BILETA Response to Department for Science, Innovation and Technology National Consultation: Growing Up in the Online World

This response is led by the British and Irish Law, Education and Technology Association (BILETA). Formed in April 1986, BILETA aims to promote, develop, and disseminate high-quality research and knowledge on technology law and policy to organizations, governments, professionals, students, and the public. BILETA also encourages the use of and research into technology at all stages of education. This response was prepared, approved, and funded by BILETA, with contributions from Professor Kim Barker, Professor Subhajit Basu, Senior Lecturer Michaela McDonald, Miss Karolin Rippich and Associate Professor Felipe Romero-Moreno.

Chapter 1: Understanding how children use technology

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

Children's use of social media and digital environments more broadly should not only be understood through a risk-based lens. While online harms are real and require proportionate regulatory responses, the evidence also shows that being online can support children's development, learning, participation, identity formation, relationships, creativity and access to rights. These benefits are particularly significant for children who are marginalised, minoritised, geographically isolated, disabled, LGBTQIA+, or otherwise underserved by offline institutions and services. A useful starting point in this regard is the "ladder of participation", which shows that children's online engagement can develop progressively.[1] At the most basic level, children may use digital media for entertainment and content consumption. As their digital skills

[1] Lucía Magis-Weinberg et al., 'Global Perspectives on Youth and the Digital Environment: Learnings from Majority World Countries', in *Handbook of Children and Screens: Digital Media, Development, and Well-Being from Birth Through Adolescence*, ed. Dimitri A. Christakis and Lauren Hale (Springer Nature Switzerland, 2025), https://doi.org/10.1007/978-3-031-69362-5_69.

increase, they often move towards online sociability through messaging, social media and other forms of peer interaction. With further skills and support, online engagement can also involve education, information-seeking, creativity, civic participation and community action.[2] This is important because the value of being online does not lie in access itself, but in children's ability to participate meaningfully and safely in a range of digital practices. Digital exclusion, poor connectivity, low digital literacy or overly restrictive access measures can prevent children from reaching the higher levels of participation that are most closely associated with social, educational and civic benefit.[3]

One central benefit of social media and online access is educational. Digital platforms can support children's right to education by providing access to formal and informal learning resources, specialist information, peer learning and educational content that may not otherwise be available locally. This was particularly visible during the pandemic but is not limited to emergency contexts.[4] For many children, online environments provide access to information about health, current affairs, culture, rights, employment pathways and training opportunities. Where children are supported to develop the digital literacies needed to assess, interpret and use this information well, online access contributes to educational development and longer-term socio-economic opportunity.[5]

Digital environments also support children's creativity, play and imagination.[6] Online spaces can provide children with opportunities to create, remix, publish, perform, collaborate and experiment with different forms of expression.[7] This includes everyday creative practices, such as making videos, sharing art, gaming, storytelling and participating in fan or interest-based communities, as well as more explicit civic forms of creativity such as youth activism.[8] These opportunities matter because creativity and play are not peripheral to children's development. Rather, they are part of children's rights and are closely connected to confidence, identity development, communication skills and social participation. Social media, in particular, can provide meaningful opportunities for civic and political participation. Online civic participation allows children and young people to access information about social and political issues, express their views, organise around injustice and connect with others who

[2] Magis-Weinberg et al., 'Global Perspectives on Youth and the Digital Environment'.
[3] Magis-Weinberg et al., 'Global Perspectives on Youth and the Digital Environment'.
[4] Kathryn Macapagal et al., 'Online Sexual Communication and Partner Seeking Among Adolescents', in *Handbook of Children and Screens: Digital Media, Development, and Well-Being from Birth Through Adolescence*, ed. Dimitri A. Christakis and Lauren Hale (Springer Nature Switzerland, 2025), https://doi.org/10.1007/978-3-031-69362-5_49.
[5] Ellen Middaugh et al., 'Youth Participatory Politics: Understanding and Supporting Civic Engagement in the Social Media Era', in *Handbook of Children and Screens: Digital Media, Development, and Well-Being from Birth Through Adolescence*, ed. Dimitri A. Christakis and Lauren Hale (Springer Nature Switzerland, 2025), https://doi.org/10.1007/978-3-031-69362-5_35.
[6] Didem Özkul et al., *Best Interests of the Child in Relation to the Digital Environment*, Working Paper (UNICEF Innocenti – Global office of Research and Foresight, 2025).
[7] Sonia Livingstone, 'Children's Rights in the Digital Age', in *The Routledge Companion to Media and Human Rights* (Routledge, 2017).
[8] Middaugh et al., 'Youth Participatory Politics'.

