CIPL's response to the UK Department for Science, Innovation and Technology (DSIT)'s Consultation on 'Growing up in the online world: a national conversation'

Submitted 26 May 2026

The Centre for Information Policy Leadership (CIPL)[1] welcomes the opportunity to respond to the Consultation by the UK Department for Science, Innovation and Technology (DSIT) entitled '*Growing up in the online world: a national conversation*'.

CIPL supports DSIT's commitment to understanding the impact of technology on children's daily lives and, in particular, the decision to also seek input directly from children themselves — an approach that CIPL has long advocated and that is essential to producing recommendations that are practical, trustworthy, and grounded in real use. The United Kingdom already has robust and layered protection for children online in place through the Online Safety Act (OSA), the UK General Data Protection Regulation (GDPR) and the Appropriate Age Design Code (AADC). Any additional contemplated measures, should we build on adequate impact assessments, must be evidence based, and child informed.

CIPL has contributed significantly to the discussion on effective and practical solutions that facilitate the protection of children online, ensuring they can participate and thrive in the digital space.[2] In particular, CIPL, together with WeProtect Global Alliance, have convened a series of Multistakeholder Dialogues on Age Assurance, one of the most consequential and contested questions in this area, with the aim of identifying the technical, practical, and legal challenges facing stakeholders and society and moving the policy conversation toward workable solutions.[3]

[1] **The Centre for Information Policy Leadership (CIPL)** is a global privacy and data policy think tank within the Hunton law firm that is financially supported by the firm, 85+ member companies that are leaders in key sectors of the global economy, and other private and public sector stakeholders through consulting and advisory projects. CIPL's mission is to engage in thought leadership and develop best practices for the responsible and beneficial use of data in the modern information age. CIPL's work facilitates constructive engagement between business leaders, data governance and security professionals, regulators, and policymakers around the world. For more information, please see CIPL's website at https://www.informationpolicycentre.com/. Nothing in this document should be construed as representing the views of any individual CIPL member company or Hunton. This document is not designed to be and should not be taken as legal advice.

[2] In April 2021, CIPL launched a special global project on children's privacy and, in October 2022, published a detailed Policy Paper on international issues and compliance challenges. Among the issues identified for further exploration was the use of age assurance and its impact on children's privacy and safety. Please see: Center for Information Policy Leadership (CIPL), "*Children's Privacy Policy Paper I: International Issues & Compliance Challenges*", October 2022, available at: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_childrens_privacy_policy_paper_i_-_international_issues___compliance_challenges__21_oct_2022_.pdf.

[3] The takeaways from these discussions are available on CIPL's website:

- Roundtable 1 (March 2024), available at *https://www.informationpolicycentre.com/resources/a-multi-stakeholder-dialogue-on-age-assurance-key-takeaways/*.
- Roundtable 2 (July 2024), available at *https://www.informationpolicycentre.com/resources/key-takeaways-from-a-multi-stakeholder-dialogue-on-age-assurance-law-and-regulation/* .

CIPL supports robust protections for children's rights, including privacy and safety, anchored in a balanced, risk-based approach as well as robust safety and privacy by design measures for children's online spaces. Rather than outright bans[4], CIPL advocates for the development of context-specific risk taxonomies that help organisations apply proportionate measures to identified harms, and the design of strong multilayered, multistakeholder solutions that protect children without foreclosing their rights to access beneficial, age-appropriate content and services.

In CIPL's view, effective governance must be steeped in organisational accountability, supported by risk-based controls, policies, procedures, and technical measures that are proportionate to individual business models and operational realities.[5] For more than a decade, CIPL has pioneered accountability as a cornerstone of effective regulation and provided guidance towards its implementation in practice. CIPL's Accountability Framework[6] (see Figure 1) is a widely recognised standard for best-in-class privacy protection and responsible business conduct. It identifies seven essential elements that can guide the

---

- Roundtable 3 (September 2024), available at *https://www.informationpolicycentre.com/resources/a-multi-stakeholder-dialogue-on-age-assurance-working-group-on-risk-assessments-key-takeaways-next-steps/* .
- Roundtable 4 (October 2024), available at https://www.informationpolicycentre.com/resources/key-takeaways-a-multi-stakeholder-dialogue-on-age-assurance-working-group-on-global-regional-perspectives/.
- Roundtables 5 & 6 (October–November 2024), available at https://www.informationpolicycentre.com/resources/key-takeaways-a-multi-stakeholder-dialogue-on-age-assurance-working-group-on-law-and-regulation/.
- Roundtable 7 (June 2025), available at https://www.informationpolicycentre.com/resources/a-multi-stakeholder-dialogue-on-age-assurance-considerations-towards-an-interoperable-age-assurance-framework/.

