vodafone

Vodafone Foundation

Save the Children

PROTECTION THROUGH EMPOWERMENT: A POLICY WHITE PAPER ON THE ONLINE PROTECTION OF MINORS

INTRODUCTION

Vodafone, Vodafone Foundation, and Save the Children share a deep commitment to promoting child safety and wellbeing in the digital world. Each organisation brings distinct strengths to this shared mission.

Vodafone has long championed child online safety through its corporate initiatives. These include advocating for stronger policy measures, deploying tools and resources to support parents, and partnering with organisations such as the Internet Watch Foundation and the GSMA Mobile Alliance to combat digital child sexual exploitation. Vodafone's efforts have contributed to shaping safer digital environments and raising awareness of the risks children face online.

Vodafone Foundation works across more than 20 countries to connect for good. Through programmes like Skills Upload Jr, the Foundation is helping to close the digital divide by equipping over 10 million students and 600,000 teachers with essential digital skills. The Foundation promotes inclusive digital education, supports teachers with innovative tools, and fosters digital wellbeing through initiatives that encourage safe, confident, and responsible online engagement.

Save the Children, a global leader in child rights and protection, brings deep expertise in safeguarding children's wellbeing, both offline and online. In partnership with Vodafone Foundation, Save the Children co-developed the Children's Digital Wellbeing Partnership, which integrates child protection principles into digital education. This includes the SMILE framework (Security, Management, Identity, Literacy, Empathy), designed to help children navigate online spaces safely and ethically, while supporting educators to teach digital life skills.

Together, these organisations recognise that while progress has been made, the digital threat landscape continues to evolve. New platforms and technologies introduce fresh risks, and existing regulation often falls short in addressing the full spectrum of harms, from exposure to inappropriate content and grooming, to addictive design features.

To better protect children online, we jointly call for a European-wide mandate requiring robust, privacy-preserving age assurance across platforms and applications that expose users to harmful content or addictive features. This recommendation aligns with EU principles of proportionality and fundamental rights, complements existing regulation such as the Digital Services Act (DSA), and supports the goals of the General Data Protection Regulation (GDPR) and the European Strategy for a Better Internet for Kids (BIK+).

Our shared principle is that children have a right to participate in the digital

ecosystem. Exclusion by default is not a viable solution. Instead, we advocate for smart, inclusive design and regulation that empowers children, parents, and educators.

In practice, this means:

- Age-gating services intended for adults (e.g. gambling or pornography platforms)
- Designing platforms accessible to children in ways that reflect their developmental needs and vulnerabilities
- Equipping children, parents, and educators with digital literacy tools through a whole-school approach that is consistent across age groups, geographies, and socioeconomic backgrounds.

This policy paper outlines five key actions we recommend governments take to better protect and empower children online.

01

AGE VERIFICATION

1. AGE VERIFICATION

a. Problem definition

There is an overwhelming body of evidence on the impact of children accessing content which is either harmful or age-inappropriate, online. In data available from the Children's Commissioner in the UK has found that 10% of children surveyed had seen online pornography before the age of 9. This figure increases to 27% by the age of 11 and 50% at the age of 13. Concerningly 38% of 16 – 21-year-olds reported that they had accidentally accessed pornography online, suggesting the platforms hosting this material are not doing enough to adequately verify the ages of their users and prevent children from stumbling upon this content.

In European data, a 2020 study about online experience with children aged 9-16 from 19 countries in the European Union, 15% of children aged 9-11 reporting seeing sexual images in the previous 12 months, and this increased to 39% of children aged 12-14, and 61% of children aged 15-16.

The problem is not contained however to specifically adult sites. Social media and content sharing platforms are often used to disseminate material that, while not necessarily illegal, could certainly be harmful to users and age-inappropriate for children, for example hate speech, revenge porn, glorification of violence etc. The Youth Endowment Fund (YEF) commissioned a survey of 10,000 children aged 13 to 17 years old in England and Wales to explore their experiences with violence, both online and offline. The findings reveal that 70% of teenage children have encountered real-life violent content online in the past year.

