

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



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.

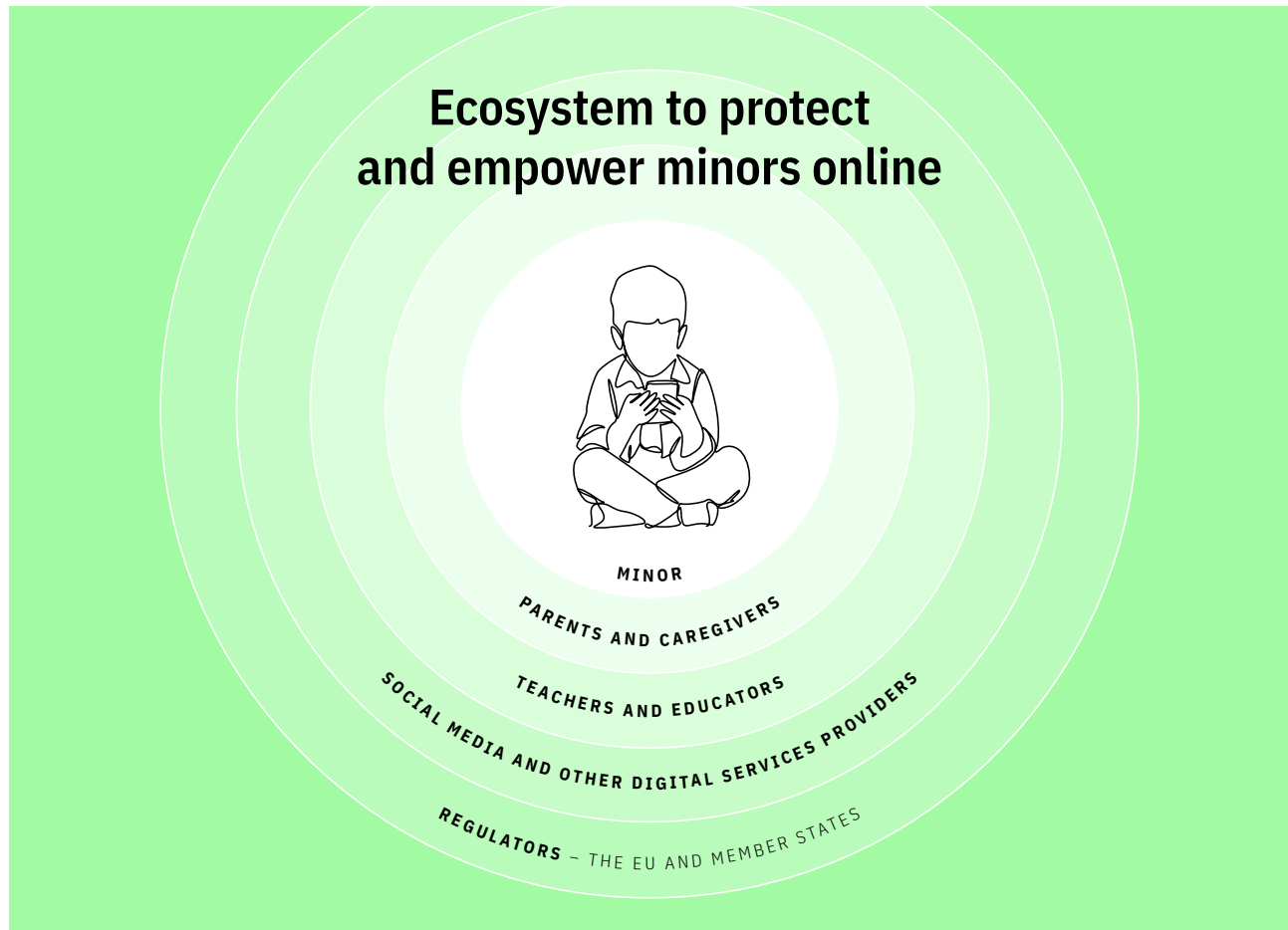
While social media and other digital services providers retain primary responsibility for the safety of their services, especially for minors, an **ecosystem of actors is needed to protect and empower children and adolescents in the social media+ environment.** From regulators who need to put in place 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

