act follows a risk-based approach and introduces rules for AI systems based on the possible level of risk they can pose.

Several AI use-cases with significant impact on children’s rights are classified as high-risk under the AI Act, such as when used in the domain of education and vocational training. High-risk AI systems must meet certain requirements to ensure they are safe and trustworthy, such as risk management, transparency and human oversight. In particular, the risk management system of a high-risk AI system needs to consider if there is a likelihood of adverse impact on persons under the age of 18.

When assessing the impact on fundamental rights of the specific use of a high-risk AI system^h, certain deployers of such systems need to consider the categories of people and groups which are likely to be affected using the system, which may include children. The European Commission has published for public consultation draft Guidelines on the classification of high-risk AI systems which include examples of which practices fall in or outside the scope of the AI Act²⁵¹.

h. The obligations for high-risk AI systems, as agreed in the Omnibus on AI, will start to apply in December 2027 (for stand-alone AI systems, such as certain AI systems in education) and August 2028 (for AI systems embedded in regulated products, for example toys).

Moreover, due to the evolving nature of AI systems, co-legislators have quickly agreed on the Digital Omnibus on AI to further strengthen rules that also contribute to better protection of minors. In particular, the new rules prohibit AI systems that generate non-consensual, sexually explicit and intimate content or child sexual abuse material, such as AI ‘nudification’ apps. The obligations for high-risk AI systems, as agreed in the Omnibus on AI, will start to apply in December 2027 (for stand-alone AI systems, such as certain AI systems in education) and August 2028 (for AI systems embedded in regulated products, such as toys).

Prohibited practices

The AI Act prohibits AI practices that manipulate, deceive or exploit the vulnerabilities of children. These prohibitions aim to prevent AI systems from manipulating minors or exploiting cognitive and other limitations that children may have in taking decisions that they would not have otherwise taken, and to protect them from harmful undue influence, manipulation and exploitation.

These prohibitions became applicable on 2 February 2025. The Commission has published guidelines on prohibited AI practices, which include examples of which practices fall in or outside the scope of the AI Act²⁵².

An example of a prohibited AI practice is an AI-enabled application that encourages minors to complete increasingly risky challenges, such as climbing furniture, exploring high shelves, or handling sharp objects, in exchange for digital rewards and virtual praise. Such systems exploit children’s vulnerabilities by abusing their natural curiosity and desire for rewards, and risk causing them significant harm.

Another example of a prohibited AI practice is games designed to be highly addictive by exploiting vulnerabilities inherent to children and adolescents (including a lack of self-control). Such games use AI to analyse children’s individual behaviour and preferences, based on which it creates personalised and unpredictable rewards through addictive reinforcement schedules and dopamine-like loops. This encourages excessive play and compulsive use.

These games are designed to be (or have the effect of being) highly addictive, exploiting the vulnerabilities inherent to children. This includes their limited ability to understand long-term consequences, their susceptibility to pressure, a lack of self-control, and inclination towards instant gratification.

General-purpose AI models

For the most performant general-purpose AI (GPAI) models with systemic risk, the AI Act imposes specific risk-assessment and mitigation obligations. To comply with these rules, most leading providers of GPAI models have signed the GPAI Code of Practice²⁵³.

GPAI providers must assess and mitigate concrete risk scenarios. This may include the dissemination of illegal, false or discriminatory content risks from illegal, violent, hateful, radicalising, or false content, and report the results of this risk management process to the European Commission before market placement.

Part of the mitigation measures providers of GPAI models need to take are monitoring and filtering the model’s input and/or inputs. This includes the prevention of generating harmful content. The obligations for general-purpose AI models became applicable on 2 August 2025.

Transparency obligations

To help avoid fraud, impersonation and deception, the AI Act imposes transparency obligations for providers and deployers of certain AI systems²⁵⁴. Under the AI Act, providers need to ensure that AI systems that are intended to interact directly with people (such as chatbots) are designed and developed in a way that people concerned are informed that they are interacting with an AI system, unless this is obvious. This obligation applies in any case for chatbots interacting with children.

Disclosure does not fully address the risks of emotional dependency. However, the interactive and often engaging nature of these systems makes it essential that users are explicitly made aware that they are engaging with an AI system, programmed to enhance their engagement, rather than a person.

Generative AI systems

An obligation on providers and deployers of generative AI systems is to mark and enable detection when content, such as images, audio or video, has been artificially generated or manipulated, and to label deepfakes and certain AI-generated publications on public matters.

Deployers of an emotion recognition system or a biometric categorisation system must inform people exposed to the operation of the system. The European Commission is facilitating compliance with these obligations through, among others, the publication of a Code of Practice on marking and labelling of AI-generated content²⁵⁵, and guidelines that are currently in preparation after being published for public consultation²⁵⁶. Obligations regarding the transparency requirements will apply as of 2 August 2026.

AI companions

AI companions are gaining increasing popularity among children, and certain risks associated with their use have been identified. Under the Act, the classification of AI companions and similar chatbots depends primarily on their intended purpose, functionality and context of use.

Depending on these factors, an AI companion may constitute a prohibited practice (for example, in cases involving the exploitation of children's vulnerabilities in significantly harmful ways). They may also qualify as a high-risk AI system (for instance, where it incorporates emotion recognition functionalities or in certain use cases in the context of education). Finally, they may be subject to transparency obligations requiring that users be informed they are not interacting with a person.

CONSUMER PROTECTION INSTRUMENTS

When addressing the harms children face in the digital environment, it is important to note the criminal liability and civil and product liability approaches.

Criminal liability could address the prohibition and punishment of specific harmful conduct, such as the distribution of child sexual abuse material or online grooming and relies on State prosecution and penal sanctions. While indispensable for the most serious offences, the prosecution of criminal offences is primarily reactive. It normally happens after harm has occurred, identifies and targets individual wrongdoers, rather than the systemic conditions that enable harm. However, the criminalisation of certain behaviours also contain important preventive and anticipatory elements.

A civil and product liability approach, on the other hand, could provide preventive and compensatory measures between different private parties. It is concerned with the allocation of rights, duties and responsibilities among private parties, including the companies that design and operate social media and other digital services, and with providing remedies where those duties are breached.

Consumer protection legislation plays a key role in civil and product liability cases. Importantly, this perspective allows regulators and private litigants to challenge the design choices by online service providers. It is this product liability perspective that has driven the most consequential recent legal developments in the United States.

In the United States, one of the recent cases on addictive designs on platforms is grounded in consumer law. A New Mexico jury ruled in March 2026 that Meta, as an operator of its online platforms, wilfully violated consumer protection laws, ordering the company to pay USD 375 million.

“Platforms should grow with the child. [...] Any recommender system serving a minor must be optimised for that child’s well-being, not for engagement.”

— GABRIELE BATTIMELLI,
BIK+ AMBASSADOR FROM ITALY

The case was brought by the State Attorney General under unfair practices legislation, targeting platform design and safety practices, including recommendation systems that exposed minors to predators. The jury found the company had misled consumers about the safety of its services, while internal documents demonstrated awareness of harm.

In parallel, in Los Angeles, the first ‘social media addiction’ bellwether trial resulted in a jury finding against Meta and YouTube on claims, including negligent design and failure to warn. The case is based in private tort law. The court explicitly identified features, such as infinite scroll, algorithmic

feeds, autoplay and engagement-maximisation mechanisms, as contributing to harm suffered by a minor. The ruling recognises that addictive design features may constitute actionable product defects, particularly where companies are aware of risks and fail to mitigate them.

In the EU, EU consumer protection law applies to children as a category of vulnerable consumers through several instruments. It acts as a horizontal ‘safety net’ applying to all traders, goods or services directed at consumers, including in the digital environment, irrespective of the business model or the technologies used.

Existing EU consumer protection rules, in particular the Unfair Commercial Practices Directive (UCPD), recognise children as vulnerable consumers requiring enhanced protection. The UCPD prohibits misleading and aggressive commercial practices that exploit children’s credulity or lack of experience.

It also prohibits exhortation to children to buy advertised products or to persuade parents to buy those products for them. As explained in the UCPD Guidelines²⁵⁷, dark patterns, spending or attention maximising features (for example, unclear in-app currencies) or unfair influencer marketing can also amount to unfair commercial practices. Despite this, the Digital Fairness Fitness Check²⁵⁸ found that consumers in general and children and teenagers in particular need enhanced protection online.

The Consumer Rights Directive (CRD) imposes pre-contractual obligations, for instance transparency about pricing, the identity of the trader, or the right of withdrawal. While not child-specific, it applies to all digital transactions (for example, the purchase of in-game virtual currencies), including those involving minors.

Moreover, the Unfair Contract Terms Directive (UCTD) renders non-individually negotiated contract terms unfair and non-binding if they create a significant imbalance to the consumer's detriment. This includes when the consumer is a minor.

Finally, the General Product Safety Regulation (GPSR) requires all consumer products in its scope, including connected products, to be safe. The scope of this Regulation is broad so that it can act as a safety net for all products placed or made available on the EU market.

When assessing the safety of products, manufacturers need to consider the categories of consumers using the product, by checking the risk for vulnerable consumers such as children. They also need to take risk mitigating measures accordingly. The Regulation focuses on protecting both the physical and mental health of consumers, which can be relevant for example for apps or chatbots popular with minors.

PRODUCT LIABILITY DIRECTIVE (PLD)

The Product Liability Directive (PLD) is a harmonised civil liability framework that ensures that victims of defective products can claim compensation from the producer in case of harm. The new PLD entered into force on 8 December 2024 and must be transposed by Member States by 9 December 2026.

The revised PLD keeps the fundamentals of the original PLD intact. It is up to the victim to prove that a product is defective and that there is a causal link between defectiveness and the specific harm suffered. The revised PLD clarifies the scope of application to cover software, including applications, operating systems and AI systems, specifies liability rules in case of a substantial modification to products giving them a 'second life'.

It also clarifies that compensable damage under the PLD can include medically recognised mental harm. The PLD also adapts liability rules to increasingly complex global value chains, by ensuring that at least one liable economic operator established within the EU can be identified (including potentially platforms).

The new PLD provides a pathway for compensation in cases where defective digital products cause harm for children. For instance, a child who develops depression due to the addictive design of an application, or who engages in self-harm following unsafe responses from a chatbot, may now be entitled to compensation under the PLD.

AUDIOVISUAL MEDIA SERVICES DIRECTIVE (AVMSD)

The AVMSD is the central piece of EU media legislation regulating audiovisual content. It sets sector-specific obligations on audiovisual media services and on Video-Sharing Platforms (VSPs) for the protection of minors from harmful audiovisual content.

Under the AVMSD, VSPs, irrespective of their size, must include the EU media content standards in their terms and conditions. This includes those aiming to protect minors from content which may impair their physical, mental or moral development. They are also required to take appropriate measures (for example, mechanisms to report or flag harmful content, age verification, parental controls and content rating

systems) to prevent minors from viewing harmful audiovisual content. The most harmful type of content, such as pornography or gratuitous violence, must be subject to the strictest measures to prevent minors from viewing harmful content.

The ongoing evaluation and upcoming review of the AVMSD planned for quarter three of 2026 will have a strong focus on the protection of minors as vulnerable viewers online. It will consider the relevance of the current rules and identify potential shortcomings in existing legislation. This will include assessing whether more should be done to ensure viewers, especially minors, are adequately protected when they view audiovisual content online. This includes content made available by influencers, considering market and regulatory developments. These developments and changing viewership habits are creating challenges that may put viewers, in particular minors, at risk.

New threats and risks have emerged in the online environment and have resulted in minors' increased exposure to harmful audiovisual content, such as cyberbullying, eating disorders, and the encouragement of suicide or self-harm. The review will consider if further specification of the concept of audiovisual harmful content is needed, and what measures are necessary to ensure minors do not watch such content.

POLITICAL ADVERTISING REGULATION (PAR)

The Political Advertising Regulation (PAR) establishes transparency and due diligence obligations for the provision of political advertising services. The Regulation introduces specific requirements for the use of targeting and ad-delivery techniques in online political advertising that rely on the processing of personal data. The Regulation fosters the protection of minors, while enabling equal conditions for first-time voters.

On the one hand, the PAR prohibits the use of profiling which involves the processing of the personal data of minors that are known to be at least one year under the national voting age. On the other, the Regulation allows transparent political advertising to reach first-time voters, allowing them to exercise their democratic choices in an informed way.

PROTECTION AGAINST CHILD SEXUAL ABUSE

AND EXPLOITATION ONLINE

Online child sexual abuse and exploitation are among the most harmful risks that children and adolescents may encounter in the digital world. Perpetrators are adults, but also other minors. Children and adolescents need to be informed about risks, including sexting and sextortion, and potential legal consequences for perpetrators.

Victims exploited by relatives and caregivers often need child protection measures based in civil law, coupled with social work and safe placement. Many victims may need psychotherapy.

Measures protecting children against child sexual abuse and exploitation online are part of the criminal law dimension of child protection, which sit at the intersection of EU and Member State competences.

By determining certain content that is either in itself or related to an activity illegal, these instruments also lead to the relevant due diligence provisions under the DSA. They address illegal content becoming applicable and provide an effective framework against the dissemination of such content.

The European Commission has taken steps to prevent and combat child sexual abuse online. In 2022, it presented a proposal for a permanent and comprehensive EU regulatory framework to prevent and combat child sexual abuse. This is comprised of obligations on online service providers to prevent the dissemination of child sexual abuse material and the grooming of children on their services. Only when prevention measures are not sufficient, online service providers could be obliged to detect, report, remove or block child sexual abuse online.

Under the proposal, competent national authorities would be empowered to request the issuance of detection, removal or blocking orders by judicial or independent administrative authorities. The orders would only be issued following a thorough assessment of their necessity and proportionality.

The proposal also foresees the establishment of a new EU Centre to prevent and combat child sexual abuse to assist digital services providers and authorities in complying with their obligations under the Regulation. Negotiations on the Regulation are ongoing. The European Commission is supporting the European Parliament and the Council in reaching an agreement that ensures the effective protection of children in full respect of all fundamental rights concerned, as well as coherence with existing legislation, notably the Digital Services Act (DSA).

In parallel, the recent agreement by the co-legislators of the Recast of the Child Sexual Abuse Directive has further strengthened the EU framework against child sexual abuse and exploitation, both online and offline. The revised rules update the existing framework to ensure that new threats, like AI-generated child sexual abuse material, grooming and sextortion, live streaming of child sexual abuse, are criminalised and effectively prosecuted.

The revised rules will also reinforce the legal framework to prevent child sexual abuse and assist victims. This will be achieved by imposing background checks for people working in close and direct contact with children, or by ensuring victims can seek prosecution for a sufficient period after the offence has been committed.

In addition to legislative initiatives, the EU also takes non-legislative actions, such as funding and facilitating coordination and cooperation. For example, the Network for the Prevention of Child Sexual Abuse brings together fifty experts to exchange best practices, inform research, and support the development and implementation of rigorously evaluated prevention measures for child sexual abuse, including online.

Criminal law is necessary to combat child sexual abuse, but it cannot be the only tool addressing this horrible crime effectively. The protection of children from sexual abuse and exploitation requires a whole-of-society approach. This should involve public authorities, law enforcement, judicial authorities, education institutions, civil society organisations, families, communities and social media and other digital services providers. Effective prevention and responses to these crimes do not solely depend on robust legislative measures, but on coordinated efforts and cross-sectoral, multi-layered action.

PREVENTING RADICALISATION

The EU Terrorist Content Online Regulation protects vulnerable populations, including children, from exposure to radicalising material online. The Regulation requires hosting service providers to remove terrorist content within one hour of the receipt of a removal order from a competent national authority.

This is complemented by several non-legislative initiatives. One such measure is the EU Internet Forum. The Forum is a public-private platform which brings together EU Member States, law enforcement authorities, industry and civil society to coordinate responses against abuse. This includes the exploitation of online platforms by terrorists, violent extremists, as well as other malicious actors, such as those grooming children for the purpose of sexual abuse, drug trafficking, organised crime, trafficking in human beings, or migrant smuggling.

Children across the EU are at risk of falling victim to and being recruited into crime, both online and offline. The European Commission is currently developing an action plan on the protection of children against crime. This is expected to complement existing instruments by identifying remaining gaps and to provide a more coherent and coordinated approach to improve the protection of children from crime, both as victims and perpetrators, online and offline.

ACTION PLAN AGAINST CYBERBULLYING

Cyberbullying is a growing problem for children and adolescents in the online world, with substantial impacts on children's mental health and well-being, participation and development.

To address its concerning prevalence, in March 2026 the European Commission adopted the Action Plan against Cyberbullying²⁵⁹. The Action Plan aims to prevent cyberbullying, to facilitate its reporting and ensure effective support for victims. Under the Action Plan, EU Member States are encouraged to take complementary action at the national level.

This includes the development of national anti-bullying strategies, strengthening prevention and early detection in schools and other settings where children spend time. Improving support services for victims and ensuring reporting systems relate to appropriate legal, social, psychological and educational support are other important areas for action under the Action Plan.

Alongside this, the Commission Recommendation on developing and strengthening integrated child protection systems in the best interests of the child²⁶⁰ invites EU Member States to take all appropriate legislative, administrative, social and educational measures to prevent and protect children from bullying, including online. This includes through the development of comprehensive anti-bullying plans.

EU AGE VERIFICATION SOLUTION

Alongside existing legislation, the European Commission has built and is expanding an operational toolkit for age verification to protect children and adolescents online and to limit their exposure to harmful content. This toolkit offers networks, platforms, technical solutions and channels to protect and empower minors online.

The Commission has developed an EU Age Verification Solution that is robust, user-friendly and privacy-preserving. To this end, a blueprint has been made available to Member States for customisation and implementation. When customised, it can take into account different age brackets. Member States can

publish the solution as a stand-alone app and/or integrate it as an age verification functionality in their EU Digital Identity Wallets. The solution is open source, so third countries or market players can also take up the solution and further develop it.

The EU Age Verification Solution could be a suitable tool to apply age restrictions in practice, if it is accompanied by appropriate options for minors to prove their age. EU Member States apply varying approaches to the use and issuance of identity documents or eIDs, and not every minor may have their own passport. As such, the nomination of trusted proof-of-age providers who can issue proof of age for the required age is essential for the effective functioning of age verification in the EU.

To accelerate this process, the European Commission issued a Recommendation on establishing a common framework for EU-wide Age Verification technologies. As part of the Recommendation, the Commission is defining an EU Age Verification Scheme in cooperation with Member States. The Scheme will detail requirements concerning the trust model, governance and requirements to be fulfilled by providers of the proof-of-age attestations and age verification solutions.

The Recommendation encourages EU Member States to make use of the EU Age Verification blueprint, to adapt it to their national contexts, and to make age verification solutions available by 31 December 2026 based on the blueprint.

Member States were further invited to submit an implementation plan to the Commission by 30 June 2026 to outline how they intend to make an EU age verification solution available. Member States are encouraged to collaborate with one another and to engage with the European Commission, researchers and civil society in the roll-out of their national solutions. The challenges for age verification, including possible risks of regulatory fragmentation across the EU, are explored later in this chapter in the section ‘Unfinished business’.

Results of existing enforcement

Existing EU legislation is only as effective as its enforcement. The DSA introduced a fundamentally new enforcement architecture, centralised at the Commission for the largest platforms and combined with national enforcement through Digital Services Coordinators. This architecture is now producing decisions, proceedings and visible compliance changes, and a track record is starting to emerge.

The AI Act opts for a similarly adapted enforcement structure, with enforcement centralised at the Commission for general-purpose AI models and most AI systems based on general-purpose AI models when the provider of the AI system and model is the same (or within the same undertaking). The AI Act Omnibus introduces a further innovation, with the enforcement related to AI systems designated or integrated in VLOPs or VLOSEs under the DSA also centralised at the Commission.

The GDPR is enforced by independent national Data Protection Authorities (DPAs). They continue to produce decisions, issuing substantial fines and other corrective measures when DPAs determine that data controllers have violated data protection rules.

The enforcement of the AVMSD is ensured by national regulatory authorities and bodies. The AVMSD introduced requirements to ensure the institutional and functional independence of national regulatory authorities and bodies, which have been reinforced by the European Media Freedom Act (EMFA).

Enforcement of consumer protection laws, including the rules stemming from EU Directives and Regulations, is primarily the competence of Member State authorities and courts. While the Commission does currently not have direct enforcement powers in the area of consumer law, it coordinates and supports Member States' enforcement work under the Consumer Protection Cooperation (CPC) Regulation. This establishes a cross-border enforcement cooperation framework for Member States' CPC authorities to address cross-border and EU-wide breaches of consumer law together.

DSA ENFORCEMENT STRUCTURE

The DSA's enforcement structure involves direct and centralised Commission competence for VLOPs and VLOSEs, as well as coordination and cooperation with several national authorities, notably in the context of the European Board of Digital Services, which also counts on a specific working group on the protection of minors.

This is a new enforcement framework which has the advantage of centralising enforcement at the Commission level for the largest platforms, which operate seamlessly across borders. Some of these platforms are among the biggest and most well-resourced companies in the world, with revenues often exceeding the GDP of EU Member States. This framework also promotes coherent application of the rules across the EU and down to the national level (for example, through the guidelines on the protection of minors and case law).

The deterrence effect is substantial, with one of the largest fining powers in the world and interim measures that can lead to swift change in platforms' practices, as shown by the commitments by TikTok and the withdrawal of TikTok Lite in the EU²⁶¹. In the context of investigations, the European Commission has robust enforcement tools and investigatory powers. Notably, this includes the ability to request granular, sensitive data and information, and to conduct inspections at the premises of providers. This allows unprecedented access to providers' systems, design and decisions.

In extreme cases where infringement persists, causing serious and urgent harm, the Commission may request the Digital Services Coordinator (DSC) of the provider's Member State of establishment to request that the competent judicial authority orders the temporary restriction of access to the service²⁶².

Enforcement action by the European Commission has required substantial capacity building and is now increasingly accelerating. Gradually, it is becoming more time-effective, as demonstrated by the preliminary findings on TikTok concerning potentially addictive design and Meta on age assurance. The compliance benchmarks set out in the guidelines on the protection of minors have helped to this end.

The initial outlining of the Commission's expectations on key issues in enforcement action, including preliminary findings and commitments, should also inform and be reflected by providers in the ongoing practice of risk assessment and mitigation cycles. This is expected to lead to changes in platform services before the opening of formal enforcement action is even required.

In view of the resources needed to take legal action against companies subject to Commission enforcement, any enforcement framework should ensure time is also invested in ensuring procedural requirements and all possible precautions are taken so cases hold up in court in all degrees of judgement.

The risk-based and technology-neutral approach of the DSA is the basis for future-proof enforcement action. This evolves, thanks to platforms' risk assessment and audit cycles, related commitments or other responses to enforcement actions, as well as the designation of new services. The recent opening of an

investigation against X related to its AI system, Grok, and the non-consensual sharing of intimate images (including those generated by AI) demonstrates how enforcement under the DSA can quickly cover new problematic practices or features incorporated into online platforms.

Similarly, the recent designation of WhatsApp as a VLOP shows how services can fall under the scope of the DSA, as they assume the features and characteristics of online platforms.

DSA DECISIONS AND PROCEEDINGS

The European Commission and national authorities have, in the period since the DSA entered into application, opened or completed a series of enforcement actions concerning the protection of minors. The decisions and proceedings below kick-started the operational benchmark against which platforms' compliance is now being assessed. This will continue to evolve as enforcement action advances, for example to cover other services and issues, and will be informed by continuous risk assessment and mitigation, as well as auditing cycles.

In February 2026, the European Commission adopted preliminary findings that TikTok's potentially addictive design does not meet the DSA's standards of protection. These findings consider that TikTok needs to change the basic design of its service, for example by disabling key addictive features, such as 'infinite scroll', implementing effective 'screen time breaks' (including during the night), and adapting its recommender system²⁶³.

In March 2026, the Commission adopted preliminary findings against four very-large pornographic platforms (Pornhub, XNXX, Stripchat, and XVideos) for their failure to instate proper age verification²⁶⁴. This was complemented by a European Board for Digital Services coordinated action against smaller pornographic content platforms²⁶⁵.

In April 2026, the European Commission also issued a preliminary report finding Meta in breach for failing to prevent minors under 13 from using Instagram and Facebook²⁶⁶.

Enforcement action is also ongoing against Snapchat to investigate suspected inadequate age assurance and default settings, insufficient protection of minors from grooming or recruitment for criminal activities, and ineffective content moderation tools preventing the spread of information directing users to the sale of illegal products, including drugs, and age-restricted goods²⁶⁷.

Among accepted commitments, AliExpress has agreed to a default system that limits the visibility of products intended for adults, including automatic blurring of adult product images using AI-powered real-time scanning²⁶⁸.

