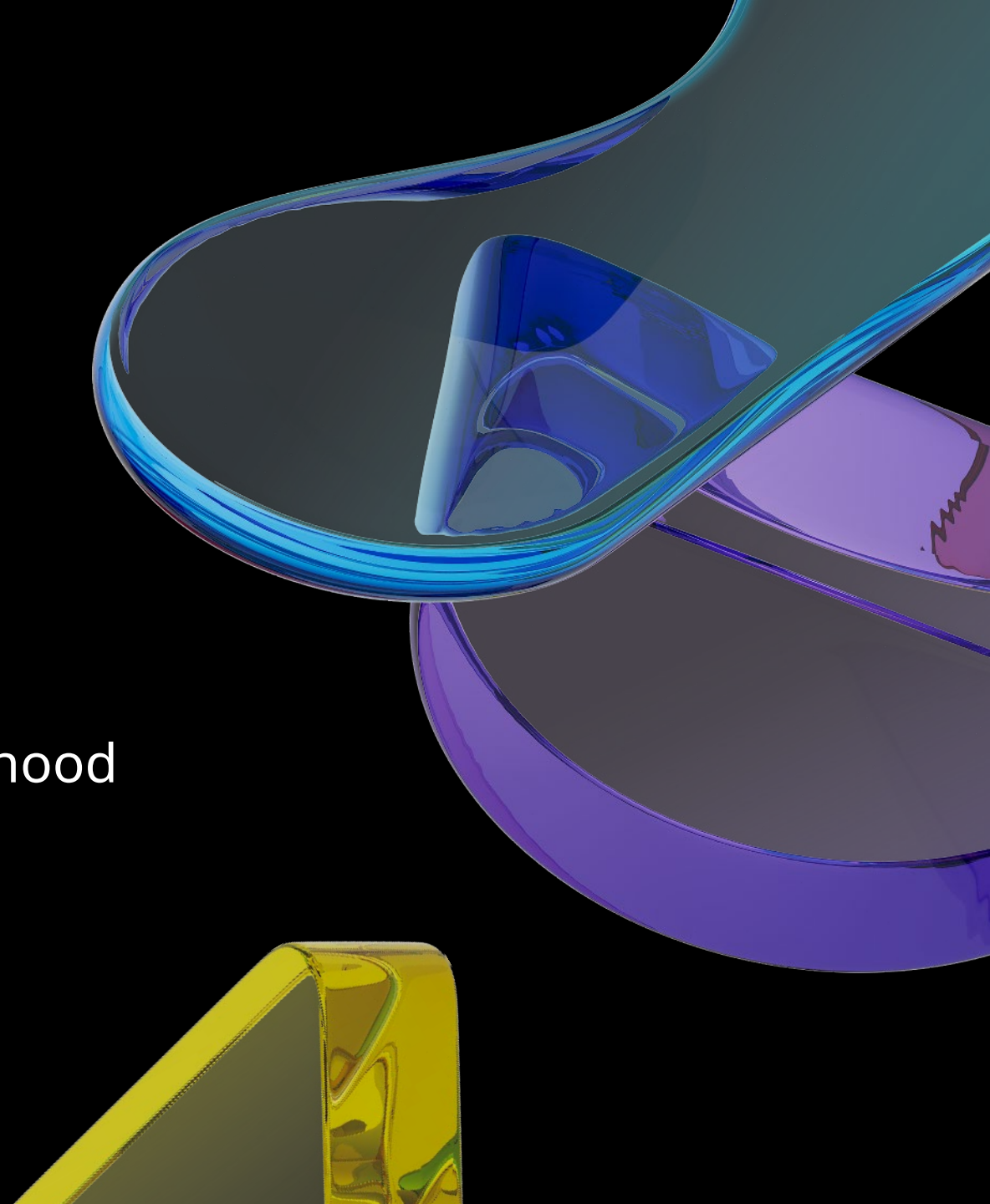




Growing up in a digital world

How can standards support safety and security as technology transforms childhood

August 2026



Introduction

In July 2026 BSI hosted policy experts, officials and representatives from industry, advocacy groups and the third sector, to explore 'Growing up in a digital world: how can standards help support safety and security as technology transforms childhood?'.

