Growing up in the online world: a national consultation by the Department for Science, Innovation and Technology

About the Institution of Engineering and Technology (IET)

The IET is a trusted adviser of independent, impartial, evidence-based engineering and technology expertise. We are a registered charity and one of the world's leading professional societies for the engineering and technology community with over 158,000 members worldwide in 148 countries. Our strength is in working collaboratively with government, industry, and academia to engineer solutions for our greatest societal challenges. We believe that professional guidance, especially in highly technological areas, is critical to good policy making.

Executive summary

The IET strongly supports the Government's efforts through legislation and regulation to put robust safeguards in place so that vulnerable people, including children and young people can use online platforms safely, develop essential digital literacy skills that will ensure they thrive in their chosen career, and maintain their privacy. As the world becomes more digitally oriented, young people must develop online skills that complement their real-world soft skills, enabling socialisation, employability, and full participation as digitally native citizens. When used responsibly and safely, social media and online platforms can help children and young people become more comfortable with the digital world early on and build crucial digital literacy skills (Social Media Benefits; Internet Matters, February 2025). Digital skills and literacy will be critical to future employment and economic growth, underscoring the need for government to support their development while also protecting children and young people online. Data from the IET's UK Engineering and Technology Skills Survey demonstrates that digital capabilities will be essential for the future workforce and states that employers have noted significant skills gaps in data engineering, software engineering, and cyber security (UK Engineering and Technology Skills; IET, April 2025).

The primary aim is safety and protecting vulnerable people online. One proposed measure to increase safety online is a ban on social media use for under-16s. If the UK proceeds with such a ban, it is important to consider and mitigate potential unintended consequences on other aspects of digital life. Government should ensure all new technologies are deployed safely and society is appropriately protected from potential harms and misuse. The Online Safety Act and oversight through Ofcom as a regulator provides significant safeguards to protect vulnerable people online, however, harms are still prevalent. The IET supports ongoing review and vigilance into ensuring that the legislation is future proof, for example, ensuring the definition of 'user' is expanded and new types of technology such as wearables are accounted for. We recognise social media can cause harm to young people and appropriate guardrails and protections are required. However, we believe that education programmes have a powerful role to play in building the knowledge to support safer use of digital technologies alongside legal safeguards.

The IET and the expertise of its members are here to support government in addressing these challenges and to provide advice on targeted policy interventions that can help mitigate unintended consequences.

Recommendations:

- **Working with industry experts and stakeholders:** The Government must work with cross-sector industry experts to ensure that new technologies are safer by design and continue to consult with a range of stakeholders including young people and youth-oriented organisations such as The Stemettes.

- **Continue to gather evidence long term:** The Government should draw on evidence from existing pilots, studies and social media bans, to evaluate the effectiveness of such interventions and ensure that the most appropriate policy levers are used, while minimising unintended consequences in the longer term.

- **Digital Skills and Digital Literacy**: Continue to develop policies to encourage both digital skills and literacy, for example in education, alongside interventions to keep children and young people safe online. Policies in this area should be forward thinking, not responsive to incidents on a case-by-case basis, establishing a greater understanding of technology and how to critically assess it.

- **Robust Safeguards:** Vulnerable users must be protected online through a combination of robust legal safeguards and education programmes that equip both young people and parents with the knowledge to stay safe online.

- **Right to digital privacy:** There should be the ability to expunge your data from social media, for example on behalf of a child, or once the child reaches 18.

- **Caution over VPN bans:** Children and young people may bypass age restrictions using VPNs. A ban on their use could undermine cybersecurity and have wider negative impacts on businesses and the economy.

- **Supporting families:** There should be greater support to parents to understand how to limit and control access to certain content on their devices within the home and school environment.

Preparing young people for a digital future

By the age of 13, 81% of children own a smart device, and this rises to 95% among those aged 13 to 17 (How to Protect Kids Online: The Building Blocks of Online Safety Policy; Ruth Whittaker, March 2026). IET expert research further predicts that the next generation of children may spend up to ten years of their lives in the metaverse (Safeguarding the metaverse; IET, April 2022). Children and young people use social media and online platforms for a wide range of purposes, however, these spaces can also present significant risks and, in some cases, the potential for harm. Age is a key factor in shaping how platforms are used and the level of protection required; for example, the needs and safeguards appropriate for a 10-year-old will differ substantially from those required by a 16-year-old. **Government must seek input from a range of experts from across different disciplines to form an evidence base.**

In an increasingly digital world, strong digital skills (using devices and the internet effectively) and digital literacy (the ability to confidently, safely, and critically find, evaluate, create, and communicate information) must go hand in hand with online safety and privacy (A Safe, Informed Digital Nation, UK Government, March 2026). According to the IET's Skills Survey, digital capabilities will be essential for the future workforce, with the most critical skills for growth identified as automation (38%), cyber security (38%), data engineering (34%), and

software engineering (33%) (UK Engineering and Technology Skills; IET, April 2025). Increasingly, employers are expecting workers to be digitally native in order to use everyday workplace tools, and social media is often the first port of call for young people to develop transferable digital skills that can then be used for the workforce, such as, managing their online presence. There is also a demand from children and young people for this skillset, in a survey conducted by the AQA, young people identified digital literacy (60%) and online safety (54%) as areas they wanted to learn more about (AQA; April 2026).

