Department for Science, Innovation, and Technology's Consultation

Growing up in the online world: a national conversation

26 May 2026

The Family Online Safety Institute (FOSI) appreciates the opportunity to submit comments to the Department of Science, Innovation, and Technology regarding the consultation titled "Growing up in the online world: a national conversation".

FOSI is an international, non-profit organization working to make the online world a safer place for children and their families. We achieve this by identifying and promoting best practices, tools, and solutions in the field of online safety. FOSI convenes leaders in industry, government, academia, and the non-profit sectors to collaborate and innovate new solutions and policies that ensure a safer, more rewarding digital experience for all. Through research, resources, events, and special projects, FOSI promotes a culture of responsibility online and encourages a sense of digital citizenship for all.

Online safety policy is complicated, nuanced, and benefits from this type of consultation from expert stakeholders who have valuable information to be shared and considered. FOSI generally does not support sweeping bans of technologies, instead favoring more targeted and proportional restrictions.

Where relevant, this submission references findings from FOSI's 2026 research on teens' online experiences in Australia and the United States. Please note this data has not yet been publicly released, is scheduled to be released on 2 June 2026, and is being shared confidentially until that date for the purposes of informing this consultation.

Chapter 1: Understanding How Children Use Technology

9. What are the benefits of social media use, and being online, for children?

In FOSI's 2024 "Promoting Wellbeing in a Digital World" research report, teenagers and parents from Brazil, the United States, and Germany participated in quantitative surveys and qualitative focus groups to share their perspectives on youth technology use and digital wellbeing. Across all three nations, young people and their parents felt digital access supported their knowledge, creativity, self-expressions, and friendships. Teens also reported having more positive than negative online experiences: nearly 9 in 10 say their digital activity has always or often led to a positive wellbeing effect, with fewer (between 58-75%) reporting negative experiences. "While online safety remains a concern, the perceived positive impact of digital life on teens' social wellbeing is undeniable" (FOSI, 2024, pg.11).

10. What are the harms or risks of social media use, and being online, for children?

In the previously discussed "Promoting Wellbeing in a Digital World" report, the most common negative effects of youth digital use were sleep quality, emotional health, social skills, and motivation. Sleep quality is the only negative effect reported at a higher rate than positive effects from the previous question. Our more recent "Ban Briefing 2.0" (publication forthcoming) found Australian and American parents and young people are most concerned about predatory behavior and cyberbullying.

11. Do you think the benefits of children using social media, and being online, outweigh the risks, or the other way around?

a. Benefits strongly outweigh the risks
b. Benefits somewhat outweigh the risks
c. Benefits and risks are roughly equal
d. Risks somewhat outweigh the benefits
e. Risks strongly outweigh the benefits
f. Don't know / Prefer not to answer

Our research suggests social media is not inherently harmful, nor does it cause emotional harm or distress to all users. The 2024 "Promoting Wellbeing in a Digital World" report shows that while risks certainly exist, teens report more positive online experiences than negative ones. While the most common online safety concern among

both parents and teenagers was the risk for scams and exposure to fraud (28% among both groups), both groups believe online spaces support peer connection (41% of parents, 44% of teenagers). Across all three countries, teens were substantially more likely to report positive negative experiences as a result of spending time online. Both the benefits and the risks of young people online are real and legitimate. Thoughtful regulation, as part of a broader approach including a wide range of stakeholders, can help minimize the risks while maximizing the benefits. For this reason, we believe the benefits of children's digital access outweigh the risks.

Chapter 2: Interventions for safer, more positive experiences

13. To what extent do you agree or disagree with the following statement: "Social media services should have a minimum age of access of at least 16 and should not be accessible to any children under that age"

a. Strongly agree
b. Somewhat agree
c. Neither agree nor disagree
d. Somewhat disagree
e. Strongly disagree
f. Don't know/ Prefer not to answer

FOSI strongly disagrees with age-based social media bans. FOSI's forthcoming "Ban Briefing 2.0" surveyed 1,003 Australian parents and 1,003 Australian children. This report found that Australia's age-based social media "delay" may be largely ineffective in preventing online harm. As of April 2026, 58% of Australian children and parents do not feel the delay has been successfully implemented. Only 19% of Australian children report losing access to all social media accounts. For these reasons, FOSI does not consider social media restrictions for people under 16 a feasible option for online safety and instead prefers a safety-by-design approach that may include targeted risk mitigation as well.