Research on age verification legislation identified technical, practical, and legal challenges. Please see: Takeaways from CIPL Roundtable: The State of Play in Age Assurance in the US, October 2024, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/the_state_of_play_in_age_assurance_in_the_us_-_key_takeaways_oct24.pdf.

In November 2025, the CIPL/WeProtect Framework for Interoperable Age Assurance Solutions outlined relevant technologies and stakeholder roles; the project was later nominated for an Age Assurance Industry Award for its contribution to policy and regulation. Please see: Proposal for a Wallet Credential Manager Framework for Age Assurance Solutions, Centre for Information Policy Leadership, November 2025, available at: https://www.informationpolicycentre.com/resources/proposal-for-a-wallet-credential-manager-framework-for-age-assurance-solutions/.

[4] In its own analysis, DSIT states that while age-based bans are a prominent subject of debate, they carry significant risks of unintended consequences, such as inadvertently driving children to less well-regulated or less-visible sites, creating a cliff-edge for older teenagers when they eventually enter digital spaces, and potentially making children less likely to seek adult help if they encounter harm after circumventing such a ban. Please see: UK Department for Science, Innovation and Technology, *Growing Up in the Online World: A National Conversation*, March 2026, p.32, available at: https://www.gov.uk/government/consultations/growing-up-in-the-online-world-a-national-consultation/growing-up-in-the-online-world-a-national-conversation.

[5] CIPL Accountability Discussion Paper 1 - The Case for Accountability: How it Enables Effective Data Protection and Trust in the Digital Society, July 23, 2018, available at: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_paper_1_-_the_case_for_accountability_-_how_it_enables_effective_data_protection_and_trust_in_the_digital_society.pdf.

[6] See CIPL resources and papers on organizational accountability: https://www.informationpolicycentre.com/topics/organizational-accountability/.

development of structured accountability programmes within organisations. The framework supports a shift from rigid, rule-based prohibitions toward adaptive, risk-based, and evidence-driven safeguards embedded within organisational practice.

Figure 1

Building on this foundation, accountability is not limited to privacy but represents a modern and future-proof governance model more broadly applicable across digital regulation. The Framework provides a coherent organising principle for addressing current policy challenges, including risk taxonomy, age assurance, AI-driven systems, such as chatbots, and the limitations of categorical bans.

Additionally, it is important to recognise that providing children with safe and beneficial online experiences rests on a broad, multistakeholder approach. Platforms and services carry a primary responsibility to ensure that their services are appropriately designed and have risk mitigation measures in place; but no single measure alone will ensure online child safety. Policymakers, industry, academia, educators, parents, and guardians, as well as children themselves through their input, all contribute to building safer digital environments and help strengthen children's resilience online. Regulatory approaches should take the full ecosystem into consideration and ensure that solutions reflect the broader digital environment in which children engage.[7] Digital literacy initiatives, parental engagement, child empowerment, and cross-sector cooperation play important roles and effective protections of children online must have a holistic foundation.[8] Ultimately, child safety and well-being online is the

[7] Andy Phippen, "The Broken Online Safety Ecosystem. In: Policy and Rights Challenges in Children's Online Behaviour and Safety, 2017–2023", 2025, Palgrave Macmillan, Cham, available at: https://link.springer.com/chapter/10.1007/978-3-031-80286-7_6.

[8] Please also in more detail see:

- Sonia Livingstone, "Child online safety – next steps for regulation, policy and practice", *Parenting* for a Digital Future, LSE Blog; Livingstone, S. et al. (2011). EU Kids Online: Final Report. LSE, available at: https://blogs.lse.ac.uk/parenting4digitalfuture/2025/02/05/child-online-safety-next-steps-for-regulation-policy-and-practice/.
- Tanya Byron, "Safer Children in a Digital World: The Report of the Byron Review", UK Department for Children, Schools and Families (DCSF), available at: https://dera.ioe.ac.uk/id/eprint/7332/7/Final%20Report%20Bookmarked_Redacted.pdf.
- Organisation for Economic Co-operation and Development (OECD), "How's Life for Children in the Digital Age?", May 2025, available at: https://www.oecd.org/en/publications/how-s-life-for-children-in-the-digital-age_0854b900-en.html.

result of a functioning ecosystem in which industry provides safe and engaging services, parents are empowered and informed, children are educated and resilient, educators deliver digital literacy as a core competency, and regulators set outcome-driven standards that activate all of these layers.

CIPL provides detailed responses to selected DSIT questions below, focusing on areas where our expertise is most relevant and can contribute constructively to the discussion.