share their concerns. Social media can give children rapid access to emerging news and sociopolitical education and can help them develop critical consciousness, i.e. an understanding of structural inequalities, their own position within those systems and the agency o act collectively.[9] These forms of participation can build practical civic competencies, including perspective-taking, persuasive communication, narrative-based expression and dissemination of information.[10] This is particularly important for marginalised children and young people. Online spaces can enable children to challenge harmful stereotypes, develop positive narratives about their identities and create counternarratives that are not always available or recognised in mainstream offline settings.[11] For example, migrant youth, LGBTQIA+ and racialised youth have used digital spaces to share lived experiences, counter discriminatory narratives, build solidarity and mobilise for community change.[12] These practices should be understood as forms of civic identity formation, social support, political education and collective participation.

In this sense, social media and online environments more broadly also support peer connection, belonging end emotional support. Children use digital spaces to maintain friendships, find communities of interest, collaborate, share advice and access support networks. These forms of relational connection may be especially valuable for children who experience exclusion, stigma or isolation offline. For some children, online communities provide affirming spaces in which they can explore identity, receive recognition and develop a sense of belonging. Such networks can also operate as important information channels, helping children find support groups, advice, resources and services that otherwise remain inaccessible. Again, these benefits are especially evident for LGBTQIA+ children and young people.[13] Digital spaces can allow them to access relevant information about sexuality, sexual health and relationships, explore their identity, communicate with peers and form meaningful connections at a safer distance.[14] This can be important where schools, families or local communities do not provide inclusive sexual health education or safe environments for identity exploration.[15] Online spaces can offer privacy, anonymity and control over self-presentation, which may reduce stigma or immediate exposure to discrimination.[16] More broadly, social media can also provide content that reflects children's own cultures, languages, identities and heritage, that may be underrepresented in mainstream media or local institutions.[17]

[9] Middaugh et al., 'Youth Participatory Politics'.
[10] Middaugh et al., 'Youth Participatory Politics'.
[11] Middaugh et al., 'Youth Participatory Politics'.
[12] Middaugh et al., 'Youth Participatory Politics' & Marisa Lyons Longworth, 'The Digital Lives of LGBTQIA+ Children', *Media@LSE*, 13 August 2025, https://blogs.lse.ac.uk/medialse/2025/08/13/global-stories-of-lgbtqia-children-and-their-digital-use/.
[13] Lyons Longworth, 'The Digital Lives of LGBTQIA+ Children'.
[14] Macapagal et al., 'Online Sexual Communication and Partner Seeking Among Adolescents'.
[15] Macapagal et al., 'Online Sexual Communication and Partner Seeking Among Adolescents'.
[16] Macapagal et al., 'Online Sexual Communication and Partner Seeking Among Adolescents'.
[17] Livingstone, 'Children's Rights in the Digital Age'.