Safety-by-design involves focusing on platform features and design to create safer and healthier environments for young people online. Safety-by-design may include limiting features such as notifications, infinite scroll, and autoplay, as well as stronger privacy and safety settings by default. Additionally, relying on age-based access does not

actually make any platform or service safer for young users. Safety-by-design can instead encourage or require thoughtful default settings, restrictions, and customizable controls to make the actual online experience safer. If effective safety-by-design requirements and practices are in place, it can be appropriate for youth under 16 to access those platforms.

15. What do you think the impacts would be of having a minimum age requirement higher than 13 for social media services? For example, impacts on the safety and wellbeing of children, or the impact for parents and carers, as well as other users. You could also comment on the impact on all users' privacy and data or on business costs, revenue, and innovation.

Raising the minimum age requirement for social media could have several unintended consequences. One concern is that younger users may migrate to lesser-known platforms that offer fewer privacy and safety features, potentially increasing risks rather than reducing them. Restricting access may also reduce opportunities for social connection among younger adolescents, which could place additional strain on mental health and wellbeing services or leave struggling youth more alone and isolated.

Underage users who still access age-restricted social media may experience hesitation to report harm or harassment experienced on the platforms. Our 2025 research revealed that 89% of kids say they feel comfortable turning to their parents if something online makes them feel unsafe. That is a significant and encouraging percentage. If kids experience online harm on platforms they are not supposed to be on, we expect that they would be less likely to turn to their parents and this number would drop dramatically.

The impacts on parents and caregivers would likely depend on how frequently parental permission is required and how age assurance is implemented. In some cases, parents may feel pressured to provide biometric data, such as facial scans, to grant their child access to age-restricted online spaces, potentially creating tension within families. Our data found parents are interested in parental controls and many remove controls earlier than anticipated as they feel their children become mature enough for full access. A nationwide mandate may remove parental feelings of autonomy over their child's best interests.

Additionally, raising the minimum age may create a false sense of security for parents and caregivers, who may feel that their children are safer simply because access to mainstream platforms is delayed. However, increasing the minimum age requirement does not inherently make platforms themselves safer when young people eventually do gain access. FOSI believes that focusing on the development and implementation of safer platform features, stronger privacy protections, and age-appropriate experiences is a more effective long-term approach to improving online safety.

25. Which of these features do you think should be age restricted? (Please select all that apply)

a. Infinite scrolling
b. Autoplay
c. Affirmation features (e.g. likes, comments)
d. Alerts and push notifications
e. Content recommendation algorithms (these are algorithms which provide personalised recommendations on a user's feed)
f. None of the above – they should not be age restricted
g. Don't know / Prefer not to answer
h. Other (please specify)

FOSI recognizes harms associated with amplifying harmful content through content recommendation algorithms. However, it is also important to note that not all personalization is bad. Most online safety tools including customizable blocking, muting, hiding, and following are considered personalization. Therefore, efforts to restrict algorithmic personalization for youth should work to avoid prohibiting useful safety and customization features. Additionally, an often-proposed alternative to "algorithmic" feeds is chronological feeds. But delivering chronological feeds also technically relies on algorithms - another indication to thoughtfully consider how online platforms work to provide any information to users.

34. What are the benefits to children of using AI chatbots? For example, this might include as a search function, for educational purposes, for creativity.

In our 2025 research report "Generative AI in Uncertain Times: How Teens are Navigating a New Digital Frontier," American teen generative AI users list convenience and speed as the top benefits of using the technology. The most common uses for generative AI technology were academic work, search engines, entertainment, jobs/internships, and day-to-day tasks. 42% of teen generative AI users report that they have talked about their feelings with a generative AI chatbot, and an additional 20% share they know someone who has. LGBTQ+ teens are significantly more likely to engage in this behavior. Teens are more likely to engage in this behavior when they feel "talking to a chatbot feels like talking to a human," though 44% of users agreed with the statement "generative AI's behaviors freak me out." In our forthcoming "Ban Briefing 2.0," American and Australian children feel more optimistic about AI than their parents. While children's optimism on AI's role in online safety has increased since 2024, it is declining among parents. Despite these differences, parents and children alike see potential positive impacts for creativity, academics, and media literacy.