Chapter 1: Understanding how children use technology

Weighing the benefits and the risks of children's online engagement on social media

Children's engagement with a broad range of digital services is now a foundational feature of how they learn, socialise, and participate in the digital society. Children will often pioneer new services and experiment with new ways to communicate or engage online. Protecting and empowering minors online, therefore, requires embedding a high level of privacy, safety, and security by design, from the onset. Online environments can support the development of essential skills — including problem-solving, critical thinking and collaboration — provide accessibility, while also fostering social connections. Structured digital engagement can promote creativity and interest in new subjects, such as Science Technology Engineering Mathematics (STEM).[9] Digital services can provide critical access to information and support on sensitive issues that young people may not feel comfortable discussing offline with their parents, guardians, or peers. This includes resources related to mental health, identity, sexual orientation, and well-being, which can play an important role in supporting children's development and resilience.

Digital services also serve as spaces for civic engagement and public discourse.[10] As future voters, children and adolescents benefit from exposure to diverse viewpoints and from the opportunity to develop the media literacy skills — including the ability to distinguish reliable information from misinformation — that informed participation in democratic life requires.

Any protective measure must strike a careful balance between protection and inclusion and take their rights, as recognised in the United Nations Convention on the Rights of the Child (UNCRC) [11] (e.g., freedom of expression, access to information, education, the right to play), into account. That said, digital services are spaces where privacy and safety risks for children exist. Privacy risks arise, for example, when children's data is exposed or used in ways they cannot meaningfully anticipate or

- UNICEF, *"The Best Interests of the Child in Relation to the Digital Environment",* UNICEF Innocenti – Global Office of Research and Foresight, available at: https://www.unicef.org/innocenti/reports/best-interests-child-relation-digital-environment.

[9] UK Department for Science, Innovation and Technology, Department for Culture, Media and Sport, and Department for Education, *A Safe, Informed Digital Nation: Media Literacy Action Plan 2026–2029*, March 2026, available at: https://www.gov.uk/government/publications/a-safe-informed-digital-nation/a-safe-informed-digital-nation.

[10] The EDPB states in its pay or ok opinion that '[…] the platform may be a key forum for public debate on political, social, cultural and economic issues.' Please see: European Data Protection Board, Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms, April 17, 2024, para. 87, available at: https://www.edpb.europa.eu/system/files/2024-04/edpb_opinion_202408_consentorpay_en.pdf.

[11] United Nations General Assembly, Convention on the Rights of the Child, 20 November 1989, United Nations, Treaty Series.

control. Children may lack cognitive maturity to fully understand how their data can be used against their interests. And similar to the offline world, safety risks emanate online from the factors of:

- Content risks (exposure to violent, extremist, or age-inappropriate material);
- Contact risks (such as unwanted or predatory interactions initiated by adults);
- Conduct risks (including cyberbullying, harassment, and peer-to-peer harm); and
- Contract or commercial risks (such as exploitative marketing or gambling-related content).

However, **not all risks are equal in severity** and the absence of a shared and evidence-based understanding of risks and their roots can lead to both under-protection where providers underestimate a risk and apply insufficient safeguards, or overprotection. Overprotection, through disproportionate restrictions might unduly limit minors' access to beneficial digital content or services, or fail to acknowledge the progressive autonomy of children. While protection from harm remains the key factor, it should not come at the expense of children's ability to engage with and benefit from the digital world.

A clearly articulated, holistic, risk taxonomy based on evidence and with illustrative examples and case studies, especially for medium- and low-risk scenarios in a variety of contexts, provides the framework of proportionate governance. Furthermore, the assessment of what constitutes a risk, including a high risk, and what constitutes an appropriate mitigation measure must be continuously evaluated. Risks can change over time as services develop, and new risks - or benefits - emerge in the online environment.

Chapter 2: Interventions for safer, more positive experiences

I. Restricting social media services by age

Efforts to protect children online must strike a careful balance between safeguarding against harm, and respecting children's fundamental rights and evolving capacities. Instead of blanket bans, a nuanced, risk-based, and proportionate regulatory approach is needed; one that is grounded in *the best interests of the child* and combines effective safety measures, accountability mechanisms, and safeguards tailored to children's maturity, cognitive development, and digital skills.

Australia's Online Safety Amendment (Social Media Minimum Age) Act 2024, which entered into force in December 2025, introduced a world-first prohibition on social media use for children under the age of 16 and will provide valuable insights towards informing this policy discussion further.[12] In a first report[13], the Australian eSafety Commissioner informs about the totality of all steps taken by platforms in scope for the ban, the effective protection against circumvention and the quantitative removal of underage accounts. However, while the eSafety Commissioner report indicates that platforms removed 4.7 million accounts initially, other reports suggest that a significant number of children aged under 16 remain on social media by declaring an age of 16 or using multiple attempts to secure a false age-check result: 61% of children aged 12–15 who had accounts on restricted platforms prior to the ban continued to maintain

[12] Government of Australia, Online Safety Act 2021 (Cth), Part 4, available at: https://www.legislation.gov.au/C2021A00076/2024-12-11/2024-12-11/text/original/epub/OEBPS/document_1/document_1.html#_Toc185687806.

