BCS, The Chartered Institute for IT

'Growing Up in the Online World: A National Conversation'

May 2026

About This Response

BCS, The Chartered Institute for IT, welcomes the opportunity to contribute to the Government's consultation, '*Growing Up in the Online World: A National Conversation*'.[1]

This response draws on the following evidence sources, which are referenced throughout as follows:

- **Member survey** - a BCS member survey of 1,229 technology professionals conducted January–February 2026, providing quantitative data on member views.[2]
- **BCS qualitative research** - facilitated discussions and written contributions from members responding against the consultation questions, providing qualitative insight from groups including computer science teachers, academics, cybersecurity experts, and professionals across early years and government advisory. This is not explicitly referenced throughout but has broadly informed this document.
- **Professor Andy Phippen** - reflective expert perspective from Professor Andy Phippen, BCS Fellow and Professor of Digital Rights with over 20 years of research in this area.[3]
- **Professor Victoria Baines** - reflective expert perspective from Professor Victoria Baines, BCS Fellow and Professor Emerita of Information Technology at Gresham College, with a background in law enforcement on online harms and independent research for the Council of Europe and the UN.[4]

Together, these sources provide a broad, technically informed and experience-based view of children's online safety, reflecting both professional expertise and lived realities.

---

[1] HM Government, *Growing Up in the Online World: A National Conversation*, May 2026. Available at: https://www.gov.uk/government/consultations/growing-up-in-the-online-world-a-national-consultation

[2] BCS Member Survey, *How can the UK best help children navigate the online world safely and effectively?*, January–February 2026. Available at: https://www.bcs.org/articles-opinion-and-research/how-can-the-uk-best-help-children-navigate-the-online-world-safely-and-effectively/

[3] Professor Andy Phippen, BCS Fellow and Professor of Digital Rights. Contribution submitted to BCS, May 2026. Profile available at: https://staffprofiles.bournemouth.ac.uk/display/aphippen1

[4] Professor Victoria Baines, BCS Fellow and Professor Emerita of Information Technology, Gresham College. Contribution submitted to BCS, May 2026. Profile available at: https://www.gresham.ac.uk/speakers/professor-victoria-baines

As the professional body for IT, BCS represents a diverse membership of technologists, including teachers, academics, AI and cybersecurity experts, through to health and care staff with practitioners working across the public, private and third sectors.

Executive Summary

BCS believes that children face systemic risks online driven primarily by platform design choices, including algorithmic amplification, engagement-maximising features and data practices, rather than purely by individual behaviour. Current protections are not keeping pace with how children use digital services.

There is strong support among BCS member survey respondents for a minimum age restriction, including an under-16 social media ban[5]. However, there is also low confidence that such a ban would be technically effective in practice. Only a small minority expressed high confidence in enforceability, with widespread concern about circumvention and weak age assurance systems.

Government must work with technologists. The policy challenges raised by this consultation are technically complex, rapidly evolving and do not lend themselves to simple or static solutions. Effective policy requires sustained engagement with technologists, industry and the professional community to ensure that policy keeps pace with changing platforms, emerging risks and new technical capabilities. BCS and its membership stand ready to support that ongoing dialogue.

Digital literacy is a core safeguard. Across all evidence sources, digital literacy emerged as an essential component of any effective response. Children and their families need real, taught skills to navigate algorithmic systems, identify misinformation and manage their online lives with confidence. There is no such thing as a digitally native generation; digital capability must be developed through education at every stage, from primary school through to adult learning and professional upskilling. BCS has long advocated for this and sees it as central to keeping children safe online.

While age bans are intuitively appealing, they risk being symbolic rather than operationally effective if implemented in isolation.