The roundtable, organized to mark BSI's 125th anniversary, looked at issues including safety, security and privacy, and covered technology ranging from AI toys, devices and educational technology, to social media, apps and chatbots. It also sought to proactively identify where standards can play a role in addressing significant societal challenges.

Chaired by BSI's Laura Bishop with support and input from Sahar Danesh, the discussion explored what a good digital childhood looks like, and the opportunities and risks presented by AI and digital technologies. This whitepaper summarizes the discussion, key takeaways and areas for BSI to take action.



Foreword

Dr Laura Bishop, AI & Cybersecurity Digital Sector Lead, BSI

There is no responsibility greater than people's safety, and that includes the safety of vulnerable members of society, children and young people. Over 125 years standards have played an important role in building trust that products are safe, secure and behave as expected.

As technology becomes ever more embedded in the fabric of society, it is essential that the frameworks around them develop at the same pace and support safe, transparent and age-appropriate use. Psychological safety must be treated not as an afterthought, but as a principle by design and a default expectation.

From AI-powered toys to global social media platforms, regulation, standards, and governance can ensure innovation is developed with human impact at its core.

It was fantastic to gather so many expert guests for this roundtable to explore how we embed psychological and physical safety, security and privacy into the digital tools and technologies that we now use every day.

While tackling the risks will require collaboration across society, and involve industry, government and parents and children themselves, we believe there is a clear opportunity for standards to help shape a safer and healthier digital future for children.

The goal is not to remove children from digital environments, but to ensure that technology supports childhood development, agency, wellbeing and safety.



Digital childhood - by numbers

47%

Young people who would prefer to grow up in a world without the internet

1 in 2

Teenagers who said a social media curfew would improve their lives

68%

Young people who said they feel worse about themselves after spending time online

42%

Teenagers who had lied to parents or guardians about what they do online

1 in 2

Children who have had an AI-enabled toy or learning device purchased for them

60%

Mums and dads who are comfortable with children interacting with AI for homework

3 in 4

Parents who worry that AI toys could expose children to unwanted content or data risks

46%

Mums and dads who think their child could distinguish between AI and a human

Data from BSI surveys: a) 2025 research covering 1,293 UK adolescents and young adults aged 16 to 21 b) 2026 survey of 1,000 UK parents of children under 16

Discussion points

1. There is no single 'good digital childhood'

Participants consistently rejected the idea there is one model digital childhood. Experiences differ by age, neurodiversity, identity, family environment and personal needs. Technology can be a source of belonging, education and support, particularly for children from marginalized groups. What's critical is to establish a rights-based, child-centred framework.

The challenge is not redefining childhood because technology exists, but ensuring technology supports existing childhood needs, rights and developmental stages in a healthy way. Ultimately, technology needs to adapt to childhood, rather than the reverse.

"It isn't necessarily that there is one good digital childhood... it's about giving young people control over how they use these technologies."

2. Technology shapes children's lives both directly and indirectly

Children have active digital lives, using platforms such as social media and chatbots for day-to-day interaction. But beyond that, children are increasingly affected by digital systems operating around them, even if they are not actively using them, from smart speakers to robot vacuum cleaners. The digital world shapes their physical one – and a digitally-excluded child may find themselves physically locked out of social interactions as well.



3. We are sending mixed messages

Several participants highlighted contradictions in current approaches. Children may be on the one hand encouraged to use digital banking, access homework online or learn from educational apps, or advised to develop digital skills for employment, then on the other warned about the implications of using technology or told it is harmful to their development. What is needed is a consistent cross-sector framework for childhood in the digital age.

Part of this is also avoiding a "cliff edge" approach to age. Participants challenged approaches where children suddenly gain access to digital platforms at a particular age, pointing out instead the value of graduated access models, like those used to determine age-appropriate advertising.