[13] *eSafety Commissioner*, "Social Media Minimum Age Compliance Update", March 2026, available at: https://www.esafety.gov.au/sites/default/files/2026-03/SocialMediaMinimumAgeComplianceUpdateMarch2026.pdf?v=1774905032806.

active accounts thereafter.[14] At the same time, preliminary data shows no discernible drop in reports of harm, such as cyberbullying, suggesting that raw account removal has so far not meaningfully reduced the risks children encounter online.[15]

Where regulatory focus is on prohibitions, it shifts organisational incentive away from the development of safer digital environments and toward the implementation of technical access barriers. Where platforms and services are not expected to host minors, they may stop investing in the necessary safety features, default settings, parental tools, and accountability mechanisms that would contribute to safer online environments form the onset.

Blanket access restrictions may generate other unintended consequences:

- **Privacy costs:** Such measures typically rely on age assurance or verification mechanisms that may require the collection of additional personal data not just from children.
- **Displacement costs:** Children denied access to certain services may migrate to less regulated alternatives offering fewer protections.
- **Equity costs:** Children in households with less engaged parents or guardians may be disproportionately affected by consent-gated access models.

Finally, from a fundamental rights perspective, such measures disproportionately restrict children's rights to access information, freedom of expression, and participation in digital environments. As established under the UN Convention on the Rights of the Child[16], and further elaborated in General Comment No. 25[17] on children's rights in the digital environment, the *best interests of the child* must be a primary consideration in all policy measures. Importantly, this principle requires a balanced approach that protects children from harm while also safeguarding their right to seek, receive, and impart information online. Blanket restrictions risk upsetting this balance by prioritising exclusion over empowerment, thereby limiting young people's ability to stay informed and engaged, with potential long-term consequences for their participation in democratic life.

A risk-based, accountability-driven alternative — in which organisations are required to identify, mitigate and demonstrate the management of risks to children, with regulatory oversight — supported by privacy and safety by design is more likely to deliver better outcomes for children, more durable legal certainty for organisations, and a more defensible regulatory settlement than categorical bans, whose effectiveness the available evidence does not bear out. Such an approach would place the regulatory focus on targeted obligations proportionate to the specific risks services create for children, including risks arising from product design, harmful content exposure, unwanted or exploitative contact, and

---

[14] *Molly Rose Foundation*, "Australia Social Media Ban Research Briefing", April 2026, available at: https://mollyrosefoundation.org/wp-content/uploads/2026/04/MRF_Australia-Social-Media-Ban-Research_Briefing-April-26.pdf.

[15] *eSafety Commissioner*, "Social Media Minimum Age Compliance Update", March 2026, available at: https://www.esafety.gov.au/sites/default/files/2026-03/SocialMediaMinimumAgeComplianceUpdateMarch2026.pdf?v=1774905032806.

[16] United Nations General Assembly, Convention on the Rights of the Child, 20 November 1989, United Nations, Treaty Series.

[17] UN Committee on the Rights of the Child (CRC). (2021). *General comment No. 25 (2021) on children's rights in relation to the digital environment*, CRC/C/GC/25, Section III, B. Best Interests of the Child, p. 3, https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-%202021-childrens-rights-relation.

commercial practices, rather than relying primarily on access restrictions that may ultimately be circumvented.

II. Age of digital consent

Amendments to the age of consent should only be considered where evidence suggests a considerable positive impact on children's well-being. An amendment places substantial compliance burdens on organisations. In practice, companies are required to build and adapt their services across different jurisdictions to accommodate varying age thresholds for the same online offering.[18] This fragmented regulatory landscape, increases complexity for businesses seeking to implement consistent safety protections.[19] At the same time, it risks producing uneven outcomes for children, resulting in inconsistent levels of protection depending on where they are located. Organisational burden should not weigh against children's protection, but fragmentation produces both higher cost and worse protection: organisations face differing obligations across jurisdictions, and children face inconsistent safeguards depending on where they live. A converged, risk-based approach to the digital age of consent — coordinated where possible across the UK, EU, and other jurisdictions — would serve both interests.

It is also important to note that the age threshold for "age to access services" is distinct from the GDPR/DUAA "age of consent" under Article 8. Article 8 establishes that where consent is the applicable legal basis for a specific processing purpose (as opposed to any other legal basis under Article 6), children above the threshold can provide that consent themselves, while for those below that threshold it must be provided by a parent or guardian. Considerations of age-based restrictions for specific digital services are separate and in addition.