35. Which AI chatbot features are most risky for children? (Please select all that apply)

a. The realism of interactions, including realism of content generated
b. The personalisation of interactions
c. How they mimic relationships (friendship)
d. How they mimic relationships (romantic)
e. How they mimic empathy
f. Flattering language
g. Features to encourage more questions/ requests (e.g. asking questions back)
h. The ability to recall interactions across sessions
i. The type of content generated – a) video, b) text, c) audio, d) image
j. Allowing children to have accounts
k. Hallucination or false, misleading responses
l. Ability to engage in and generate mature content (e.g. sexual / romantic roleplay)
m. Other (please specify)
n. None of the above/AI chatbot features are not risky for children

o. Don’t know/ Prefer not to answer

It is hard to answer definitively because what features are most risky depends a lot on the individual child themself. The UK government (specifically the ICO) has done well to recognize that child development is a spectrum and not all children have the same maturity, capabilities, and motivations. We will try to answer this question in a nuanced way with anecdotal examples and as much evidence as we have.

Companion chatbots are AI characters that simulate social and sometimes romantic relationships. For companion chatbots, potential harms include the ability for minors to access these features that promote social and personal relationships. FOSI’s “Ban Briefing 2.0” found that children from higher-income families are more likely to develop an emotional connection with an AI chatbot than those from mid-income or low-income families. These chatbots are not suitable for children and should only be used by older teens with caution.

Chatbots can also function as assistants to licensed professionals, such as doctors, therapists, lawyers, and financial advisors. These can be helpful to bridge gaps in service or provide information quickly, but can also present extremely high risk if the chatbots are not bound by strict guardrails and oversight by the human professional. General use chatbots come in a variety of forms, including ChatGPT, Claude, Gemini, AI voice assistants, smart speakers, and connected devices like toys and e-readers. There are also simple examples such as a chat assistant on an e-commerce website.

Disclosure and transparency are good starting point protections for interacting with AI chatbots. Notifications that the user is interacting with a machine, and not a human, should be baseline requirements. It is a good idea to have either additional notifications and disclosures or full prohibitions of chatbots advising users from the perspective of a licensed expert, such as the medical, financial, or legal fields. Another important piece of this is for companies to provide crisis messages and crisis services information directly to the user who is at risk. Timeliness is important. It makes sense to have serious suicide and self harm incidents be flagged and escalated promptly.

Teens in our "Generative AI in Uncertain Times" report were most concerned about the loss of critical thinking skills (19%), impact on future generations (15%), impact on the arts and creative industries (13%), and mis/disinformation (13%). Girls were significantly more likely to be concerned about the loss of critical thinking skills (25% compared to boys' 13%) while boys were more likely to be concerned with the impact on the job market (16% compared to girls' 9%). LGBTQ+ teens were more likely to be concerned about the impact on arts and creative industries (19% compared to peers' 9%) and privacy/data protections (14% compared to peers' 8%).

36. Which functionalities of AI chatbots should minimum age restrictions apply to?
While FOSI is generally against bans, our findings suggest age-based restrictions on companion chatbots may be appropriate. Chatbots designed to provide professional advice such as legal, financial, and medical advice may also be inappropriate for young users. When discussing sensitive issues, chatbots should implement escalations and interventions as appropriate. This may include sending users to credible sources relevant to the discussed topic such as support hotlines.

Chapter 3: Enforcement and compliance

43. What should be considered when assessing the effectiveness of age verification and age-assurance technologies?
FOSI has foundational principles that guide our approach to age assurance. Per our principles, any age assurance system should meet as many of the following foundational principles as possible:

- Is proportional to the risk, privacy-preserving, secure, interoperable, easy to use, high confidence, and content neutral
- Adheres to local, national and international laws and regulations
- Is mindful of the free expression rights of users (including minors)
- Is effective without being intrusive
- Has considered national and international standards body recommendations
- Is flexible to emerging requirements

We believe that an age assurance solution should be proportional to the risks posed by the service or platform. In practice, this means that for the vast majority of websites, apps, and services that pose minimal risk to users, it is appropriate to use age assurance mechanisms with a lower level of confidence and invasiveness, if at all. For

the minority of online activities that pose a high risk, it would be appropriate to require much greater levels of certainty and enhanced verification.