At the national level, the Dutch regulator Authority for Consumers and Markets (ACM) is investigating the video game platform Roblox in connection with possible risks faced by minors on the platform²⁶⁹.

Further proceedings on addictive design, recommender systems, the dissemination of illegal content (including child sexual abuse material), and marketplace safeguards are open against Facebook, Instagram, X concerning Grok²⁷⁰, Shein²⁷¹, and Temu²⁷². An earlier investigation into TikTok Lite resulted in the Commission's commitment decision and the permanent withdrawal of this feature from the EU market.

The effects of upcoming enforcement actions concerning the services and issues mentioned above will clarify the concrete expectations of the Commission and set a high compliance bar. This will inform changes to the service provision not only of individual online platforms under investigation, but also by all other providers in scope of the DSA.

To leverage the full potential of the DSA, now that this enforcement architecture is up and running, it may need to be further reinforced to ensure enforcement cases can be conducted with the necessary speed and urgency and deliver the full effect of the DSA. To do so, all authorities involved in enforcement at the national and EU levels should consistently have the appropriate resources to fulfil their mandate.

AI ACT ENFORCEMENT STRUCTURE

The AI Act's enforcement structure involves direct and centralised Commission competence for enforcement regarding general-purpose AI models (including GPAI models with systemic risk) and AI systems based on general-purpose AI models, where the model and the system are developed by the same provider or a provider that is part of the same undertaking.

The AI Act omnibus introduces a further innovation, with enforcement related to AI systems designated or integrated in VLOPs or VLOSEs under the DSA also being centralised at the European Commission. Enforcement concerning other AI systems in scope of the AI Act is the responsibility of national market surveillance authorities.

The enforcement powers of the EU AI Office and national market surveillance authorities will become applicable on 2 August 2026. As of this date, the AI Office will enforce the rules regarding general-purpose AI models²⁷³, general-purpose AI systems with systemic risk²⁷⁴ and AI systems based on GPAI models where the model and the system are developed by the same provider or a provider that is part of the same undertaking, and for AI systems integrated into VLOPs and VLOSEs. The obligations for high-risk AI systems, as agreed in the Omnibus on AI, will start to apply in December 2027 (for stand-alone AI systems, such as certain AI systems in education) and August 2028 (for AI systems embedded in regulated products, such as toys).

GDPR ENFORCEMENT STRUCTURE

The GDPR is enforced by Data Protection Authorities in each EU Member State, which are empowered to investigate complaints, to conduct audits, to order corrective measures, and impose administrative fines for violations of data protection law.

When a company (data controller) processes personal data in more than one Member State, the lead Data Protection Authority, that being the Data Protection Authority where the company has its main establishment, is responsible for the supervision of that company.

The lead supervisory authority cooperates and coordinates its actions with the data protection supervisory authorities of the other EU Member States where the data processing has an impact. This is called the 'one-stop-shop' mechanism.

Data Protection Authorities may initiate investigations based on individual complaints, mandatory breach notifications, media reports, or their own inquiries. Organisations found in breach of data protection rules can face processing bans, compliance orders, or fines of up to EUR 20 million or 4% of global annual turnover, whichever is higher.

As laid down in the EU Charter of Fundamental Rights and reiterated in the GDPR, all Data Protection Authorities must be independent. All Member States must ensure Data Protection Authorities are provided with the human, technical and financial resources for the effective performance of their tasks and powers.

The European Data Protection Board (EDPB) brings together all supervisory authorities to ensure the consistent application of the GDPR. It produces guidance on the GDPR's application. The EDPB is currently working on guidelines on the processing of children's data. The EDPB also promotes cooperation between Data Protection Authorities.

The GDPR is technology-neutral and takes a risk-based approach. This means that organisations must implement the relevant technical and organisational measures proportional to the risk posed by their data processing activities.

Late last year, the GDPR Procedural Regulation was passed. It introduced new rules to improve cooperation between national data protection bodies when they enforce the GDPR to speed up the process of handling cross-border data protection complaints. In May 2025, Data Protection Authorities released the Helsinki Statement on enhanced clarity, support and engagement. In this statement, they agreed to enhance the consistency of the application and enforcement of the GDPR.

SELECTED GDPR ENFORCEMENT ACTIONS AND PROCEEDINGS

The GDPR has been in force since 2018. In that time, fines of over EUR 7 billion have been issued to organisations for violating data protection rules²⁷⁵. Data Protection Authorities can use their powers to require companies to bring their processing activities into compliance. This allows Data Protection Authorities to engage with controllers before launching an investigation, saving time and resources.

As an example, in February 2023, the Irish Data Protection Commission engaged with Meta in relation to tagging on Instagram. When a child wanted to tag a public account they did not follow, they would receive the statement 'Account couldn't be tagged. Make your account public to tag others who don't follow you'.²⁷⁶

This notification also contained a 'Go to settings' button that took the user to a menu where they could change their account from private to public. This configuration didn't warn children of the potential consequences of making this change, nor did it redirect children to any frequently asked question (FAQ) or help centre article.

Following discussions with the data protection controller, changes were made to user notifications. The notification was updated to read 'Account couldn't be tagged. Your account is private, so you can tag only your followers. You can manage your privacy in Settings'.

'Go to settings' was replaced with a 'Learn more' button that takes users to a help centre article where they could find out how to make their user account private at any time, the differences between private and public accounts, how users can manage privacy on Instagram, and information for parents on 'who can see my teen's posts on Instagram'.

Data Protection Authorities have made multiple decisions on violations of the GDPR relating to children's data. They have also enacted processing bans prohibiting a controller to process data subjects' personal data, including children's data until their processing was in line with GDPR requirements. A selection of such actions is highlighted below.

Several Data Protection Authorities have launched investigations into controllers for not complying with the data protection by design and default principle. For example, the Irish Data Protection Commission fined TikTok EUR 345 million, as it was found to violate several provisions of the GDPR.

This included data protection by design and default, and the data minimisation principle. The Data Protection Commission found that TikTok violated these provisions, as it made children's accounts public to anyone on or off TikTok by default.

The Irish Data Protection Commission also found that TikTok used dark patterns to nudge children to opt for public accounts by default. This meant that anyone could view their content, violating data protection by design and default and the fairness principle. It also found that TikTok failed to ensure adult users overseeing a child's account through 'family pairing' were verified as the parent or guardian of the child²⁷⁷.

Moreover, the Irish Data Protection Commission fined Instagram EUR 450 million, as it found they had violated the principle of data protection by design and default. Instagram had permitted children to set up business accounts, which were required to display public-facing contact details in their profile. The Data Protection Commission found that Instagram violated this principle, as all user accounts were set to public by default. This meant that anyone could view the child's content, unless they changed the setting²⁷⁸.

The Italian Data Protection Authority imposed a temporary ban on TikTok's processing activities due to concerns about child safety, in particular considering the death of a 10-year-old Italian girl. The ban imposed an immediate limitation on TikTok's processing activities for users whose age could not be established with certainty. This led to the platform rechecking the age of its Italian users and closing over half a million accounts suspected of belonging to minors under 13, the age TikTok permits children to use its service²⁷⁹.

Earlier this year, the Irish Data Protection Commission launched an inquiry into X regarding the creation of non-consensual sexualised images, including of children using the AI tool Grok. The Data Protection Commission will examine X's compliance with several articles, including data minimisation and data protection by design and default²⁸⁰.

AVMSD ENFORCEMENT AND THE PROTECTION OF MINORS ONLINE

The protection of minors is a priority area for enforcement by media regulators. In 2024, the European Regulators Group for Audiovisual Media Services (ERGA) evaluated the measures adopted by media regulators regarding the protection of minors. It concluded that there was a need to establish and refine criteria for classifying harmful content for minors.

An example of the implementation of the AVMSD concerning Video-Sharing Platforms (VSPs) regarding the protection of minors can be found in Italy. AGCOM, the Italian Communications Regulatory Authority, noted the presence on TikTok of 'French scar' videos. In accordance with the regulation on VSPs, AGCOM initiated an intervention procedure leading TikTok, a VSP based in Ireland, to remove the videos.

The German regulator DLM has adopted measures against porn platforms established in Cyprus and Czechia. The cross-border procedure was based on the e-commerce Directive, as foreseen under the AVMSD. The legal basis was the Interstate Treaty on the Protection of Minors in the Media (JMStV), which transposes the AVMSD, and the relevant provision was the prohibition to distribute pornography to minors and rules on age verification.

The European Media Freedom Act (EMFA)²⁸¹, which sets up a cross-border procedure to request the enforcement of obligations for VSPs established in another Member State, has also been activated concerning several porn platforms established in Cyprus. This incited the platforms concerned to respect the AVMSD's obligations on the protection of minors, including age verification. The Cypriot regulator is currently assessing the replies provided by relevant providers (Stripchat) concerning how they have deployed age verification in several countries, for example Germany.

CONSUMER PROTECTION COOPERATION (CPC)

REGULATION NETWORK

As stated in the 2030 Consumer Agenda, the European Commission will propose a revision of the Consumer Protection Cooperation (CPC) Regulation to further strengthen consumer law enforcement. This could potentially help to centralise direct enforcement powers in specific cases at the EU level.

This would make enforcement under the CPC Regulation both faster and a stronger deterrent. It would also help to better protect minors who, due to their heightened vulnerability and lack of experience, are at high risk of being exposed to unfair commercial practices online.

SELECTED CPC NETWORK ENFORCEMENT ACTIONS

For the digital sector, in March 2025 the European Commission published the CPC Network's common position on Star Stable Online²⁸². The Network found violations of the UCPD and CRD, such as exhortation to children, urging them to buy, or to persuade adults to buy for them in-game currency or items; dark patterns (scarcity claims with respect to in-game virtual currency or in-game content); a lack of clear and transparent information adapted to children about buying and using in-game virtual currency, and a lack of disclosure of commercial content by influencers. The Commission is currently facilitating dialogue between the CPC Network and the company to bring these violations of EU consumer law to an end.

In March 2025, the Commission published the CPC Network's key principles on in-game virtual currencies, reflecting the CPC authorities' shared interpretation of existing EU consumer protection legislation (mainly the UCPD and CRD). These key principles aim to promote transparency and fairness in the video game industry's use of purchasable virtual currencies and to ensure that consumer vulnerabilities, especially those of children, are respected²⁸³.

The topic of influencer marketing is of high interest to the CPC Network, including when these practices concern children. In 2023, national CPC authorities from 22 Member States conducted a sweep on the posts of 576 influencers, to verify whether they disclose their advertising activities, as required under EU consumer law. As a result of the sweep, 62% of checked influencers were earmarked for further investigation²⁸⁴. The European Commission has also launched the Influencer Legal Hub, where influencers can find practical information on compliance with EU law²⁸⁵.

In February 2022, a coordinated action of the CPC Network against TikTok was launched. It addressed concerns of CPC authorities related to hidden marketing, aggressive advertising techniques targeting children, and certain contractual terms in TikTok's policies that could be considered misleading and confusing for consumers.

In June 2022, TikTok committed to align its practices with EU rules on advertising and consumer protection²⁸⁶. CPC authorities are monitoring TikTok's compliance, especially whether its commercial practices (for example, advertising) are sufficiently transparent for children to understand their nature.

CONSUMER EDUCATION AND REDRESS

Through the recent adoption of Directive 2025/2647/EU, which reviews the Alternative Dispute Resolution Directive, consumers may revert to out-of-court dispute resolution to resolve disputes related to digital services and content, and disputes related to pre-contractual information when a contract has been finalised.

The extension of the scope of the Directive made out-of-court dispute resolution fit for the digital age by ensuring more consumer disputes could be resolved in this way. Examples could be a dispute related to a video game subscription, or to the description provided about a product targeting minor. The Representative Actions Directive enables designated qualified entities, such as consumer organisations and public bodies, to bring legal actions for the protection of the collective interests of consumers. This includes minors concerned by unlawful traders' practices.

Actions may seek the cessation of unlawful practices and consumer collective redress. Actions may be brought to enforce consumer rights covered by more than 70 EU acts listed in Annex I to the Directive, such as the Unfair Commercial Practices Directive, the GDPR, the Digital Markets Act (DMA), the DSA, or the AI Act. Whenever a new EU instrument relevant for the protection of the collective interests of consumers is considered by EU legislators, it may be added to the Annex, rendering its enforcement possible via the EU model of consumer collective redress.

Unfinished business

HARMFUL DESIGN IS NOT ADDRESSED SUFFICIENTLY

While the enforcement of existing legislation is in many cases in its initial stages, given sufficient time and resources, it is expected to bring change to social media and other digital services providers' business model by defining which elements of this model are ultimately compatible with fundamental rights in the EU, including the rights of the child.

A clear example of this is the prohibition of advertising based on profiling to minors. Similar to the prohibition of advertising based on profiling using special categories of sensitive data, this prohibition directly rejects the acceptability of a practice at the core of several platforms' business model.

Another example is the risk assessment and mitigation obligations imposed on social media and other digital services providers. These obligations force providers to further invest in understanding the risks their services pose to fundamental rights, including the rights of the child, and to prevent and mitigate these risks.

Despite this, several shortcomings remain. First, existing EU legislation often relies on enumerated practices (for instance, specific addictive features). This creates a structural lag. A feature-based approach may lead to regulatory gaps, as digital services evolve with time beyond the features specifically enumerated and addressed in legislation. This evolution may take place intentionally to avoid enforcement by regulators.

Furthermore, risks are often cross-cutting and arise not from a single feature or functionality in isolation, but from the interaction of multiple features or the design of a service more broadly. Consider new forms of audiovisual content. Immersive environments built on extended-reality technology and short-format autoplay videos, for instance, have created risks for children that were not anticipated when relevant legislative instruments were put in place.

Legislation can adapt during implementation, as the X / Grok DSA investigation and the WhatsApp VLOP designation demonstrate. However, this adaptation occurs feature by feature after the harm has been identified at the speed of formal enforcement proceedings.

Moreover, existing EU legislation addresses the core business of platforms in an indirect way, by providing a framework based on fundamental rights within which any business model should operate. As an example, VLOP and VLOSE providers must adhere to specific transparency and design requirements related to recommender systems²⁸⁷, and VLOP providers are required to offer at least one option for each of their recommender systems that is not based on-profiling²⁸⁸, but how concretely they should or should not design their recommender systems may be determined in the context of enforcement action.

Currently, regulators are often ‘on the back foot’ attempting to enforce legislation in a rapidly evolving social media+ environment, which may define explicit features and functionalities that continue to evolve, after digital services have been placed on the market. This potentially exposes millions of users, including children and adolescents, to risks of harm. In some cases, risks may only materialise or become clear after services have been placed on the market, for example due to how these features or functionalities are used in practice or depending on context. In terms of enforcement, when contesting with providers that they have not fulfilled their due diligence obligations, the burden of proof may – today – often fall on the EU and national enforcing bodies to demonstrate that social media and other digital services are harmful through extended and costly legal processes against very well-equipped, large companies.

It could therefore become the rule that social media and other digital services providers launching, operating or updating services that may pose risks to children and adolescents must demonstrate that their services or new functionalities are safe for minors to use before market deployment.

“Our aim is not to shut children out but to ensure the digital world caters to them as they grow. If tech providers want to access our children, they will need to prove they meet the bar.”

— LEANDA BARRINGTON-LEACH,
EXECUTIVE DIRECTOR,
5RIGHTS FOUNDATION

DIVERGING NATIONAL APPROACHES TO AGE RESTRICTIONS AND CHILDREN'S CONSENT

The age question is the most visible policy gap in existing legislation. Two strands should be considered. First, the GDPR has generally set 16 years of age for children to provide their consent to 'Information Society Service' to process their personal data. The GDPR provides the option for Member States to lower this age anywhere between 13 and 16. Where the child is below 16 (or another age prescribed by a Member State), the processing is only lawful if consent is given or authorised by the holder of parental responsibility.

Second, several EU Member States are now legislating, or considering legislating, on age restrictions for minors to access social media and other digital services, with some even having distinct approaches to the EU's and Member States' thresholds for consent. Member States' approaches to minimum ages diverge in scope, in age threshold, in the services covered, and whether parental consent can override the threshold.

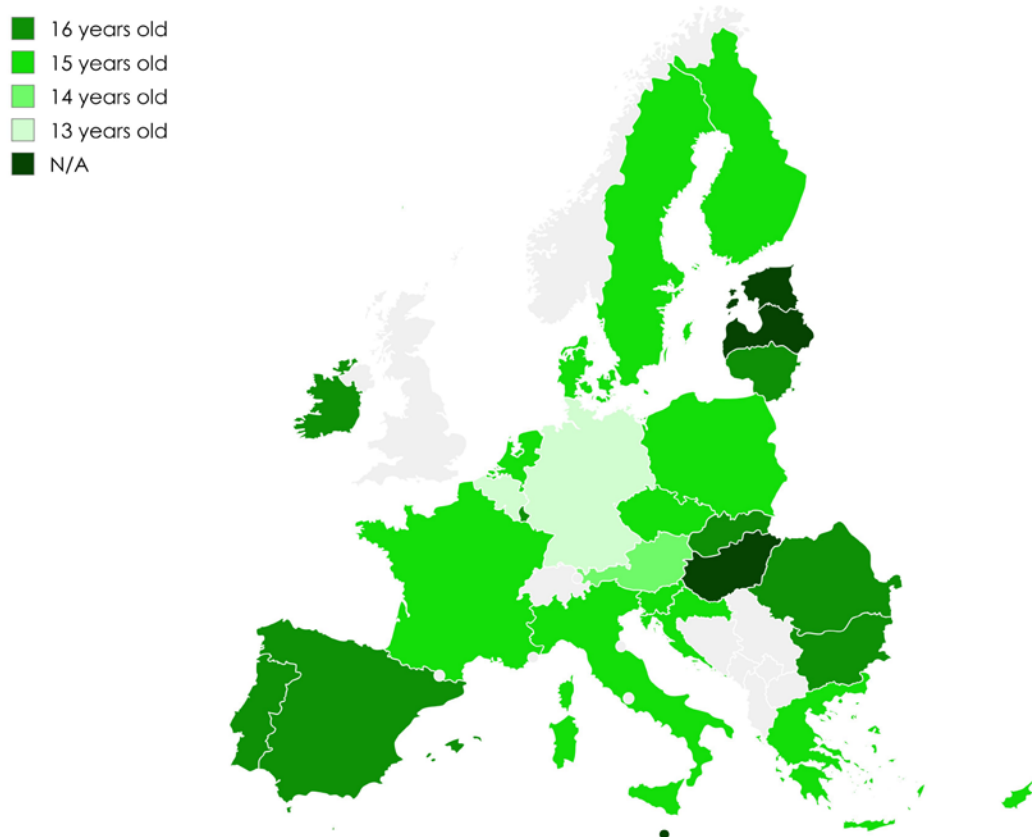
The proliferation of national initiatives setting age restrictions to access social media and other digital services raises risks concerning the fragmentation of the Single Market and unequal levels of protection for minors across the EU. Several Member States, including Austria, Cyprus, Denmark, France, Luxembourg, Greece, Spain and Slovenia, are calling for an EU-wide approach to age restrictions to access social media+.

The Jutland Declaration signed in October 2025 by 25 Member States upon initiative of the Danish Council Presidency called for a safer digital environment for minors, including through age verification and assessments on the age at which minors should be allowed access to social media and other digital services. The European Council conclusions of 23 October 2025 and the European Council conclusions of 19 March 2026 highlight the importance of protecting minors online.

Debates are ongoing in all Member States, either in national parliaments, governments, or in civil society focusing on introducing age restrictions at different levels. Proposed restrictions range from 13 to 16, sometimes allowing different age levels, with or without parental consent. Italy, France and Greece have formally notified the Commission with draft laws via the Technical Regulations Information System (TRIS).

France, Italy and Denmark are considering restrictions under 15. Cyprus and Romania propose a limit at 16, and Germany at 13. Greece and Denmark propose two tiers with restricted access below 15 and access only with parental consent for 12 to 15 year-olds (13 to 15 for Denmark).

Figure 1: EU Member States proposing or considering age restrictions to social media and other digital services



As many Member States are considering establishing a minimum age for social media+, with diverging scopes and accompanying obligations, a harmonised approach at the EU level would be important to ensure minors benefit from the same level of protection online across the EU. To ensure an equal level of protection, it is also crucial to consider how potential age restrictions may relate to safety measures, notably imposed by EU legislation, including the DSA.

Age restrictions proposed by Member States may relate to or seek to address specific risks presented by individual types of social media and other digital services. To ensure an equal level of protection for minors, a harmonised approach to age verification must go hand in hand with safety measures effectively enforced by regulators and safety features deployed by social media and other digital services providers (either through a safety by design or by default approach).

“A clear EU-wide minimum age would in the immediate term support parents, reduce peer and social pressure on children, and create a strong incentive for platforms to redesign their services in line with children’s safety and well-being.”

— LIES CRAEYNEST,
FOUNDER, KIDSUNPLUGGED

APPROACHES ON AGE RESTRICTIONS AND CONSENT

Member State	State of play on national discussions and potential actions on age restrictions for digital services	Proposed or considered minimum age	Children's age to consent on data processing online
Belgium	In April 2026, the Flemish government approved a preliminary draft decree introducing a legal age limit of 13 years for certain online platforms that may be harmful to minors.	13	13
Bulgaria	In May 2026, amendments were proposed to the Child Protection Act by a non-governing political party for a restriction for children under 16 to access social media. Access could be permitted from the age of 13 with parental consent.	16	14
Czechia	No proposal yet. The governing party ANO (PfE) plans to propose legislation this year to ban children under the age of 15.	15	15
Denmark	Legislative proposal under development. In November 2025, the government announced a political agreement on the prohibition for children under 15 to access social media, although access would be permitted from the age of 13 with parental consent.	15	15
Estonia	Overall opposition to the idea of imposing age restrictions on social media.	N/A	13
Germany	No legislative proposal so far. In November 2025, government declared support in principle for possible regulation and established an expert committee, which published its report on 24 June, proposing a minimum limit at 13 and limitations on market access for services that are not safe, asking for an EU level approach. Political parties and NGOs have made various proposals.	13	16
Ireland	No legislative initiative yet. Tánaiste (Deputy Prime Minister) expressed support for restriction of access to social media for children under 16. The Joint Committee on Arts, Media, Communications, Culture and Sport did not support such ban in May 2026.	16	16
Greece	Law expected to be voted in summer 2026 and implemented as of January 2027.	15	15
Spain	In April 2025, the ES government made a legislative proposal to raise the age of consent for children for the processing of their personal data. In February 2026, the President announced that Spain will prohibit access to digital platforms for children under 16.	16	14
France	Legislative proposal made in 2025 (both parliamentary chambers have adopted their positions but still have to agree on the compromise text). Expected entry into force of the law in September 2026. France proposes a differentiated regime, with a ban for under 15s on certain social media services designated as harmful and parental consent for access to other social media services.	15	15

Member State	State of play on national discussions and potential actions on age restrictions for digital services	Proposed or considered minimum age	Children's age to consent on data processing online
Croatia	Legislative proposal made in 2025 but rejected in March 2026.	15	16
Italy	The government is planning a legislative initiative to prohibit children under 15 to access social media. In parallel, two separate parliamentary initiatives were tabled in 2024 and 2026, but are not advancing at present, as Prime Minister declared a ban may not be the preferred option.	15	14
Cyprus	Legislative initiative announced by the government in 2026.	15	14
Latvia	No legislative proposal yet. In March 2026, the government coalition agreed to develop a regulation to restrict access to social media under a certain age.	N/A	13
Lithuania	Legislative proposal made in 2026.	16	14
Luxembourg	Parliament resolution (January 2026) calling for the creation of an EU framework, or coordinating actions with BE, DE and FR.	16	16
Hungary	No proposal yet.	N/A	16
Malta	In February 2026, a public consultation on social media reform was held. Currently in post-consultation phase.	N/A	13
Netherlands	Coalition plans (January 2026) call for setting at EU level a minimum age for accessing social media.	15	16
Austria	Federal government announcement; legislative proposal expected in summer 2026.	14	14
Poland	Announcements by certain Members of the lower chamber of the Parliament (Sejm) and the Ministry of Digital Affairs.	15	16
Portugal	Preparation of a parliamentary legislative initiative in 2026 (hearing stage).	16	13
Romania	A legislative proposal on the age of digital majority was published in 2025. Others are also being discussed at different procedural stages.	15-16	16
Slovenia	In February 2026, the government announced preparations to regulate the use of social media for children until the age of 15.	15	15
Slovakia	Legislative proposal announced in 2026 by the Ministry of Investment, Regional Development and Informatics.	16	16
Finland	The Prime Minister and his party published in November 2025 a position paper supporting a prohibition for children under 15 to access social media. National recommendations recommend no social media use under age 13.	15	13
Sweden	Government set up a committee to investigate potentially prohibiting children's access to social media under a certain age, which proposed to have a limit at 15 years old on social media.	15	13

MEMBER STATE UPTAKE OF THE EU AGE VERIFICATION SOLUTION

The EU Age Verification Solution is technically state-of-the-art and its blueprint is ready for customisation by Member States and market players. However, the effectiveness of these tools in strengthening online child protection will ultimately be determined by their actual uptake by Member States, market players and social media and other digital services providers.