Strategic Policy Direction

BCS evidence strongly suggests that effective policy should move beyond access restrictions alone and focus on system-level reform. BCS's evidence points to five priorities for effective policy:

[5] BCS Member Survey (2026)

1. **Safety-by-design and platform accountability.** The most consistent recommendation is to shift focus from "who can access services" to "how those services are designed." This includes restricting high-risk features such as algorithmic recommendation feeds, infinite scroll, autoplay, public metrics (likes/followers), and unrestricted contact with unknown adults. Safety should be built in by default, with responsibility placed on platforms rather than parents or children.
2. **Risk-based and functionality-led regulation.** Not all online services carry the same level of risk. A tiered, risk-based approach (targeting harmful features and functionalities rather than applying blanket rules) is more proportionate and effective.
3. **Restricting functionality for children.** There is strong support amongst BCS members for graduated access models, where children can use online services but with restrictions on high-risk or addictive features. This approach better reflects how children engage with technology and avoids unnecessary exclusion from beneficial uses.
4. **Digital literacy and resilience.** Across all evidence sources, there is clear consensus that digital literacy is essential to safeguarding. Children, and their parents or carers, need the skills to understand online risks, algorithmic systems and misinformation, alongside access to trusted support when problems occur. This is seen not as a "soft" intervention but as a core component of effective protection.
5. **Improving age assurance, but not relying on it alone.** While stronger age verification is necessary, current approaches are seen as easy to bypass, inconsistent and privacy-sensitive. BCS member polling suggests a call for more robust, privacy-preserving and interoperable solutions, potentially at device or system level. There is strong agreement that age assurance should be a supporting measure, not the primary safeguard.[6]

Expert Perspective

BCS experts reinforce that overreliance on bans and age limits risks creating a false sense of safety. They highlight that children may circumvent restrictions or move to less regulated spaces, that overly restrictive approaches may limit beneficial opportunities,

[6] BCS Member Survey (2026)

and that education, support and safer system design are more effective long-term interventions.[7][8]

Conclusion

The evidence gathered by BCS points to a clear conclusion: effective online safety policy must prioritise system-level change over access restrictions alone. While there is support for age limits, they are unlikely to succeed without complementary measures. The most effective approach combines safety-by-design regulation, clear accountability for technology companies, risk-based restrictions on high-risk features, and sustained investment in digital literacy and user support. In short, policy should focus on how platforms operate, not just whether children can access them.

[7] Professor Andy Phippen, BCS Fellow and Professor of Digital Rights. Contribution submitted to BCS, May 2026.
[8] Professor Victoria Baines, BCS Fellow and Professor Emerita of Information Technology, Gresham College. Contribution submitted to BCS, May 2026.

1. Understanding How Children Use Technology

1.1 Benefits of being online for children

BCS members consistently recognise genuine benefits of being online for children, including access to learning resources and informal education; connection with peers, particularly for children who are geographically isolated, for SEND young people (Special Educational Needs and Disabilities) or those who are marginalised; creative expression through writing, video, art and music; civic participation, community-building and identity formation; and structured, moderated platforms designed specifically for children that can support language development, early STEM skills, and social confidence.

However, members repeatedly stressed that these benefits are not inherent to mainstream social media platforms, but tend to arise in purpose-built educational tools, moderated community spaces, and low-risk communication environments where the environment is designed with children's interests at heart, rather than for a commercial product optimised for engagement.

One frequently expressed view was that mainstream platforms deliver benefits incidentally rather than intentionally, as they are primarily optimised for engagement and data extraction rather than children's wellbeing.

1.2 Harms and risks of being online for children

There was strong convergence on the key harms, including: exposure to harmful, age-inappropriate or radicalising content via algorithmic amplification; grooming and contact from unknown adults facilitated by stranger-pairing and messaging features; addictive design mechanisms (infinite scroll, push notifications, affirmation loops) that displace sleep, physical activity and focused learning; privacy violations through the harvesting of behavioural data from children who lack the cognitive maturity to understand the implications; social comparison harms including anxiety, depression and disordered eating, particularly in adolescent girls; and from a cybersecurity standpoint, children are also disproportionately vulnerable to phishing, sextortion, identity exploitation and account compromise.

BCS members who were polled and supported restricting under-16s' access to social media most frequently cited mental health concerns, child and adolescent development, addictive platform design, and safeguarding risks including cyberbullying, online abuse and exploitation.[9]

[9] BCS Member Survey (2026)

Members repeatedly emphasised that these harms are structural, arising from business models and design choices rather than individual behaviour.