Employers also report significant skills gaps in data engineering, software engineering, and cyber security (each cited by 17%), making these areas particularly challenging to recruit for and reinforcing the importance of early, safe engagement with digital technologies (UK Engineering and Technology Skills; IET, April 2025). **Given the importance of these skills to the future workforce, the IET recommends ensuring that policies continue to encourage digital literacy are considered alongside interventions to keep children and young people safe online.** Whichever career they choose to pursue, digital skills are going to be necessary to thrive.

We do not yet have sufficient evidence to say what the impact of restrictions on children may have on whether they become a digitally literate citizen in future. The Government should carefully consider the unintended consequences a widespread ban on social media could result in, especially in a world where children need to grow up to be digitally literate. Digital technologies, including social media and AI, bring significant benefits to society. We have the opportunity to equip the future generation with adaptability to technology, in particular, the ability to question and challenge what they see not just simply use it. The IET supports ongoing reforms to the curriculum, to ensure that children are exposed to and learn about emerging technologies, such as AI, which will be not only a part of work, but life, for most people.

To encourage digital literacy and maintain safety, policies in this area should be forward thinking, not responsive to incidents on a case-by-case basis. For example, regulators should look to future technology trends, such as wearables, and the impact they might have on privacy, social media in VR, deepfakes, AI content generation and personal data. These technologies evolve rapidly, with new technologies emerging every day; **therefore, the Government must be prepared to respond to change and ensure they are kept under continuous review with input from cross-sector experts and stakeholders.**

Social media restrictions

A key priority is to safeguard vulnerable people online. If the UK chooses to proceed with a ban on social media for children, there may be some unintended consequences that should be considered and mitigated against. **It will be important to regularly review evidence from existing bans on social media in countries such as Australia, to assess their effectiveness in preventing harm in the long term.**

We must continue to make sure that legislation and regulation is future proof and able to adapt quickly. If a ban is implemented, it is going to be critical that traffic is not driven to unregulated parts of the internet or that children simply find a platform that is not within regulation, for example, certain e-learning or video chats, with less safeguarding in place to protect them. Data from the Molly Rose Foundation reports that despite the social media ban for under-16s in Australia, three in five 12-15 year-olds still have access to one or more platforms and major platforms have retained a majority of their child users (Molly Rose Foundation, April 2026). This suggests that the social media bans may not necessarily work as intended.

Whichever policy route is taken, it is vital that government continues to work with and support industry to embed safeguards at an early stage of technological development, ensuring products are safer by design. This will help get to the root cause of issues and future proof policy in this area. In all cases, evidence is critical to success, we must work together with charities, professional bodies, industry and government to combine expertise and address the digital challenges not just of today, but tomorrow.

The right to digital privacy

Online platforms should enable the deletion of personal data, for example at the request of a parent or guardian, or once a child reaches the age of 18. This is essential to protect children's privacy, limit the long-term impact of digital footprints created without informed consent, and reduce the risk of data misuse as young people transition into adulthood.

VPNs

One potential way that children and young people may circumvent age restrictions is through the use of virtual private networks (VPNs). **While some argue that banning VPNs could address this issue, the IET advises caution against imposing broad restrictions on their use as part of age limitation legislation.** VPNs play an important role in safeguarding cybersecurity, particularly for businesses and organisations seeking to protect data and systems. A general ban could therefore have negative consequences for the UK, including undermining cyber resilience and weakening security across the wider economy.

Supporting families

Some proposed policies assume that all parents have equal capacity, technical literacy, and resources to monitor and control their children's use of online platforms. In practice, this is not the case, and such assumptions risk exacerbating existing inequalities. Research by the IET on virtual reality outlines that almost two thirds (62%) of parents of children aged between 5 and 10 do not currently understand the metaverse (Safeguarding the metaverse; IET, April 2022). This is reinforced by ICO findings, which report that 46% of parents do not feel confident protecting their children's privacy online; 44% say they try but are unsure whether they are doing enough; and 42% believe they probably do not spend sufficient time reviewing their child's privacy settings (Information Commissioners Office, April 2026). **The IET therefore recommends that the Government continues to provide greater support to parents, particularly in improving awareness and understanding of parental control tools.** This should include guidance on how to limit and manage access to age-inappropriate content across devices in both home and school environments, helping to ensure that safeguards are effective and consistently applied.

Conclusion

Children and young people are growing up in a rapidly evolving digital environment that presents both significant opportunities and real risks. While safeguarding vulnerable users online must remain a priority, policies should be carefully designed to avoid unintended consequences, including circumvention, displacement to less regulated platforms, and impacts on digital literacy and skills. Supporting parents, strengthening digital literacy, enabling meaningful data rights, and future-proofing legislation to account for emerging technologies will be essential to ensuring that young people are protected while still equipped with the skills they need for a digital future. Through the expertise of its members, the IET offers, independent, timely, evidence-based advice to the Government, regulators, industry, and civil society to develop targeted interventions that balance safety, privacy, and opportunity for the next generation.

Contact details
For more information or to arrange a meeting please contact The Digital Futures Policy Team at policy@theiet.org.