Risk-based decisions will be inevitable to support a healthy digital childhood, for example as more apps and platforms provide group communication channels. Imagine a 16-year-old doing a weekend job being prohibited from accessing certain apps where shifts are allocated or older teammates socialise. A simple ban may not be feasible at that stage.

The question to ask will be: do the risks of accessing this platform outweigh the potential impacts of isolation or access to knowledge?

4. It's not simply screen time – it's how digital life is experienced

The group challenged simplistic narratives around screen time. Concerns were instead focused on persuasive design, addictive engagement loops, streaks, notifications, dark patterns and commercially driven behavioural engineering.

This links to a changing understanding of how digital tools work. The internet was historically built around openness, anonymity and free information exchange – but this is not necessarily working for children today. Instead, participants discussed the value of shifting towards identity verification, age assurance, managed spaces or walled gardens.

“Children being online isn’t inherently the problem.”

5. AI is intensifying existing risks

Participants discussed AI-generated child abuse imagery, deepfakes, sexual extortion and manipulative chatbots. Equally, children are increasingly interacting with systems capable of forming emotionally engaging relationships, providing advice and shaping behaviour.

The view was not that children should be excluded from AI – not least because that is near-impossible given its pervasiveness – but that AI products and tools require stronger governance, transparency and testing.

6. Look at psychological wellbeing and the future

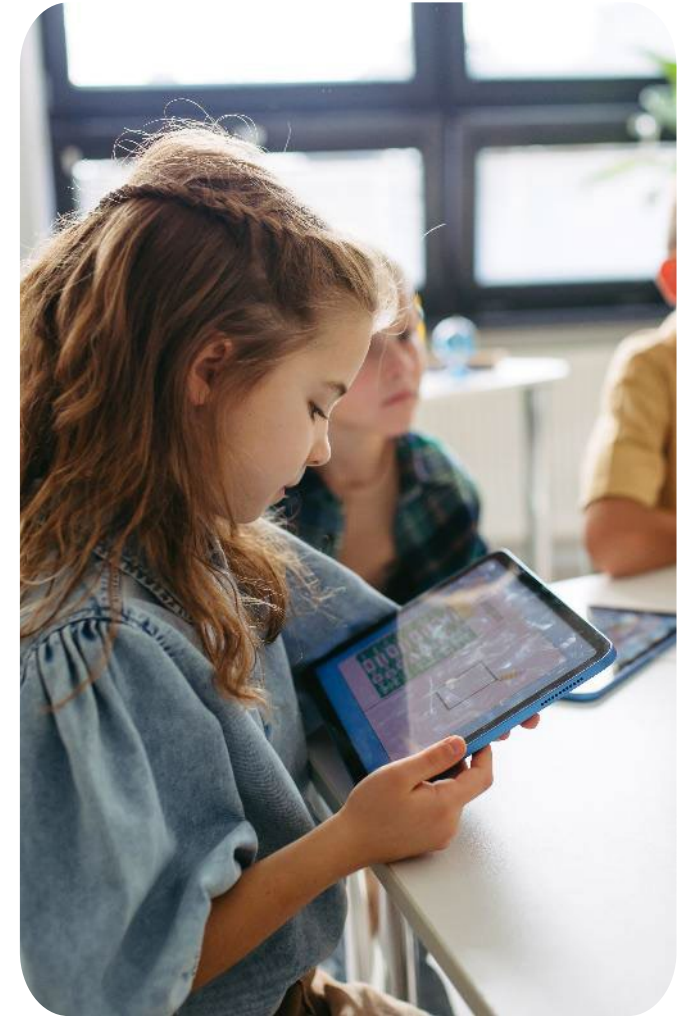
Preventing or mitigating harm is critical, but consideration of children's digital lives should also look at proactive steps to support positive wellbeing.

A good digital childhood should not only be safe, but actively support healthy development, confidence, creativity and participation. This includes considering changes to offline experiences, with participants pointing out that traditional outlets such as youth clubs, or helpline services, may no longer be available.