III. Restricting access to services based on design features and functionalities[20]

CIPL welcomes DSIT's recognition that certain functionalities and design features can play a privacy-preserving role for children, as well as the acknowledgement that no clear causal link has been established between screen time and children's mental health. Policy measures must be grounded in evidence especially when it comes to the protection of children and the delicate balance between safety, privacy, and exclusion.

Many online platforms have already developed a wide variety of tools to ensure children are protected online[21] and CIPL would urge DSIT to consider a nuanced holistic, risk-based approach to any assessment of features and functionalities. Features that might appear problematic in isolation can, depending on context, default settings, user controls, transparency, and user age, also serve important protection when understood in context. Features are often not single purpose, for example:

---

[18] Centre for Information Policy Leadership, "International Issues and Compliance Challenges", October 2022, available at: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_childrens_privacy_policy_paper_i_-_international_issues___compliance_challenges__21_oct_2022_.pdf.

[19] Centre for Information Policy Leadership, "Response to Canada Office of the Privacy Commissioner Consultation on Age Assurance", September 2024, available at: https://www.informationpolicycentre.com/wp-content/uploads/2024/09/cipl_response_to_canada_opc_age_assurance_consultation_sept24.pdf.

[20] This part of the response serves as input to both sections: **Restricting access to services based on features and functionalities** and **'Addiction', compulsive design and displacement.**

[21] Centre for Information Policy Leadership (CIPL), 2024, August 30, Good Practices for the Guidelines Under Article 28 of the DSA: Consultation Response.

- Disappearing content can also be privacy-preserving by reducing children's digital footprint and limiting the long-term exposure of information shared during formative years.
- Location sharing can be a vital safety mechanism, helping children reach emergency services quickly or enabling parents to locate them.[22]
- Notification features can support media literacy, deliver security alerts, and provide safety warnings in real time.
- Recommender systems can also help children discover new content that is age-appropriate, educational, and enriching — opening access to information, creativity, communities of interest, and entertainment suited to their developmental stage.

In practice, many services already implement layered, age-appropriate safeguards by default for younger users, including restrictions on communication features, enhanced privacy settings, limitations on interactions with unknown users, and parental consent mechanisms for access to certain functionalities. Restricting specific features and functionalities requires a comprehensive assessment of the context in which they are used and the specific risks and benefits they may present, with due consideration given to any potential detriment to a minor's best interests.

IV. To what type of services should restrictions apply

CIPL supports DSIT's commitment to ensuring that any potential future age-based access restrictions are applied in a targeted manner. Age based restrictions must be risk-based and proportionate.

Additionally, whether an app, website or service is specifically targeted at children ("likely to be accessed by children") should be a determinative factor for the application of age assurance measures. Subject matter, terms of service, the use of animated characters, child-oriented activities, music, and child-specific language form part of that assessment. Certain types of platforms, such as gaming, educational, or entertainment platforms, may intrinsically be more likely to attract child users. Restrictions should only apply when the likelihood of access by children is "significant" (more than *de minimis*), rather than when access is merely incidental or through a parent's shared device.[23]

The Online Safety Act provides examples, such as internal business services, services with limited functionalities and services provided by persons offering education or childcare. Further examples include:

- Websites focused on professional, business-to-business (B2B), or technical topics, should be excluded as they are not designed to be attractive to children. In the case of the CIPL's site, an older child might wish to access information on privacy debates in connection with a school or college project without any discernible risk and will, therefore, not require any measures to restrict access.

[22] Centre for Information Policy Leadership (CIPL), CIPL Response to the ICO Consultation on Age Appropriate Design: A Code of Practice for Online Services, May 2019, available at: https://www.informationpolicycentre.com/resources/cipl-response-to-the-uk-icos-consultation-on-age-appropriate-design-a-code-of-practice-for-online-services/.

[23] Centre for Information Policy Leadership (CIPL), CIPL Response to the Office of the Australian Information Commissioner's (OAIC) Consultation on the Children's Online Privacy Code, July 2025, available at: https://www.informationpolicycentre.com/resources/cipl-response-to-the-office-of-the-australian-information-commissioners-office-oaic-consultation-on-the-childrens-online-privacy-code/.

- Banking, healthcare, travel, and hospitality services should also be excluded from additional restrictions. These services are already subject to their own sectoral age-gating mechanisms — a child cannot open a bank account, consent to medical treatment, or book a hotel room without parental or guardian involvement as a matter of law. Access to these services inherently requires either financial capacity (a payment card or account controlled by an adult) or the active, documented intervention of a parent or legal guardian. Additional age-verification layers add complexity without any corresponding safety benefit.
- Services whose primary purpose is the delivery of educational content should benefit from flexible and scalable assessments that weigh potential risks against the tangible benefits of digital learning.
- Platforms that offer specifically curated child or teen versions with built-in safety-by-design features should be considered as responsible alternatives.