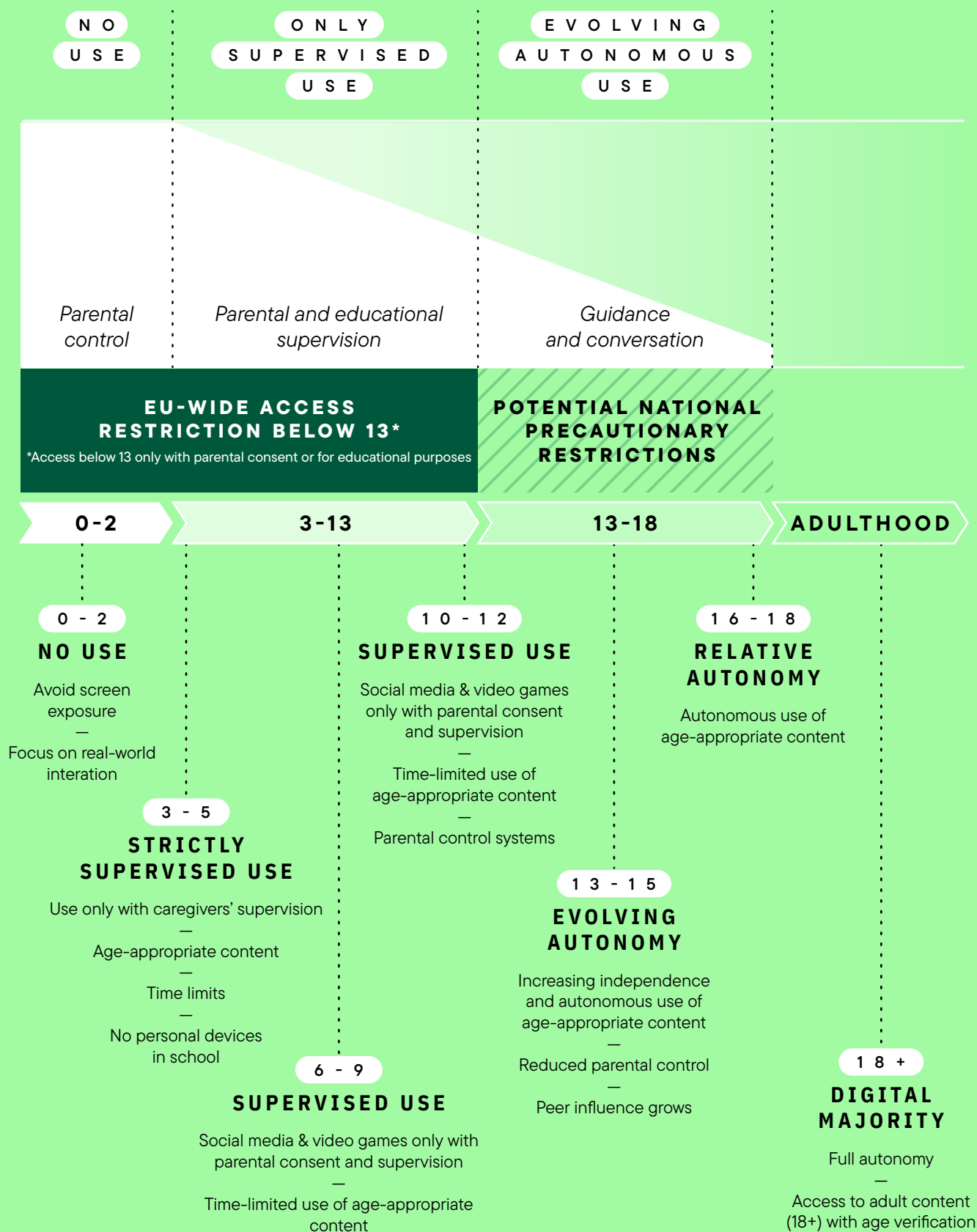
Children should not be allowed unsupervised use of internet-enabled devices. Schools should provide the facilities for supervised and limited use of devices for educational purposes supporting digital and media literacy, emotional resilience, and critical reflection on risks. Parents and caregivers should 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.