7. Trust is a critical consideration

Children are increasingly accessing news and information online, through apps or on social media. Even with a ban, this is unlikely to change, so more attention needs to be given to supporting them to assess what is true and what is false.

This also needs to recognize how trust evolves at different ages and stages; young children trust uncompromisingly, while teenagers may be more sceptical yet still heavily influenced by what they see in the digital world, particularly content from those they deem as role models.



8. International landscape

The global landscape of child online protection reflects a spectrum of approaches rather than a consensus. Most countries are moving toward greater protection for children online, but they differ in where they place responsibility: on children and parents (through age limits), on platforms (through safety-by-design obligations), on governments (through direct controls), or on education systems (through digital literacy and resilience).

Countries that have put in place strict age limit bans are now facing challenges on how to enforce restrictions, and in some cases face backlash on the impact of restrictions on youth digital rights and child development.



Taking action – areas for society, government and industry to focus on



1. Perfect should not be the enemy of the good

Participants were clear that the status quo cannot be maintained. While parts of industry may suggest change is complicated or risks unintended consequences, and parents may feel overwhelmed by the challenge – society is not powerless. There is a clear and urgent opportunity for policymakers, civil society, industry and parents to collaborate and find solutions that can support a good digital childhood.

For example, participants highlighted that some parts of the digital sphere are already proving progress is possible. Since the introduction of the Online Safety Act, adult websites have been required to undertake greater age verification.

While some are complaining of user drop off, they have been able to put things in place. Age assurance is accepted in offline life, even when it brings inconveniences.

Equally, the existence of parental controls indicates that certain features on digital platforms can be turned on or off, without there being a precondition of access. Finally, there are already standards that can be used to support child safety. These include the Age Assurance Framework (BS ISO/IEC 27566-1:2025).

The consensus was that while change may not happen overnight, waiting for a perfect solution puts an unnecessary barrier up. Participants highlighted that we are still trying to manage social media nearly 20 years on, yet now also grappling with AI. Change may need to be flexible, iterative and responsive – but there is an urgent need to act.

2. Protection – and empowerment

Participants made clear that empowerment of young people is as important as protection. They need the skills, confidence and understanding to navigate digital environments. Limiting access, blocking features and stronger controls have a role to play, but bans alone risk being insufficient and potentially counterproductive if they do not equip children to engage safely with technology as adults.

An overly protectionist approach risks creating children who are shielded from technology rather than prepared for it.

“It’s about empowerment and them having choice and understanding of the technology.”

The view was that a healthy digital childhood should not be defined solely by reducing exposure to harm. Children will become tomorrow’s students, workers, voters, parents and technology developers. They will be expected to use AI tools, access digital services, evaluate information online and engage with sophisticated technologies.

Completely insulating children from these environments is neither practical nor desirable. Instead, they need positive, safe opportunities to develop the knowledge, confidence, critical thinking and agency required to navigate a digital world safely and independently.

Standards should therefore support both protection from harm and the gradual development of digital autonomy, appropriate to developmental stages of childhood, ensuring that children are safe online and equipped to thrive in the digital society of tomorrow.



3. Agency is the real objective

The discussion repeatedly returned to agency. Participants argued that children should have increasing levels of control and responsibility as they mature. The aim should be so children understand how digital systems work, why technologies are designed in particular ways, how data is collected, and when to trust information and when to challenge it.

While many children already use digital platforms with competence, and recognize how algorithms or attention-based systems work, participants noted that young people still report feeling unable to control their experiences. The underlying platforms have been designed to maximise engagement, for example encouraging streaks, regular notifications, gamification, or infinite scroll.

“Kids say to us, I wish I could put my phone down.”

This means that empowerment requires system redesign, not just education or placing responsibility onto children or parents. Users of digital tools cannot be expected to overcome industrial-scale behavioural design simply because they have received digital literacy training.

Empowerment means creating environments in which children can exercise meaningful choice. It does not mean expecting children or parents to shoulder the burden of managing risks that have been deliberately engineered or compensating for poor design decisions.