Teenagers are frequently exposed to violent content made available by social media companies. Among those who reported seeing such material, 25% said they found it because social media platforms promoted it to them through features like 'Newsfeed', 'Stories' and 'For You' recommendations. Only 6% actively searched for it. Half said they saw it on someone else's profile or feed, and over a third (35%) had the content directly shared with them.

b. Regulatory gaps

Many of the trends above are not new, and policy makers have been grappling with the issue of age verification for several years.

UK:

The UK's Online Safety Act requires that platforms hosting pornography or other content harmful to children implement robust age verification measures to prevent minors from accessing such content. This includes using technologies like facial age estimation, digital identity wallets, and photo ID matching, among others. Ofcom, the regulatory body, expects these measures to be in place on applicable services by July 2025.

France:

In October 2024, Arcom, (Audiovisual and Digital Communication Regulatory Authority), announced new rules for adult operators and platforms with pornographic content. They must not show any content to a user until their age has been verified. These rules came into effect on 11th January 2025, with platforms given a transition period to implement suitable age verification solutions. That transitional period ended on 11th April. From this date, adult content sites must:

i) No longer use temporary methods like bank card verification.

ii) Only use age checks that are effective, privacy-preserving and data minimising

iii) Offer users at least one 'double blind approach'.

iv) Use an age verification provider that is legally and technically independent of any online platform hosting or providing porn content.

EU (Digital Services Act):

The EU Digital Services Act (DSA) explicitly lists protection of minors as a systemic risk, and mandates age verification for online platforms, particularly those accessible to minors, to protect their privacy and safety. This involves implementing measures like age assurance systems to restrict access to age-restricted content, parental controls, and reporting mechanisms for harmful content. Platforms may use various age verification methods, including digital identity solutions, to ensure users are of the required age for certain services. In July the EC released its updated guidelines on the protection of minors under the DSA, including more granular detail on the types of age assurance deemed compliant with the DSA. Although not legally binding, they are seen as a golden standard for compliance.

Despite the above, it is apparent that age verification methods are not consistently applied and/or effective. Furthermore, with individual EU member states pursuing their own age verification regulations with varied levels 'levels' of verification from self-declaration, up to stricter trusted third party verification across different online platforms and jurisdictions. There is a significant risk of undermining the integrity of the EU single market and creating a fragmented situation where children in some member states benefit from greater protections than children in others as technology providers grapple with divergent and inconsistent national rules.

In recent months, the discussion on age verification has become even more critical as some content providers have taken steps to lower their content moderation standards and cut back on the resources required to effectively moderate content at scale. As such, those platforms lack the means to adequately guarantee that they are not being used as channels for the wide dissemination of harmful and age-inappropriate material to children. Consequently, there is sufficient justification for the introduction of EU-wide rules on age verification ensuring: i) a strong degree of harmonisation and alignment between EU member states and ii) more robust age assurance techniques are mandated for social media and content sharing platforms who fail to implement effective content moderation and therefore exhibit a higher risk to children.

c. Policy Recommendations

The following actions should be prioritised by policy makers:

i) All digital platforms should complete a risk assessment to determine what age assurance measures should be implemented. In limited circumstances, there may be justification for platforms providing services to under 18's to be seen as low risk which may provide rationale for age estimation or self-declaration methods e.g. if a platform has implemented proven methods ensure that harmful and age-inappropriate content is removed quickly, efficiently and effectively. However, such cases should be independently verified and assured.

ii) For high-risk platforms age estimation and self-declaration methods should not be allowed as an appropriate age assurance tools. Platform providers must ensure that effective age assurance measures are applied to their service, where age assurance is provided by a 3rdparty or implemented at a different level platforms must take appropriate steps to ensure it is effective.

iii) Guidelines should go further to mandate that no adult content on platforms is visible to users until after they complete the age assurance process, effectively blocking access to content until the age is verified. This approach is taken in the UK's Online Safety Act.

the Commission should extend regular mandatory audits and transparency to age assurance process, to ensure the designated age assurance method is effective and accurate.

iv) Age verification requirements must be equally effective across all devices. Helpful in this regard is the prototype of an age-verification app under the DSA released by the EC in July, as a basis for a user-friendly and privacy-preserving age verification method across Member States. The blueprint on age verification provides a method to enable users to prove they are over 18 when accessing restricted adult content, such as online pornography, without revealing any other personal information. It is based on open-source technology and designed to be robust, user-friendly, privacy-preserving and fully interoperable with future European Digital Identity Wallets.