The nomination of trusted proof-of-age providers is also essential for the effective functioning of the EU Age Verification Solution. Despite repeated calls from the European Commission, many Member States have yet to act in nominating trusted proof-of-age providers.

A harmonised EU age restriction to access social media and other digital services cannot be enforced without an age verification ecosystem that can be used to prove the age of minors. The current EU Age Verification Solution can be technically extended from 18+, to other ages, including for example adolescents, in line with national legislation.

However, without trusted proof-of-age providers that can issue age credentials to minors, social media and other digital services providers risk falling back on other less robust (for instance, self-declaration) and/or less privacy-preserving methods, and Member States may struggle to ensure effective age verification.

ENFORCEMENT NEEDS: CAPACITY,

SPEED AND CROSS-REGULATOR COORDINATION

Enforcement to date demonstrates that existing legislative instruments can produce decisions and visible compliance changes. It also brings to the fore several challenges.

Efficient enforcement is critical to ensure child safety online. This requires sufficient powers and well-resourced authorities. In practice, conflicting enforcement architectures may create several issues. These include the further spreading of limited resources, set-up time, increased complexity, and potentially competing or overlapping competences. These issues may disincentivise compliance, or even offer possible grounds for social media and other digital services providers to avoid or delay compliance.

A significant challenge for regulators is maintaining adequate staffing with the necessary expertise. As providers' operations become increasingly complex, regulators must ensure they have enough appropriately skilled personnel to effectively assess whether social media and other digital services comply with legislation. This applies at both the EU and national levels.

More broadly, the availability and coordination of human and financial resources allocated to child protection systems (including to support public enforcement) is another a challenge²⁸⁹. Reversing the burden of proof for enforcement, as discussed above, may help to enhance enforcement capacity and deliver greater results, without putting additional strain on the limited resources of regulators at both the EU and national levels.

CHILD SAFETY GAP: ONLINE SEXUAL ABUSE AND EXPLOITATION

The Interim Regulation, applicable from 2021 until 3 April 2026, laid down temporary rules derogating from certain obligations of the e-Privacy Directive. This enabled providers of certain interpersonal communications services to employ technologies for the processing of personal and other data to detect and report child sexual abuse material and grooming, and to remove material from their services.

In December 2025, the European Commission proposed an extension of the Interim Regulation until 2028 as a temporary solution pending the adoption of the long-term Regulation to prevent and combat child sexual abuse. However, the European Parliament and the Council did not reach an agreement on the proposal. As a result, the Interim Regulation ceased to apply as of 3 April 2026, creating legal uncertainty at the EU level.

A solution must be found as soon as possible in the long-term Regulation for the detection of child sexual abuse in private communications, where most of these crimes occur. The proactive detection by providers of these services has been the main source of child sexual abuse investigations for over 15 years.

The scope of detection should cover not only known child sexual abuse material to prevent revictimisation, but also new child sexual abuse material, which often indicates ongoing abuse, and includes AI-generated child sexual abuse material. The latter has increased exponentially in the past years (from 5,000 reports in 2023 to 1.3 million reports in 2025). Detection should also include grooming to prevent imminent abuse and to stop ongoing abuse, which has also increased exponentially (by 12 times in the last three years).

Other gaps in current legislation relate to emerging forms of child sexual abuse and exploitation linked to technological developments, such as AI-generated child sexual abuse materialⁱ, online grooming, the live streaming of abuse, the dissemination of instruction on how to commit offences, and the operation of an online service for the purpose of child sexual abuse. These issues are being addressed in the proposed revision of the criminal law framework (Directive 2011/93/EU).

Recommendations

RECOMMENDATION 1

Propose a harmonised EU-wide access restriction to social media and other digital services for children under 13

A harmonised EU-wide access restriction to social media and other digital services, including AI companions, for children under 13 is necessary. A harmonised access restriction would facilitate the implementation of proportionate and rights-respecting age assurance and encourage safety by design requirements for social media and other digital services providers. Under the age of 13, children should have time-limited access to age-appropriate social media+ environments only with parental authorisation and supervision or in educational contexts. From the age of 13, adolescents should benefit from evolving autonomous use of age-appropriate and safe social media and other digital services.

Harmonised rules on an EU-wide minimum age of 13 would contribute to the proper functioning of the Single Market by ensuring a single compliance framework for providers. Harmonised rules would facilitate enforcement and supervision by regulators at both the national and EU levels. It would also ensure an equal level of protection for all minors online across the EU, regardless of socio-economic, cultural and national contexts.

ⁱ. To ensure greater protection of children's rights, the European Parliament and the Council have agreed in the context of the AI Omnibus to include a prohibition of AI systems that generate non-consensual intimate content and child sexual abuse material. This prohibition will apply as of 2 December 2026.

RECOMMENDATION 2**Introduce effective age-assurance systems to check age and underpin safety-by-design and age-appropriate approaches to protect and empower minors online**

Age-assurance methods – both age verification or age estimation – must be proportionate and uphold minimum requirements, notably concerning the fundamental rights of users, including children’s rights and related safeguards. Any method employed to check age should uphold the highest privacy and data protection standards, and should not lead to the processing of identity documents and biometric data for the purpose of age estimation. Technical standards such as ‘Zero Knowledge Proof’ should be implemented to ensure that both the platform required to assess the age and the age verification provider do not receive any information that can lead to the tracking or identification of the user.

Age-assurance methods should be accurate in determining the age or age groups required and easy and reliable to use in practice, in real-life conditions. Methods should be robust to avoid circumvention and cybersecurity threats, inclusive (and non-discriminatory), and available equally to all who need to use them. Social media and other digital services providers must uphold their obligation to prevent minors from being exposed to risky services or users impersonating children and adolescents.

To enforce an EU-harmonised age restriction in practice, providers will have to be able to rely on clear guidance and criteria on the use of age assurance technologies for the purpose of implementing age restrictions. In addition, users and providers will have to be able to access effective, privacy-preserving, secure, inclusive and user-friendly age verification technologies to enforce it in practice. In this context, EU Age Verification solutions, building on the EU’s Age Verification blueprint, could provide a harmonised, privacy-preserving state-of-the-art and interoperable tool for the enforcement of such obligations at the EU level.

To further strengthen this framework, Member States, as well as market players, need to make available operational age verification tools, which are aligned with or build on the EU Age Verification Blueprint, and follow the Commission Recommendation on establishing a common framework for EU-wide Age Verification technologies. The Commission Recommendation sets out a scheme that will define the requirements for the trust model, governance, and the obligations for providers of age verification solutions and proof-of-age attestations.

Member States should swiftly nominate trusted proof-of-age providers. For effective age verification of minors, they will also need to ensure that under-18 age credentials are provided and/or recognised. This would include ensuring that all minors can access some means to prove their age even without a national ID.

It is important that there is clear legal basis established by the EU for the implementation of age verification solutions to ensure that social media and other digital services providers accept trusted providers of proof-of-age attestations. Age assurance is key for well-functioning complaint systems that empower children and adolescents to seize their rights and to navigate safely online.

RECOMMENDATION 3**Extend and harmonise rules on key safety features in the design of social media and other digital services**

Clear safety by design and age-appropriate safeguards (for example, potential limits on infinite scrolling, autoplay, push notifications, and problematic personalised recommendation engines) should be embedded into social media and other digital services. To tackle addictive design, dark patterns, unsolicited contact and rabbit holes, protective default settings should be an integral part of social media and other digital services. Extending and harmonising rules on key safety features would ensure certainty and uniformity across the social media+ environment. Due to the rapid development of technology, any rules on key safety features should be adaptable to continuously address new harmful design features.

RECOMMENDATION 4**Shift the burden of proof to social media and other digital services providers to demonstrate that their products and services are safe for minors**

Specific age restrictions should apply until key safety design features protecting children and adolescents are introduced by social media and other digital services providers. Until providers have demonstrated safe and age-appropriate features, therefore complying with EU and national measures, they should not have access to minors. Where there is a 'safe by default' version, age-inappropriate features (features for adults) should only be activated following effective age assurances.

RECOMMENDATION 5**Strengthen enforcement and evaluation capacities**

Given the multiple rules now applying to child safety online (the DSA, GDPR, AI Act, etc.), supervisory authorities should intensify cooperation and exchange information across legal frameworks. This is key to avoid inconsistencies and to ensure a coherent, predictable and effective legal environment grounded in the protection of fundamental rights. The European Commission should explore mechanisms enabling seamless cooperation between supervisory authorities to leverage existing enforcement structures. Moreover, there is a need to assess whether additional resources and restructuring are needed for regulators responsible for enforcement and evaluation. Actions should be considered to strengthen the role of civil society in enforcement and their contribution to enforcement capacity, including through existing structures. Enforcement should be complementary and avoid conflicting actions.

RECOMMENDATION 6**Swiftly adopt measures to ensure that social media and other digital services providers have clear obligations to prevent, detect, report and block child sexual abuse online, including in interpersonal communication**

The child safety gap that currently exists due to the expiration of the Interim Regulation laying down rules to prevent and combat child sexual abuse (CSA Interim Regulation) must be quickly filled. EU co-legisla-

tors should swiftly adopt the proposed long-term Regulation to prevent and combat child sexual abuse. More than 80% of child sexual abuse investigations start from reports submitted by social media and other digital services providers. Children are often too afraid to report abuse. Detecting child sexual abuse material, including in interpersonal communication, is often the only way to stop it.

Together with the Recast of the Child Sexual Abuse Directive, recently agreed by the co-legislators, these instruments will strengthen the EU framework against child sexual abuse and exploitation, both online and offline. They will improve prevention, investigation and support for victims. In addition, online platforms should strengthen intra-industry cooperation on serious online crimes affecting children by sharing signals on harmful content and malicious actors. Social media and other digital services providers should strengthen cooperation with the EU Internet Forum to share information on emerging threats and patterns of abuse. This will support early detection and reporting of suspected criminal offences. Moreover, intensified enforcement of child-protective legal frameworks, such as the Victims' rights Directive, or the Directive on Violence against Women and Domestic Violence is needed.

RECOMMENDATION 7

Member States can introduce additional precautionary access restrictions to social media and other digital services as of 13

Additional precautionary access restrictions should be complimentary to the EU-wide access restriction to social media and other digital services under 13. Adolescents can have access only to a social media+ environment that is safe, with respect to content and design features, age-appropriate and designed with their rights and needs in mind. Member States have varied historical and national contexts and may prefer to adopt a higher age threshold than 13. All additional precautionary national access restrictions should be subject to continuous evaluation, and possibly reassessed, once social media and other digital services have been made safe by default for children and adolescents.

RECOMMENDATION 8

Strengthen consumer protection policies to protect children

Consumer protection law plays an important role as a child protection instrument covering all types of traders – e-commerce web shops, subscription-based streaming and digital content and services, video games, and apps – ensuring that no trader interacting with children falls outside the scope of enforceable consumer protection obligations. Protections for children against misleading, aggressive and harmful online marketing practices, including by online influencers, should be strengthened.

The safety net and the rules governing its enforcement should be strengthened to ensure every child interacting with a commercial digital service in the European Union benefits from a baseline level of consumer protection, regardless of the type of service, the type of trader, or the Member State in which the trader is established.

The upcoming Digital Fairness Act and the revision of the Consumer Protection Cooperation (CPC) Regulation are a key opportunity to embed the protection of children and adolescents at the heart of EU consumer law.

RECOMMENDATION 9**Continuously monitor and evaluate the impact of measures being implemented**

All new instruments proposed following the recommendations of this chapter should include data-driven mechanisms and approaches to continuously evaluate their impact and effectiveness. The Commission should also improve the coordination of enforcement efforts and the streamlining of evaluation and monitoring processes specifically concerning child safety online.

Drawing on the model applied to follow the implementation of the Australian social media law (including the continuous integration of knowledge and insights from experts), the establishment of an EU-wide access restriction should be accompanied by a comprehensive evaluation. It should focus on the effectiveness, impacts and adaptations of the minimum age regime, prioritising child participation. This could be achieved by using existing mechanisms such as the EU Children's Participation Platform and Better Internet for Kids (BIK+), and by streamlining research on this matter across the EU and different fields of study, including in the structure research programmes.

These evaluations may rely on ongoing work under the DSA and by the European Centre for Algorithmic Transparency (ECAT). The Centre continuously monitors how the landscape of child safety online evolves in terms of developing trends, affordances and the use of new and emerging technologies. This can provide the basis to establish a system of structured and regular data acquisition from representative samples of minors of relevant age cohorts across the EU.

The main focus of evaluation is the wellbeing of minors. Evaluation frameworks should include developmental outcomes, mental health indicators, well-being measures and resilience outcomes, rather than focusing exclusively on compliance, exposure or use metrics. Child safety policies should ultimately be assessed against their contribution to healthy development.

RECOMMENDATION 10**When processing children's data under the GDPR, social media and other digital services should ensure children's best interests are a primary consideration**

When social media and other digital services, as a controller or processor, are processing children's personal data, they should ensure they are relying on the most appropriate legal basis under the GDPR. Data Protection Authorities assess whether controllers are processing children's data under an appropriate legal basis and that the relevant conditions are met.

If a controller chooses to process a child's personal data on the basis of consent, they should ensure that they have obtained valid consent from the child, and where necessary, the consent of the holder of parental responsibility.

If a controller chooses to rely on legitimate interest as the legal basis for processing children's personal data, they should ensure that all of the requirements of Article 6(1)(f) are satisfied before carrying out the processing. One of these requirements is that the controllers' legitimate interests are not overridden by the interests or fundamental rights and freedoms of the concerned data subject. In this regard, particular attention should be paid when the data subject is a child.

As noted in the European Data Protection Board (EDPB) guidelines on legitimate interest, when conducting this assessment, controllers should consider the extent and intensity of any interference with the child's rights and freedoms. They should take into account the child's reasonable expectations regarding how their personal data will be used. Furthermore, they should demonstrate that the child's best interests were taken into account as a primary consideration and that appropriate safeguards are in place. The best interests of the child should be a primary consideration when balancing the competing interests at stake.

Where a controller's legitimate interests conflict with a child's interests or fundamental rights and freedoms, the child's interests and rights should generally take precedence. If this cannot be ensured, the controller should either find a more appropriate legal basis or not process the child's personal data.

RECOMMENDATION 11

Ensure effective implementation of the Product Liability Directive (PLD)

Originally adopted in 1985, the Directive was updated during the last mandate of the European Commission to reflect significant technological, economic and case law developments. The aim was to guarantee a fair level playing field, bringing legal certainty to businesses, while guaranteeing effective redress for victims. The revised Directive entered into force on 8 December 2024 and must be transposed by Member States by 9 December 2026.

Considering the evolving product liability cases against digital services around the world, it is crucial to ensure the effective and timely transposition and implementation of the PLD. Moreover, regulators should effectively promote to citizens the rights stemming from the PLD (for example, promoting the updated redress mechanisms for individuals seeking to bring a cause of action for the use of a defective product, especially for software).

04

Empowering minors to safely navigate the digital world

The previous chapter examined existing legislation and tools available to the EU and Member States to protect children online, presented results of ongoing enforcement, and identified areas where legislation and tools need strengthening and completing to enhance child safety online.

However, the social media+ world cannot be reduced to risks alone. It is also a space of opportunity, for creativity and participation. This chapter investigates the evidence, albeit limited by comparison, regarding the opportunities presented by minors' use of social media and other digital services. It takes into account contributions from a youth representative, Marta Gonçalves, who took part in the Special Panel meetings and in discussions leading to the formulation of the recommendations by the Co-Chairs.

This chapter continues by reviewing select EU policies and tools promoting the empowerment and participation of minors online. It closes with a series of recommendations on how to support children and their supporting circles (parents and caregivers, teachers and educators) in seizing the opportunities of the online world.

This chapter is grounded in pillars five and six of the Six Guiding Principles presented by the Co-Chairs to steer efforts to strengthen child safety online: empowerment and media education, and children's rights and participation. This analysis takes as a starting point the respective international and EU frameworks on the rights of the child^a.

To be effective, online child protection measures must go hand in hand with actions promoting minors' empowerment and participation. Measures must be age-appropriate for children's and adolescents' evolving capacities and tailored to caregivers' and educators' changing roles along minors' path to adulthood.

Beyond risks, it should be recognised that the digital world also offers children and adolescents many opportunities. When minors are empowered to interact safely online and have solid digital skills, social media and other digital services use could benefit well-being, social connectedness, provide supportive peer networks, opportunities for self-expression, civic engagement and independent learning.

The next section examines potential opportunities related to children's and adolescents' use of social media+. But first, this chapter gives the floor to the voice of a youth representative.

^a. Notably, the United Nations Convention on the Rights of the Child and the general comments of the Committee on the Rights of the Child, the Charter of Fundamental Rights of the European Union, and the EU Strategy on the Rights of the Child.

Shaping a better digital world

A CALL TO ACTION BY MARTA GONÇALVES,

BETTER INTERNET FOR KIDS+ AMBASSADOR FROM PORTUGAL

I grew up in a world where the internet was never separate from everyday life. For my generation, being online is not an occasional activity. The digital space is where we learn, create, communicate, build friendships, discover opportunities and develop our identities. This is why empowering children and young people to use social media and other digital technologies safely is not simply about protecting them from harm. It is about enabling them to fully participate in the world they are growing up in.

Too often, discussions about children's digital lives happen without children themselves. Governments, companies, educators and adults make decisions on behalf of young people while rarely asking those most affected what they actually need. This is not only unfair, it is counterproductive. We cannot build better digital environments by guessing children's experiences.

Through my own work in peer counselling and youth representation, I have seen the incredible potential of young people when they are trusted and given responsibility. Children and teenagers can accomplish remarkable things through their creativity, empathy, determination and willingness to help one another. When young people come together, they do not simply consume technology. They use it to learn, create, solve problems and build communities. They become role models for their peers in ways that adults cannot.

Young people are experts in their own realities. They know the opportunities they value, the challenges they face and the solutions that would genuinely make a difference. Meaningful youth participation should not be treated as a symbolic exercise, but recognised as an essential part of designing digital policies, platforms and services that truly work.

The Special Panel process offered a powerful example of what meaningful youth participation can look like. Throughout the three meetings, children and young representatives were fully integrated into the discussions, participating alongside other experts, contributing their perspectives and sharing the concerns that mattered most to them.

Moreover, I also had the opportunity to be involved in the drafting of the report itself, to write sections and provide input throughout the development of the recommendations. I was not merely consulted, I was meaningfully integrated into the process and contributed with my knowledge and experience, as reflected in this chapter (see, for example, the section on peer counselling). Taking part in the discussions where decisions were shaped, exchanging arguments, listening to different perspectives and gaining new insights reinforced the value of involving young people throughout the process and in recognising their lived experiences as expertise.

Although the Special Panel's primary focus was on developing an approach to keep children safe online, I was equally committed to contribute to highlighting the opportunities offered by the digital world.

The online world has opened doors that previous generations could hardly imagine. It allows children to learn new languages, how to play musical instruments, to discover scientific topics, develop artistic skills, explore new cultures and connect with people who share their passions, regardless of geography. For many young people, especially those who may feel isolated in their local communities, digital spaces become places where they find belonging, inspiration and confidence. The internet can create opportunities that shape lives, but only if children are given the knowledge and support to navigate it safely.

Experience has also taught me that informed children are empowered children. When young people understand how digital platforms work, how to protect their privacy, how to identify manipulation, misinformation or harmful behaviour, they become more confident in recognising when something is not right. They are better equipped to seek help, support friends and contribute to safer online communities. Digital literacy is not about teaching children to fear technologies. It is about giving them the confidence and knowledge to use it critically, responsibly and positively.

Knowledge is one of the most powerful tools we can give a child. Information enables informed decisions, builds resilience and creates independence. Every child deserves access to clear, age-appropriate guidance that helps them understand both the opportunities and the risks of the digital world. The more we invest in education, participation and digital literacy, the more we empower young people to protect themselves and others online.

The future of the digital world will be shaped by today's children. They are not simply future citizens, they are already active participants whose voices, ideas and experience matter. If we empower them today, they will not only navigate the digital world. They will redefine it for the better.



Marta Gonçalves

*Better Internet for Kids+
Ambassador, Portugal*

Marta Gonçalves

Opportunities for minors in the digital world

CONNECTION AND SELF-EXPRESSION

As already alluded to in chapter 2, many children and adolescents use social media+ to connect, interact and share their interests with others online – and evidence underlines these findings²⁹⁰.

Social media+ may also enable adolescents to share their interests with peers online, to nurture friendships initiated offline, and to stay in contact with close friends and family living far away²⁹¹.

More broadly, the use of social media and other digital services can allow adolescents to share entertainment together and to reflect on common experiences online, with research hinting at potential benefits for adolescents' mood and well-being²⁹².

Social media+ may also provide spaces for adolescents to express themselves and explore their identity²⁹³. Research suggests that online spaces may offer perceived 'lower-stakes' environments for selective self-disclosure²⁹⁴. Moreover, some minors may use private social accounts in ways similar to offline journals²⁹⁵.

Adolescents increasingly use social media+ in particular as a creative outlet. A 2022 survey of 1,316 US teenagers found that 71% viewed social media as a space to express their creativity²⁹⁶. However, such uses may expose adolescents to harm.

In short, the potential benefits of minors' use of social media and other digital services for connection and self-expression must be weighed by supporting circles against the risks for children's and adolescents' safety, health and well-being. This includes risks of unwanted contact and exposure to age-inappropriate content online, in particular grooming and child sexual abuse.

Maintaining open conversations with minors about their experiences online is key to ensure children and adolescents feel comfortable to report to parents or caregivers, in particular, unwanted contact or experiences. In addition, caregivers and educators need to be equipped with the skills to supervise (and where necessary, restrict) minors' use of social media+, and to know where to turn to get professional help when needed.

"There is a desperate need for an autonomy-based approach to young people. Kids are restricted from all sides by anxious parents, and social media is an escape from that. Youth need to be involved in decisions and discussion about online spaces because only then will they follow the regulations, and be empowered through resilience, in having critical reception and self-management skills for the unpredictable digital future."

— ZUZANNA,
17-YEAR-OLD REPRESENTATIVE OF THE EU
CHILDREN'S PARTICIPATION PLATFORM

SUPPORT AND INFORMATION

Many adolescents use social media and other digital services to seek support with issues they are experiencing online. Some research suggests that adolescents' use of social media+ may foster open conversations and allow them to find help online²⁹⁷.

An idea which is commonly expressed among minors is that online spaces offer 'safe' alternatives for self-expression or more approachable sources of support compared to 'traditional' options, including talking to parents or counsellors²⁹⁸.

As explored in chapter 2, adolescents with good self-esteem and offline friendships may succeed in reinforcing offline relationships and finding support online. However, for those with lower self-esteem and weaker social networks offline, social media+ environments may increase adolescents' exposure to unwanted contact and age-inappropriate content.

Vulnerable minors, including those belonging to LGBTIQ+ communities, with special educational needs, experiencing mental health issues, eating disorders or self-harming may be especially inclined to use social media and other digital services to connect with others having similar experiences or to seek support.

Limited research indicates that some adolescents may find comfort concerning issues they are experiencing not only through direct interaction online, but also from the knowledge that others are having similar experiences²⁹⁹.

However, minors' use of social media+ to seek support may expose already vulnerable individuals to harms, such as cyberbullying and social exclusion, with potential negative consequences for their health and well-being.

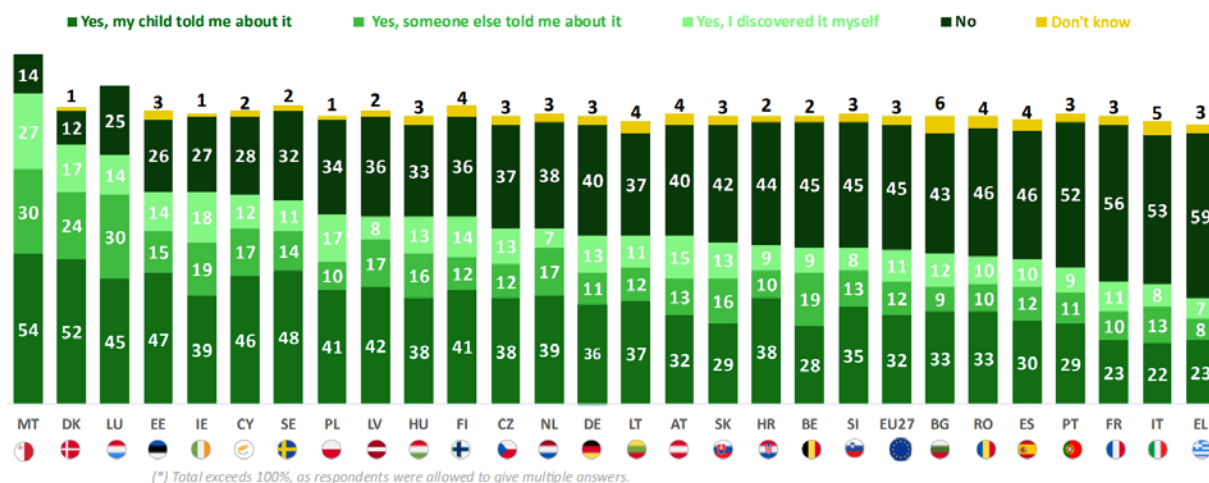
With the right safeguards in place, social media+ spaces may be able to offer support to minors. Managed online discussion forums moderated by healthcare professionals, for example, might present an alternative to those seeking help or information on social media+ platforms.