For these – and many more – benefits to be realised, children need more than access to devices or platform. They need age- and developmentally appropriate digital environments, meaningful digital literacy education, privacy protections, inclusive design and opportunities to participate in shaping both government and platform policies that affect them. Thus, as Bagirzade (2025, 10) suggests, "[p]olicymakers are advised to consider not only the measurable risks but also the opportunities in order to make the digital environment safe and beneficial for children".[18]

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

As Gelman et al. (2025) note, digital technologies bring "not only benefits but also risks".[19] This is particularly true considering that children often use services that are not targeted at them, or where providers are unaware of, or insufficiently attentive to, their status as minors.[20] Moreover, neither social media nor the internet were originally designed with children (and their rights) in mind.[21] As a result, children may be exposed to environments that are poorly adapted to their developmental needs, lack child-friendly safeguards and provide limited mechanisms for redress when harm occurs.[22]

A useful way of thinking of possible risks is through the 4Cs framework developed by Livingstone & Stoilova (2021), which distinguishes between Content, Contact, Conduct and Commercial risks. Content risks arise when children are exposed to harmful, age-inappropriate or distressing content. This includes pornography, violent content, hate speech, self-harm-related content, extremist content and misinformation or disinformation. Contact risks concern interactions with others online, particularly where adults or unknown users exploit children's openness, trust or limited ability to assess risk. These include unwanted contact from strangers, grooming, sexual exploitation, and abuse, catfishing and coercive sexual communication. Livingstone (2017) notes that online sexual risks are especially concerning because longstanding offline harms, such as grooming, may be intensified by the affordances of digital environments, including anonymity, convenience, constant connection and the ease with which images and personal information can be shared or misused.[23] Conduct risks arise from children's own interactions with peers and others online. These include cyberbullying, harassment, hate speech, exclusion, peer aggression and the non-consensual sharing of intimate images. These can have serious consequences for

[18] Nihat Bagirzade, 'Children's Legal Protection on Social Networks: Legal Gaps and the Need for New Regulations', SSRN Scholarly Paper no. 5362378 (Social Science Research Network, 24 May 2025), https://doi.org/10.2139/ssrn.5362378.
[19] Susan A. Gelman et al., 'Children's Understanding of Digital Tracking and Digital Privacy', in *Handbook of Children and Screens: Digital Media, Development, and Well-Being from Birth Through Adolescence*, ed. Dimitri A. Christakis and Lauren Hale (Springer Nature Switzerland, 2025), https://doi.org/10.1007/978-3-031-69362-5_87: 1.
[20] Özkul et al., *Best Interests of the Child in Relation to the Digital Environment*.
[21] Özkul et al., *Best Interests of the Child in Relation to the Digital Environment*.
[22] Özkul et al., *Best Interests of the Child in Relation to the Digital Environment*.
[23] Livingstone, 'Children's Rights in the Digital Age', 107.

children's mental health, social relationships, reputation and sense of safety and are, unfortunately, difficult to address as online abuse can follow children across platforms and into private/offline spaces.[24] A particularly serious form of conduct and contact risk is technology-facilitated sexual abuse and cyberdating violence among young adolescents. Online relationships may provide opportunities for intimacy and identity exploration, but they can at the same time involve deception, coercion, surveillance and abuse. More specifically, such abuse may involve cyber psychological aggression, monitoring a partner's online activity, GPS tracking, sextortion, grooming, image-based sexual abuse, cyberflashing and exclusion from online spaces. Similar to some forms of offline abuse, these harms are associated with poor mental health outcomes, including depression, anxiety and suicidal thoughts.[25]

Importantly, research has shown that risks are not distributed equally. Online environments can amplify existing inequalities, meaning that children who are already marginalised may face heightened exposure to harm. Girls, Black girls, LGBTQIA+ children, transgender and non-binary adolescents, Muslim youth and other minoritised groups may experience harassment shaped by racism, sexism, homophobia, transphobia, religious discrimination or intersecting forms of stigma. For example, Black adolescent girls may have to navigate both sexualised and racist stereotypes in online dating contexts, while transgender and non-binary adolescents may fear hostile or violent reactions to disclosure of their gender identity.[26]