1.3 Do the benefits outweigh the risks?

The prevailing views of members in facilitated discussion was that for under-16s using mainstream social media platforms as currently designed, the risks outweigh the benefits. Though there was a split between whether that was strongly or somewhat the case. One contributor noted that the benefits are genuine and should not be dismissed, but that the current design of most platforms prioritises commercial engagement over child safety.

These conclusions were qualified by important distinctions: children being online is not inherently harmful, and the right regulatory response is not to eliminate online access but to structurally change the environment, including an enforceable minimum age, restriction of harmful features, and holding platforms accountable for design choices that harm children.

2. Interventions for Safer, More Positive Experiences

2.1 Legal age limits and minimum age of access

2.1.1 Support for a legal minimum age

In facilitated discussions, BCS members expressed overwhelming support for a legal requirement for social media services to have a minimum age of access. This was echoed in the member survey: 56.7% of respondents supported the principle of banning under-16s from social media; 28.8% opposed such a ban; and 14.5% were undecided.[10]

Supporters argued that voluntary self-regulation has failed, that responsibility must rest with platforms rather than parents, and that a legal requirement would provide clarity, consistency and enforceability. Importantly, many supporters also cautioned that legislation alone will not be effective without complementary technical and design interventions.

2.1.2 The question of age threshold

Many members favour 16 as a defensible regulatory threshold, citing evidence on adolescent cognitive and emotional development, consistency with other age-based protections, and the concentration of harms among younger teenagers. Members also noted that a clear national threshold can reduce conflict between parents and children, support consistent school policies, and counteract peer pressure driven by platform norms.

This question generated significant discussion. Members supporting 16 argued that the unsupervised, solo nature of social media engagement via smartphones means there is limited parental intervention or protection; that misinformation, negative body imaging and hate content more adversely affects children under 16 as they are especially vulnerable to persuasive design and social comparison; that under-16s cannot meaningfully consent to algorithmic profiling; that the addictive nature of social media and lack of self-regulation means many spend more hours online than they otherwise would; and that a higher threshold better reflects the duty to protect children from engineered harm.

Other members argued that 13 is a more socially realistic threshold, particularly given the role of digital communication in early teenage friendships and the risks of social exclusion, isolation or stigma if younger teens are barred entirely.

A strong theme was the need to distinguish between messaging tools used for social organisation and content-driven, algorithmically amplified platforms. Several members

[10] BCS Member Survey (2026)

felt that treating services such as WhatsApp in the same way as TikTok, Snapchat or Instagram failed to reflect meaningful differences in risk. Practical enforceability was also cited: existing 13+ limits are already only partially enforced, and raising the threshold could increase circumvention rather than reduce exposure.

2.1.3 Cross-cutting consensus on age

Despite disagreement on the precise age threshold, members broadly agree that a single age line cannot address differing risk profiles, and that regulation must focus on what platforms do, not just who can access them. Many members advocated graduated or feature-based access, restrictions on high-risk functionality for under-16s and in some cases under-18s, and film- or game-style age ratings for social media features.

2.1.4 Anticipated impacts of a higher minimum age

Anticipated benefits included reduced exposure to harmful content in early adolescence, clearer norms and boundaries for parents and schools, and reframing society's expectations so that social media is seen as non-essential to childhood.

However, members were frank about technical challenges. Only 4.7% of member survey respondents were extremely confident a ban could be effectively enforced[11]. Members felt children would find a way around any restrictions, expressed limited confidence in current age-assurance capabilities and noted that young people could seek social connection in other areas of the internet that are potentially more harmful than mainstream social media sites. Members stressed that acknowledging enforcement difficulty should inform better policy design rather than delay any protective action.

2.2 Age of digital consent

The general consensus was that a tiered approach to the digital age of consent makes sense. The case for a higher age of consent was strongest where platforms rely on consent to process data for profiling, targeted advertising or personalised recommendation. It was weaker for services that collect minimal data for a clearly functional purpose, such as an educational tool that requires an account to save progress. A risk-based and purpose-based approach to exemptions would preserve access to beneficial services while protecting children from commercial data exploitation.