Some evidence indicates that engagement with this type of forum can help adolescents to overcome reluctance in seeking professional help in 'traditional' forms³⁰⁰. This may also help to address problems related to the spread of disinformation and misinformation online, for instance concerning medical issues.

Caregivers, educators and public services (including mental health and sexual healthcare providers) should reflect on how best to inform and support minors to safely use social media and other digital services as a source of information or support.

Figure 1: Family awareness of minors' negative experiences online

Question: *Has your child ever come to you, or have you ever discovered, that your child had a negative experience online?*



Source: European Commission (2026). *Impact of excessive screen time and social media on young people's mental health – June 2026 – Eurobarometer survey.*

LEARNING AND SKILLS DEVELOPMENT

Studies on the use of digital tools for learning suggest that the use of digital tools and services may have a small to moderate positive effect on children's learning outcomes at secondary school level³⁰¹.

Digital technologies provide teachers and pupils with additional opportunities for teaching and learning, and appear to be most effective when used to complement, rather than replace traditional instruction³⁰².

In subjects such as science, mathematics and languages, digital technologies can enrich learning through interactive experiences. This includes simulations, modelling, animations, digital games, multimedia resources and sound effects. These approaches can increase student engagement and help to make abstract or complex concepts more accessible and understandable³⁰³.

Digital tools and services can also support personalised learning. By allowing pupils to progress at their own pace and explore topics from different angles, they introduce greater flexibility into the learning process. This can enhance motivation, in particular for students who benefit from repeated practice or self-directed inquiry³⁰⁴.

AI-based technologies are an additional tool that can support individualised instruction. These tools allow teachers the chance to adjust methods according to students' performance, to provide timely feedback and adaptation, and to tailor individualised support accordingly³⁰⁵.

Research indicates that the use of generative AI has become embedded in many students' academic routines³⁰⁶. While students acknowledge the risks for their learning and cognitive development, they tend to focus on the potential opportunities³⁰⁷, for example time saved using an AI tool.

The use of learning platforms in schools may allow primary and secondary school students access to a wider variety of quality learning resources, enabling independent learning, as well as the possibility for self-review and review by their peers³⁰⁸.

These opportunities need to be balanced against risks, including digital devices' potential to distract children and adolescents from learning, physical risks (for instance, concerning minors' vision), and regarding the 'overdigitalisation' of education.

The impact of AI tools on children's and adolescents' education and skills development need to be more extensively analysed to understand potential benefits and risks, as discussed in chapter 2. Similarly, more evidence is needed concerning the potential positive effects of social media+ use in educational settings.

Digital education, including media and AI literacy, is vital to empower children and adolescents to navigate the online world safely. The main question is how to practically integrate the acquisition of digital skills and literacy into education curricula in ways that are beneficial to minors' overall learning and development.

Cultures and attitudes concerning the use of digital devices and tools in learning environments vary widely at the national level across the EU. However, there is broad recognition of the importance of enhancing minors', caregivers' and educators' competencies, of providing safe, age-appropriate tools for learning, and of the need to mainstream the concept of digital well-being in schools.

"Young people need clear rights, understandable information, effective reporting tools, and a real voice in shaping the digital spaces they use every day. The internet is not only a place of risk. For many young people, it is also a place of learning, connection, creativity, and support. So instead of banning or restricting, make it a place of inspiration, safe for everyone. That is why my message is simple: build the internet with us, not just for us."

— AYATA,
15-YEAR-OLD REPRESENTATIVE OF THE EU
CHILDREN'S PARTICIPATION PLATFORM

SMARTPHONE RESTRICTIONS IN SCHOOLS

Mobile phones have become omnipresent in the lives of children and adolescents across Europe. As explored in chapter 1, minors' use of smartphones at school can distract from learning, threaten academic performance, reduce social interaction, and at the same time increase the risks of harms, such as cyberbullying and social exclusion.

For adolescents, smartphone use may increase the risk of experiencing mental health issues, including anxiety and depression. More broadly, minors' use of smartphones in the classroom may subject teachers to 'surveillance anxiety' and extra stress related to the need to police device use.

These identified risks have sparked debates in EU Member States and beyond about whether to ban children's and adolescents' use of smartphones at school. Proposed measures range from total bans during school hours, to more nuanced restriction policies involving conditional or supervised use.

As of late 2025, the majority of EU Member States had implemented, or were planning to implement, some form of restriction on mobile phones in schools. Measures range from total bans during the school day (Austria, Belgium, Cyprus, France, Hungary, Portugal, and Slovenia) often involving mandatory device collection, to classroom-only restrictions that leave broader actions to school discretion (Netherlands, Romania, and Slovakia). Some countries (Bulgaria and Sweden) are transitioning from advisory frameworks to legally binding rules.

Full-day bans are the most common solution, but enforcement varies (for example, in Sweden there was an 80% positive response, while 20% struggled to implement bans) ³⁰⁹.

Identified challenges and unintended consequences of restrictive measures include strain on non-teaching staff to collect devices, substitution effects (minors substituting their use of smartphones, for example with tablets or laptops), the displacement of cyberbullying to out-of-school hours, and overcompensation of smartphone use during evenings.

EU policies and tools

Having examined the opportunities for children's and adolescents' use of social media and other digital services balanced in light of the risks these activities pose to minors' health and well-being, the next section presents select EU policies and tools promoting the empowerment and participation of minors online.

The analysis focuses on policies and tools which the Co-Chairs consider can be complemented or completed with further actions.

EU STRATEGY ON THE RIGHTS OF THE CHILD

The European Commission adopted the EU Strategy on the Rights of the Child in 2021 as a comprehensive policy framework to uphold children's rights across EU policies and to ensure that vulnerable children have secure access to basic services.

The Strategy is structured around six pillars:

1. Child participation in political and democratic life, including the EU Children's Participation Platform;
2. Socioeconomic inclusion, health and education, including the European Child Guarantee;
3. Combating violence against children and ensuring child protection;
4. Child-friendly justice;
5. Digital environment;
6. Global dimension.

The digital pillar, which committed to continued support for the Safer Internet Centres and Better Internet for Kids, ensures that children can enjoy safe digital environments and equal access to digital tools.

The Strategy invited EU Member States to ensure effective equal access to digital tools, to support media literacy actions through education, to develop children's ability to critically evaluate online content, and to detect disinformation and abusive material.

In addition, it invites Member States to promote and support the EU co-funded Safer Internet Centres, child helplines, and reporting hotlines. Finally, the Strategy invites EU Member States to encourage children's (especially girls') participation in science, technology, engineering and mathematics (STEM) education.

In the EU Strategy on the Rights of the Child, the European Commission invites ICT companies to:

- // Ensure that children's rights, including privacy, personal data protection, and access to age-appropriate content, are included in digital products and services by design and by default, including for children with disabilities;
- // Equip children and parents with adequate tools to control their screen time and behaviour, and to protect them from the effects of overuse and addiction to online products;
- // Strengthen measures to help tackle harmful content and inappropriate commercial communication, for example through easy-to-use reporting and blocking channels or effective age-verification tools;
- // Continue their efforts to detect, report and remove illegal online content, including child sexual abuse, from their platforms and services to the extent that those practices are lawful.

BETTER INTERNET FOR KIDS

The European Commission works directly with children, together with experts, parents, caregivers, teachers and other relevant stakeholders, to ensure that diverse perspectives are taken into account in the development and implementation of policies related to the digital environment.

The Better Internet for Kids (BIK+) Strategy provides a comprehensive framework aiming to protect, empower and respect minors online, including the most vulnerable. The Strategy supports the implementation of the EU's legislative instruments in this area by complementing obligations with awareness raising, capacity building, and support measures.

The Better Internet for Kids platform offers a comprehensive collection of educational resources designed to support children and young people in developing the digital skills necessary to participate safely, responsibly, and confidently in online environments.

The platform adopts a multi-stakeholder approach offering dedicated learning corners for children and young people, parents and caregivers, and teachers and educators. This reflects the role of caregivers and educators as part of children's and adolescents' supporting circles in supervising and guiding minors' social media+ use.

Children's Corner

The Children's Corner of the Better Internet for Kids platform is designed to empower children and young people to navigate the digital world by providing a variety of engaging and interactive learning materials. These include educational games that strengthen knowledge and awareness concerning child safety online, responsible online behaviour, and the prevention of internet overuse and abuse.

The Children's Corner also provides learning materials introducing children to the work of the EU and opportunities for civic engagement through initiatives, such as the EU Children's Participation Platform (explored later in this chapter).

Parent Corner

The Better Internet for Kids platform's Parent Corner supports parents, caregivers and adults with responsibility for children by providing practical guidance and evidence-based educational resources on a range of issues associated with children's online experiences.

Dedicated sections address topics, such as parental supervision tools, online gaming, and managing screen time. In addition, the platform offers a series of learning modules and deep-dive sessions intended to strengthen parents' understanding of both the risks and opportunities presented by social media and digital technologies.

Core training modules cover subjects including cybersecurity, tackling gender-based violence online, online gaming, manipulative marketing practices in games, understanding misinformation and disinformation, sexting, cyberbullying, and the role of parents in supporting and educating children in the digital world.

Each module incorporates explanatory content, suggested activities, and supplementary resources to facilitate self-paced learning.

Teacher Corner

Finally, the Teacher Corner provides teachers, educators and other professionals working with children and young people with a range of educational resources designed to enhance their capacity to address child safety online and digital citizenship within educational settings.

Introductory learning modules focus on foundational aspects of child safety online and educators' responsibilities in supporting children and young people. They address themes, such as key online safety risks, the teaching of media literacy and digital citizenship in primary and secondary schools, the implementation of whole-of-school approaches to child safety online, and children's rights in the digital world.

SAFER INTERNET CENTRES

At the heart of the Better Internet for Kids (BIK+) strategy is a network of Safer Internet Centres, co-funded by the EU.

In 2025 alone, the Safer Internet Centres reached more than 46.4 million Europeans, organised 448,000 school visits and trainings, and handled over 57,000 contacts via the Insafe helplines³¹⁰.

The network is also the promoter, together with the European Commission, of the annual Safer Internet Day, the worldwide campaign celebrated each year in February to raise awareness about online safety.

The Safer Internet Centres provide a range of services addressing both prevention and support. They offer training sessions and public-friendly material for families and schools aiming to strengthen digital literacy and to promote responsible online behaviour.

Many Safer Internet Centres across Europe have now been designated as ‘trusted flaggers’ under the DSA, reinforcing the protection of minors online by enabling the prioritised reporting of illegal content affecting children and young people. The Centres play a crucial role in informing Digital Services Coordinators about risks affecting children and young people, supporting the enforcement of the DSA³¹¹.

The Centres also operate helplines, which provide direct support to children and families facing online risks, including cyberbullying, and hotlines which enable the anonymous reporting of suspected child sexual abuse material.

The Safer Internet Centres carry out awareness-raising campaigns at the national and the European levels promoting child safety and empowerment online. This includes targeted initiatives, such as ‘DSA for YOUTH’, which explains the EU Digital Services Act (DSA) and its guidelines on the protection of minors in an accessible way to young people.

More broadly, awareness campaigns help to inform children, caregivers and educators about online risks for minors and safe practices. This includes through initiatives addressing exposure to digital devices during early childhood.

DIGITAL EDUCATION AND LITERACY

EU Member States are responsible for the organisation of national education and training systems, school curricula, and the delivery of education and training. The EU supports Member States’ collaboration and exchange of good practices, and provides funding support for education and training initiatives through EU programmes, including Erasmus+.

In March 2025, the European Commission adopted the Union of Skills strategy. The Union of Skills aims to strengthen the attainment of basic and advanced skills, including digital skills, across the EU by promoting continued lifelong learning. A cornerstone of the strategy is the Action Plan on Basic Skills, which seeks to address shortfalls in basic skills attainment, including digital and citizenship skills^b.

Findings from the 2023 International Computer and Information Literacy Study (ICILS) indicate that 42.5% of 13 to 14-year-olds lack basic information and computer literacy skills³¹². Socioeconomic background is a

b. Citizenship skills refer to the ability to act responsibly and to participate fully in civic life, and to skills such as critical thinking (relevant to engage constructively with artificial intelligence) and media literacy.

strong predictor of computer and information literacy. The underachievement rate of pupils with at least one parent having completed university education is 16 percentage points lower than of children whose parents have lower-level qualifications (32.4% and 48.6% respectively)³¹³.

Moreover, the latest data from the OECD's Teaching and Learning International Survey (TALIS) shows that only 45.9% of teachers in EU Member States feel prepared to use digital resources and tools for teaching³¹⁴. This evidence highlights the need not only to strengthen pupils' digital skills and literacy, but also teachers' and educators' skills through improved initial and continued teacher training to help protect and empower children and adolescents online.

At the EU level, the European Education Area initiative promotes the development of a 'whole-system, whole-school approach' to address mental health and well-being in schools, and to build positive learning environments. EU Member States have recognised the importance of supporting parents, schools and teachers in promoting children's mental health and well-being³¹⁵.

Consultations with parents and caregivers show that parents often feel overwhelmed and that they are 'constantly playing catch-up' with the latest technological developments in the social media+ environment. At the same time, awareness on how to support children when they encounter harmful or illegal content is often limited³¹⁶.

Member States have also stressed the need for social media and other digital services providers to refrain from deploying intentionally addictive design practices targeting children and to promote the age-appropriate design of social media and other digital services³¹⁷.

"Position teacher education as a non-legislative pillar for children's online safety [...] Embed digital education across teacher education programmes in an integrated manner and empower teachers to work effectively with parents."

— LOUISE HEERAN FLYNN,
ASSISTANT PROFESSOR IN TEACHER
EDUCATION, TRINITY COLLEGE DUBLIN

DIGITAL EDUCATION ACTION PLAN

Digital education and literacy are fundamental to equip children and adolescents with the skills they need to safely navigate the online world. However, children's and adolescents' digital skills and literacy are lagging behind the pace of technological change in the social media+ environment, contrary to the idea that minors today are 'digital natives'.

Embedding digital skills and literacy in national education systems is crucial. According to a 2025 Eurobarometer survey, 92% of Europeans agree that digital skills should be taught to everyone at all levels of education and that schools should teach students how to manage the impact of digital technologies (including social media) on their mental and physical health³¹⁸.

To support EU Member States in delivering high-quality, inclusive and accessible digital education, the European Commission is delivering the Digital Education Action Plan (2021-2027). The Plan enables EU Member States to adapt their education systems to rapid technological change and the increasing importance of digital skills.

The Digital Education Action Plan's two main strategic priorities are building a strong European digital education ecosystem and enhancing digital skills and competencies. Concretely, the Plan supports the improvement of digital learning infrastructure and environments, internet connectivity and digital equipment in schools, the provision of high-quality digital learning content and platforms, and teachers' training in the use of digital tools and pedagogies.

As part of the Digital Education Action Plan, in March 2026 the Commission published four sets of guidelines³¹⁹ supporting teachers and educators on issues, including tackling disinformation and promoting digital literacy, the ethical use of AI and data in education, high-quality digital education content, and teaching informatics.

The guidelines for teachers and educators on tackling disinformation and promoting digital literacy through education and training offer resources on informed and safe social media use, generative AI, pre-bunking^c, and provide lesson plans for teachers to address cyberbullying alongside topics like gender stereotypes and deepfakes³²⁰.

Under the Digital Education Action Plan, the European Digital Education Hub provides an online community bringing together educators, policymakers, researchers and other stakeholders. Using the Hub, they share knowledge and good practices, and co-create digital education solutions. The Hub also supports teachers and educators in connecting and participating in activities, such as peer learning, on digital education.

Moreover, the Erasmus+ and European Solidarity Corps programmes, and the European School Education Platform (ESEP) and the eTwinning community offer additional support to empower minors and educators online. This includes opportunities for non-formal learning and engagement, and support for spaces where school communities can interact, grow, and develop their skills.

At the end of 2026, the European Commission will launch an Education package. The package will support the futureproofing of national education ecosystems by addressing structural challenges, including the need for safe, sovereign and trustworthy European digital education infrastructure. The package will help to equip children and adolescents with essential skills to engage constructively with AI and digital technologies by striving to embed digital well-being and literacy, and online safety in national education systems.

c. Pre-bunking is a preventative measure that aims to prepare audiences to recognise and resist information risks, including misinformation and disinformation.

‘AI≠HUMAN CAMPAIGN – TALK TO A PERSON’

Awareness-raising initiatives at the national level, including the ‘AI ≠ Human – Talk to a person’ campaign, illustrate the importance of supporting children and adolescents in understanding the nature and limitations of AI-based tools, including chatbots, and how to use these tools in critical and responsible ways.

Such initiatives convey a clear message to children and adolescents: while artificial intelligence can be a useful tool when used with the right safeguards, it cannot replace human relationships.

The campaign took place in spring 2026 and was developed by Luxembourg’s Ministry of Education, Children and Youth, in collaboration with the ‘BEE SECURE’ Safer Internet Centre, the Psycho-Social and School Support Centre (CePAS), and the Luxembourgish student association (CNEL).

It drew attention to a number of potential risks associated with uncritical or excessive use of AI. These include the possibility of increased social isolation, the use of AI as a substitute for human interaction, and a decline in real dialogue and face-to-face communication.

Moreover, the campaign highlights concerns related to ‘cognitive offloading’, referring to situations in which users increasingly rely on AI systems to structure thoughts, to generate responses or make decisions. This can potentially reduce opportunities for independent reflection and active cognitive engagement. The campaign also underscores issues around data protection and privacy concerning the use of AI.

AI LITERACY FRAMEWORK

In June 2026, the OECD and the European Commission presented an AI Literacy Framework for Primary and Secondary Education³²¹. The initiative promotes common approaches to the development of AI literacy in national education systems.

The framework supports teachers, education systems and schools in equipping children with the competencies they need to understand and engage critically with AI. It aims to enable children to interact safely with, to manage and shape the development of AI, and to critically evaluate the opportunities and risks these tools present.

CHILD PARTICIPATION

Children and adolescents must be given meaningful opportunities to participate in democratic life and be systematically involved in decisions that affect their daily lives. This includes the design and implementation of policies promoting the protection and empowerment of minors online.

Meaningful child participation is based on mutual respect, transparency and the voluntary nature of participation. Any participation involving children should provide clear and age-appropriate information about the objectives and process concerning their participation and outline appropriate safeguards. Minors should be clearly informed about how their input will be used.

Ensuring minors are recognised as stakeholders in decisions shaping their lives is fundamental to uphold their rights, both offline and online. The first pillar of the EU Strategy on the Rights of the Child recognises the importance of children's participation, promoted for example through the EU Children's Participation Platform.

Youth participation actions, including the Youth Check, the Youth Policy Dialogues, the President's Youth Advisory Board, and the EU Youth Dialogue also play an important role in enhancing the involvement of young people in policymaking at the EU level.

By actively involving children and adolescents in discussions about online safety, policymakers not only fulfil legal and ethical obligations, but also harness minors' unique perspectives in protecting and upholding their rights online. Measures should be taken to ensure child participation involves children and adolescents from diverse backgrounds and geographic areas, to ensure the inclusiveness and effectiveness of measures designed to protect and empower minors online.

Moreover, it is crucial that children and adolescents are empowered to be part of making the social media+ space safe. Minors' complaints have to be treated as a priority in content moderation procedures by social media and other digital services providers.

The European Commission's Recommendation on developing and strengthening integrated child protection systems calls on EU Member States to ensure children's participation, for a consistent legal and policy framework for child protection, safe, confidential and child-friendly complaint and reporting mechanisms, and quality family and community-based services and care³²².

EU CHILDREN'S PARTICIPATION PLATFORM

Children have the right to freely express their views and for their views to be taken into account on issues that concern them³²³. To put these rights into practice, the European Commission established the EU Children's Participation Platform.

The EU Children's Participation Platform offers a dedicated space where children under 18 can engage directly with policymakers and decision-makers. The platform provides a safe space for children and adolescents to share their views and to discuss topics that impact them. The platform organises activities, including meetings, workshops, trainings, online and in-person surveys to gather children's views.

Through the EU Children's Participation Platform, the European Commission has consulted thousands of children, including on issues such as cyberbullying, online safety and digital well-being, and the upcoming Digital Fairness Act. This process has resulted in the creation of a 'Call to Action to EU Decision-Makers'³²⁴ addressing matters that matter most to children.

"Efforts to improve child safety online should focus on creating digital environments that are safe and supportive, while preserving children's opportunities to learn, play, participate, communicate and access information."

— ALEXANDRA WEILENMANN,
PROFESSOR OF INTERACTION DESIGN,
UNIVERSITY OF GOTHENBURG

As part of these consultations, children stressed their desire to be actively involved in shaping the rules that affect their activities online. Many also made clear that adults – not children – are responsible for how the online world and social media+ have been designed and operate today, and that children should not be ‘punished’ for its failings.

Children’s message is clear: they want the online world to be safer, fairer and easier to understand, with stronger rules where online services may be unfair, harmful or addictive. They also called for alternatives to social media+, including afterschool activities and sport, and for decision-makers to address well-being and mental health issues related to children’s use of social media.

RECOMMENDATIONS FROM CHILDREN

From 16 to 18 April 2026, 20 children and young people from different EU Member States met in Berlin for the EU Children’s Participation Platform’s study visit on well-being and mental health.

Over two days, they shared, learned, and put together recommendations on how children can feel safe, supported, respected and listened to concerning mental health issues, and how adults, schools, families and services can better support children’s well-being.

As part of the study visit, children made several recommendations about what they need to strengthen their well-being:

- // We should have the freedom to stay in or to leave a conversation, have a safe space to speak up, and know who to talk to;
- // We need stable and reliable support systems, structures to be heard, and a community we can rely on;
- // We should have access to ‘emotional outlets’: exercise and sport, hobbies, journaling, relaxation, safe spaces to play and be active;
- // Schools should normalise mental health conversations and introduce regular days to address mental well-being. Safe environments should be created where we feel comfortable discussing our mental health and teachers should be trained in providing mental health support, just as they are in first aid. Every school should have a trained psychologist or counsellor who is genuinely accessible and trusted by students;
- // We need clear, open and effective communication with adults;
- // We need clear signposting to identify which adults we can approach for help in different settings and for different issues;
- // Health topics must be sufficiently covered in schools, so we don’t need to use online spaces to fill gaps^d.

d. In Bulgaria, as an example, children reported receiving information about health topics mainly through AI tools.

Peer counselling

Peer counselling can play an important role in promoting both online and offline well-being among children and adolescents by creating a supportive environment to discuss challenges with trained peers. As children often find it easier to confide in someone close to their own age, peer counselling can encourage early help-seeking and help to prevent issues from escalating, as well as ensuring there is a safe space offline for them to connect and form meaningful bonds based on shared experiences.

In the context of child safety online, peer counsellors can help to raise awareness of risks including cyber-bullying, healthy screen and social media+ use, misinformation and disinformation, artificial intelligence, and the importance of protecting personal data.

Peer counsellors can encourage positive digital behaviours, including respectful communication, empathy, critical thinking, and responsible online participation.

As support comes from peers of a comparable age sharing similar experiences, peer counselling is often perceived as more relatable and credible, and less formal or intimidating for children and adolescents to engage with. It can foster a sense of belonging, inclusion and mutual support within schools or communities, empowering minors to play an active role in supporting each other in having safe online experiences.

“Real online safety goes beyond regulation. It requires digital literacy, accessible support, and investment in offline spaces.”

— MARTINA TÓTHOVÁ,
PRESIDENT'S YOUTH ADVISORY BOARD,
YOUTH COUNCIL OF SLOVAKIA

BEST PRACTICE EXAMPLES OF PEER COUNSELLING

The International Federation of the Red Cross and Red Crescent Societies (IFRC) Reference Centre for Psychosocial Support developed the **‘Psychological First Aid for Young Peers’** toolkit to help young people to support their peers during difficult times³²⁵.