On the other hand, services, such as pornography sites and similar high-risk content, must be subject to rigorous age restrictions due to their inherent nature and the high risk of harm they pose to minors. The primary goal is to ensure that access restrictions are **proportionate to the actual level of risk** while safeguarding children's right to seek and receive information.

V. Chatbots and AI

CIPL believes that AI-driven tools, including chatbots or recommender systems, carry significant opportunities for children to participate in and benefit from the digital environment. AI technologies can enable children to create, collaborate, and express themselves in ways aligned with their age, abilities, and maturity, supporting their rights to freedom of expression and access to information to play and participate.

At the same time, it is important to distinguish between different types of AI systems, their intended uses, and the distinct functions they perform:

- AI-driven recommender systems, when responsibly designed and implemented, can enhance child protection by prioritising age-appropriate, educational, and enriching content, while reducing exposure to harmful material.
- Purpose-built AI tools designed for children, such as educational or accessibility-focused chatbots, can play a valuable role in supporting learning and inclusion. These tools can facilitate access to information, enable new forms of interactive learning (including virtual classrooms), and support children in exploring subjects in a structured and age-appropriate manner.
- General-purpose conversational AI systems, on the other hand, will require the implementation of appropriate safeguards when made available to children, reflecting their broader functionality and being commensurate with the potential risks. For example, a basic embedded commercial chat function presents a lower risk profile even when interacting with a child than a chatbot capable of companion-style communication.

Children will not always be able to distinguish clearly between human and AI-driven interactions, particularly in the case of conversational systems designed to simulate human-like responses. This can create risks of misplaced trust, emotional reliance, or undue influence without the appropriate safeguards in place. Regulatory focus should be on identifying those deployments of AI that warrant enhanced safeguards, including systems involving simulated empathic or romantic interaction, use in higher-risk contexts, or functionalities that may increase the likelihood of user overreliance.

Proportionate transparency obligations also play a central role in mitigating these risks. Organisations should ensure that children are clearly informed when they are interacting with an AI system, using communication methods that are appropriate to their age, maturity, and level of understanding, consistent with principles reflected in the UK AADC[24]. Importantly to be meaningful, such information notices need to be carefully designed in a child appropriate manner and deployed in meaningful ways throughout the interaction.

In parallel, CIPL supports broader digital literacy initiatives to help children and families better understand the nature and limitations of AI systems, including the distinction between human and automated interactions. Transparency at the point of interaction and education over time are complementary strategies. The goal is not to shield children from AI, but to equip them with the understanding to engage with it critically and safely, similar to other efforts such as media literacy programmes to ensure children can critically evaluate television, advertising, or online content. It is also important to understand that AI literacy rests on multiple pillars: in addition to platforms and services, public institutions whose mandate includes child welfare, social services, parents, guardians, educators, all have a role to play in equipping children with the tools to engage with their digital environment critically and safely.

DSIT's approach should be grounded in accountability, transparency, and proportionate safeguards, enabling organisations to address identifiable risks, empowering parents, guardians, and educators, and having due regard to the *best interests of the child* as the north star guiding the implementation of measures and design choices to preserve children's access to beneficial AI-enabled services and to support continued innovation – consistent with the UK's wider pro-innovation regulatory framework.

Chapter 3: Effective compliance and enforcement of online safety rules

I. Improving age assurance

In a joint statement from March 2026 more than 300 security and privacy researchers on age assurance set out the substantive concern in clear terms: requiring age verification of everyone, including of adults, across routine online services would impose data-protection costs that go beyond anything required in the offline world, and would do so without commensurate evidence of safety gain.[25] CIPL agrees that age-assurance measures must be weighed against established privacy rights also of the adult population, the risk of exclusion for users without standard forms of identification, and the security risks of concentrating sensitive verification data. Age assurance should be implemented only where proportionate, in a privacy-preserving way that avoids excessive data collection when it enables effective risk-based protection. Any age assurance framework must be designed and implemented with a paramount focus on safeguarding personal data.

As mentioned in Chapter 2, age checks should initially depend on the likelihood of access by children and the risk context of the underlying service(s). Secondly, the method of age assurance should be proportionate to the level of risks and be steeped in consideration of the *best interests of the child*,

[24] Information Commissioner's Office (ICO), "Age Appropriate Design: A Code of Practice for Online Services", 2022, available at: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/.
[25] Joint Statement of Security and Privacy Scientists and Researchers on Age Assurance, March 2026, available at: https://csa-scientist-open-letter.org/ageverif-Feb2026.

which encompass access to information, education, social participation, and developmentally appropriate digital experiences.