4. Safety by design culture is paramount

There was consensus around a need for a cultural shift to prioritize safety of children over commercial drivers. The discussion highlighted the limits of education and parental oversight as safety mechanisms.

Digital literacy cannot compensate for products that have been designed without sufficient regard for child welfare. The clear message was that child safety should be built into digital from the outset rather than addressed only after harms emerge.

Participants repeatedly challenged the current model whereby new technologies are released first and only subject to intervention once evidence of harm has accumulated.

Society has already experienced this pattern with social media and is at risk of repeating it with AI-powered systems, chatbots, immersive technologies and AI-enabled toys. The feeling was not that children should be prevented from accessing such technologies altogether – since this is largely inevitable and there are benefits - but that products should be risk-assessed, tested and designed to mitigate foreseeable harms before deployment.

Rather than asking whether a product is innovative first and safe second, industry should be expected to demonstrate that child safety has been considered throughout the design, development and deployment process. This would align with the physical product approach, where products are released to children after robust safety testing.

Ultimately, developers, platforms and service providers should bear primary responsibility for ensuring that products are safe by default.

This includes considering issues such as harmful engagement mechanisms, manipulative design, inappropriate interactions, escalation pathways to human support and ongoing risk monitoring.

A range of voices with distinct perspectives need to be considered, for example involving behavioural scientists or psychologists in the design process and development of standards or guidelines.

“We need a fundamental principle that when children engage in the digital world safety checks and robust tests have been put in place first, so they are having safe experiences and that's been built into the design of that service.”

5. We also need to consider mitigation after harm has occurred

Shifting towards safety by design culture rather than retrofitting measures after harm is the end goal, but a holistic approach is needed, especially in the interim.

The question becomes not simply prevention, but what mechanisms exist when harm has already occurred? This might include robust parental controls that are clearly understandable, contestability and right of redress, reporting of issues or even content removal.

In addition, platform accountability needs expanding, requiring companies to assess and mitigate risks rather than relying solely on user or parental responsibility, with platforms that are aimed at children required to consider when to have a human in the loop to intervene if harms are detected.



6. Industry incentives need strengthening

A recurring theme was that standards alone are unlikely to drive widespread change unless organizations have a clear incentive to adopt them. Participants questioned why companies would prioritize child safety if doing so conflicts with commercial incentives.

A comparison was drawn with cybersecurity. Organizations have strong incentives to adopt standards such as ISO/IEC 27001 because cyber incidents directly threaten their operations, reputation and profitability. The current suite of standards does not create the same level of business incentive.

“It should be... if you don't meet these standards, then children can't use your platform.”

Unlike cybersecurity, the business case for online child safety is often less immediate, particularly where harms are psychological, developmental or societal rather than directly financial. Commercial incentives are often aligned with maximizing engagement rather than maximizing child wellbeing. As a result, companies may view child safety requirements as a cost rather than a commercial necessity. Participants suggested that standards are most effective when they form part of a broader system of incentives, whether that is regulatory compliance or procurement requirements.

This suggests a future role for trust marks or independent assurance schemes that companies can certify against.

The goal should be for standards to help parents and consumers identify products that have been independently assessed as safe, and become a market differentiator, giving companies a commercial reason to comply.

“A company has a massive incentive to use a cybersecurity standard because it defends their data and the integrity of their business. Do they currently have the same incentive to use a safety standard?”



7. Accountability changes behaviour

A significant strand of the discussion focused on accountability. Participants argued that companies are more likely to prioritize safety when responsibility is clearly assigned and there are consequences for failing to act. Others challenged the tendency to place responsibility on parents rather than platforms, arguing that it should not be up to individuals. However, there was also agreement that parental controls are too complex, and simplification should happen as a matter of urgency. Participants strongly supported consistent and interoperable controls.

The discussion explored whether stronger accountability mechanisms could incentivise organizations to invest in child safety earlier in the design process. This included discussion around safety sign-offs, human in the loop and human oversight requirements, product testing, and risk assessments taking place before a digital platform goes live.