This toolkit empowers young people by equipping them with the skills and knowledge needed to help their peers, while also raising awareness about the importance of self-care³²⁶. The overarching objective of the toolkit is to strengthen young people’s resilience when encountering adversity and crisis events, and to equip them with knowledge and skills in psychological first aid³²⁷. It includes a handbook that introduces the concept of psychological first aid and offers practical examples of how young people can apply it to help their peers³²⁸.

The toolkit also provides a training package for schools, youth and sports clubs and scouts organisations. Participants learn about which challenges affect people of their age, crisis events and reactions, to apply the core principles of psychological first aid, and self-care practices³²⁹. Participants also learn to recognise when someone may need assistance beyond what they can provide³³⁰.

Another good practice example is the Portuguese **‘Líderes Digitais’** (Digital Leaders) initiative, developed by the SeguraNet Awareness Centre³³¹. Through a peer-to-peer approach, the initiative empowers students to act as digital ambassadors within their schools.

Participating students receive training on topics such as digital citizenship, online safety, cyberbullying, privacy and data protection, misinformation, media literacy and the responsible use of emerging technologies, including artificial intelligence. They then share this knowledge with their peers through awareness-raising activities, workshops, classroom discussions and informal support, contributing to a safer and more positive digital culture within the school community.

Peer-led initiatives, such as ‘Líderes Digitais’, demonstrate how children can play an active role in promoting online well-being and digital resilience. By encouraging dialogue between peers, these initiatives foster positive digital behaviours, including respectful online communication, critical thinking, empathy and responsible participation in digital environments, while strengthening children’s sense of belonging and mutual support.

The long-term success and scalability of peer counselling initiatives, however, depend on sustained funding and institutional support to ensure continuity and enable more schools and children to benefit from these initiatives. It is therefore imperative to recognise their value and invest in their continued development, given their significant contribution to children’s online safety and well-being.

Recommendations

RECOMMENDATION 1

Expand safe opportunities for children to actively participate in shaping the social media+ environment

Children and adolescents should have meaningful opportunities to actively shape legislation, policies, and educational initiatives promoting child safety and empowerment online. The use of the child and youth participation tools to inform this work should be expanded. More specifically, children should be included in the co-design of safety policies, training programmes, evaluations and guidelines. Measures should be continuously monitored and evaluated to assess their impact on children's safety and rights.

Participation processes should ensure that children receive clear information, understand how their contributions will be used, and receive feedback on outcomes. Special efforts should be made to include children from disadvantaged, marginalised, and vulnerable groups. Appropriate safeguarding measures should accompany all participation activities involving children.

RECOMMENDATION 2

Strengthen complaint and reporting mechanisms and consumer rights for children and adolescents

Reports and complaints by children and adolescents should be treated as a priority in content moderation procedures by social media and other digital services providers. Providers' obligations under existing frameworks need to be strengthened to appropriately fund helplines and complaint mechanisms. These mechanisms must be age-appropriate, user-friendly, accessible, privacy-preserving, and effective.

RECOMMENDATION 3

Fund and promote the establishment and use of EU-values-based social media and other digital services where minors can safely interact with each other

Support with public investment the establishment and mainstreaming of EU-values-based, safe-by-design and age-appropriate social media and other digital services. Such services should ensure the availability of trustworthy information where children and adolescents (but also adults) are empowered to have safe online interactions without being exposed to harmful features.

RECOMMENDATION 4**Mainstream digital education and literacy actions for minors, parents and caregivers, teachers and educators**

Digital education and literacy should be embedded at all levels of education as a key basic skill for minors, parents and teachers. Digital well-being should be integrated into digital education for all.

Education should enable children and adolescents to critically evaluate online information and sources, and to recognise manipulation techniques, including disinformation, deepfakes and targeted advertising. It should also build an understanding among minors, parents and teachers of how digital content is created and shared, and how algorithms shape what users see and experience in the social media+ world.

Structured online safety education should build practical skills in protecting personal data, managing privacy settings, maintaining secure digital identities, and identifying risks on social media+, messaging and gaming environments in particular. These skills should be developed progressively, beginning with basic safety habits and advancing to more complex understanding of digital footprints, consent, and platform risks. Healthy screen use should be addressed through guidance on balance, attention management, and recognising excessive or harmful patterns of use.

Safer Internet Centres should continue to play a key role in delivering training, awareness-raising activities, resources and support for children, parents, caregivers and teachers. The development of easily accessible online courses for parents, teachers and young users should be funded.

Alongside safety, education should emphasise opportunities and empowerment: how students can use digital tools for learning, creativity, collaboration, and civic participation.

RECOMMENDATION 5**Create more opportunities and adequate infrastructure to support offline activities**

Member States and local authorities should maintain and expand access to affordable sport, arts, youth clubs, libraries, and community spaces to encourage healthy offline engagement and create attractive alternatives to excessive screen use among minors. This should include investment in safe, inclusive and age-appropriate environments where minors can connect, learn, play and build positive relationships within their communities.

RECOMMENDATION 6**Promote the co-creation of Guidelines for Parents**

Together with Parents' Associations, the EU and Member States should promote the development of a Guidelines for Parents. The Guidelines could provide clear, accessible advice to empower parents and caregivers in supporting minors' safe, responsible and positive engagement with social media+ environments. The Guidelines should provide practical advice on key areas, including online safety and privacy, digital well-being, ethical and responsible use, and access to support.

RECOMMENDATION 7**Ensure parents and carers are continuously supported by state-of-the art and up-to-date control and supervision tools**

Efforts to empower minors should be complemented by continuous support for parents and carers, not only concerning digital skills and literacy, but also tools equipping carers to guide minors' use of social media and other digital services, without disproportionately restricting children's rights. This includes making available and raising awareness of practical parental supervision tools, complemented by reliable information on risks, safe practices, and how to engage with children. Awareness-raising with parents should take place face-to-face (for example, in meetings with teachers at school, during paediatric visits, pregnancy or parental leave).

Parental supervision tools should be effective, easy-to-use, interoperable and age-appropriate, in line with the evolving capacities of minors, as well as designed to foster communication, learning and empowerment rather than control. This is key to promoting minor's gradual path to autonomous social media+ use. These tools should ensure changes can only be made with the same degree of authorisation required for their activation, apply regardless of the device or operating system, and include safeguards informing minors against potential misuse by parents (for instance, clear notice for minors when supervision tools are activated).

RECOMMENDATION 8**Ensure sufficient public funding and common standards for civil society organisations and peer counselling**

The EU and Member States should ensure that the Safer Internet Centres and comparable civil society organisations continue to receive sufficient financial resources and that their work is based on common standards, developed by experts. This is vital to maintain and further develop their activities, including awareness-raising, training and support services. Public funding is crucial to guarantee independence and cohesion.

Funding should also support the further development of peer counselling, helplines, hotlines, educational resources, awareness-raising campaigns and capacity-building activities. Additional investment should be directed to increase the visibility, accessibility and reach of these facilities, including among vulnerable minors, and to support initiatives promoting safer social media+ environments.

RECOMMENDATION 9**Enable the health system to diagnose and treat addictions and other mental health disorders related to the use of social media and other digital services**

Health systems should implement diagnostic ICD-11 standards for behavioural addictions, including gaming disorder and compulsive social media+ use. Evidence-based treatment of these disorders should be made accessible within the healthcare system. Medical professionals and psychotherapists should be aware of potential consequences of harm caused by 'digital neglect' and involuntary confrontation with age-inappropriate content, cyberbullying, online grooming, sextortion and other harms.

Evidence-based treatments for PTSD and other psychopathological consequences should be provided by healthcare systems. Moreover, systems could integrate digital risk assessment into paediatric screening, and selective prevention approaches for vulnerable minors. Prevention and behavioural challenges, including ‘online fasting’ or ‘digital detox’, could promote offline experiences and a change in culture concerning minors’ online use.

RECOMMENDATION 10

Support teachers’ training to include digital and media literacy and involve parents

The EU and Member States should ensure that initial and continuous teacher education systematically integrates digital skills and literacy, including AI literacy, and digital well-being. Teachers must be equipped to develop children and adolescents’ critical and media literacy alongside digital skills competence for safe social media+ use.

Teachers should be made aware of the risk of ‘overdigitalisation’ in schools. New digital tools, such as AI, should be used for specific pedagogical purposes, where appropriate. Teacher education should also include close collaboration with parents to better support minors’ healthy and balanced screen use, understand how children and adolescents interact with social media and other digital services, and develop age-appropriate strategies for discussing online risks and experiences in the classroom and at home.

RECOMMENDATION 11

Promote AI literacy as an integral part of digital education

AI literacy should be incorporated into digital education in schools and other education and training institutions. Minors should understand the opportunities, limitations and risks associated with AI technologies (i.e. AI chatbots/companions, recommendation systems, and generative AI), including the possibility of inaccurate information, manipulation, and synthetic content.

Promoting literacy could be inspired by the AI Literacy Framework for Primary and Secondary Education developed by the European Commission and the OECD. Minors should not be exposed to anthropomorphic AI companions that imply human-like relationships without supervision.

RECOMMENDATION 12

Schools should provide structured opportunities to improve mental health and digital well-being

Schools must play a proactive role in mitigating social media+ risks and support children and adolescents’ mental health and well-being. Schools should organise information and training opportunities for parents, and with minors and their parents, to inform about online safety, mental health and well-being.

Schools should expand access to school-based counselling and other mental health support for issues related to minor’s social media+ use. Safe, stigma-free physical and online spaces should be available where pupils feel able to discuss struggles (i.e. mental health, well-being etc.) from their online experiences in social media+ environments. Schools should have access to qualified health and social care pro-

professionals, including stepped care mental health. Mental health professionals should receive specialised training in digital well-being and online harms.

Schools should also establish accessible, confidential, and child-friendly reporting mechanisms for minors' experiencing issues online. To further strengthen safeguarding, schools should have referral pathways to external child protection, mental health and specialist support services.

RECOMMENDATION 13

Educational responses should pay particular attention to vulnerable groups

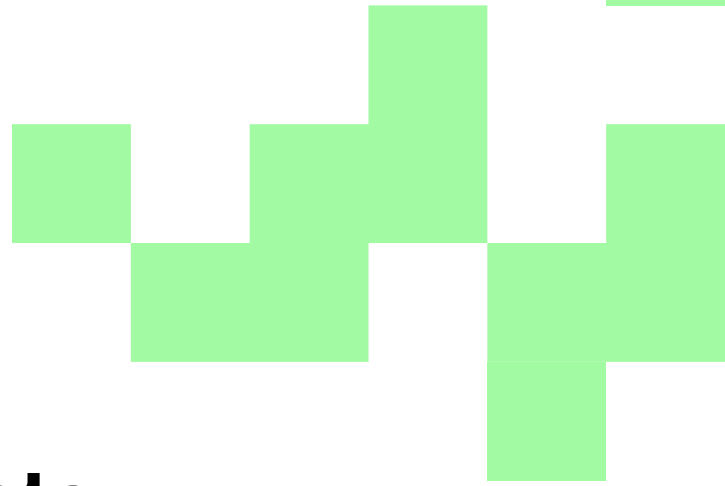
Minors facing socioeconomic disadvantages, special educational needs, adverse childhood experiences, discrimination, or mental health difficulties may be exposed to elevated social media+ risks. Educational and support measures should be inclusive, targeted where necessary, and designed to reduce inequalities in both social media and digital participation and well-being.

In schools, proactive, targeted interventions to address the disproportionate impact of online harms on vulnerable and marginalised minors could be put in place to protect and support vulnerable groups. Equitable access to devices, connectivity and assistive technologies should be expanded, including for children with disabilities.

RECOMMENDATION 14

Invest in secure, preventive, robust and trusted educational digital infrastructure

Schools need secure, robust and trusted digital infrastructure and tools to strengthen minors' digital skills and ensure Europe's digital sovereignty. European schools rely heavily on third-country applications, and the adoption of EU-made solutions faces continued challenges. The EU should prioritise and support the development and deployment of safe and interoperable digital infrastructure and tools for education and reduce strategic dependencies.



Acknowledgements

Our task as Co-Chairs and Special Advisers was to guide and steer the multi-layered, process: gathering knowledge by engaging with experts during the Special Panel meetings, collecting evidence from experts, and maintaining exchanges and contacts with numerous stakeholders.

This report owes its existence to a great number of people committed to ensuring children and adolescents can safely navigate the social media+ world. While the responsibility for the recommendations lies solely with us, we owe a great deal to the input of other renowned experts, parents' and youth representatives, and to the European Commission.

First and foremost, we would like to acknowledge the President of the European Commission, **Ursula von der Leyen**, for her constant interest and support for our work. Her attendance and engagement in the Special Panel meetings underscore her commitment to child safety online and were greatly appreciated by us and all participants. We thank the President for her longstanding interest and dedication to child safety, which made it possible to carry out this work and to develop concrete recommendations for the well-being of children and adolescents across Europe. We would also like to thank the President's Head of Cabinet, **Björn Seibert**, who accompanied the entire process from the very beginning, and **Patricia Reilly**, Member of the President's Cabinet, for her constant support.

In addition, we would like to thank all the participants of the Special Panel meetings. We are grateful to all who shared with us an extraordinary amount of knowledge, experience and dedication for the benefit of Europe's youth. We would like to express our special gratitude to **Julie Inman Grant**, Australia's eSafety Commissioner and **Lucas Borges**, Superintendent of Regulation at the Brazilian Data Protection Agency for providing us with insights and lessons from their countries on child safety online.

We listened carefully to all, yet the conclusions of this report are our own responsibility.

WE THANK THE SPECIAL PANEL PARTICIPANTS*:

**non-exhaustive list*

// **Ayata**, 15 year-old representative of the EU Children's Participation Platform

// **Zuzanna**, 17 year-old representative of the EU Children's Participation Platform

// **Kimmo Alho**, Psychologist and Professor Emeritus, University of Helsinki

// **Mehdi Arfaoui**, Sociologist, Commission nationale de l'informatique

- // **Leanda Barrington-Leach**, Executive Director, 5Rights Foundation
- // **Gabriele Battimelli**, Better Internet for Kids+ Ambassador from Italy
- // **Owen Bennett**, Independent expert in the regulation of digital technologies
- // **Elena Bozzola**, Paediatrician and National Councillor of the Italian Society of Paediatrics
- // **Matthias Brand**, Professor and Head of Department of General Psychology, Duisburg University
- // **Urs Buscke**, Senior Legal Officer, The European Consumer Organisation
- // **Ana Caballero**, Chair, Expert Group to improve the protection of minors in the digital realm, Spain
- // **Alex Cooney**, CEO & Co-founder, CyberSafeKids
- // **Lies Craeynest**, Founder, KidsUnplugged
- // **Jutta Croll**, Chairwoman, Stiftung Digitale Chancen
- // **María del Mar España Martí**, Director Plataforma Control Z
- // **Sigge Eriksson**, Chairperson, National Council of Swedish Children and Youth Organisations
- // **Marina Fernández**, President, Adolescència Lliure de Mòbils
- // **Louise Flynn**, Assistant Professor, Trinity College Dublin
- // **Tobiáš Bruno Galia**, Czech Council of Children and Youth
- // **Catalina Goanta**, Associate Professor in Private Law and Technology, Utrecht University
- // **Konstantinos Karachalios**, Advisor to the Executive Director, IEEE and Board Member, 5Rights Foundation
- // **Maija Katkovska**, Head, Latvian Safer Internet Centre
- // **Rasmus Kjedahl**, Director, Børns Vilkår
- // **Petra Kogelnig**, Secretary-General, European Parents' Association
- // **Pavel Kordik**, Associate Professor, Czech Technical University
- // **Marta Gonçalves**, Better Internet for Kids+ Ambassador from Portugal
- // **Beckett LeClair**, Head of Technology, 5Rights Foundation
- // **Sonia Livingstone**, Professor of Social Psychology, London School of Economics
- // **Aisling Maloney**, National Youth Council of Ireland
- // **Giovanna Mascheroni**, Professor, Catholic University Milan
- // **Helen Mason**, Executive Director, Child Helpline International

- // **Elvira Mentzelioti**, Chairwoman, Hellenic National Youth Council
- // **Eva Möhler**, Chair and Clinical Doctor of Child and Adolescent Psychiatry, Saarland University
- // **Alberto Monge Roffarello**, Assistant Professor, Politecnico di Torino
- // **Théo Mouhoud**, Child Psychiatrist, Hopitaux de Paris
- // **Servane Mouton**, Medical doctor, neurologist and neuropsychologist
- // **Mie Oehlenschläger**, Independent researcher and advisor on AI, Ethics and Public Policy
- // **James O'Higgins Norman**, Professor of Education and Society, Dublin City University
- // **Maja Olszewska**, Better Internet for Kids+ Ambassador from Poland
- // **Brian O'Neill**, Professor Emeritus, Technological University of Dublin
- // **Kerstin Paschke**, Medical Specialist in Child and Adolescent Psychiatry and Psychotherapy, Universitätsklinikum Hamburg-Eppendorf
- // **Leo Pekkala**, Deputy Director, Finnish Audiovisual Institute
- // **María Soledad Pera**, Associate Professor, TU Delft
- // **Tanja Petelin**, Associate Professor, Université de Poitiers
- // **Christoph Pieh**, Head of Department for Psychosomatic Medicine and Psychotherapy, University for Continuing Education Krems
- // **Jessica Piotrowski**, Professor, University of Amsterdam
- // **Declan Qualter**, Practice Placement Supervisor and PhD candidate, University College Dublin
- // **Kai Rannenberg**, Professor and Chair of Mobile Business and Multilateral Security, Goethe University Frankfurt
- // **Anna Schwabegger**, Chair of the Austrian National Youth Council
- // **Judith Simon**, Professor for Ethics in Information Technologies, University of Hamburg
- // **Lore Sleeckx**, European Youth Delegate, Flemish Youth Council
- // **Petr Slovak**, Associate Professor in Human Computer Interaction, King's College London
- // **Elisabeth Staksrud**, Professor, Department of Media and Communication, University of Oslo
- // **Sophie Stalla-Bourdillon**, Research Leader, Law, Science, Technology & Society Research Group, VUB
- // **Argyris Stringaris**, Clinical Scientist and Chair, Child and Adolescent Psychiatry, University College London
- // **Lisa Thorell**, Professor, Department of Clinical Neuroscience, Karolinska Institutet

- // **Hanne-Mari Schiøtz Thorud**, Physiologist and Professor, University of South-Eastern Norway
- // **Piotr Toczyski**, Associate Professor, APS Maria Grzegorzewska University
- // **Antonia Torrens**, President, COFACE – Families Europe.
- // **Martina Tóthová**, Senior Delegate, Youth Council of Slovakia
- // **Dimitris Tsalavos**, Better Internet for Kids+ Youth Ambassador from Cyprus
- // **Laura Vandenbosch**, Associate Professor and Director of the Media Psychology Lab, KU Leuven
- // **Sørine Vesth Rasmussen**, Advisor on children's rights and tech policy, Børns Vilkår
- // **Mieke Visser-Schuurman**, Director of Child Rights & Capacity Building, Eurochild
- // **Rareş Voicu**, President, European Youth Forum
- // **Alexandra Weilenmann**, Professor at the Department of Applied IT, University of Gothenburg
- // **Niels Zagema**, Dutch Youth Representative, Nationale Jeugdraad

For us, it was crucial to ensure not only youth representation as participants of the Special Panel meetings, but also involve young people in the co-creation of this report. This is why we would like to thank **Marta Gonçalves**, who not only joined the panel as a Better Internet for Kids+ ambassador from Portugal, but contributed to drafting this report.

This report would not have been possible without the support of many staff at the European Commission.

First, we would like to thank IDEA and its Acting Head **David Müller**, for hosting us and for providing excellent working conditions.

Our work profited enormously from the support of a dedicated team within IDEA: We would like to thank **Undine Ruge** for the oversight and support of the process. We owe a lot to **Asen Dimitrov**, who as the Lead Coordinator for the Co-Chairs of the Special Panel on child safety online, was our extraordinary go-to person, providing assistance, advice and support on process and content, as well as moving forward the realisation of our plans, processing all meetings and exchanges and coordinating the work on the report within IDEA and – together with colleagues from the Secretariat-General – also within the Commission.

This report would not have taken shape without further support from IDEA: We would like to thank **Thomas Hopkins**, who was an excellent editor of the English version of the report; **Anna Magdalena Comploi** who contributed her expertise, research and helped on all organisational fronts, as well as **Quinlan Rijks** who was involved in developing the visuals. We also would like to thank **Alexander Hempfing** for his analysis, and **Yee-Sol Chang** and **Konrad Rose** for their participation.

Together with IDEA, colleagues from the Secretariat-General have coordinated the work performed within the Commission and provided valuable insights, both in process and in content. We therefore thank Deputy Secretary-General **Nils Behrndt** for his time and dedication, as well as **Nacira Boulehouat**, **Ioana-Maria Gligor**, **Alessandra Falcinelli**, **Tarik Draidj**, **Louis Dancourt** and **Armande Lorentz**.

We first started out to better understand the existing legislation and tools available to the EU and Member States to protect children and adolescents online, and its enforcement to date. This context provided a basis for us to discuss with experts current gaps and the way forward. For this, we thank the leadership of DG CNECT and its Director-General **Roberto Viola** and Deputy Director-General **Renate Nikolay**, and DG JUST and its Director-General **Ana Gallego Torres** and Deputy Director-General **Hubert Gambis**.

We thank experts from DG CNECT who provided valuable expertise and insights: **Prabhat Agarwal, Julia Van Best, Martin Harris Hess, Andrea Tognoni, Manon Baert, Emma O'Mahony** and **Irene Roche Laguna**.

We thank experts from DG JUST who also provided valuable expertise and insights: **Maria-Myrto Kanellopoulou, Benedicte Van Ormelingen, Denisa Alexandroaiei, Caoimhe Sheridan, Marie-Cécile Rouillon** and **Marta Kuljon**.

This report profited from research and input by experts from across different departments in the European Commission (JRC, DG SANTE, DG EAC, DG HOME, DG RTD, DG GROW, SJ and others): **Andrea Ceglia, Yves Punie, Marianne Takki, Martine Ingvorsen, Francesca Maltauro, Marta Touyкова, Chiara Colella, Marta Markowska, Leonie Wahlmann, Katarzyna Janicka-Pawlowska, Veronica Travisani, Alessia Donna, Eva Gerhards, María del Pilar González Pantaleón, Amaryllis Verhoeven, Philipp Runge, Lorna Armati** and **Paul-John Loewenthal**.

We thank everyone for their expertise and patience in answering our countless questions and their ability to synthesise and make understandable complex legal and technical issues.

We would also like to thank experts from DG COMM and SG who provided excellent support on communication aspects: **Chloe Lahousse Juarez, Anguel Konstantinov Beremliysky, Emma Kristina Kvennberg** and others. Also, the very creative and patient graphic designers and translation experts: **Laurie Janssen, Camille Palandjian** and **Benedetta Benedetto** and others.

Our work would not have been possible without the organisational support of many coworkers in the Commission for the Special Panel meetings, travel and other meetings with stakeholders: **Carmen Tresguerres, Rozaliya Petkova, Martina Gunda, Nuria Paredes, Alexandre Verin, Mariola De Las Heras Ojeda, Anne Catherine Louppe, Margarita Biacho Varela, Hafize Balci** and **Vaia Tsiampazi**.

We as Co-Chairs also profited from the support by our home institutions and our closest collaborators in the field:

Prof. Dr. Fegert's team at the Ulm University Hospital - **PD Dr. Franziska Köhler-Dauner, Assistant Prof. Dr. Ann-Christin Haag, Emily Sitarski, Lena Peter, Karen Schlaegel, Claudia Rau, Annette Claus** and **Ariane Saccarello**.

Dr. Maria Melchior's team at the Sorbonne Public Health Institute with Sorbonne Université and French National Institute of Health and Medical Research (INSERM): **Fabienne El Khoury, Camille Davisse-Paturet, Hamid Massoumi, Bertrand Redonnet**, and **Mays Kabakibi**.