02

ADDICTIVE DESIGN FEATURES

2. ADDICTIVE DESIGN FEATURES

a. Problem definition

Addictive platform design features such as autoplay, constant scroll and algorithmic recommender systems are driving societal harms, for children, for example through excessive screen time, dissemination of harmful material, radicalisation and extremism. This is not a fringe problem. A 2019 study by the European Parliament Research Service indicated that digital addiction affects millions of EU consumers. A more recent BEUC study showed that 83% of consumers report spending more time on social media than they intended. The term 'doomscrolling' has entered popular vernacular. This issue is likely to compound as advancements in AI spur increasingly personalised and targeted content, thus driving further engagement.

This issue is compounded by opaque algorithms which have been found to push the consumption of content that promotes highly harmful material, such as content related to self-harm, suicide, 'fake news', eating disorders, misogyny, racism, and terrorism. In many cases, end-users do not even intend to access this kind of content. A recent study in the UK revealed that 59% of boys who have accessed misogynistic content came to it through unrelated searches but were pushed to this harmful content through AI algorithms.

b. Regulatory gaps

ATo date, there is no comprehensive regulation addressing the risks posed by addictive design, or indeed an agreed legal definition of what constitutes addictive design, although policy makers have made some preliminary steps in this direction, for example: a 2023 resolution by the European Parliament identifies some of the potential harms stemming from addictive design and calls for a ban on addictive techniques not covered by the Unfair Commercial Practices Directive, including infinite scroll and autoplay).

The Internal Market and Consumer Protection Committee adopted a report warning of the mental health risks posed by these features, especially for children. The Parliament has also proposed a "right to not be disturbed", reinforcing the need for user-centric, non-intrusive design.

Despite this the Digital Services Act (DSA) and AI Act, current EU and UK frameworks do not explicitly regulate addictive design features. Key gaps include: i) Absence of a legal definition for "addictive design" in consumer protection law, ii) no legally binding requirement to disable addictive features by default, iii) lack of harmonized standards for age-appropriate design and iv) insufficient enforcement mechanisms for ethical design principles.

c. Policy recommendations

Vodafone supports the EC in bringing forward new rules to curb the deployment of addictive design features; we support an outright ban on children's exposure to addictive design features and limitations on how and where these features can be deployed on services used by adults. As a baseline requirement, these features should always be turned off for children by default, with the user having to exert an informed choice to activate them.

Specifically, we are calling for the EU to:

i) **Strengthen the DSA** to include addictive design features as a systemic risk requiring mitigation. We recommend that the Commissions guidelines go further and mandate that platform design features which put minors' safety or security at risk should be disabled and never active for minors. This includes targeted advertising (already a requirement of the DSA), infinite scroll, autoplay and opaque content recommender systems that are not driven by explicit user engagement signals and choices.

ii) **Introduce new requirements in the proposed Digital Fairness Act** that mandates ethical design and that addictive design features are turned off by default and never activated for users that are minors. In addition, the DFA should stipulate that minors should be protected from manipulative commercial practices, including hidden advertising and in-app purchases. We recommend the Commission develop further guidance on age-appropriate advertising transparency and labelling standards, especially in under 18 influencer and user-generated content.

iii) **Establish a regulatory framework** for age-appropriate defaults, with oversight competent digital regulators, at both the national and supranational level.

iv) **Fund independent research** into the long-term effects of addictive design on youth mental health.

03

ACCOUNTABILITY BY DESIGN

3. ACCOUNTABILITY BY DESIGN

a. Problem definition

Platforms often lack basic incentives to take full accountability for their societal impact. According to research by the Centre for Countering Digital Hate, the problem manifests in several ways: The process of designing safety features is highly reactive and emphasizes band-aid solutions to harm. Safety features are often opt-in and place the onus on users to protect themselves from harm. Safety measures are also often poorly maintained and implemented.

b. Regulatory gaps

The Digital Services Act (DSA) introduces important transparency and accountability obligations for Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs), including:

- Mandatory risk assessments and independent audits of systemic risks (e.g. disinformation, mental health harms).
- Transparency around recommender systems and their parameters (Art. 27).
- Enhanced protections for minors, including age-appropriate design and content moderation tools.