CIPL supports the development of interoperable age-assurance solutions, as set out in the CIPL/WeProtect Framework for Interoperable Age Assurance Solutions.[26] This can reduce the burden of repeated verification across services by allowing a proportionate attestation, established in a trusted context, to be reused across the ecosystem, while narrowing the surface area for breaches, and improving the user experience for adults and parents alike. The use of these signals should be tightly governed and restricted to safety and compliance purposes, and in a privacy preserving manner.

To that effect, CIPL encourages further incentivising the application of privacy-enhancing technologies (PETs) in the context of age assurance. PETs can play a crucial role in age assurance by enabling the verification of a user's age without requiring access to excessive personal data, thereby upholding privacy and data minimisation principles. In this regard, the government could also play an important role by supporting a privacy-preserving age assurance infrastructure and review existing enforcement gaps, such as challenges of verifying under-18 users in the UK, in the context of the digital ID discussion.

II. Circumvention of age limits

Children's ability to circumvent online safety measures[27] is an important consideration when assessing the effectiveness of age restrictions and related regulatory interventions. In practice, children with high digital skills can employ a wide range of methods that go well beyond the use of VPNs. In addition, peer-to-peer knowledge sharing plays a significant role, with young users exchanging tips and workarounds within their communities to bypass restrictions.

Recognising that children are often technologically adept and increasingly capable of circumventing technical safeguards,[28] highlights the importance of complementary strategies with a focus on the content and design of online environments. This means moving beyond a singular focus on age-based restrictions toward a nuanced, safety-by-design approach, with risk-based and proportionate age assurance, supported by digital literacy and resilience initiatives.

---

[26] Proposal for a Wallet Credential Manager Framework for Age Assurance Solutions, Centre for Information Policy Leadership, November 2025, available at: https://www.informationpolicycentre.com/resources/proposal-for-a-wallet-credential-manager-framework-for-age-assurance-solutions/.

[27] As mentioned above: 61% of children aged 12–15 who had accounts on restricted platforms prior to the ban continued to maintain active accounts thereafter. Please see: Molly Rose Foundation, "Australia Social Media Ban Research Briefing", April 2026, available at: https://mollyrosefoundation.org/wp-content/uploads/2026/04/MRF_Australia-Social-Media-Ban-Research_Briefing-April-26.pdf.

[28] 70% of children still using restricted sites say that it was 'easy' to circumvent the ban. In most cases, social media platforms have failed to detect or seek to remove under 16s accounts. Please see: Molly Rose Foundation, "Australia Social Media Ban Research Briefing", April 2026, available at: https://mollyrosefoundation.org/wp-content/uploads/2026/04/MRF_Australia-Social-Media-Ban-Research_Briefing-April-26.pdf.
Please also see: eSafety Commissioner, "Social Media Minimum Age Compliance Update", March 2026, available at: https://www.esafety.gov.au/sites/default/files/2026-03/SocialMediaMinimumAgeComplianceUpdateMarch2026.pdf?v=1774905032806.

Chapter 4: Preparing children for a digital future and enriching their online experiences

I. Media and digital literacy

Online engagement plays a crucial role in developing the digital literacy skills required for safe and independent online navigation.[29] Digital literacy can protect children *across* services and jurisdictions. While regulation sets legal thresholds, education travels with the child across the entire digital ecosystem. Investment in digital literacy must, therefore, be treated as a priority.

A key element will be the provision of clear and accessible guidance that children can use independently. Such guidance must go beyond technical instructions and include concepts such as consent, online safety, and the long-term implications of children's digital footprint. It should also be tailored to children's age, maturity, and cognitive development, and delivered through engaging and accessible formats, such as visuals, storytelling, short videos, and interactive tools, rather than lengthy or overly technical policies.[30] This approach is particularly important for children with specific communication needs or learning differences, for whom traditional written formats may be less effective.

Parents and guardians as well as educators should equally be equipped with digital know-how, as they play a key role in shaping children's online experiences. Both groups often have a relative lack of familiarity with and ability to meaningfully navigate new technologies compared to children and young people due to a multitude of factors, including time and resources. Providing them with clear, standardised information about how services work, how data is collected and what safety features are available can enable more meaningful engagement. Practical tools and resources, like those included in the Media Literacy Action Plan[31], can also facilitate informed conversations about online safety, helping to bridge generational gaps in digital understanding.

II. Promoting access to high quality content

CIPL agrees with the emphasis placed by DSIT on the importance of high-quality online content, as it is a cornerstone for a digital environment in which children can thrive. High quality content supports digital literacy, teaches critical thinking, and informed decision-making.