We believe that everyone has a role to play in making children's online experiences safer and age-appropriate. This includes governments, tech companies, parents, educators, child safety organizations, and the kids themselves. The tech industry has a specific part to play, from credential issuers and credential holders to operating systems, app store operators, apps and websites conducting age assurance and providing age appropriate experiences. Establishing minimum standards is beneficial to building trust across the age assurance ecosystem. These can include data privacy best practices such as collection, use, retention, deletion limitations and practices, as well as thresholds for accuracy and variability between gender, race, and ethnicity.

Age assurance is not an online safety solution in and of itself. Knowing the age or age range of someone is the first step – the real benefit comes from apps and platforms taking that information and providing age appropriate experiences to all users. By knowing the age or age range of their users, apps and platforms can deliver safer online experiences.

47. What do you think the impacts would be if VPNs were age-restricted? For example, impacts on the safety and wellbeing of children, or the impact for parents and carers, as well as other users. You could also comment on the impact on all users' privacy and data or on business costs, revenue, and innovation.
Virtual Private Networks (VPNs) are an important tool used by many internet users for a variety of purposes. These tools can prevent location-based tracking and maintain user privacy. Children should have access to these resources to protect their information online. Age-based restrictions to VPNs would not only disadvantage children but place their data at risk.

However, FOSI recognizes that some VPN services are more trustworthy and secure than others, and that young people's use of VPNs raises legitimate concerns when such tools are used to intentionally bypass online safety features, parental controls, or age-appropriate protections. Policymakers considering restrictions or regulations related to youth VPN use must carefully balance children's rights to privacy, free

expression, and access to information with broader online safety goals. We believe additional research is needed to better understand how young people use these tools, identify child-appropriate and reliable VPN services, and explore approaches that support both safety and digital rights. While there may not yet be a clear consensus solution, these issues warrant thoughtful, evidence-based consideration.

Chapter 4: Preparing children for a digital future

52. Which areas of media or digital literacy do children and families most need additional help with? (Please select all that apply)

a. Managing screen time and online habits
b. Spotting adverts, sponsored posts or AI generated content
c. Keeping personal information private
d. Online behaviour and experiences (bullying, respect, comparison or peer pressure)
e. Checking if information is true
f. Understanding how social media works (for example, 'likes' or algorithms)
g. Staying safe online (including how to have conversations about online safety)
h. Reporting harmful or upsetting content
i. Knowing which apps or sites are right for their age
j. None of the above
k. Don't know/ Prefer not to answer
l. Other (please specify)

Our "Ban Briefing 2.0" found that a majority of parents and children are interested in learning more about online safety, with parents of children 10-13 reporting the highest interest. Children and parents cited cyberbullying as the topic of highest interest as well as expressing interest in social media safety, parental controls, privacy and safeguarding personal information, and AI-generated content. Our 2024 "Promoting Wellbeing in the Digital Age" report found that parents are also interested in how to promote healthier screen time for their children and educate their children about harmful content. Based on our research, we believe all the suggested areas are important for educating families.

54. Where, if anywhere, would you like to see more support available in the future? This could include places you already use but don't offer support and you would like them to, or places that could offer more support with help from government or others. (Please select all that apply)

a. Schools or childcare settings
b. Community or youth spaces (for example libraries, youth clubs or local charities)
c. Parent or carer groups or networks
d. Public services (such as family hubs, GP surgeries or community centres)
e. Faith or cultural groups
f. Non-governmental online sources (such as websites, platforms or online communities)
g. Government websites
h. None of the above/I would not use these to find help
i. Don't know/ Prefer not to answer
j. Other (please specify)

In our "Ban Briefing 2.0," we found that 60% of American parents and 67% of Australian parents use resources to prepare them to teach their children about online safety. Common resources included offline resources, platform-provided safety centers, and FOSI resources. Of those who used resources, 68% of Americans and 66% of Australians felt better prepared to speak to their children about online safety. Australian and American parents felt they had the primary responsibility of teaching their children about online safety, but responses also included teachers, children themselves, technology companies, community leaders, and the government. Liberal-learning Americans were more likely to trust teachers and technology companies than conservative-leaning Americans. American children showed a sizable distrust in community leaders such as the police and religious leaders. These findings emphasize the importance of cultural consideration for designing online safety education programs.