2.3 Feature-based restrictions and platform design

2.3.1 Harmful features

[11] BCS Member Survey (2026)

There was near unanimous agreement that certain features pose disproportionate risks to children and should be restricted, regardless of overall age thresholds. Features consistently identified as harmful include: infinite scrolling and autoplay; algorithmic recommendation feeds; public follower and "likes" metrics; disappearing messages; livestreaming and location sharing; and unrestricted contact with unknown adults.

BCS members strongly support safety-by-default approaches, including mandatory removal or dampening of persuasive design features for under-16s, non-dismissible time limits and night-time protections and clear stopping cues.

2.3.2 Impacts of restricting features and introducing time limits

BCS members emphasised that restricting high-risk features and introducing time limits would produce meaningful improvements in children's wellbeing, including reduced compulsive use patterns, improved sleep, educational outcomes and attention and lower rates of anxiety linked to excessive social media use.

Evidence cited suggests that even light-touch interventions such as behavioural nudges can significantly reduce usage, with stronger mandatory measures likely to produce greater impact. Restrictions that directly target engagement-maximising design are likely to reduce total time spent and frequency of return. This will have downstream effects on wellbeing but will also reduce platform revenues derived from attention, which should be understood as an intended outcome rather than a side effect.

Impacts will vary by age and context; younger children may benefit most from hard limits, while teenagers respond better to a combination of limits and transparency. Measures must be designed to avoid simply displacing activity onto less regulated platforms. Some members noted risks of market concentration, where only the largest platforms can afford compliance, potentially reinforcing monopolistic dynamics.

2.4 Scope of restrictions

2.4.1 Key principles

BCS members strongly support a risk-based, functionality-led approach in determining which services should be in scope. Core factors to determine scope include: user-to-user interaction, particularly with unknown adults; algorithmic recommendation systems that shape content exposure; public or semi-public content sharing models; personal data processing for profiling or targeted advertising; and high-risk features such as livestreaming, disappearing messages and geolocation.

The consultation should avoid relying on platform categories. Instead, services should be assessed dynamically against these risk factors, as platform functionality evolves rapidly

2.4.2 Gaming and hybrid platforms

There was strong consensus that gaming environments with social functionality meet the threshold for inclusion. In practice, children often experience social gaming platforms as social media. Regulatory scope should therefore reflect user experience rather than sector labels.

2.4.3 Exemptions

Appropriate exemptions were identified as: closed educational systems with verified participants; family-controlled or small-group services without profiling or advertising; and safety-critical communications services. Any exemption framework should include clear, testable criteria and external oversight, to prevent commercial platforms from restructuring features to avoid regulation.

2.5 Chatbots and AI

2.5.1 Risks of AI chatbots for children

BCS members identified the following features as presenting the highest levels of risk to children: simulation of romantic or intimate relationships; simulation of friendship and companionship; mimicking empathy and emotional understanding; personalisation of interactions; persistent memory and recall across sessions; use of flattering or affirming language; hallucinations (false or misleading responses presented with confidence); and the ability to generate or engage in mature or adult content.

There was strong agreement amongst BCS members that features which simulate emotional intimacy and sustained relationships represent the greatest risk category. These features are not incidental but are core to engagement-driven design. Anthropomorphic AI behaviours such as empathy simulation and conversational persistence are intentionally deployed to maximise user retention. For children, this increases the likelihood of parasocial attachment, where AI systems are perceived as trusted companions rather than tools.

There is particular concern about the cognitive and behavioural impact of highly personalised, affirming systems. Where chatbots consistently validate user views without challenge, they may reinforce beliefs and influence mindset development. Over time, this could contribute to distorted thinking patterns or reduced critical reflection.

The finding that a proportion of children report using chatbots because they have "no one else to talk to" highlights the risk of AI substituting for human support mechanisms, including friendship, family, or professional help. BCS members also raised concerns about the use of AI as a substitute for emotional or therapeutic support, where children may rely on systems that are not equipped to provide safe or appropriate guidance.

Hallucination was identified as a distinct and significant risk: children may rely on AI outputs for learning or advice and receive confident but incorrect information, with limited ability to critically assess accuracy.