Endnotes

- 01.** Aries, P. (1962). *Centuries of childhood: A social history of family life*. Knopf Doubleday Publishing Group.
- 02.** Berk, L.E. (1994). *Infants and Children Prenatal Through Early Childhood*.
- 03.** Kessler, R. C., Magee, W. J. (1993). Childhood adversities and adult depression: basic patterns of association in a US national survey. *Psychological Medicine*, 23(3), 679–690.
- 04.** Taylor, G., Sala, G., Kolak, J., Gerhardstein, P., Lingwood, J. (2024). Does adult-child co-use during digital media use improve children's learning aged 0–6 years? A systematic review with meta-analysis. *Educational Research Review*, 44, 100614.
- 05.** Rideout, V. (2020). The Common Sense Census: Media Use by Kids Age Zero to Eight.
- 06.** Taylor, G., Sala, G., Kolak, J., Gerhardstein, P., Lingwood, J. (2024). Does adult-child co-use during digital media use improve children's learning aged 0–6 years? A systematic review with meta-analysis. *Educational Research Review*, 44, 100614.
Uhls, Y. T., Ellison, N. B., Subrahmanyam, K. (2017). Benefits and costs of social media in adolescence. *Pediatrics*, 140 (Supplement 2), S67–S70.
- 07.** Odgers, C. L., Jensen, M. R. (2020). Annual research review: Adolescent mental health in the digital age: Facts, fears, and future directions. *Journal of Child Psychology and Psychiatry*, 61(3), 336–348.
Nesi, J., Telzer, E. H., Prinstein, M. J. (2020). Adolescent Development in the Digital Media Context. *Psychological Inquiry*, 31(3), 229–234.
- 08.** Montag, C., Lachmann, B., Herrlich, M., Zweig, K. (2019). Addictive features of social media/messenger platforms and freemium games against the background of psychological and economic theories. *International journal of environmental research and public health*, 16(14), 2612.
- 09.** Steinberg, L. D. (2014). *Age of opportunity: Lessons from the new science of adolescence*. Houghton Mifflin Harcourt.
Casey, B. J., Getz, S., Galvan, A. (2008). The adolescent brain. *Developmental review*, 28(1), 62–77.
- 10.** Li, C., Cheng, G., Sha, T., Cheng, W., Yan, Y. (2020). The relationships between screen use and health indicators among infants, toddlers, and preschoolers: A meta-analysis and systematic review. *International Journal of Environmental Research and Public Health*, 17(19), 7324.
Teague, S., Somoray, K., Shatte, A. Miller, D., Moss, K., Crawford, A. et al. (2026). *Digital Media Use and Child Health and Development*. Deakin University. Journal contribution.
- Jing, X., et al. (2023). Effects of foreground screen media use on vocabulary development in young children: A meta-analysis. *Child Development*, 94(5), 1398–1415.
- 11.** Johnston MV. Neurotransmitters and vulnerability of the developing brain. *Brain Dev.* 1995 Sep-Oct;17(5):301-6.
- 12.** Ahmer, A., Raza, M., Azhar, M., Rahman, A., Das, J. K., Jafri, S. K. (2025). A systematic review and meta-analysis on the impact of screen-time on the social-emotional development of children under five years. *Journal of the College of Physicians and Surgeons Pakistan*, 35(3), 351–358.
Vasconcellos, R. P., Sanders, T., Lonsdale, C., Parker, P., Conigrave, J., Tang, S., Noetel, M. (2025). Electronic screen use and children's socioemotional problems: A systematic review and meta-analysis of longitudinal studies. *Psychological Bulletin*, 151(5), 513–543.
- 13.** Boxer, P., Groves, C. L., Docherty, M. (2015). Video games do indeed influence children and adolescents' aggression, prosocial behavior, and academic performance: A clearer reading of Ferguson (2015). *Perspectives on psychological science*, 10(5), 671–673.
Coyne, S. M., Radesky, J., Collier, K. M., Gentile, D. A., Linder, J. R., Nathanson, A. I., Rogers, J. (2017). Parenting and digital media. *Pediatrics*, 140(Supplement 2), S112–S116.
- 14.** Calvert, S. L. (2017). Parasocial relationships with media characters: Imaginary companions for young children's social and cognitive development. In *Cognitive development in digital contexts* (pp. 93–117). Academic Press.
Mallawaarachchi S., Burley J., Mavilidi M., et al (2024). Early Childhood Screen Use Contexts and Cognitive and Psychosocial Outcomes: A Systematic Review and Meta-analysis. *JAMA Pediatr.* 2024;178(10):1017–1026.
- 15.** Mallawaarachchi S., Burley J., Mavilidi M., et al (2024). Early Childhood Screen Use Contexts and Cognitive and Psychosocial Outcomes: A Systematic Review and Meta-analysis. *JAMA Pediatr.* 2024;178(10):1017–1026.
- 16.** Calvert, S. L. (2017). Parasocial relationships with media characters: Imaginary companions for young children's social and cognitive development. In *Cognitive development in digital contexts* (pp. 93–117). Academic Press.
Mallawaarachchi S., Burley J., Mavilidi M., et al (2024). Early Childhood Screen Use Contexts and Cognitive and Psychosocial Outcomes: A Systematic Review and Meta-analysis. *JAMA Pediatr.* 2024;178(10):1017–1026.
- 17.** Taylor, G., Sala, G., Kolak, J., Gerhardstein, P.,

- Lingwood, J. (2024). Does adult-child co-use during digital media use improve children's learning aged 0–6 years? A systematic review with meta-analysis. *Educational Research Review*, 44, 100614.
18. American Academy of Pediatrics (2024). Screen time guidelines. Center of Excellence on Social Media and Youth Mental Health.
 19. Qian, H., Wang, C., Li, H. (2024). Parental risk factors and moderators of prolonged digital use in preschoolers: a meta-analysis. *Education and Information Technologies*, 29(13), 17601-17619. Jackson, D. B., Testa, A., Fox, B. (2021). Adverse childhood experiences and digital media use among US children. *American journal of preventive medicine*, 60(4), 462-470.
 20. Li, C., Cheng, G., Sha, T., Cheng, W., Yan, Y. (2020). The relationships between screen use and health indicators among infants, toddlers, and preschoolers: A meta-analysis and systematic review. *International Journal of Environmental Research and Public Health*, 17(19), 7324. Ahmer, A., Raza, M., Azhar, M., Rahman, A., Das, J. K., Jafri, S. K. (2025). A systematic review and meta-analysis on the impact of screen-time on the social-emotional development of children under five years. *Journal of the College of Physicians and Surgeons Pakistan*, 35(3), 351-358.
 21. Bochicchio, V., Keith, K., Montero, I., Scandurra, C., Winsler, A. (2022). Digital media inhibit self-regulatory private speech use in preschool children: The “digital bubble effect”. *Cognitive development*, 62, 101180.
 22. Yang, C. C., Holden, S. M., Ariati, J. (2021). Social media and psychological well-being among youth: The multidimensional model of social media use. *Clinical child and family psychology review*, 24(3), 631-650. Vasconcellos, R. P., Sanders, T., Lonsdale, C., Parker, P., Conigrave, J., Tang, S., Noetel, M. (2025). Electronic screen use and children's socioemotional problems: A systematic review and meta-analysis of longitudinal studies. *Psychological Bulletin*, 151(5), 513-543.
 23. Qian, H., Wang, C., Li, H. (2024). Parental risk factors and moderators of prolonged digital use in preschoolers: a meta-analysis. *Education and Information Technologies*, 29(13), 17601-17619. Jackson, D. B., Testa, A., Fox, B. (2021). Adverse childhood experiences and digital media use among US children. *American journal of preventive medicine*, 60(4), 462-470.
 24. Madigan, S., Browne, D., Racine, N., Mori, C., Tough, S. (2019). Association between screen time and children's performance on a developmental screening test. *JAMA pediatrics*, 173(3), 244-250. Teague, S., Somoray, K., Shatte, A. Miller, D., Moss, K., Crawford, A. et al. (2026). Digital Media Use and Child Health and Development. Deakin University. Journal contribution.
 25. Calvert, S. L. (2017). Parasocial relationships with media characters: Imaginary companions for young children's social and cognitive development. In *Cognitive development in digital contexts* (pp. 93-117). Academic Press. Marshall, S. J., Biddle, S. J., Gorely, T., Cameron, N., Murdey, I. (2004). Relationships between media use, body fatness and physical activity in children and youth: a meta-analysis. *International journal of obesity*, 28(10), 1238-1246.
 26. Madigan, S., Browne, D., Racine, N., Mori, C., Tough, S. (2019). Association between screen time and children's performance on a developmental screening test. *JAMA pediatrics*, 173(3), 244-250. Mallawaarachchi S., Burley J., Mavilidi, M., et al (2024). Early Childhood Screen Use Contexts and Cognitive and Psychosocial Outcomes: A Systematic Review and Meta-analysis. *JAMA Pediatr*. 2024;178(10):1017-1026.
 27. Korat, O., Shamir, A., Heibal, S. (2013). Expanding the boundaries of shared book reading: E-books and printed books in parent-child reading as support for children's language. *First language*, 33(5), 504-523. Taylor, G., Sala, G., Kolak, J., Gerhardstein, P., Lingwood, J. (2024). Does adult-child co-use during digital media use improve children's learning aged 0–6 years? A systematic review with meta-analysis. *Educational Research Review*, 44, 100614.
 28. Kidron, B., Evans, A., Afia, J., Adler, J. R., Bowden-Jones, H., Hackett, L., Juj, A., Przybylski, A. K., Rudkin, A., Young Scot. (2018). Disrupted childhood: The cost of persuasive design. 5Rights Foundation. Stoilova, M., Bulger, M., Livingstone, S. (2024). Do parental control tools fulfil family expectations for child protection? A rapid evidence review of the contexts and outcomes of use. *Journal of Children and Media*. Chao, M., Lei, J., He, R., Jiang, Y., Yang, H. (2023). TikTok use and psychosocial factors among adolescents: Comparisons of non-users, moderate users, and addictive users. *Psychiatry Research*, 325, 115247.
 29. Taylor, G., Sala, G., Kolak, J., Gerhardstein, P., Lingwood, J. (2024). Does adult-child co-use during digital media use improve children's learning aged 0–6 years? A systematic review with meta-analysis. *Educational Research Review*, 44, 100614. Zgambo, M., Anyango, E., Arabiat, D. H., Ngune, I., Mörelius, E., Zhang, M., Whitehead, L. C. (2025). Effect of Digital Safety Interventions on Parental Practices in Safeguarding Children's Digital Activities: Systematic Review and Meta-Analysis. *JMIR Pediatrics and Parenting*, 8(1), e70745.
 30. Qian, H., Wang, C., Li, H. (2024). Parental risk factors and moderators of prolonged digital use in preschoolers: a meta-analysis. *Education and Information Technologies*, 29(13), 17601-17619. Jackson, D. B., Testa, A., Fox, B. (2021). Adverse childhood experiences and digital media use among US children. *American journal of preventive medicine*, 60(4), 462-470.
 31. Yang, C. C., Holden, S. M., Ariati, J. (2021). Social media

- and psychological well-being among youth: The multidimensional model of social media use. *Clinical child and family psychology review*, 24(3), 631–650.
- Uhls, Y. T., Ellison, N. B., Subrahmanyam, K. (2017). Benefits and costs of social media in adolescence. *Pediatrics*, 140 (Supplement 2), S67–S70.
32. Teague, S., Somoray, K., Shatte, A. Miller, D., Moss, K., Crawford, A. et al. (2026). Digital Media Use and Child Health and Development. Deakin University. Journal contribution.
 33. Vasconcellos, R. P., Sanders, T., Lonsdale, C., Parker, P., Conigrave, J., Tang, S., Noetel, M. (2025). Electronic screen use and children's socioemotional problems: A systematic review and meta-analysis of longitudinal studies. *Psychological Bulletin*, 151(5), 513–543.
 34. Qian, H., Wang, C., Li, H. (2024). Parental risk factors and moderators of prolonged digital use in preschoolers: a meta-analysis. *Education and Information Technologies*, 29(13), 17601–17619.
 - Jackson, D. B., Testa, A., Fox, B. (2021). Adverse childhood experiences and digital media use among US children. *American journal of preventive medicine*, 60(4), 462–470.
 35. Qian, H., Wang, C., Li, H. (2024). Parental risk factors and moderators of prolonged digital use in preschoolers: a meta-analysis. *Education and Information Technologies*, 29(13), 17601–17619.
 - Zgambo, M., Anyango, E., Arabiat, D. H., Ngune, I., Mörelus, E., Zhang, M., Whitehead, L. C. (2025). Effect of Digital Safety Interventions on Parental Practices in Safeguarding Children's Digital Activities: Systematic Review and Meta-Analysis. *JMIR Pediatrics and Parenting*, 8(1), e70745.
 36. Calvert, S. L. (2017). Parasocial relationships with media characters: Imaginary companions for young children's social and cognitive development. In *Cognitive development in digital contexts* (pp. 93–117). Academic Press.
 - Marshall, S. J., Biddle, S. J., Gorely, T., Cameron, N., Murdey, I. (2004). Relationships between media use, body fatness and physical activity in children and youth: a meta-analysis. *International journal of obesity*, 28(10), 1238–1246.
 37. Böttger, T., Zierer, K. (2024). To ban or not to ban? A rapid review on the impact of smartphone bans in schools on social well-being and academic performance. *Education Sciences*, 14(8), 906.
 38. Boztas, S. (2025, July 4). Smartphone bans in Dutch schools have improved learning, study finds. The Guardian.
 39. Wedekind, K. (2026, March 11). So abgelenkt sind Schüler, wenn es kein Handyverbot gibt. n-tv.
 40. Korat, O., Shamir, A., Heibal, S. (2013). Expanding the boundaries of shared book reading: E-books and printed books in parent–child reading as support for children's language. *First language*, 33(5), 504–523.
 41. Calvert, S. L. (2017). Parasocial relationships with media characters: Imaginary companions for young children's social and cognitive development. In *Cognitive development in digital contexts* (pp. 93–117). Academic Press.
 - Marshall, S. J., Biddle, S. J., Gorely, T., Cameron, N., Murdey, I. (2004). Relationships between media use, body fatness and physical activity in children and youth: a meta-analysis. *International journal of obesity*, 28(10), 1238–1246.
 42. Purba, A. K., Thomson, R. M., Henery, P. M., Pearce, A., Henderson, M., Katikireddi, S. V. (2023). Social media use and health risk behaviours in young people: systematic review and meta-analysis. *bmj*, 383.
 43. Nesi, J., Telzer, E. H., Prinstein, M. J. (2020). Adolescent Development in the Digital Media Context. *Psychological Inquiry*, 31(3), 229–234.
 - Uhls, Y. T., Ellison, N. B., Subrahmanyam, K. (2017). Benefits and costs of social media in adolescence. *Pediatrics*, 140 (Supplement 2), S67–S70.
 44. Schwartz, D., Zhang, M., Troop-Gordon, W., Taylor, L. M., Chung, J. (2025). Are social media use and popularity in the peer group linked during adolescence? A meta-analytic review. *Journal of Adolescence*, 97(3), 575–592.
 45. Madigan, S., Browne, D., Racine, N., Mori, C., Tough, S. (2019). Association between screen time and children's performance on a developmental screening test. *JAMA pediatrics*, 173(3), 244–250.
 - Teague, S., Somoray, K., Shatte, A. Miller, D., Moss, K., Crawford, A. et al. (2026). Digital Media Use and Child Health and Development. Deakin University. Journal contribution.
 46. Children's Hospital of Philadelphia (2026). Age Limits Alone Won't Fix Smartphone Risks, Suggests Children's Hospital of Philadelphia Study. Accessed on 12 July 2026.
 47. Vasconcellos, R. P., Sanders, T., Lonsdale, C., Parker, P., Conigrave, J., Tang, S., Noetel, M. (2025). Electronic screen use and children's socioemotional problems: A systematic review and meta-analysis of longitudinal studies. *Psychological Bulletin*, 151(5), 513–543.
 - Teague, S., Somoray, K., Shatte, A. Miller, D., Moss, K., Crawford, A. et al. (2026). Digital Media Use and Child Health and Development. Deakin University. Journal contribution.
 48. Nesi, J., Choukas-Bradley, S., Prinstein, M. J. (2018). Transformation of adolescent peer relations in the social media context: Part 1 – A theoretical framework and application to dyadic peer relationships. *Clinical child and family psychology review*, 21(3), 267–294.
 - Uhls, Y. T., Ellison, N. B., Subrahmanyam, K. (2017). Benefits and costs of social media in adolescence. *Pediatrics*, 140 (Supplement 2), S67–S70.
 49. Werling, A. M., Kuzhippallil, S., Emery, S., Walitza, S., Drechsler, R. (2022). Problematic use of digital media in children and adolescents with attention-deficit/hyperactivity disorder compared to controls: A meta-analysis. *Journal of Behavioral Addictions*, 11(2), 305–325.
 50. Nesi, J., Telzer, E. H., Prinstein, M. J. (2020).

- Adolescent Development in the Digital Media Context. *Psychological Inquiry*, 31(3), 229–234.
- Uhls, Y. T., Ellison, N. B., Subrahmanyam, K. (2017). Benefits and costs of social media in adolescence. *Pediatrics*, 140 (Supplement 2), S67–S70.
51. Orben, A., Przybylski, A. K. (2019). The association between adolescent well-being and digital technology use. *Nature Human Behaviour*, 3, 173–182.
 52. Orben, A., Meier, A., Dalgleish, T., Blakemore, S. J. (2024). Mechanisms linking social media use to adolescent mental health vulnerability. *Nature Reviews Psychology*, 3(6), 407–423.
 53. Vasconcellos, R. P., Sanders, T., Lonsdale, C., Parker, P., Conigrave, J., Tang, S., Noetel, M. (2025). Electronic screen use and children's socioemotional problems: A systematic review and meta-analysis of longitudinal studies. *Psychological Bulletin*, 151(5), 513–543.
 54. Keles, B., McCrae, N., Grealish, A. (2020). A systematic review: The influence of social media on depression, anxiety and psychological distress in adolescents. *International Journal of Adolescence and Youth*, 25(1), 79–93.
 - Liu, M., Kamper-DeMarco, K. E., Zhang, J., Xiao, J., Dong, D., Xue, P. (2022). Time spent on social media and risk of depression in adolescents: A dose-response metaanalysis. *International Journal of Environmental Research and Public Health*, 19.
 55. Orben, A., Meier, A., Dalgleish, T., Blakemore, S. J. (2024). Mechanisms linking social media use to adolescent mental health vulnerability. *Nature Reviews Psychology*, 3(6), 407–423.
 56. Vasconcellos, R. P., Sanders, T., Lonsdale, C., Parker, P., Conigrave, J., Tang, S., Noetel, M. (2025). Electronic screen use and children's socioemotional problems: A systematic review and meta-analysis of longitudinal studies. *Psychological Bulletin*, 151(5), 513–543.
 - Qian, H., Wang, C., Li, H. (2024). Parental risk factors and moderators of prolonged digital use in preschoolers: a meta-analysis. *Education and Information Technologies*, 29(13), 17601–17619.
 57. Yang, C. C., Holden, S. M., Ariati, J. (2021). Social media and psychological well-being among youth: The multidimensional model of social media use. *Clinical child and family psychology review*, 24(3), 631–650.
 58. Vasconcellos, R. P., Sanders, T., Lonsdale, C., Parker, P., Conigrave, J., Tang, S., Noetel, M. (2025). Electronic screen use and children's socioemotional problems: A systematic review and meta-analysis of longitudinal studies. *Psychological Bulletin*, 151(5), 513–543.
 59. Pagano, M., Bacaro, V., Crocetti, E. (2023). "Using digital media or sleeping... that is the question". A meta-analysis on digital media use and unhealthy sleep in adolescence. *Computers in Human Behavior*, 146, 107813.
 - Orben, A., Przybylski, A. K. (2019). The association between adolescent well-being and digital technology use. *Nature Human Behaviour*, 3, 173–182.
 60. Orben, A., Meier, A., Dalgleish, T., Blakemore, S. J. (2024). Mechanisms linking social media use to adolescent mental health vulnerability. *Nature Reviews Psychology*, 3(6), 407–423.
 61. Uhls, Y. T., Ellison, N. B., Subrahmanyam, K. (2017). Benefits and costs of social media in adolescence. *Pediatrics*, 140 (Supplement 2), S67–S70.
 62. Orben, A., Meier, A., Dalgleish, T., Blakemore, S. J. (2024). Mechanisms linking social media use to adolescent mental health vulnerability. *Nature Reviews Psychology*, 3(6), 407–423.
 63. Vasconcellos, R. P., Sanders, T., Lonsdale, C., Parker, P., Conigrave, J., Tang, S., Noetel, M. (2025). Electronic screen use and children's socioemotional problems: A systematic review and meta-analysis of longitudinal studies. *Psychological Bulletin*, 151(5), 513–543.
 - Teague, S., Somoray, K., Shatte, A., Miller, D., Moss, K., Crawford, A. et al. (2026). *Digital Media Use and Child Health and Development*. Deakin University. Journal contribution.
 64. Vasconcellos, R. P., Sanders, T., Lonsdale, C., Parker, P., Conigrave, J., Tang, S., Noetel, M. (2025). Electronic screen use and children's socioemotional problems: A systematic review and meta-analysis of longitudinal studies. *Psychological Bulletin*, 151(5), 513–543.
 65. Madigan, S., Browne, D., Racine, N., Mori, C., Tough, S. (2019). Association between screen time and children's performance on a developmental screening test. *JAMA pediatrics*, 173(3), 244–250.
 - Teague, S., Somoray, K., Shatte, A., Miller, D., Moss, K., Crawford, A. et al. (2026). *Digital Media Use and Child Health and Development*. Deakin University. Journal contribution.
 66. Qian, H., Wang, C., Li, H. (2024). Parental risk factors and moderators of prolonged digital use in preschoolers: a meta-
Education and Information Technologies, 29(13), 17601–17619.
 67. Pagano, M., Bacaro, V., Crocetti, E. (2023). "Using digital media or sleeping... that is the question". A meta-analysis on digital media use and unhealthy sleep in adolescence. *Computers in Human Behavior*, 146, 107813.
 68. Odgers, C. L., Jensen, M. R. (2020). Annual research review: Adolescent mental health in the digital age: Facts, fears, and future directions. *Journal of Child Psychology and Psychiatry*, 61(3), 336–348.
 - Sala, A., Porcaro, L., Gómez, E. (2024). Social Media Use and adolescents' mental health and well-being: An umbrella review. *Computers in Human Behaviours Report*, volume 14.
 69. Sala, A., Porcaro, L., Gómez, E. (2024). Social Media Use and adolescents' mental health and well-being: An umbrella review. *Computers in Human Behaviours Report*, volume 14.
 70. Staksrud, E., Livingstone, S. (2009). Children and online risk. *Information, Communication and Society*, 12 (3).