Platform design can further intensify harm. Features such as autoplay, recommender systems, engagement-based ranking, notifications and algorithmic personalisation are designed t maximise attention and time spent online. For children, these design choices may reduce autonomy and self-regulation, contribute to excessive use, interfere with sleep and education and expose the to narrow, repetitive or harmful content. Such features together with the fact that digital environments are highly commercialised – meaning children's data may be collected, tracked, profiled, monetised and in some cases sold without meaningful consent, require closer scrutiny of the way platforms are built.[27]

This is especially true considering that young people increasingly use social media to express political views and participate in public debate, meaning they may not only encounter hate speech, harassment, surveillance, censorship or self-censorship, but might also end up in echo chambers and filter bubbles that pipeline them towards extremist platforms. More generally, youth activists are increasingly concerned about being monitored by adults, schools, employers, governments or law enforcement agencies. At the same time, misinformation, disinformation, generative AI and deepfakes make it harder for young people to assess credibility, context and source

[24] Magis-Weinberg et al., 'Global Perspectives on Youth and the Digital Environment'.
[25] Macapagal et al., 'Online Sexual Communication and Partner Seeking Among Adolescents'.
[26] Middaugh et al., 'Youth Participatory Politics'.
[27] Valerie Verdoodt et al., 'The EU Approach to Safeguard Children's Rights on Video-Sharing Platforms: Jigsaw or Maze?', *Media and Communication* 11, no. 4 (2023): 151–63, https://doi.org/10.17645/mac.v11i4.7059.

reliability. Although many young people report fact-checking behaviours and preferences for evidence-based posts, they may still struggle to evaluate information when news is fragmented, decontextualised or circulated through social media only.[28]

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

Social media use and being online can expose children to a range of risks; however, these should not be understood in isolation from possible opportunities, children's rights and agency. A children's rights-based approach requires recognising that the digital environment, including social media, can be both beneficial and harmful. As Livingstone (2017) observes, "[o]nline activities can be particularly ambiguous in terms of whether they turn out to be opportunities or risk" and "[a]dults do not always see eye to eye with children about what counts as a risk or an opportunity online".[29] This means two things:

> First, that the harms of social media cannot be addressed adequately without engaging directly with children and taking their experiences seriously. Crucially, children's own accounts suggest that they want to engage online without fear but are concerned that speaking out may expose them to discrimination or safety risks.[30]
>
> Second, harm arises where adults, including parents, caregivers, policymakers or institutions, dismiss or denigrate children's online expression and experiences. The risk here is the marginalisation of children's voices in decisions about the digital environment.
>
> Jointly this means that if children are excluded from the design, development and evaluation of online safety measures, those measures fail to reflect their lived experiences and may be less effective in practice.[31]

In addition to a children's rights-based approach, a multidimensional and intersectional approach is needed because children's experiences online are shaped by various factors such as gender, class, ethnicity, family context, school environment and whether they live in urban or rural areas. The same platform or online activity may create different risks and opportunities for different children. Some children may be more vulnerable to harassment, exclusion, surveillance, discrimination or exploitation because of their identity, social position or offline circumstances. This means that general claims about "children" and social media risk overlooking which children are

[28] Middaugh et al., 'Youth Participatory Politics'.
[29] Livingstone, 'Children's Rights in the Digital Age', 108.
[30] Sonia Livingstone et al., 'Children vs Adults: Negotiating UNCRC General Comment No. 25 on Children's Rights in the Digital Environment', in *Handbook of Media and Communication Governance*, ed. Manuel Puppis et al. (Edward Elgar Publishing, 2024), https://doi.org/10.4337/9781800887206.00042.
[31] Livingstone et al., 'Children vs Adults'.

most affected, in what ways and under what conditions.[32] Another risk is that policy responses may assume harm rather than assess it. Debates about screen time illustrate this problem. Treating all screen time as inherently harmful overlooks the different ways children use digital technologies. A more appropriate approach would consider quality, context and purpose of children's online interactions, as well as the child's age, maturity, circumstances and support structures.[33] On this note, there is a risk that protective measures themselves may become harmful if they are disproportionate. The United Nation's Convention on the Rights of the Child requires a balance between children's rights to protection and their rights to participation and provision. Measures to keep children safe may undermine those rights if they unnecessarily exclude children from digital spaces or restrict access to beneficial online resources.[34]

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

Should the listed features be age-restricted?