2.5.2 Age restrictions and regulatory approach for AI chatbots

BCS members support graduated, feature-level age restrictions based on risk, rather than blanket restrictions on all chatbot use. High-risk features requiring the strongest restrictions include romantic or intimate relationship simulation modes, which should be restricted to 18+, and the generation of adult or mature content, which should be subject to robust age assurance equivalent to online pornography standards. Moderate-risk features requiring conditional access include persistent memory and cross-session personalisation, which should require parental consent for under-16s and advanced personalisation or emotional modelling, which should require transparency and user controls. Lower-risk functionality, such as general-purpose conversational AI without emotional simulation or persistent profiling may be permitted with content moderation and safety controls.

BCS members also support a tiered regulatory model aligned to functionality and risk: prohibition or strict restriction of high-risk relational features; controlled access to personalisation and memory features; and safeguarded access to general-purpose tools.

Regulation should focus on the features that materially increase risk, rather than restricting access to all AI systems. Age restrictions alone are insufficient; they must be combined with clear explanations of how systems work, what data is used, and what limitations exist, to support informed use by both children and parents.

An additional recommendation from members is the development of a UK Children's AI Standard, providing operational guidance similar to the ICO's Age-Appropriate Design Code, that sets clear design requirements for any AI service likely to be used by children.

3. Enforcement and Compliance

3.1 Age assurance

3.1.1 Key challenges

BCS members identified the following key challenges in implementing effective age assurance: privacy risks associated with data-intensive verification; fragmentation across platforms leading to inconsistency; and high rates of circumvention under current approaches.

The privacy implications of ubiquitous age verification must be carefully managed. The current model, where each platform independently runs its own age verification and retains user identity data, creates significant data security and privacy risks. A better architecture would be a trusted, government-backed digital identity credential, such as building on GOV.UK Verify or similar frameworks, which then allows a single age attestation to be shared across services without each platform storing identity documents. Adults should accept this friction for the purpose of protecting children, but government must ensure the infrastructure does not create new risks of data breach, profiling or misuse.

3.1.2 Making age restrictions effective and workable

Key technical considerations include: verification must be cryptographically robust and resistant to spoofing; age estimation technologies such as facial analysis should be used as a supplementary rather than primary mechanism given their documented inaccuracies for younger users; device-level OS-integrated age verification via Apple ID, Google Account or equivalent offers a lower-friction approach that should be explored as a standard; interoperability between age assurance providers should be mandated so users are not required to re-verify for each service; and a layered or successive validation approach, as used in Australia, is more robust than any single method. The government should also consider whether platforms above a certain size should be required to share age assurance infrastructure rather than each building proprietary systems.

3.1.3 Impacts of wider age assurance requirements

Positive impacts would include significantly improved child protection, reduced ability of platforms to claim ignorance of user age and clearer accountability when children access age-restricted content. Negative impacts would include increased friction for adult users, privacy risks if poorly implemented, potential exclusion of adults without standard identity documents and compliance costs for smaller platforms. These negatives are manageable with good policy design and should not be used as a reason to avoid effective age assurance.

BCS members support a system-level solution: government-backed, privacy-preserving digital identity infrastructure; device or operating system-level age credentials; and interoperability across services to avoid duplication.

Members also suggested that the consultation prioritise the following evaluation criteria: false positive rates, specifically incorrectly admitting children, which is the critical measure for child safety; addressing known circumvention methods; privacy preservation and whether the technology minimises data collection; accessibility for users without standard identity documents; and performance across different demographic groups, since some age estimation technologies have documented bias by ethnicity and gender.

Members broadly supported a graduated model akin to: under 13, full parental control; 13–15, restricted and supervised access; 16–17, increasing autonomy with safeguards.

3.2 Circumvention of age limits

The most prevalent circumvention behaviours identified were false age declaration, use of shared or adult accounts and switching to web or alternative services.

Members recommended combining technical controls with user education, and exploring proportionate restrictions on VPN access for under-18s while preserving legitimate uses. Members emphasised that while complete prevention is unrealistic, policy should aim for measurable reduction in access to high-risk environments. The consultation should prioritise addressing simple, high-frequency circumvention methods before more complex technical solutions.

3.3 Mobile phones in schools

When asked, BCS members broadly supported making the Department for Education's (DfE) non-statutory guidance on mobile phones in schools statutory. Benefits identified include reduced disruption to teaching, lower incidence of bullying and peer pressure via devices as well as clearer expectations for parents, pupils and schools.