- 71.** Fegert, J.M. (2026). European child and adolescent psychiatry in a digital world. *European Child and Adolescent Psychiatry*, 35, 309–315.
- 72.** WeProtect (2021). Estimates of childhood exposure to online sexual harms and their risk factors, p.5.
- 73.** European Commission (2026). Action Plan against Cyberbullying.
- 74.** Hamm, M. P., Newton, A. S., Chisholm, A., Shulhan, J., Milne, A., Sundar, P., Ennis, H., Scott, S. D., Hartling, L. (2015). Prevalence and effect of cyberbullying on children and young people: A scoping review of social media studies. *Journal of the American Medical Association Southeast Asia. Supplement. Pediatrics*, 169, 770–777.
Ronis, S., Slaunwhite, A. (2017). Gender and Geographic Predictors of Cyberbullying Victimization, Perpetration, and Coping Modalities Among Youth. *Canadian Journal of Psychology*, 34 (1).
- 75.** European Commission (2021). Study to support the preparation of the European Commission's initiative to extend the list of EU crimes in Article 83 of the Treaty on the Functioning of the EU to hate speech and hate crime. Final report.
- 76.** European Institute for Gender Equality (EIGE). 2026. Growing up online: how violence follows girls across platforms. Accessed on 29 June 2026.
- 77.** Abendroth Dias, K., Arias Cabarcos, P., Bacco, F.M., Bassani, E., Bertoletti, A., et al. (2025). Generative AI Outlook Report – Exploring the Intersection of Technology, Society and Policy. Navajas Cawood, E., Vespe, M., Kotsev, A., van Bavel, R. (editors). Publications Office of the European Union, Luxembourg, JRC142598.
- 78.** Ofcom. (2024). A deep dive into deepfakes that demean, defraud and disinform. Accessed on 29 June 2026.
- 79.** Rousay, V. (2023). Sexual Deepfakes and Image-Based Sexual Abuse: Victim-Survivor Experiences and Embodied Harms. Master's thesis, Harvard University Division of Continuing Education.
- 80.** Cataldo, I., Lepri, B., Neoh, M. J. Y., Esposito, G. (2021). Social Media Usage and Development of Psychiatric Disorders in Childhood and Adolescence: A Review. *Frontiers in Psychiatry*, 11.
- 81.** McCrae, N., Gettings, S., Pursell, E. (2017). Social media and depressive symptoms in childhood and adolescence: A systematic review. *Adolescent Research Review*, Vol. 2, pp. 315–330.
- 82.** Cataldo, I., Lepri, B., Neoh, M. J. Y., Esposito, G. (2021). Social Media Usage and Development of Psychiatric Disorders in Childhood and Adolescence: A Review. *Frontiers in Psychiatry*, 11.
- 83.** Svensson, R., Johnson, B. Olsson, A. (2022). Does gender matter? The association between different digital media activities and adolescent well-being. *MC Public Health*, 10 (22), 273.
- 84.** Svensson, R., Johnson, B. Olsson, A. (2022). Does gender matter? The association between different digital media activities and adolescent well-being. *MC Public Health*, 10 (22), 273.
- 85.** Twenge J.M., Martin G.N. (2020). Gender differences in associations between digital media use and psychological well-being: Evidence from three large datasets. *Journal of Adolescence*, 79, 91–102.
- 86.** Svensson, R., Johnson, B. Olsson, A. (2022). Does gender matter? The association between different digital media activities and adolescent well-being. *MC Public Health*, 10 (22), 273.
- 87.** Dreßing, H., Hoell, A., Scharmann, L., Simon, A. M., Haag, A. C., Dölling, D., Meyer-Lindenberg, A., Fegert, J. M. (2025). Sexual Violence Against Children and Adolescents: A German Nationwide Representative Survey on Its Prevalence, Situational Context, and Consequences. *Deutsches Ärzteblatt International*, 122(11), 285.
- 88.** Ronis, S., Slaunwhite, A. (2017). Gender and Geographic Predictors of Cyberbullying Victimization, Perpetration, and Coping Modalities Among Youth. *Canadian Journal of Psychology*, 34 (1).
- 89.** Sala, A., Porcaro, L., and Gómez, E. (2024). Social Media Use and adolescents' mental health and well-being: An umbrella review. *Computers in Human Behaviours Report*, 14.
- 90.** eSafety Commissioner (2025). How common are experiences of seeing online hate among children in Australia? Accessed 16 June 2026.
- 91.** Kowalski, R.M., Limber, S.P., McCord, A. (2019). A developmental approach to cyberbullying: Prevalence and protective factors. *Aggression and Violent Behavior*, 45.
- 92.** 5Rights Foundation (2020). Why digital platforms must be designed with LGBTQ children in mind. Accessed on 29 June 2026.
- 93.** 5Rights Foundation (2020). Why digital platforms must be designed with LGBTQ children in mind. Accessed on 29 June 2026.
- 94.** FRA (2024). LGBTIQ equality at a crossroads: Progress and challenges, p.72.
- 95.** 5Rights Foundation (2020). Why digital platforms must be designed with LGBTQ children in mind. Accessed on 29 June 2026.
- 96.** Ybarra, M.L., Mitchell, K.J., Palmer, N.A., Reisner, S.L. (2015). Online social support as a buffer against online and offline peer and sexual victimization among U.S. LGBT and non-LGBT youth. *Child Abuse Neglect*, 39.
- 97.** Ronis, S., Slaunwhite, A. (2017). Gender and Geographic Predictors of Cyberbullying Victimization, Perpetration, and Coping Modalities Among Youth. *Canadian Journal of Psychology*, 34 (1).

98. Koch, T., Laaber, F., Florack, A. (2024). Socioeconomic status and young people's digital maturity: The role of parental mediation. *Computers in Human Behaviour*, 154.
Li, H., Luo, M., Duan, B., Kawulia, A., Su, M., Di, H. (2024). Family socioeconomic status and young children digital addiction: a moderated mediation model. *Frontiers in Psychology*, 27 (5).
99. Lu, Z. (2026). Mapping adolescent problematic social media use patterns across 41 countries/ regions: A multilevel latent class analysis with social determinants. *Addictive Behaviors*, 172.
Gracia, P., Fernandez-Urbano, R., Rubio-Cabañez, M., Celik, S., Cineli, B. (2026). World Happiness Report 2026. Chapter 7: Problematic social media use and adolescent wellbeing: the role of family socioeconomic status across 43 countries. Helliwell, J.F., Layard, R., Sachs, J. D., De Neve, J.-E., Aknin, L. B., Wang, S. (editors). Wellbeing Research Centre, University of Oxford.
100. Prkno, D., Grafe, N., Schulz, M.S., Kiess, W., Poulain, T. (2025). Children's and adolescents' negative internet experiences and the association with quality of life and behavioural difficulties: a cross-sectional study. *BMJ Paediatrics Open*, 17:9 (1).
101. Ofcom. (2022). Research into risk factors that may lead children to harm online.
102. Koch, T., Laaber, F., Florack, A. (2024). Socioeconomic status and young people's digital maturity: The role of parental mediation. *Computers in Human Behaviour*, 154.
103. World Happiness Report (2026). Chapter 7: Problematic social media use and adolescent wellbeing: the role of family socioeconomic status across 43 countries.
Lu, Z. (2026). Mapping adolescent problematic social media use patterns across 41 countries/ regions: A multilevel latent class analysis with social determinants. *Addictive Behaviors*, 172.
104. Ronis, S., Slaunwhite, A. (2017). Gender and Geographic Predictors of Cyberbullying Victimization, Perpetration, and Coping Modalities Among Youth. *Canadian Journal of Psychology*, 34 (1).
105. Hong, J.S., et al. (2016). Understanding the correlates of face-to-face and cyberbullying victimization among U.S. adolescents: A social-ecological analysis. *Violence and Victims*, 31(4), 638–663.
Thomas, A., Yeqing, L. (2025). Helping teens navigate online racism – study shows which parenting strategy works best.
106. FRA (2023). Online content moderation – Current challenges in detecting hate speech.
107. Bermudez-Villalva, A., Mehrnezhad, M., Toreini, E. (2025). Measuring Online Hate on 4chan using Pre-trained Deep Learning Models. *IEEE Transactions on Technology and Society*, 6 (2), June 2025.
108. FRA (2024). Being Muslim in the EU – Experiences of Muslims.
109. FRA (2023). Being Black in the EU – Experiences of people of African descent.
110. Council of Europe (2026). Hate speech levels across Europe alarming, stronger action needed. Accessed on 25 June 2026.
111. United Nations (2021). Report of the Special Rapporteur on minority issues, Fernand de Varennes. Human Rights Council, Forty-sixth session, 22 February–19 March 2021.
112. FRA (2022). Bias in Algorithms – Artificial Intelligence and Discrimination.
113. Ofcom. (2022). Research into risk factors that may lead children to harm online. p. 27.
114. eSafety Commissioner, 2023. A new playground: The digital lives of young people with disability.
Childlight Global Safety Institute (2023). The nature of online CSEA among children living with disabilities.
115. WeProtect (2025). How do we protect disabled young people from abuse and exploitation in digital spaces?
116. Childlight Global Safety Institute (2023). The nature of online CSEA among children living with disabilities.
117. eSafety Commissioner (2023). Young people with disability more likely to express themselves online despite higher rates of abuse.
118. eSafety Commissioner (2023). A new playground: The digital lives of young people with disability.
119. Werling, A.M., Kuzhippallil, S., Emery, S., Walitza, S., Drechsler, R. (2022). Problematic use of digital media in children and adolescents with a diagnosis of attention-deficit/hyperactivity disorder compared to controls. A meta-analysis. *Journal of Behavioral Addictions*, 11 (2).
120. Villar Onrubia, D., Barreda Angeles, M., Cachia, R., Economou, A., Lopez Cobo, M., (2025). Cyberbullying: Insights from science, policy and legislation. Publications Office of the European Union, Luxembourg, JRC144335.
121. Shou, Q., Yamashita, M., Mizuno, Y. (2025). Association of screen time with attention-deficit/hyperactivity disorder symptoms and their development: the mediating role of brain structure. *Translational Psychiatry*, 15:447.
122. eSafety Commissioner (2023). A new playground: The digital lives of young people with disability.
123. World Health Organization (2025). Mental health of adolescents. Accessed on 29 June 2026.
124. European Commission (2023). Flash Eurobarometer 530: Mental health.

125. World Health Organization (2025). Mental health of adolescents. Accessed on 29 June 2026.
126. World Health Organization (2025). Over a billion people living with mental health conditions – services require urgent scale-up. Accessed on 29 June 2026.
127. World Health Organization (2025). Suicide. Accessed on 16 June 2026.
128. OECD (2021). *Fitter Minds, Fitter Jobs: From Awareness to Change in Integrated Mental Health, Skills and Work Policies*. OECD Publishing, Paris.
129. Bertoni, E., Centeno, C., Cachia, R. (2025). Social media usage and adolescents' mental health in the EU. European Commission, Joint Research Centre (JRC), Ispra.
130. Bertoni, E., Centeno, C., Cachia, R. (2025). Social media usage and adolescents' mental health in the EU. European Commission, Joint Research Centre (JRC), Ispra.
131. Beullens, K., Bozzola, E., Cataldo, I., Hale, L., Kent, M., Montag, C., Nivins, S., O'reilly, M., Rubæk, L., Schiøtz Thorud, H.-M., Sterpenich, V., Vandenbosch, L. (2025). Minors' health and social media: an interdisciplinary scientific perspective. Manolios, S., Sala, A., Sundorph, E., Chaudron, S., Gomez, E. (editors), Publications Office of the European Union, Luxembourg. P.8.
132. Vidal, C., Lhaksampa, T., Miller, L., Platt, R. (2020). Social media use and depression in adolescents: A scoping review. *International Review of Psychiatry* (Abingdon, England), 32(3), 235-253.
133. Prkno, D., Grafe, N., Schulz, M.S., Kiess, W., Poulain, T. (2025). Children's and adolescents' negative internet experiences and the association with quality of life and behavioural difficulties: a cross-sectional study. *BMJ Paediatrics Open*, 17;9 (1).
134. Sarmiento, I., Olson, C., Yeo, G., Chen, Y., Toma, C., Brown, B., Bellmore, A., Mares, M. L. (2020). How does social media use relate to adolescents' internalizing symptoms? Conclusions from a systematic narrative review. *Adolescent Research Review*, 5, 381-404.
135. Sala, A., Porcaro, L., Gómez, E. (2024). Social Media Use and adolescents' mental health and well-being: An umbrella review. *Computers in Human Behavior Reports*, Vol 14. McCrae, N., Gettings, S., Pursell, E. (2017). Social media and depressive symptoms in childhood and adolescence: A systematic review. *Adolescent Research Review*, Vol 2, 315-330.
136. Li, H., Zhang, R., Lee, Y.C., et al. (2023). Systematic review and meta-analysis of AI-based conversational agents for promoting mental health and well-being. *NPJ Digital Medicine*, 6, 236.
137. Kooli, C., Chakraoui, R. (2025). AI-driven assistive technologies in inclusive education: benefits, challenges, and policy recommendations. *Sustainable Futures*, 10.
138. Unicef (2025). Guidance on AI and Children. Accessed on 29 June 2026.
139. Hudon, A., Stip, E. (2025) Delusional Experiences Emerging From AI Chatbot Interactions or "AI Psychosis". *JMIR Mental Health*, 3 (12). European Parliament (2026). The spread of AI companions and the challenges they generate. European Parliamentary Research Service (EPRS). Nature (2025). Can AI chatbots trigger psychosis? What the science says. Accessed on 16 June 2026.
140. Vice (2023). 'He Would Still Be Here': Man Dies by Suicide After Talking with AI Chatbot, Widow Says. Accessed on 16 June 2026.
141. Kurian, N. (2024). 'No, Alexa, no!': designing child-safe AI and protecting children from the risks of the 'empathy gap' in large language models. *Learning, Media and Technology*, 50.
142. Kurian, N. (2023). AI's empathy gap: the risks of conversational artificial intelligence for young children's well-being and key ethical considerations for early childhood education and care. *Contemporary Issues in Early Childhood*, 26(1), 132-139.
143. Commission nationale de l'informatique et des libertés (CNIL) (2026). L'impact des usages de l'AI sur la santé mentale des jeunes européens.
144. Ganapini, M., Panai, E. (2023). An Audit Framework for Adopting AI-Nudging on Children. Tech Ethics Lab.
145. Kurian, N. (2024). 'No, Alexa, no!': designing child-safe AI and protecting children from the risks of the 'empathy gap' in large language models. *Learning, Media and Technology*, 50.
146. Fegert, J. M. (2026). European child and adolescent psychiatry in a digital world. *European Child and Adolescent Psychiatry*, 35, 309-315.
147. Sala, A., Porcaro, L., Gómez, E. (2024). Social Media Use and adolescents' mental health and well-being: An umbrella review. *Computers in Human Behavior Reports*, Vol. 14.
148. Cataldo, I., Lepri, B., Neoh, M. J. Y., Esposito, G. (2021). Social Media Usage and Development of Psychiatric Disorders in Childhood and Adolescence: A Review. *Frontiers in Psychiatry*, 11.
149. Liu, L. (2024). Research on the relationship between virtual social interaction and the degree of loneliness based on algorithm matching technologies: A quantitative analysis on the SOUL APP-A virtual social software for strangers. *PLoS One*, 3:19.
150. eSafety Commissioner (2025). Online risks for children in your community. Accessed on 17 June 2026.
151. 5Rights Foundation (2021). Pathways: How digital design puts children at risk. p.5.

152. Cataldo, I., Lepri, B., Neoh, M. J. Y., Esposito, G. (2021). Social Media Usage and Development of Psychiatric Disorders in Childhood and Adolescence: A Review. *Frontiers in Psychiatry*, 11.
Bottaro, R., Faraci, P. (2022). The use of social networking sites and its impact on adolescents' emotional well-being: A scoping review. *Current Addiction Reports*, 9, 518–539.
153. Keles, B., McCrae, N., Grealish, A. (2020). A systematic review: The influence of social media on depression, anxiety and psychological distress in adolescents. *International Journal of Adolescence and Youth*, 25 (1), 79–93.
Ivie, E. J., Pettitt, A., Moses, L. J., Allen, N. B. (2020). A meta-analysis of the association between adolescent social media use and depressive symptoms. *Journal of Affective Disorders*, 275, 165–174.
154. Cataldo, I., Lepri, B., Neoh, M. J. Y., Esposito, G. (2021). Social Media Usage and Development of Psychiatric Disorders in Childhood and Adolescence: A Review. *Frontiers in Psychiatry*, 11.
155. Bozzola, E., Spina, G., Agostiniani, R., Barni, S., Russo, R., Scarpato, E., Di Mauro, A., Di Stefano, A. V., Caruso, C., Corsello, G., Staiano, A. (2022). The use of social media in children and adolescents: Scoping review on the potential risks. *International Journal of Environmental Research and Public Health*, 19.
156. Course-Choi, J., Hammond, L. (2021). Social media use and adolescent well-being: A narrative review of longitudinal studies. *Cyberpsychology, Behavior, and Social Networking*, 24, 223–236.
157. Consumer Science and Analytics (2022). Les adolescents et l'info. Research by Milan Presse and YouTube.
Notley, T., Zhong, H.F., Dezuanni, M., et al. (2023) Comparing children's and teens' news engagement practices and affective news experiences. *Journal of Youth Studies*, 26 (7): 878–893.
158. University of Southern Denmark (2025). Children and misinformation on social media. Accessed on 25 June 2026.
159. University of Southern Denmark (2025). Children and misinformation on social media. Accessed on 17 June 2026.
160. Calvin, A., Lenhart, A., Mann, S., and Robb, M. (2025). Teens, Trust, and Technology in the Age of AI: Navigating Trust in Online Content. *Common Sense Media*.
161. European Parliament (2025). Youth survey 2024.
162. Ali, S., DiPaola, D., Lee, I., et al. (2021). Children as creators, thinkers and citizens in an AI-driven future. *Computers and Education: Artificial Intelligence*, 2.
163. Howard, P.N., et al. (2021). Digital Misinformation / disinformation and children. UNICEF.
Melchior, C., Oliveira, M. (2024) A systematic literature review of the motivations to share fake news on social media platforms and how to fight them. *New Media and Society*, 26 (2): 1127–1150.
164. Howard, P.N., et al. (2021). Digital Misinformation / disinformation and children. UNICEF.
165. Ma, I., Mubashir, S., Kozyreva, A., van den Bos, W. (2025). Understanding the impact of misinformation on adolescents. *Nature Human Behaviour*, 10, 18–28.
166. NewsGuard (2021). Toxic TikTok: Popular social-media video app feeds vaccine misinformation to kids within minutes after they sign up. Accessed on 17 June 2026.
167. Ludwig-Walz, H., Bujard, M., Fegert, J.M., et al. (2025). Integrating European contexts and needs into WHO guiding principles on online mental health content for young people: Five recommendations. *European Child and Adolescent Psychiatry*, Vol. 34, 1221–1224.
168. Moss, C., Wibberley, C., Witham, G. (2023). Assessing the impact of Instagram use and deliberate self-harm in adolescents: A scoping review. *International Journal of Mental Health Nursing*, 32, 14–29.
169. World Health Organization (2025). Suicide worldwide in 2021: Global health estimates.
170. Arendt, F., Scherr, S., Romer, D. (2019). Effects of exposure to self-harm on social media: Evidence from a two-wave panel study among young adults. *New Media and Society*, Vol. 21 (11-12).
Nesi, J., et al. (2022). Social Media Use and Self-Injurious Thoughts and Behaviors: A Systematic Review and Meta-Analysis. *Clinical Psychology Review*, 8;87.
171. Nesi, J., et al. (2022). Social Media Use and Self-Injurious Thoughts and Behaviors: A Systematic Review and Meta-Analysis. *Clinical Psychology Review*, 8;87.
172. Memon, A. M., Sharma, S. G., Mohite, S. S., Jain, S. (2018). The role of online social networking on deliberate self-harm and suicidality in adolescents: A systematized review of literature. *Indian Journal of Psychiatry*, 60 (4).
173. Nesi, J., et al. (2022). Social Media Use and Self-Injurious Thoughts and Behaviors: A Systematic Review and Meta-Analysis. *Clinical Psychology Review*, 8;87.
174. Beullens, K., Bozzola, E., Cataldo, I., Hale, L., Kent, M., Montag, C., Nivins, S., O'reilly, M., Rubæk, L., Schiøtz Thorud, H.-M., Sterpenich, V., Vandenbosch, L. (2025). Minors' health and social media: an interdisciplinary scientific perspective. Manolios, S., Sala, A., Sundorph, E., Chaudron, S., Gomez, E. (editors), Publications Office of the European Union, Luxembourg.
175. Yue, C., Wenyaoy, G., Xudong, Y., Shuang, S., Zhuying, S., Yizheng, Z., Linlin, Z., Jinxin, C., Xingqi, W., Yujia, L. (2023). Dose-response relationship between daily screen time and the risk of low back pain among

- children and adolescents: A meta-analysis of 57831 participants. *Environmental Health and Preventive Medicine*, 28, 64–64.
176. American Optometric Association. (Undated). Computer vision syndrome (Digital eye strain). American Optometric Association. Accessed 29 June 2026.
Thorud, H.-M. S., Aurjord, R., Falkenberg, H. K. (2021). Headache and musculoskeletal pain in school children are associated with uncorrected vision problems and need for glasses: A case-control study. *Scientific Reports*, 11(1).
Thorud, H.-M. S., Mork, R., Bjørset, C. O., Gilson, S. J., Hagen, L. A., Langaas, T., Pedersen, H. R., Svarverud, E., Vikesdal, G. H., Baraas, R. C. (2022). Labouring reading and musculoskeletal pain in school children – the role of lifestyle behaviour and eye wear: A cross-sectional study. *BMC Pediatrics*, 22(1).
Thorud, H.-M. S., Mudvari, P. R., Falkenberg, H. K. (2024). Academic performance and musculoskeletal pain in adolescents with uncorrected vision problems. *BMC Pediatrics*, 24(1).
 177. Bozzola, E., Irrera, M., Hellmann, R., Crugliano, S., Fortunato, M. (2024). Media Device Use and Vision Disorders in the Pediatric Age: The State of the Art. *Children (Basel, Switzerland)*, 11(11).
 178. Morningstar, B., Clayborne, Z., Wong, S.L., Roberts, K.C., Prince, S.A., Gariépy, G., Goldfield, G.S., Janssen, I., Lang, J.J. (2023). The association between social media use and physical activity among Canadian adolescents: a Health Behaviour in School-aged Children (HBSC) study. *Canadian Journal of Public Health*, 114(4): 642–650.
Foreman, J., Salim, A.T., Praveen, A., Fonseka, D., Ting, D.S.W., Guang He, M., Bourne, R.R.A., Crowston, J., Wong, T.Y., Dirani, M. (2021). Association between digital smart device use and myopia: a systematic review and meta-analysis. *Lancet Digit Health*, 3(12).
Ahmed, O., Walsh, E.I., Dawel, A., Alateeq, K., Espinoza Oyarce, D.A., Cherbuin, N. (2024) Social media use, mental health and sleep: A systematic review with meta-analyses. *Journal of Affective Disorders*, 15;367: 701–712.
Purba, A.K., Thomson, R.M., Henery, P.M., Pearce, A., Henderson, M., Katikireddi, S.V. (2023) Social media use and health risk behaviours in young people: systematic review and meta-analysis. *BMJ*, 383.
 179. Czeisler, C. A. (2015). Duration, timing and quality of sleep are each vital for health, performance and safety. *Sleep Health*, 1(1), 5–8.
Matricciani, L., Paquet, C., Galland, B., Short, M., Olds, T. (2019). Children's sleep and health: A meta-review. *Sleep Medicine Reviews*, 46, 136–150.
Short, M. A., Blunden, S., Rigney, G., Matricciani, L., Coussens, S., M Reynolds, C., Galland, B. (2018). Cognition and objectively measured sleep duration in children: A systematic review and meta-analysis. *Sleep Health*, 4(3), 292–300.
 180. Wheaton, A. G., Claussen, A. H. (2021). Short Sleep Duration Among Infants, Children, and Adolescents Aged 4 Months–17 Years – United States, 2016–2018. *MMWR. Morbidity and Mortality Weekly Report*, 70(38).
Gariépy, G., et al. (2020). How Are Adolescents Sleeping? Adolescent Sleep Patterns and Sociodemographic Differences in 24 European and North American Countries. *Journal of Adolescent Health*, 66 (6) Supplement.
 181. Chang, A.M., Aeschbach, D., Duffy, J. F., Czeisler, C. A. (2015). Evening use of light-emitting eReaders negatively affects sleep, circadian timing, and next-morning alertness. *Proceedings of the National Academy of Sciences*, 112(4), 1232–1237.
Hale, L., Guan, S. (2015). Screen time and sleep among school-aged children and adolescents: A systematic literature review. *Sleep Medicine Reviews*, 21, 50–58.
 182. Tähkämö, L., Partonen, T., Pesonen, A.K. (2019). Systematic review of light exposure impact on human circadian rhythm. *Chronobiology International*, 36(2): 151–170.
 183. Lund, L., Sølvhøj, I. N., Danielsen, D., Andersen, S. (2021). Electronic media use and sleep in children and adolescents in western countries: A systematic review. *BMC Public Health*, 21(1), 1598.
 184. Mammeri, K., Riontino, L., Schwartz, S., Sterpenich, V. (2025). Influence of parental rules about screen electronic device use in the evening on sleep in adolescents. *Discover Public Health*, 22:517
 185. Perrault, A. A., Bayer, L., Peuvrier, M., Afyouni, A., Ghisletta, P., Brockmann, C., Spiridon, M., Hulo Vesely, S., Haller, D. M., Pichon, S., Perrig, S., Schwartz, S., Sterpenich, V. (2019). Reducing the use of screen electronic devices in the evening is associated with improved sleep and daytime vigilance in adolescents. *Sleep*, 42(9).
Bartel, K., Scheeren, R., Gradisar, M. (2019). Altering Adolescents' Pre-Bedtime Phone Use to Achieve Better Sleep Health. *Health Communication*, 34(4), 456–462.
 186. World Health Organization. Regional Office for Europe (2024) A focus on adolescent social media use and gaming in Europe, central Asia and Canada: Health Behaviour in School-aged Children international report from the 2021/2022 survey.
 187. Digital Services Act.
 188. European Commission (2023). Consumer protection: manipulative online practices found on 148 out of 399 online shops screened.
 189. Flayelle, M., et al. (2023). A taxonomy of technology design features that promote potentially addictive online behaviours. *Nature Reviews Psychology*, 2: 136–150.
Perales, J.C., et al. (2020). Learning to lose control: A process-based account of behavioral addiction. *Neuroscience and biobehavioural reviews*, 108: 771–780.