CIPL believes that multiple stakeholders play a role in determining what high-quality online content for children should encompass. This should include:

---

[29] Sonia Livingstone, "Parenting for a Digital Future: Child Online Safety: Next Steps for Regulation, Policy and Practice", London School of Economics and Political Science, February 2025, available at: https://blogs.lse.ac.uk/parenting4digitalfuture/2025/02/05/child-online-safety-next-steps-for-regulation-policy-and-practice/.

[30] Center for Information Policy Leadership (CIPL), "Children's Privacy Policy Paper I: International Issues & Compliance Challenges", October 2022, available at: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_childrens_privacy_policy_paper_i_-_international_issues___compliance_challenges__21_oct_2022_.pdf.

[31] UK Department for Science, Innovation and Technology, Department for Culture, Media and Sport, and Department for Education, A Safe, Informed Digital Nation: Media Literacy Action Plan 2026–2029, March 2026, available at: https://www.gov.uk/government/publications/a-safe-informed-digital-nation/a-safe-informed-digital-nation.

- **Regulators** who are responsible for setting regulatory frameworks and minimum standards, for providing practical guidance for online platforms and for collaborating at a national and international level to ensure greater consistency across jurisdictions and less fragmentation;
- **Online platforms** and their trust and safety teams, who play a central role in designing age-appropriate and child protective environments;
- **Parents, carers, and trusted adults**, who guide children's everyday engagement, and help shaping healthy digital habits and calibrating access to their individual child's maturity and needs;
- **Children** must also be included in this process, as their lived experience is essential to ensuring that policies are practical, credible, and aligned with real usage. Children are rights-holders with perspectives that must inform policy; they are also creators of online content;
- **Educators, youth workers, and child advocacy organisations**, all contribute unique insights and expertise with respect to children's cognitive development, learning environments, community contexts, and rights-based considerations.

Building on this collaborative foundation, further action from regulators to support positive online spaces for young people could include:

- The development of best practice principles for industry, such as recognised codes of conduct that promote safe and age-appropriate design;
- The provision of clear and accessible guidance for parents and carers to support informed digital mediation at home; and
- Tailored educational resources for children that help them strengthen their ability to navigate risks and build autonomy online.

Any measures should be guided by the *best interests of the child*, which must remain the central consideration in the design of children's digital environment. This requires a balanced assessment that encompasses protection from harm as well as the child's right to access information, participate in digital culture, develop autonomy, and benefit from technological innovation.

Chapter 5: Supporting families

Parental controls

CIPL recognises the important role parents and caregivers have in ensuring children's well-being. Robust parental controls can be a valid tool and risk-mitigation measure.

Parental controls should be balanced against the *best interests of the child* and designed to *empower* informed parental decision-making and enable dialogue with the child— not one-sided surveillance of the child. The objective is to give parents meaningful agency: the ability to set age-appropriate boundaries, adjust access as their child matures, and receive relevant signals about risk — while respecting the child's developing right to privacy and autonomy.

Regulatory approaches to parental control tools must recognise that older adolescents have different levels of maturity and should be afforded increasing autonomy in line with their developing abilities. Overly restrictive measures applied to older children may be counterproductive. Treating adolescents as lacking capacity for independent judgment can incentivise them to circumvent controls, undermining both the effectiveness of safeguards and trust in digital systems. It is important to ensure that older

adolescents can safely access information and support on sensitive issues, such as mental health or identity, without undue interference.

Conclusion

Overall, the choice should not be between protecting children online and enabling them to thrive in digital environments. The two are mutually reinforcing, and the regulatory architecture that delivers them is one that:

- Places **organisational accountability** at its center: requiring services to identify the risks their products pose to children, to mitigate those risks proportionately, and to demonstrate that they have done so.
- Recognises the **benefits of children's digital participation**, supporting children's development, learning, accessibility, and social connection online commensurate with the *best interests of the child*.
- Favors **risk-based and proportionate** approaches over categorical restrictions.
- Is grounded in a **shared and evidence-based understanding of risks**.
- Assesses specific **features and functionalities in light of their context**, risks, and benefits.
- Is **outcome-driven and flexible** — avoiding prescriptive technical mandates that become outdated and instead setting standards that allow for continuous innovation in safety tools and approaches.
- Takes account of existing regulatory frameworks and **avoids creating overlapping, duplicative, or inconsistent obligations** by ensuring that any new measures are preceded by appropriate impact assessments, stakeholder consultation, and evidence-based gap analysis.
- **Empowers parents** and caregivers by equipping them with the literacy, tools, and information to guide their child's digital life.

CIPL is happy to further support developing that architecture, building on the work already begun under the Online Safety Act and the Children's Code, and on the substantial body of CIPL's own work on accountability, age assurance, and the responsible use of children's data.