Caveats include implementation challenges around storage, enforcement and cost, and the need for exceptions for SEND, safeguarding and health needs. Policies should focus on behaviour and environment rather than device type alone, as blunt restrictions may not address underlying issues. Ofsted's planned inspection of mobile phone policy implementation from April 2026 is a positive step, but statutory backing is necessary for full effectiveness.

A proposed smartphone ban in schools may be appealing in principle but is harder to implement in practice, as phone use is deeply embedded in daily life, for example for transport access. While schools should be able to confiscate devices when misused,

wider practical impacts, such as requiring simplified devices, must be carefully considered.

4. Preparing Children for a Digital Future

4.1 Digital skills and media literacy

In our polling, BCS members selected 'all areas' of media and digital literacy as ones where children and families most need additional help[12]. In facilitated discussion, members also highlighted the importance of understanding algorithmic systems and persuasive design, identifying misinformation and synthetic content as well as managing time, attention and online interactions.

Literacy must include how platforms are designed to influence behaviour, not just how to use them safely. Provision should be accessible, inclusive and allow anonymity to encourage uptake.

The most useful sources of support identified were parent or carer groups or networks, non-governmental online sources and government websites[13]. Members identified schools or childcare settings, community or youth spaces such as libraries and youth clubs, and parent or carer groups or networks as where more support should be available in future[14].

Outside of schools, government could better support children and young people by supporting parents and carers, by working with platforms and services that children already use, by making help or advice easy to access when something goes wrong online, and by involving children and young people in designing support.

4.2 High quality online content

BCS members support a multi-stakeholder definition of high-quality content, including child development experts, educators, civil society organisations as well as children and young people themselves. Independent standards and verification mechanisms are necessary to ensure credibility.

Industry best practice principles should be published as a baseline, with Ofcom empowered to enforce them as part of its Online Safety Act duties. The EU's Better Internet for Kids framework[15] is a useful reference point, as is Australia's approach. Guidance directly aimed at children, in age-appropriate and engaging formats, should be developed with children's input rather than produced by adults and distributed at them.

---

[12] BCS Member Survey (2026)
[13] Ibid
[14] Ibid
[15] European Commission, *Better Internet for Kids*, available at: https://better-internet-for-kids.europa.eu/en

A key risk in any positive content initiative is that it becomes a vehicle for platform self-promotion rather than genuine child benefit. Standards must be independently set and independently assessed. Platforms should not be able to self-certify as providers of positive content to avoid or reduce regulatory obligations. Any framework should also explicitly address the structural tension between commercial incentives, which drive platforms towards engagement-maximising content, and child wellbeing, which requires content that is genuinely enriching rather than merely popular.

5. Supporting Families

5.1 Parental control

BCS member responses to whether parents should have control over the online experiences of their children was mixed. On one hand, for under-16s parents still play a fundamental role in shaping their lives, and parents and caregivers are the primary agents for the proximal processes, interactions that occur daily that support development. On the other hand, as much as parents should have control, this has not worked for many young people so far and parents need guidance and support to make the right choices for their children.

A flexible, tiered model of restrictions and parental controls is preferred, where age thresholds act as guidance rather than fixed rules. Parents would retain discretion to adjust levels of access based on their child's maturity. This approach is seen as less rigid and more empowering for families than strictly age-based limits.

5.2 Making parental controls more effective

The most impactful changes would be: standardisation of parental control interfaces across platforms so parents learn one system rather than a different one for each app; making parental controls a mandatory setup step when a child account is created, not an optional feature buried in settings; requiring platforms to provide a plain-English summary of what each control does and does not do; providing parental controls at the device or OS level as a universal layer rather than relying solely on per-app controls; and ensuring parental controls are non-dismissible by the child without a separate parental authentication step.

The government should also consider whether parental control setup should be incentivised or required at the point of device purchase, similar to how car manufacturers are required to include safety features as standard rather than optional extras. Platforms should be required not to design systems that undermine parental controls or informed consent.

6. Expert Perspectives from BCS Fellows

6.1 Professor Andy Phippen

Professor Andy Phippen is a BCS Fellow and Professor of Digital Rights with over 20 years of research in online safety and digital citizenship.