- Yes.
- Livestreaming, stranger messaging, location sharing, disappearing messages, and the sharing of explicit imagery should be age-restricted for children.

What minimum ages should apply to these features?

- We support a tiered approach.
- Livestreaming: 16+
  Stranger messaging/random chat: 16+
  Location sharing: 16+
  Disappearing messages: 16+
  Sending or receiving explicit images: 18+

Do you agree that restricting these features would make children safer?

- Partially agree.

[32] Magis-Weinberg et al., 'Global Perspectives on Youth and the Digital Environment'.
[33] Özkul et al., *Best Interests of the Child in Relation to the Digital Environment*.
[34] Özkul et al., *Best Interests of the Child in Relation to the Digital Environment*.

- Restricting high-risk features would reduce exposure to grooming, coercion, exploitation, and compulsive use. However, restrictions should remain proportionate.

What impacts would mandatory age restrictions have?

- Mandatory restrictions would improve child safety overall, but they would also create significant operational, technical, and privacy challenges.

- Positive impacts include:
  • Reduced exposure to harmful content and predatory behaviour
  • Better protection of children's privacy
  • Reduced compulsive or excessive use
  • Clearer expectations for platforms
  • Better support for parents
- Potential downsides include:
  • Increased compliance costs for businesses
  • More extensive age-verification systems and associated privacy concerns
  • Greater incentive for circumvention
- Requirements should focus on genuinely high-risk functions rather than blanket restrictions.

Which features are especially persuasive or addictive for children?

- All of the listed features can be highly persuasive to children.
- In particular:
  • Infinite scroll
  • Autoplay
  • Algorithmic recommendation feeds
  • Push notifications
  • Likes and social feedback systems

Which persuasive features should be age-restricted?

- We support restrictions or default limitations on all of these features for younger users.
- For example:
  • Infinite scroll and autoplay should be disabled by default for children.
  • Push notifications should be limited, particularly overnight.
  • Recommendation feeds for children should prioritise chronological or safety-filtered content.

What ages should apply to persuasive features?

- A reasonable threshold for most persuasive features is around 16.
- Under-16 accounts should receive stronger protections by default, including:
  • No autoplay
  • No infinite scroll
  • Reduced notifications
  • Safer recommendation systems

Do you support screen-time limits and overnight restrictions?

- Yes.

What do you think the impacts would be if online platforms were required to restrict specific features or functionalities, or to introduce time limits? 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.

Requiring platforms to restrict specific features or introduce time limits could have positive impacts on children's safety and wellbeing, provided the measures are granular, proportionate and supported by clear guidance for families. The video games industry shows that this is technically and socially feasible, without relying only on blunt age bans. Major games platforms already provide parental controls for blocking content by age rating, limiting time spent, controlling purchases, and restricting communication features[35]. This sits alongside PEGI[36], which is used in 41 countries and provides age categories and content descriptors for parents and carers. A combination of well-designed self-regulation, parental controls and responsible use by families are at their most effective when implemented correctly.

This shows that feature restrictions can improve children's safety and wellbeing when they are granular, transparent and supported by education. For example, Nintendo allows parents to set daily play-time limits and suspend software when limits are reached; Xbox Family Settings allows parents to manage screen time, privacy, social interactions and mature content; and PlayStation provides controls for playtime, spending, messaging and content access. These tools also address the risks identified by the European Commission report[37], including harmful communication, commercial influence, inappropriate content, grooming and excessive play. The lesson for wider online platforms is that restrictions should be designed as layered safety systems: default protections for younger users, adjustable controls for families, clear child-facing explanations, and accessible guidance from trusted sources such as PEGI, the Games Rating Authority and platform safety hubs.