55. Outside of schools, how could the UK government better support children and young people to stay safe and feel supported online? (Please select all that apply)

a. By providing clear guidance that children can use on their own
b. By supporting parents and carers to support children online

c. By working with online platforms and services that children already use
d. By supporting youth organisations and community groups to help children online
e. By making help or advice easy to access when something goes wrong online
f. By involving children and young people in designing support
g. None of the above
h. Don't know/ Prefer not to answer

FOSI's research from the 2026 "Ban Briefing 2.0" found that parents prefer short videos, reading materials (i.e. blog posts, articles), presentations at schools, and hands-on activities. Children also liked short videos, presentations at schools, and hands-on activities, but also liked learning from influencers. FOSI also recommends a public awareness campaign and increased visibility on parental controls.

Chapter 5: Supporting families

60. To what extent do you agree or disagree with the following statement: "Parents should have control over the online experiences of their children"

a. Strongly agree
b. Somewhat agree
c. Neither agree nor disagree
d. Somewhat disagree
e. Strongly disagree
f. Don't know/ Prefer not to answer
Please explain the reasoning behind your answer.

While FOSI strives to empower families to engage with technology in a meaningful way and openly discuss online safety with their children, a child's right to privacy must be considered. Parental controls must be privacy preserving for children and not become surveillance controls. High level information and settings such as total time spent, time spent per app, purchase restrictions, and communication restrictions are more appropriate than full access to all searches, messages, and more private information. One such initiative is the Family Smart Start project, on which we have collaborated with South West Grid for Learning.

61. How should this level of control change for children of different ages? For example, a 16-year-old and an 11-year-old.

The use of parental controls can be unique to each family and child. While a majority of American and Australian parents consider 14-17 to be the ideal age range to remove parental controls, in practice, a majority removed controls between ages 10-13. The most common reason for parents in both countries was feeling the child was mature enough to navigate the platform without controls. Among families, maturity is a key factor in determining how children experience parental controls. This should be considered when approaching the differing needs of an 11 year old compared to a 16 year old.

62. What would help parents and carers to more effectively use parental controls? For example, more information on how to do this on purchase of a phone, help from platforms on how to set up, or greater standardisation across tools.

In our "Ban Briefing 2.0" parents reported highest interest in learning about cyberbullying, parental controls, social media safety, and privacy/safeguarding personal information. Another way to reach parents and carers directly is through the joint Family Smart Start project with SWGfL.

FOSI appreciates the opportunity to contribute to this important national conversation. The issues surrounding children's online experiences are complex and require thoughtful, evidence-based policymaking. We believe solutions should carefully balance safety, privacy, access to information, and children's digital rights. While there is no simple solution, we believe policies should prioritize meaningful safety-by-design measures and continued collaboration among policymakers, industry, researchers, parents, and young people.

FOSI does not believe age-based bans on social media access are a feasible solution to children's digital safety. Based on our data, these policies appear to be ineffective in

preventing young people from accessing platforms and insufficiently address targeted harms related to harmful content and social media misuse. Similarly, FOSI believes age assurance is a powerful tool for confirming age, but is not a solution alone. In place of age-based restrictions, FOSI advocates for safety-by-design measures that focus on platform features to create safer and healthier digital environments. Safety-by-design may include limiting features such as notifications, infinite scroll, and autoplay as well as stronger privacy and safety settings by default. These features could be related to the age of the user to ensure an age-appropriate experience. Safety-by-design can encourage or require thoughtful default settings, restrictions, and customizable controls to make the actual online experience safer.

Children and parents consistently express a desire for clearer, more accessible information about digital wellbeing and the tools available to support safer online experiences. In our research, families are most interested in learning about parental controls, cyberbullying, privacy safeguarding, managing screentime, and AI-generated content. Public awareness campaigns can play an important role in helping families better understand online risks, platform features, reporting mechanisms, and age-appropriate digital practices.

However, to be effective, these efforts should be delivered through a variety of channels and formats to ensure they reach diverse audiences. Parents prefer short videos, reading materials (i.e. blog posts, articles), presentations at schools, and hands-on activities. Children also liked short videos, presentations at schools, and hands-on activities, but also liked learning from influencers. Educational resources should also be designed to be accessible to both children and caregivers, recognizing that families engage with technology in very different ways.

FOSI appreciates DSIT's thoughtful approach to online safety regulation and the opportunity to contribute to this consultation. If any questions or concerns arise, please do not hesitate to contact us.