Professor Phippen has argued that UK debates often default to device bans, platform restrictions, or age-based control, while insufficiently addressing the real-world ways children experience risk and seek help, and failing to address the responses of those around the child.

He has emphasised that routes for disclosure, and supportive response to disclosure, are, young people tell us, far more important than bans. Children consistently report wanting better guidance, understanding and support. Many harms arise from social dynamics rather than technology alone, and restriction without literacy risks leaving children unprepared when exposure inevitably occurs.

A ban is not a solution as it does not make the problem go away, as we can see in other areas of social policy such as vaping, smoking and alcohol consumption among young people. A ban does not mean that the responsibilities of areas of the online safety ecosystem disappear or that risk of harm goes away.

Professor Phippen therefore cautions that age limits can create a false sense of safety, that over-reliance on regulation may crowd out investment in education, response and recovery, and that digital literacy is itself a safeguarding intervention, not a soft alternative.

He also notes that BCS members' comments around mental health harms and social media are not strongly supported by research. Large studies show only weak correlation between social media and mental health, and causation is very difficult to demonstrate.

He suggests that, should bans be viewed as the correct policy direction, they need more nuance than simple age limits, and limits should be varied depending on the nature of the platform and online interactions, in the same way that films are treated.

6.2 Professor Victoria Baines

Professor Victoria Baines is a BCS Fellow and Professor Emerita of Information Technology at Gresham College. She has worked in law enforcement on online harms and at Facebook on law enforcement outreach, and now provides independent research to international organisations including the Council of Europe and the UN.

The following is Professor Baines's contribution in full:

"The concerns over children's use of social media are understandable and well-founded. It is reasonable to expect that platforms do their utmost to prevent and

combat illegal harms, while also reducing children's exposure to harmful content and adverse experiences. This is what the Online Safety Act (OSA) is designed to address. Recent reports from Ofcom indicate that this legal obligation and oversight mechanism is meeting with some success, most notably resulting in a number of platforms improving their ability to prevent children being groomed for sexual activity.[16]

The OSA sensibly prioritises action against the most serious harms posed to children by illegal content and illegal contact. It also requires platforms to conduct assessments of other risks to children and to share those with Ofcom. According to Ofcom's published timeline, these assessments are in train, with platforms due to report by the end of July, and publication of Ofcom's statutory report on content harmful for children by October 2026.

Of particular concern to caregivers and child safety stakeholders currently are the issues of screen time and the effect on mental health of 'doom scrolling', facilitated by platforms' recommendation engines and auto-play features. It is important to note that the evidence base on the impact of screen time on children and young people's mental health is far from definitive and far from damning. Research conducted by the Oxford Internet Institute found no evidence that screen time is negative for children's cognitive development and well-being, while the World Health Organisation has assessed that evidence of the impact of technology use is mixed, with studies indicating both positive and negative associations between technology use and young people's well-being.[17]

This is not to dismiss the lived experience of caregivers or evidence that use of social media can have a negative impact on children's mental health. Investigating online harms and analysing their policy and operational responses for almost two decades, I have consistently found that the rhetoric surrounding children's use of technology often does more to heighten caregivers' and society's fears than it does to make children safer and healthier in actuality. Jonathan Haidt's The Anxious Generation is perhaps the most popular and extreme example of this currently. But it is by no means isolated.

In such circumstances, ensuring that policy and regulatory responses are driven by robust, independent evidence rather than emotion and self-interest is both paramount and more challenging. Untested perceptions can generate ineffective and absolutist responses, as is the risk with the recommendation of a ban from social media for under 16s. To my knowledge there is no evidence that children's access to social media is uniformly harmful, and that removing social media from children will improve their safety and mental health.