190. van der Wal, A., Beyens, I., Janssen, L.H.C., Valkenburg, P.M. (2025). Diverse platforms, diverse effects: Evidence from a 100-day study on social media and adolescent mental health. *Current Psychology*, 45 (36).
191. Owenz, M., Freed, R. (2021). The ethics of persuasive design in technology used by children and adolescents. *Ethical Human Psychology Psychiatry*, 23, 89–99.
192. Andreassen, C.S., et al. (2016). The Relationship between Addictive Use of Social Media and Video Games and Symptoms of Psychiatric Disorders: A Large-Scale Cross-Sectional Study. *Psychology of Addictive Behaviors*. 30(2): 252–62.
193. European Commission (2024). Commission Staff Working Document Fitness Check on EU consumer law on digital fairness.
194. Saura, J.R., Palacios-Marqués, D., Iturricha-Fernández, A. (2021). Ethical design in social media: Assessing the main performance measurements of user online behavior modification. *Journal of Business Research*, 129.
195. United Nations (2021). General comment No. 25 (2021) on children's rights in relation to the digital environment. Committee on the Rights of the Child. European Commission (2025). Guidelines on measures to ensure a high level of privacy, safety and security for minors online, pursuant to Article 28(4) of Regulation (EU) 2022/2065.
196. Curtis, B. L., Lookatch, S. J., Ramo, D. E., McKay, J. R., Feinn, R. S., Kranzler, H. R. (2018). Meta-Analysis of the Association of Alcohol-Related Social Media Use with Alcohol Consumption and Alcohol-Related Problems in Adolescents and Young Adults. *Alcoholism: Clinical and Experimental Research*, 42(6), 978–986. Vannucci, A., Simpson, E. G., Gagnon, S., Ohannessian, C. M. (2020). Social media use and risky behaviors in adolescents: A meta-analysis. *Journal of Adolescence*, 79(1), 258–274.
197. Beullens, K., Schepers, A. (2013). Display of alcohol use on Facebook: A content analysis. *Cyberpsychology, Behavior and Social Networking*, 16(7), 497–503. Vanherle, R., Hendriks, H., Beullens, K. (2023). Only for Friends, Definitely Not for Parents: Adolescents' Sharing of Alcohol References on Social Media Features. *Mass Communication and Society*, 26(1), 47–73. Vranken, S., Kurten, S., Beullens, K. (2024). Time to 'Wine': A Content Analysis Investigating How Social Media Influencers Refer to Alcohol Use in Instagram's Feed Posts and Stories. *Mass Communication and Society*, 27(6), 1468–1494.
198. Geusens, F., Beullens, K. (2018). The Association Between Social Networking Sites and Alcohol Abuse Among Belgian Adolescents: The Role of Attitudes and Social Norms. *Journal of Media Psychology*, 30(4), 207–216.
- Geusens, F., Beullens, K. (2021). Triple spirals? A three-wave panel study on the longitudinal associations between social media use and young individuals' alcohol consumption. *Media Psychology*, 24(6), 766–791. Vanherle, R., Hendriks, H., Beullens, K. (2023). Only for Friends, Definitely Not for Parents: Adolescents' Sharing of Alcohol References on Social Media Features. *Mass Communication and Society*, 26(1), 47–73.
199. Geusens, F., Beullens, K. (2018). The Association Between Social Networking Sites and Alcohol Abuse Among Belgian Adolescents: The Role of Attitudes and Social Norms. *Journal of Media Psychology*, 30(4), 207–216. Geusens, F., Beullens, K. (2019). A Longitudinal Examination of the Moderating Influence of Peer and Parental Socialization on Alcohol-Related Social Media Self-Effects Among Late Adolescents. *Media Psychology*, 22(2), 273–297. Geusens, F., Beullens, K. (2021). Triple spirals? A three-wave panel study on the longitudinal associations between social media use and young individuals' alcohol consumption. *Media Psychology*, 24(6), 766–791. Vanherle, R., Hendriks, H., Beullens, K. (2023). Only for Friends, Definitely Not for Parents: Adolescents' Sharing of Alcohol References on Social Media Features. *Mass Communication and Society*, 26(1), 47–73.
200. Geusens, F., Beullens, K. (2019). A Longitudinal Examination of the Moderating Influence of Peer and Parental Socialization on Alcohol-Related Social Media Self-Effects Among Late Adolescents. *Media Psychology*, 22(2), 273–297.
201. Rutherford, B.N., et al. (2025). #TurntTrending: a systematic review of substance use portrayals on social media platforms. *Addiction*, 8;118 (2).
202. Liu, J., Charmaraman, L., Bickham, D. (2024). Association between social media use and substance use among middle and high school-aged youth. *Substance Use and Misuse*, 59 (7).
203. Europol (2025). Europol coordinates operation against terrorist content online targeting minors. Accessed on 29 June 2026.
204. Europol (2026). 2025 Serious and Organised Crime Threat Assessment (SOCTA): The changing DNA of serious and organised crime.
205. Smahel, D., Machackova, H., Mascheroni, G., Dedkova, L., Staksrud, E., Ólafsson, K., Livingstone, S., Hasebrink, U. (2020). EU Kids Online 2020: Survey results from 19 countries. EU Kids Online. Dreßing, H., Hoell, A., Scharmann, L., Simon, A. M., Haag, A. C., Dölling, D., Meyer-Lindenberg, A., Fegert, J. M. (2025). Sexual Violence Against Children and Adolescents: A German Nationwide Representative Survey on Its Prevalence, Situational Context, and Consequences. *Deutsches Ärzteblatt International*, 122(11), 285.

206. Chauviré-Geib, K., et al. (2025). The increase in online child sexual solicitation and abuse: Indicator 16.2.3 of the UN Sustainable Development Goals (SDG) documents a hidden and growing pandemic. Population-based surveys fail to capture the full picture. *Child Abuse and Neglect*, 164.
Dreßing, H., Hoell, A., Scharmann, L., Simon, A. M., Haag, A. C., Dölling, D., Meyer-Lindenberg, A., Fegert, J. M. (2025). Sexual Violence Against Children and Adolescents: A German Nationwide Representative Survey on Its Prevalence, Situational Context, and Consequences. *Deutsches Ärzteblatt International*, 122(11), 285.
207. Internet Watch Foundation (2026). 2025 Internet Watch Foundation Annual Data and Insights Report.
208. Insoll, T., Ovaska, A., Vaaranen-Valkonen, N. (2024). CSAM Users in the Dark Web: Protecting Children Through Prevention. *Protect Children*.
209. Internet Watch Foundation (2026). 2025 Internet Watch Foundation Annual Data and Insights Report.
210. Our Voice (2025) Survey for survivors of sexual violence in childhood – voices of the Nordic survivors.
211. Haag, A. C., Bonanno, G. A., Chen, S., Herd, T., Strong-Jones, S., S. S., Noll, J. G. (2023). Understanding posttraumatic stress trajectories in adolescent females: A strength-based machine learning approach examining risk and protective factors including online behaviors. *Development and Psychopathology*, 35 (4).
212. Chauviré-Geib, K., Fegert, J. M. (2023). Victims of Technology-Assisted Child Sexual Abuse: A Scoping Review. *Trauma, Violence, & Abuse*, 25(2).
213. Haag, A. C., Bonanno, G. A., Chen, S., Herd, T., Strong-Jones, S., S. S., Noll, J. G. (2023). Understanding posttraumatic stress trajectories in adolescent females: A strength-based machine learning approach examining risk and protective factors including online behaviors. *Development and Psychopathology*, 35 (4).
214. Chauviré-Geib, K., Fegert, J. M. (2023). Victims of Technology-Assisted Child Sexual Abuse: A Scoping Review. *Trauma, Violence, & Abuse*, 25(2).
215. Haag, A. C., Bonanno, G. A., Chen, S., Herd, T., Strong-Jones, S., S. S., Noll, J. G. (2023). Understanding posttraumatic stress trajectories in adolescent females: A strength-based machine learning approach examining risk and protective factors including online behaviors. *Development and Psychopathology*, 35 (4).
Chauviré-Geib, K., Fegert, J. M. (2023). Victims of Technology-Assisted Child Sexual Abuse: A Scoping Review. *Trauma, Violence, & Abuse*, 25(2).
216. Haag, A. C., Bonanno, G. A., Chen, S., Herd, T., Strong-Jones, S., S. S., Noll, J. G. (2023). Understanding posttraumatic stress trajectories in adolescent females: A strength-based machine learning approach examining risk and protective factors including online behaviors. *Development and Psychopathology*, 35 (4).
Chauviré-Geib, K., Fegert, J. M. (2023). Victims of Technology-Assisted Child Sexual Abuse: A Scoping Review. *Trauma, Violence, & Abuse*, 25(2).
217. Chauviré-Geib, K., Gerke, J., Haag, A. C., Sachser, C., Finkelhor, D., Rassenhofer, M., Fegert, J. M. (2025). The increase in online child sexual solicitation and abuse: Indicator 16.2.3 of the UN Sustainable Development Goals (SDG) documents a hidden and growing pandemic. *Child Abuse Neglect*, 164.
218. Eurostat (2025). EU Terrorism Situation and Trend Report.
219. Krahé, B., Möller, I., Huesmann, L.R., Kirwil, L., Felber, J., Berger, A. (2011). Desensitization to Media Violence: Links With Habitual Media Violence Exposure, Aggressive Cognitions, and Aggressive Behavior. *Journal of Personality and Social Psychology*, 100(4).
220. Article 17 GDPR.
221. European Data Protection Board (2022). Guidelines 9/2022 on personal data breach notification under GDPR. Version 2.
222. Schlegel, L., (2022). Playing Against Radicalization: Why extremists are gaming and how P/CVE can leverage the positive effects of video games to prevent radicalization.
223. European Commission (2023). Understanding the value of a European video games society – Final report. Directorate-General for Communications Networks, Content and Technology (DG CNECT), ECORYS and KEA, section. 5.1.2.
Kowert, R., et al. (2026). Editorial: Extremism in games. *Frontiers in Psychology*, Vol. 16, p. 12.
224. European Commission (2025). The European media industry outlook – September 2025. Directorate-General for Communications Networks, Content and Technology (DG CNECT), p. 99.
225. Radicalisation Awareness Network (2021). Digital Grooming Tactics on Video Gaming & Video Gaming Adjacent Platforms: Threats and Opportunities – Conclusion paper.
226. Brooks, G.A., Clark, L. (2019). Associations between loot box use, problematic gaming and gambling, and gambling-related cognitions. *Addictive Behaviors*, 96.
227. Boniel-Nissim, M., Marino, C., Galeotti, T., Blinka, L., Ozoliņa, K., Craig, W., et al. (2024). A focus on adolescent social media use and gaming in Europe, central Asia and Canada. Health Behaviour in School-aged Children international report from the 2021/2022 survey. Volume 6. WHO Regional Office for Europe.
228. PEGI (2026). PEGI expands age rating criteria with interactive risk categories. Accessed on 17 June 2026.

229. OECD (2021). Children in the digital environment – Revised typology of risks.
230. Livingstone, S., Stoilova, M. (2021). The 4Cs: Classifying Online Risk to Children (1.0.0).
231. European Commission, Joint Research Centre
232. Beullens, K., Bozzola, E., Cataldo, I., Hale, L., Kent, M., Montag, C., Nivins, S., O'reilly, M., Rubæk, L., Schiøtz Thorud, H.-M., Sterpenich, V., Vandenbosch, L. (2025). Minors' health and social media: an interdisciplinary scientific perspective. Manolios, S., Sala, A., Sundorph, E., Chaudron, S., Gomez, E. (editors), Publications Office of the European Union, Luxembourg.
233. Bursztyn, L., Duckworth, A., JiménezDurán, R., Leonard, A., Milojević, F., Roth, C., Sunstein, C. R. (2026). Why bans fail: Tipping points and Australia's socialmedia ban. (BFI Working Paper No. 202657). Becker Friedman Institute for Economics.
234. Article 28 DSA.
235. Articles 34 and 35 DSA.
236. Article 25 GDPR.
237. Article 6(1) GDPR.
238. Article 4(11) GDPR.
239. EDPB Guidelines 05/2020 on consent under Regulation 2016/679, pp. 62.
240. Case C-252/21, Meta v. Bundeskartellamt (ECLI:EU:C:2023:537), paragraph 106.
241. CJEU C-252/21 Bundeskartellamt, paragraph 111.
242. EDPB guidelines on legitimate interest, para 96.
243. EDPB Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR, §54. Case C-252/21, Meta v. Bundeskartellamt (ECLI:EU:C:2023:537), paragraph 111.
244. EDPB Guidelines 8/2020 on the targeting of social media users, paragraph 16.
245. EDPB guidelines on legitimate interest, paragraph 95.
246. Article 17 and recital 65 GDPR.
247. Article 22 and recital 71 GDPR.
248. Recital 38 GDPR.
249. Article 29 Data Protection Working Party Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679.
250. Article 35 and 36 GDPR.
251. European Commission (2026). Draft Commission guidelines on the classification of high-risk AI systems.
252. European Commission (2025). Commission publishes the Guidelines on prohibited artificial intelligence (AI) practices, as defined by the AI Act. Accessed on 2 July 2026.
253. European Commission (2026). The General-Purpose AI Code of Practice.
254. Article 50 AI Act.
255. European Commission (2026). Code of Practice on marking and labelling of AI-generated content.
256. European Commission (2026). Draft of the guidelines on the implementation of the transparency obligations for certain AI systems under Article 50 of the AI Act.
257. European Commission (2021). UCPD Guidelines.
258. Digital Fairness Fitness Check
259. European Commission (2026). Action Plan against Cyberbullying.
260. European Commission (2024). Commission Recommendation on developing and strengthening integrated child protection systems in the best interests of the child.
261. European Commission (2024). TikTok commits to permanently withdraw TikTok Lite Rewards programme from the EU to comply with the Digital Services Act. Accessed on 2 July 2026.
262. Article 82 DSA.
263. European Commission (2026). Commission preliminarily finds TikTok's addictive design in breach of the Digital Services Act. Accessed on 2 July 2026.
264. European Commission (2026). Commission preliminarily finds Pornhub, Stripchat, XNXX and XVideos in breach of the Digital Services Act for allowing minors to access their services. Accessed on 2 July 2026.
265. European Commission (2025). The European Board for Digital Services launches a coordinated action to reinforce the protection of minors as regards pornographic platforms. Accessed on 2 July 2026.
266. European Commission (2026). Commission preliminarily finds Meta in breach of Digital Services Act for failing to prevent minors under 13 from using Instagram and Facebook. Accessed on 2 July 2026.
267. European Commission (2026). Commission investigates Snapchat's compliance with child protection rules under the Digital Services. Accessed on 2 July 2026.
268. European Commission (2025). Commission accepts commitments offered by AliExpress under the DSA and takes further action. Accessed on 2 July 2026. European Commission (2026). Commission launches investigation into Shein under the Digital Services Act. Accessed on 2 July 2026.

- European Commission (2025). Commission preliminarily finds Temu in breach of the Digital Services Act. Accessed on 2 July 2026.
- 269.** Authority for Consumers and Markets (2026). ACM launches investigation into Roblox in connection with risks that minors are facing. Accessed on 2 July 2026.
- 270.** European Commission (2026). Commission investigates Grok and X's recommender systems under the Digital Services Act. Accessed on 2 July 2026.
- 271.** European Commission (2026). Commission launches investigation into Shein under the Digital Services Act. Accessed on 2 July 2026.
- 272.** European Commission (2024). Commission opens formal proceedings against Temu under the Digital Services Act. Accessed on 2 July 2026.
- 273.** Article 53 AI Act.
- 274.** Article 55 AI Act.
- 275.** DLA Piper (2026). DLA Piper GDPR Fines and Data Breach Survey: January 2026.
- 276.** Data Protection Commission (2023). Annual Report 2023.
- 277.** Data Protection Commission (2023). Irish Data Protection Commission announces €345 million fine of TikTok. Accessed on 2 July 2026.
- 278.** Data Protection Commission (2022). Data Protection Commission announces decision in Instagram Inquiry. Accessed on 2 July 2026.
- 279.** Garante per la Protezione dei Dati Personali (2021). Provvedimento del 22 gennaio 2021.
- 280.** Data Protection Commission (2026). Data Protection Commission opens investigation into X (XIUC). Accessed on 2 July 2026.
- 281.** Art 15 EMFA.
- 282.** European Commission (undated). Social media, online games and search engines. Accessed on 24 June 2026.
- 283.** European Commission (undated). Social media, online games and search engines. Accessed on 24 June 2026.
- 284.** European Commission (undated). Sweeps. Accessed on 24 June 2026.
- 285.** European Commission (undated). Influencer Legal Hub. Accessed on 24 June 2026.
- 286.** European Commission (undated). Social media, online games and search engines. Accessed on 24 June 2026.
- 287.** Article 37 DSA.
- 288.** Article 38 DSA.
- 289.** FRA (2025). Towards Integrated Child Protection Systems - Challenges, promising practices and ways forward, p.79.
- 290.** Popat, A., Tarrant, C. (2023). Exploring adolescents' perspectives on social media and mental health and well-being – A qualitative literature review. Special Issue: Social Media and Mental Health, 28 (1), p. 329.
- 291.** Singleton, A., Abeles, P., Smith, I.C. (2016). Online social networking and psychological experiences: The perceptions of young people with mental health difficulties. Computers in Human Behavior, vol. 61.
- 292.** Sala, A., Porcaro, L., and Gómez, E. (2024). Social Media Use and adolescents' mental health and well-being: An umbrella review. Computers in Human Behavior Reports, vol. 14, p. 8.
- 293.** Sala, A., Porcaro, L., and Gómez, E. (2024). Social Media Use and adolescents' mental health and well-being: An umbrella review. Computers in Human Behavior Reports, vol. 14, p. 8.
- 294.** Sala, A., Porcaro, L., and Gómez, E. (2024). Social Media Use and adolescents' mental health and well-being: An umbrella review. Computers in Human Behavior Reports, vol. 14, p. 8.
- 295.** Sala, A., Porcaro, L., and Gómez, E. (2024). Social Media Use and adolescents' mental health and well-being: An umbrella review. Computers in Human Behavior Reports, vol. 14, p. 8.
- 296.** Anderson, M., Vogels, E.A., Perrin, A., Lee, R. (2022). Connection, Creativity and Drama: Teen Life on Social Media in 2022. Pew Research Center. As cited in: Manolios, S., Chaudron, S., Fortuna, P., Sala, A., Gomez, E. (2026). Opportunities for young users on social media. European Commission, Joint Research Centre (JRC), Seville, JRC147510.
- 297.** Sala, A., Porcaro, L., and Gómez, E. (2024). Social Media Use and adolescents' mental health and well-being: An umbrella review. Computers in Human Behavior Reports, vol. 14, p. 8.
- 298.** Shankleman, M., Hammond, L., Jones, F.W. (2021). Adolescent Social Media Use and Well-Being: A Systematic Review and Thematic Meta-synthesis. Adolescent Research Review, vol. 6.
- 299.** Shankleman, M., Hammond, L., Jones, F.W. (2021). Adolescent Social Media Use and Well-Being: A Systematic Review and Thematic Meta-synthesis. Adolescent Research Review, vol. 6.
- 300.** Popat, A., Tarrant, C. (2023). Exploring adolescents' perspectives on social media and mental health and well-being – A qualitative literature review. Special Issue: Social Media and Mental Health, 28 (1), p. 329.
- 301.** Hillmayr, D., Zierwald, L., Reinhold, F., Hofer, S.I., Reiss, K.M. (2020). The potential of digital tools to enhance mathematics and science learning in secondary schools: A context-specific meta-analysis. Computers & Education, vol. 153.

- 302.** Timotheou, S., Miliou, O., Dimitriadis, Y., Villagrà Sobrino, S., Giannoutsou, N., Cachia, R., Martínez Monés, A., Ioannou, A. (2022). Impacts of digital technologies on education and factors influencing schools' digital capacity and transformation: A literature review. Education and Information Technologies, vol. 28.
- 303.** Forsström, S., Njå, M., Munthe, E., Houldsworth, L., Álvarez-Galván, J.-L. (2025). Key findings and integration strategies on the impact of digital technologies on students' learning: Results from a literature review. OECD Education Working Paper No. 336.
Barrot, J.S. (2022). Social media as a language learning environment: A systematic review of the literature (2008-2019). Computer Assisted Language Learning, 35 (9).
Zachos, G., Paraskevopoulou-Kollia, E.-A., Anagnostopoulos, I. (2018). Social Media Use in Higher Education: A Review. Education Sciences, 8 (4), Article 4.
- 304.** Forsström, S., Njå, M., Munthe, E., Houldsworth, L., Álvarez-Galván, J.-L. (2025). Key findings and integration strategies on the impact of digital technologies on students' learning: Results from a literature review. OECD Education Working Paper No. 336.
- 305.** Villar Onrubia, D., Cachia, R., Rietz, C., Feltrero, R., Niemi, H. et al. (2025). Generative Artificial Intelligence in secondary education – Uses and perceptions from the perspective of early adopters across five EU Member States. Luxembourg, JRC144345.
Forsström, S., Njå, M., Munthe, E., Houldsworth, L., Álvarez-Galván, J.-L. (2025). Key findings and integration strategies on the impact of digital technologies on students' learning: Results from a literature review. OECD Education Working Paper No. 336.
- 306.** Villar Onrubia, D., Cachia, R., Rietz, C., Feltrero, R., Niemi, H. et al. (2025). Generative Artificial Intelligence in secondary education – Uses and perceptions from the perspective of early adopters across five EU Member States. Luxembourg, JRC144345.
- 307.** Villar Onrubia, D., Cachia, R., Rietz, C., Feltrero, R., Niemi, H. et al., (2025). Generative Artificial Intelligence in secondary education – Uses and perceptions from the perspective of early adopters across five EU Member States. Luxembourg, JRC144345.
- 308.** Timotheou, S., Miliou, O., Dimitriadis, Y., Villagrà Sobrino, S., Giannoutsou, N., Cachia, R., Martínez Monés, A., Ioannou, A. (2022). Impacts of digital technologies on education and factors influencing schools' digital capacity and transformation: A literature review. Education and Information Technologies, vol. 28.
- 309.** Crêteur, S., Dunajeva, J., Frydman, B., Berg Mulvik, I., Del Cogliano, D., Nada, C., Siarova, H., Sankalaite, S. (2026). Mobile phone bans in schools across the EU: ENESET analytical report. European Commission, Directorate-General for Education, Youth, Sport and Culture (DG EAC).
- 310.** European Commission (2026). Better Internet for Kids: Review of the year 2025. Accessed on 2 July 2026.
- 311.** European Commission (2026). Better Internet for Kids: Review of the year 2025. Accessed on 2 July 2026.
- 312.** European Commission (2024). International Computer and Information Literacy Study (ICILS) in Europe, 2023: Main findings and educational policy implications. Directorate-General for Education, Youth, Sport and Culture (DG EAC).
- 313.** European Commission (2025). Education and Training Monitor: Comparative Report. Chapter 2 – Young people's basic skills.
- 314.** European Commission (2026). The teaching profession in the EU – A comparative analysis building upon the TALIS 2024 results. Directorate-General for Education, Youth, Sport and Culture (DG EAC).
- 315.** Council conclusions on promoting and protecting the mental health of children and adolescents in the digital era.
- 316.** COFACE Families Europe (2026). Towards digital safety and well-being for children and their families: Moving beyond social media age restrictions as the sole solution.
- 317.** Council conclusions on promoting and protecting the mental health of children and adolescents in the digital era.
- 318.** European Commission (2025). Flash Eurobarometer survey: Future needs in digital education.
- 319.** European Commission (2026). New guidelines to help teachers lead Europe's digital education. Accessed on 1 July 2026.
- 320.** European Commission (2026). Guidelines for teachers and educators on tackling disinformation and promoting digital literacy through education and training. Directorate-General for Education, Youth, Sport and Culture (DG EAC).
- 321.** OECD / European Union (2026). Empowering Learners for the Age of AI: An AI Literacy Framework for Primary and Secondary Education. OECD Publishing, Paris.
- 322.** Commission Recommendation (EU) 2024/1238 of 23 April 2024 on developing and strengthening integrated child protection systems in the best interests of the child.

- 323.** Article 24 Charter of Fundamental Rights of the European Union.
- 324.** European Commission (2025). Call to Action: from children to EU decision-makers. Accessed on 1 July 2026.
- 325.** O'Connell, R. (2021). Psychological first aid for Young Peers. Training manual. IFRC Reference Centre for Psychosocial Support, Copenhagen.
- 326.** O'Connell, R. (2021). Psychological first aid for Young Peers. Training manual. IFRC Reference Centre for Psychosocial Support, Copenhagen.
- 327.** O'Connell, R. (2021). Psychological first aid for Young Peers. Training manual. IFRC Reference Centre for Psychosocial Support, Copenhagen.
- 328.** O'Connell, R. (2021). Psychological first aid for Young Peers. Training manual. IFRC Reference Centre for Psychosocial Support, Copenhagen.
- 329.** European Commission (Undated). Promising practices – Summary. Denmark – Psychological First Aid for Young Peers.
- 330.** European Commission (2024). Best Practices Portal – Psychological First Aid for Young Peers. Accessed on 1 July 2026.
- 331.** Seguranet (2026) Digital Leaders | SeguraNet. Accessed on 7 July 2026.