However, these obligations apply only to platforms with more than 45 million monthly EU users (or exceptionally other services subject to a risk assessment by the European Commission), leaving out many services accessed by children. Despite the DSA's progress, several critical gaps remain:

- No mandatory audits for platforms below the VLOP/VLOSE threshold, even if they are widely used by children.
- Lack of child-specific safeguards in algorithm design, such as content filtering or age-sensitive ranking.
- Limited enforcement of transparency obligations, especially for non-EU platforms.
- No requirement for explainability of algorithmic decisions to children or guardians.

c. Policy Recommendations

Accountability by design should be mandated for all social media and content sharing platforms. We recommend the European Commission prioritise the following actions to achieve this:

i) Extend mandatory algorithmic audits to all high-risk platforms (defined as above), with oversight by national Digital Services Coordinators.

ii) Require child rights impact assessment (CRIA) for new products and services developed by high-risk platforms.

iii) Mandate safety settings in recommender systems for users under [18], incl. chronological feeds (vs. algorithmic), no autoplay or infinite scroll, no personalized content based on engagement with harmful material. Ensure data minimisation by default and by design, including (no) retention of biometrics.

iv) Fund independent research into the impact of recommender systems on children.

v) Ensuring harmonisation across the DSA, GDPR, UCPD, and upcoming DFA.

vi) Strengthen regulatory oversight and fund national authorities to monitor compliance with accountability by design. Platforms that fall short of their obligations could be mandated to implement robust controls to ensure all users are above the age of 18. Systematic non-compliance may result in sanctions being applied, including fines.

04

CSAM BLOCKING

4. CSAM BLOCKING

a. Problem statement

Vodafone undertakes to block child sexual abuse material (CSAM) wherever possible, albeit that our ability to do so is diminishing with increasing privacy controls implemented by 3rd parties. However, our ability to do so is currently constrained by:

- Legal uncertainty under the ePrivacy Directive and GDPR.
- Net neutrality obligations under the Open Internet Regulation (Regulation (EU) 2015/2120).
- The lack of a harmonized EU legal basis for mandatory or permitted CSAM blocking.
- Despite these constraints, the scale of online CSAM continues to grow, with Europol and INHOPE reporting millions of new images and videos annually. Blocking access to known CSAM is a proven harm-reduction measure that can be implemented without inspecting user content or violating privacy rights.

b. Regulatory gaps

The legal framework for blocking of CSAM material across Europe remains fragmented and legally incoherent, with discrepancies between providers of different technologies and contradictory obligations concerning content blocking and privacy/net neutrality.

Since 2021, providers of number-independent interpersonal communications services (ICS) have operated under a temporary legal regime known as the Interim Derogation, which allows voluntary detection of CSAM. However, this does not extend to telecom providers or infrastructure-level blocking.

The proposed EU CSAM Regulation (2022) introduces: i) detection orders issued by judicial or independent authorities, ii) legal clarity for voluntary and mandatory use of detection and blocking technologies, iii) a framework for trusted flaggers and blocking orders based on vetted URL lists. This regulation, if adopted, would provide the legal certainty telecom providers need to block CSAM using IWF or similar lists. However, negotiations on the proposal in Council remained blocked, with Member States divided on the balance between protection of minors and upholding privacy and the confidentiality of communications (including using encryption protocols). The Danish Presidency has introduced a fresh compromise text, with a view to achieving a General Approach on the file before the end of the year. Key changes include: a narrowing of the scope of detection orders removing "solicitation of children" from the material that detection technologies must identify, leaving only known CSAM and an additional age verification requirement for service providers, where applicable, to describe in their terms and conditions the age verification and age assessment measures they apply.

c. Policy Recommendations

To enable effective CSAM blocking while respecting fundamental rights, the EU should:

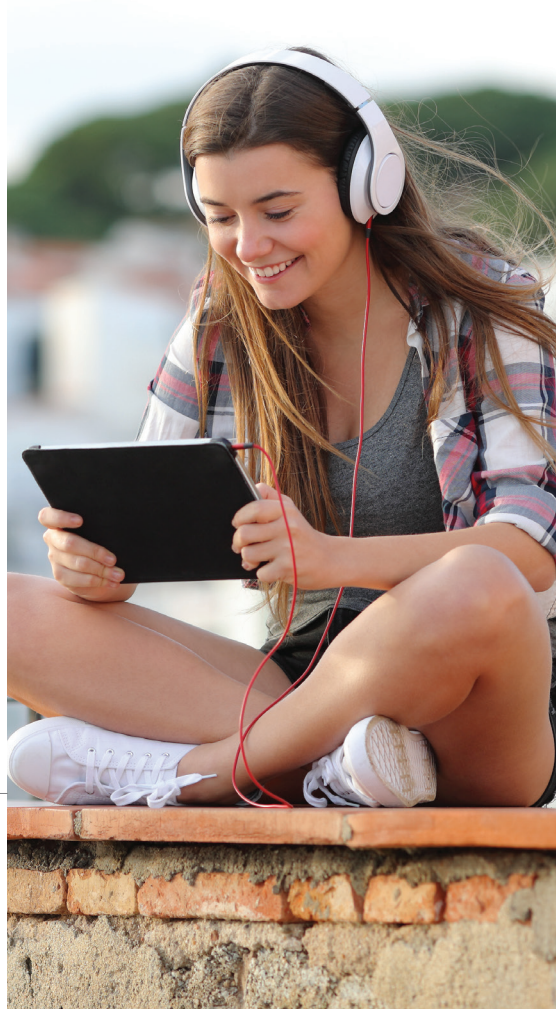
i) Adopt a targeted and proportionate version of the proposed CSA Regulation with explicit provisions allowing telecom and infrastructure providers to block access to CSAM using trusted URL lists (e.g. from the IWF). Detection orders should be appropriately targeted to ensure consistency with other EU legal instruments and fundamental rights.

ii) Amend the Open Internet Regulation to clarify that blocking of illegal content, including CSAM, is compatible with net neutrality when based on a legal mandate.

iii) Establish a centralized EU clearinghouse for CSAM URL lists, vetted by independent authorities and shared securely with providers.

iv) Mandate transparency reporting and independent audits of blocking practices to ensure accountability and prevent misuse.

v) Provide legal indemnity for providers acting in good faith under authorized blocking regimes.



05

DIGITAL SKILLS

5. DIGITAL SKILLS

a. Problem statement

While regulatory and technological interventions are essential to protecting children online, they are not sufficient on their own. Children, parents, and educators must be equipped with the knowledge, skills, and confidence to navigate digital environments safely and meaningfully. However, digital literacy levels remain uneven across Europe, with significant disparities by age, region, and socioeconomic background. According to the European Commission's BIK+ evaluation, children consistently identify parents and teachers as their first line of support online, yet both groups report feeling underprepared to guide children through digital risks. The OECD has also highlighted that digital skills education often lacks coherence, with fragmented national strategies and limited integration into broader wellbeing and inclusion frameworks.

b. Regulatory gaps

Despite the growing recognition of the importance of digital skills, there is currently no EU-wide mandate for digital wellbeing education that is aligned with children's rights. Online safety is inconsistently integrated into school curricula and teacher training across Member States. Mechanisms for meaningful child participation in digital policy design remain limited, and there is insufficient support for vulnerable groups, including children with disabilities, those in rural areas, and those from low-income families.

c. Policy Recommendations

i) **Encourage system-strengthening and whole-school approaches** that embed digital wellbeing and online safety into policies, learning environments and broader mental health and inclusion strategies. Ministries of education should integrate digital resilience into teacher training, school policies, and mental health strategies. This should include outcome indicators that track protective and developmental competencies.