---

[16] https://www.ofcom.org.uk/online-safety/protecting-children/tech-firms-commit-to-stronger-anti-grooming-measures-in-response-to-ofcom-demands

[17] https://www.oii.ox.ac.uk/news-events/no-evidence-screen-time-is-negative-for-childrens-cognitive-development-and-well-being-oxford-study/ ; https://www.who.int/europe/publications/i/item/WHO-EURO-2025-12187-51959-79685

In this respect, children's views as expressed in Ofcom's Online Nation report to some extent challenge the responses of IT professionals to the BCS survey:

- Over half (56%) of children felt that being online had a 'mostly' good effect on how they feel about themselves. A small minority (3%) felt it had a 'mostly' bad effect, while a third (34%) felt it had a bit of both good and bad.
- Aiding their education is one area where children feel the internet benefits them. Nearly eight in ten (78%) of 13-17s say the internet helps with their schoolwork
- Two-thirds (65%) of 13-17s see the online world as beneficial in building and maintaining their friendships, especially among girls (71% compared to 60% of boys).
- Social media and messaging apps play a big role, as 72% of 13-17s who use them agree that it helps them feel closer to their friends.

Moreover, in my career I have encountered scenarios in which children who lacked capable guardians or who experienced abuse by their caregivers found social media to be a lifeline in terms of peer support and access to specialist services such as child helplines. In the last decade we have also witnessed the advocacy and changemaking of which children are capable when they have a public platform — including Greta Thunberg and Malala Yousafzai — the impact of whose activism has been enabled and amplified by their presence on social media. A blanket ban on social media for children under a certain age would remove opportunities for freedom of expression, avenues for building life skills, and in some cases result in missed opportunities to remove them from harm.

Early indications from Australia suggest that it would also be hard to enforce. The eSafety Commissioner's early report that 70% of under 16s still have access to social media appears to be corroborated by research published by the University of Chicago[18]. Operationalising highly effective age assurance has proved challenging, and Ofcom's recent finding that platforms with a minimum age of 13 are not enforcing this effectively is unsurprising[19]. Age assurance tools that rely on official documentation such as passports and credit card data are unsuitable for children, and the efficacy of facial age

[18] Australian eSafety Commissioner, *Under the New Age Restrictions: Early Insights from Australian Parents*, March 2026. Available at: https://www.esafety.gov.au/sites/default/files/2026-03/Under-the-new-age-restrictions-Early-insights-from-Australian-parents-March2026.pdf

[19] Drozd, O. et al., *Why Bans Fail: Tipping Points and Australia's Social Media Ban*, Becker Friedman Institute, University of Chicago, 2026. Available at: https://bfi.uchicago.edu/working-papers/why-bans-fail-tipping-points-and-australias-social-media-ban/

estimation, while continuously improving, has been frequently overstated[20]. One can add to this the challenge of scope creep. Having been social for many years, online games are increasingly immersive and multi-modal. Accordingly, any prohibition on access to social media under a certain age would need to consider whether the advisory PEGI ratings would require reform and a consequent enforcement mechanism.

A more effective alternative to prohibition already exists, is technically possible, and there is a regulatory structure able to incorporate it. Using agreed age-appropriate design codes, platforms can be obliged to introduce further measures to protect children from adverse effects and experiences, including restriction of autoplay features and reduction or restriction of recommendation engines in children's experience of social media. Neither of these measures would inhibit children's discovery of content should they actively search for it. But, along with trusted adult oversight and time limits, they would introduce a level of friction that may reassure caregivers and campaigners. Some of these features have already been tried or are in development — for instance, Meta's Messenger Kids, Instagram Teen accounts, Snap's Family Center, TikTok's time limits, and Fortnite's cabined accounts[21]. The challenge of correctly identifying the age of a child user would remain. But in a case of additional protection rather than absolute prohibition, this can be addressed by applying these restrictions only until such time as proof is shared that the child has reached the age of 16."

[20] Hanaoka, K., Ngan, M., Yang, J., Quinn, G.W., Hom, A. and Grother, P., *Face Analysis Technology Evaluation: Age Estimation and Verification*, NIST IR 8525, National Institute of Standards and Technology, May 2024. Available at: https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8525.pdf

[21] Disclosure: Professor Baines serves on Snapchat's Safety Advisory Board in an independent and unpaid capacity.

Contact

For further information about this response or BCS's work on online safety and digital policy, please contact:

Claire Penketh, BCS' Head of Policy Development at Claire.Penketh@bcs.uk

BCS welcomes continued engagement with government, industry and civil society on the issues raised in this response.