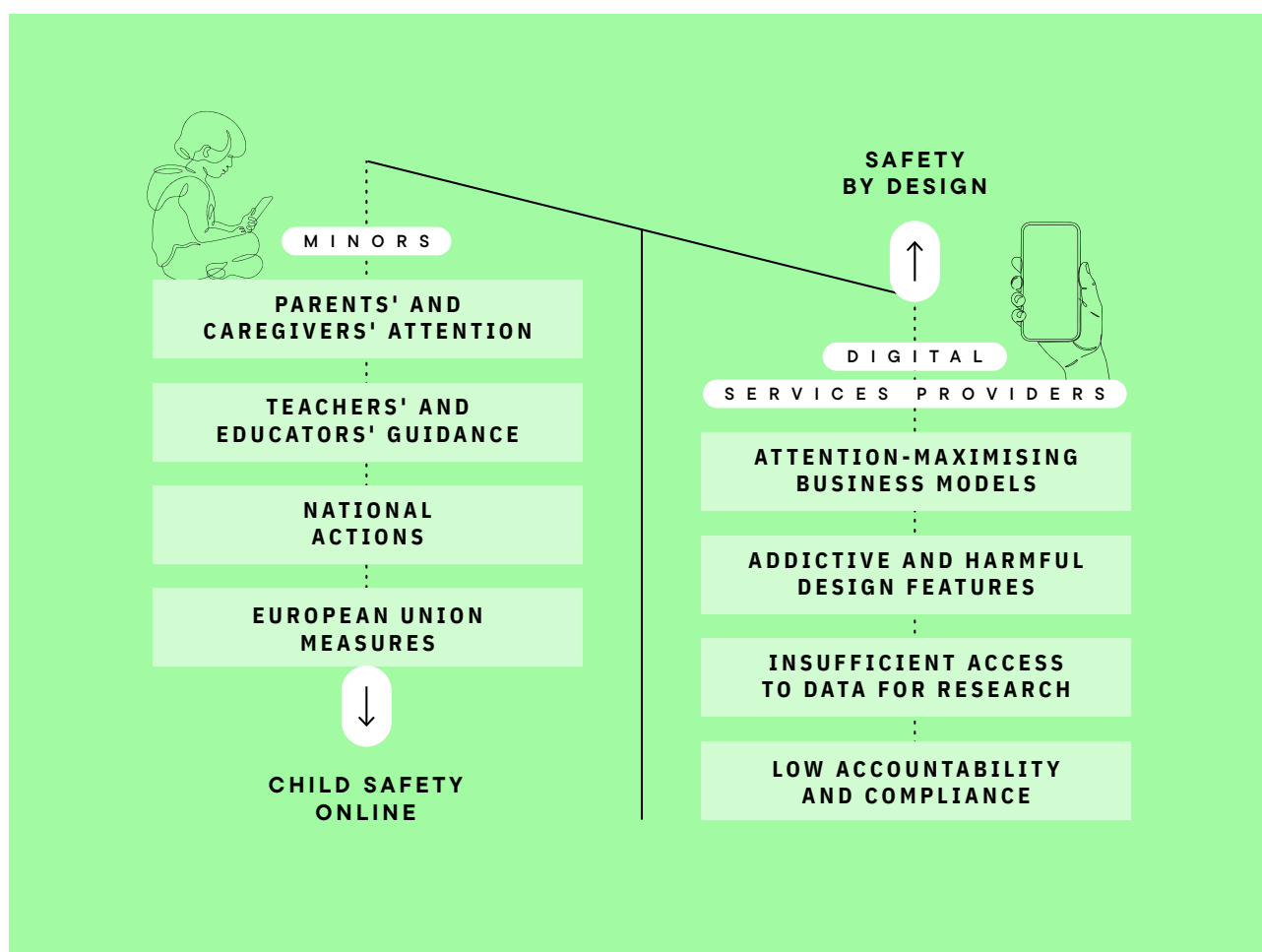
Funding should also support the further development of peer counselling, helplines, hotlines, educational resources, awareness-raising campaigns and capacity-building activities. Additional investment should be directed to increase the visibility, accessibility and reach of these facilities, including 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.



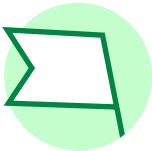
Protect your personal information – do not share private details such as your full name, address, school, phone number, passwords, or live location online.



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