ii) **Strengthen teacher (and by iassociation, parent/ caregiver) training and professional development in the wellbeing and online safety space.** Ring-fenced funding for mandatory, accredited continued professional development (CPD) that covers algorithmic profiling, trauma-informed responses and inclusive pedagogy for children with disabilities (Mastam & Zaharudin, 2024). Judgement free workshops for parents and carers should demystify platform mechanics, model open dialogue after incidents and reinforce shared home-school norms. This also includes equipping educators with tools to identify and support students at risk of digital harm, how to recognise and respond to gender-specific risks but also how to develop more simplified tools that offer conversation starters rather than longer lists of controls. Positioning adults as relational enablers rather than surveillance agents will strengthen the wider ecosystem associated with digital wellbeing.

iii) **Promote a balanced, inclusive approach to digital literacy** that moves beyond restrictive or protective-only strategies by embedding online safety modules inside existing digital literacy programmes, fostering healthy online/offline habits, teaching resilience to online risks and emphasising technology's potential to support creativity, inclusion, and student agency. Children's emotional wellbeing is supported by digital skills and acknowledging their digital identities and reducing fear-based messaging. In line with that curriculum content should be expanded to include algorithmic awareness, commercial intent, and ethical reflection and translate abstract privacy rules into everyday choices through practical, age-appropriate exercises. Digital resilience strategies also include teaching a better understanding of data management and consent, and how to respond to hate comments, fake news, or online pressure. Emerging trends such as AI literacy and critical thinking should also be included. Digital literacy programmes should be age-appropriate, participatory, and gender-sensitive, particularly addressing issues like body image, sextortion, and misogynistic content, while offering trauma-informed support (WHO, 2025; NSPCC, 2025) and encouraging children to engage meaningfully in digital governance (Livingstone et al., 2021).

iv) **Develop policies and initiatives that are developmentally tailored and use age-appropriate approaches by differentiating between age groups** (e.g., early childhood, middle childhood, adolescence) and align digital protections and supports accordingly. This recognises that children's needs and vulnerabilities evolve with age and focusses initiatives to provide more effective support, for example in adolescence, particularly in mid-adolescence, children are uniquely vulnerable to reputation-based harms due to the heightened importance of peer validation. By prioritizing support for children from disadvantaged backgrounds, rural areas, minority groups, children from low-income families and those with disabilities, we ensure equity & inclusion. Interventions should be specifically tailored to address intersecting vulnerabilities (e.g., socio-economic status, disability, ethnicity). This includes designing inclusive digital tools and accessible learning environments and ensuring that early learners (under 10) and neurodiverse students have age-appropriate and inclusive digital wellbeing resources.

v) **Child centred approach:** Children and young people must be meaningfully involved in the design of digital policies, education programmes, and platform safety codes. This includes co-developing materials with children, ensuring accessibility and relevance, and establishing a permanent EU-level youth panel on digital wellbeing. The 2025 European Year of Digital Citizenship Education provides a timely opportunity to institutionalise this approach.

1. https://www.bmj.com/content/388/bmj-2024-082569.full
2. https://assets.childrenscommissioner.gov.uk/wpuploads/2023/07/CCO-Pornography-and-Young-People-1.pdf
3. Smahel D, Machackova H, Mascheroni G, Dedkova L, Staksrud E, Ólafsson K, et al. EU Kids Online 2020: Survey results from 19 countries. 2020
4. https://youthendowmentfund.org.uk/news/70-of-teens-see-real-life-violence-on-social-media-reveals-new-research/
5. The government has chosen to require services that publish or allow pornography on their sites to explicitly use age verification or age estimation measures to prevent children from accessing this content. Platforms will be held to a higher account and need to use age checking measures which are highly effective at correctly determining whether or not a particular user is a child – to prevent under 18s from being able to access pornography https://www.yoti.com/blog/understanding-age-verification-online-safety-act/
6. https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-protection-minors
7. https://digital-strategy.ec.europa.eu/en/news/commission-makes-available-age-verification-blueprint
8. The DSA guidelines on the protection of minors Guidelines include provisions on addictive design features, however these are not legally binding and we are calling for policy makers to go further in outlawing the use of these technologies in certain contexts (for example for children or other high-risk users) and ensure they are deactivated by default for all users.
9. https://counterhate.com/wp-content/uploads/2024/09/CCDH.STAR-Framework.Report-FINAL.pdf