The view was that when organizations know they will be held accountable for outcomes, they are more likely to proactively adhere to standards.



Key takeaways

Safe and empowered

We should be working towards a broader vision of digital childhood where safety and empowerment are mutually reinforcing rather than competing goals.

Proof from the outset

Digital services should be expected to prove they are safe for children, just as physical products are expected to meet safety requirements.

Cultural shift

Child-centred safety by design should become a cultural expectation across the technology sector – supported by interventions at every stage to protect children.

Connect the dots

Safety, privacy, security, wellbeing and children's rights should be treated as a connected ecosystem.

Platform responsibility

Parents need support, but responsibility must ultimately sit with platforms and service providers - with the right incentives in place.

Positive vision

We need a shift from harm reduction alone towards defining what a positive digital childhood looks like.

Priority actions for BSI

The implication for BSI is clear: standards can play a role in moving the sector from reactive harm mitigation towards a preventative, safety-by-design, holistic approach in which child safety is treated as a core product requirement rather than an afterthought.

Having the right mix of standards could both prevent harms and play a role in answering questions such as whether the digital product, platform or experience supports informed consent and choice, is easy to disengage from, or at its core is age appropriate and safe.

This means a standards ecosystem which supports safe participation and developmentally appropriate progression that moves children more gently towards digital autonomy.

Standards alone cannot solve the challenge, but they can provide a practical bridge between policy ambition and operational implementation. However, the challenge is not simply developing the right standards, but creating the conditions that make organizations want, or need, to adopt them. This means a role for BSI, in partnership with government, regulators and industry, to create an ecosystem that incentivizes accountability at all stages.

We have identified the following priority actions:



01 Fast-track a chatbot safety standard

Chatbot usage is moving faster than regulation. A fast-track standard could establish minimum expectations around disclosure, safeguarding, escalation to humans, transparency of chatbot personas, risk assessment and testing. This should be developed as an openly available standard to encourage rapid uptake.

02 Launch an AI literacy framework

Develop practical guidance for parents, educators, schools and children that explains what AI is, how to question outputs and how to identify risks. The framework should focus on critical thinking rather than technical literacy.

03 Consider new areas for standardization

Convene platform providers, child safety organizations and policymakers to determine where standardization can play a constructive role, for example around parental controls, manipulative design and dark patterns. This could include a standard to define common principles and terminology for parental controls or standardizing design features that encourage compulsive use and reduce agency.

Any future standard on parental controls should include expectations around human-centred design, accessibility and user testing with children and parents. Providers should be able to show that controls are easy to find, understand and use; and work for families with different needs and levels of digital confidence.

65%

Parents who are concerned that AI toys could replace real friendships or emotional connections

04 Explore establishing a child safety certification programme

Consider a certification or trust-mark model that allows industry to demonstrate compliance with relevant standards, for example around age assurance, privacy or safety-by-design. This could then also give consumers confidence that products have been independently assessed.

05 Build stronger communication around existing standards

Participants felt that existing standards, including for age assurance, are not well understood. BSI should invest in simplified communications, practical toolkits and stakeholder engagement. This could include producing a simple roadmap covering existing standards on privacy, cybersecurity, age assurance, governance, safety and AI. The current ecosystem is difficult to navigate even for experts.

06 Convene around the future of childhood

Bring together policymakers, academics, charities and industry to identify emerging risks around areas such as AI toys, embodied AI, immersive technology and digital companions before harms become entrenched.





Products and services

There are several standards technology organizations can utilize to ensure children remain safe from harms, secure from cyber-attacks and privacy is by design and default.

These standards include but are not limited to:

- [BS EN ISO/IEC 27701:2025](#) Privacy Information Management System Standard
- [BS ISO 31700-1](#) Privacy by Design for consumer goods
- [BS ISO/IEC 27566-1:2025](#) Age Assurance Framework
- [BS ISO/IEC 42005:2025](#) AI System Impact Assessment.

Explore more AI insights [here](#).

Get in touch [online](#).