What factors are important when determining which apps, sites or services to apply minimum age of access restrictions to? For example, user-to-user interaction, the ability to post material, persuasive design features, risky functionalities, the ability to generate non-text mediums such as video or images, the target age group, the size of the service.

The guiding principle should be that minimum-age rules are feature-specific and risk-based, not sector-wide.

[35] 3.2.3 of *Understanding the value of a European Video Games Society* (European Commission, 2023) https://op.europa.eu/en/publication-detail/-/publication/075b8bbe-6bd5-11ee-9220-01aa75ed71a1
[36] PEGI (Pan European Game Information); https://pegi.info/
[37] See n. 1.

The European Commission report on the video games sector makes this distinction clear: even where a game has an appropriate age rating, risks can arise from specific connected features such as chat functions, user-generated content, communication tools, or adjacent social networks. It also notes that many games mitigate these risks through parental controls, age-rating systems, disabled interactive features without parental consent, automated detection of harmful language, muting / blocking, reporting tools and moderation[38].

A game with no open chat, no user-generated content, no spending, no algorithmic feed and strong parental controls should not be treated the same as a platform built around public posting, direct messaging, viral sharing and algorithmic recommendation.

Are there any types of apps, sites or services that you would want to be captured by minimum age of access restrictions?

I would support minimum-age restrictions for services or features that create increased risks through open communication, algorithmic amplification, persuasive design or exposure to harmful content, but I do not believe broad platform bans are the most effective approach.

From my own experience as a parent of two teenage boys who have grown up online, I have found that some services, such as WhatsApp, can be really useful and shape communication, coordination and maintaining friendships and family connections in a positive way. However, certain functionalities within those services – for example large, unmanaged group chats, open discovery features or contact from unknown users – may require stronger safeguards, moderation tools or adult oversight for younger users.

More broadly, many of the features now associated with concerns around children's wellbeing are not only harmful to children, but harmful to users generally: infinite scrolling, compulsive engagement loops, manipulative nudges, opaque recommendation systems and the amplification of toxic or extreme content. The focus should therefore not simply be on banning children from platforms, but on designing healthier digital environments overall. In my view, if a platform would be uncomfortable publicly explaining or defending a feature because it appears manipulative, exploitative or psychologically harmful, then that feature should be reconsidered for all users, not only children (the so-called creep test).

What factors are important when determining which apps, sites or services to apply age-restrictions on specific features and functionalities? For example, user-to-user interaction, the ability to post material, persuasive design features,

[38] Ibid.

risky functionalities, the ability to generate non-text mediums such as video or images, the target age group, the size of the service.

For age restrictions on specific features and functionalities, the key factor should be the risk created by the feature itself, not the broad category of app, site or service. This is where the video games sector provides a useful model: games are not regulated only at the level of “access to the game”, but also through age ratings, parental controls, spending limits, communication restrictions, reporting tools and settings that can disable or manage interactive features. Risks to children and young adults often arise from connected functionalities such as chat, user-generated content, commercial features and online interaction, rather than from play itself. This distinction matters because a video game may be social without being social media, and social media may be gamified without being a game.

The most important factors should therefore include open user-to-user interaction, contact with unknown adults, private messaging, livestreaming, posting or sharing user-generated content, algorithmic recommendation, in-app purchases, loot-box style mechanics, compulsive design features, and the ability to create or circulate images, audio or video. These features should attract stronger age-appropriate controls, default protections, parental settings, transparency duties and effective reporting/moderation systems. A risk-based approach would avoid overbroad restrictions while still targeting the features most likely to create harm.

Further reading / resources:

https://www.videogameseurope.eu/responsible-gameplay/

https://www.videogameseurope.eu/parental-controls/

https://ukie.org.uk/consultation-responses/ukie-responds-to-ofcom-consultation-on-user-controls-under-the-online-safety-act

https://ukie.org.uk/news/ofcoms-childrens-risk-assessment

Ukie response to Ofcom’s children’s risk assessment

29. Should AI chatbots have minimum age restrictions?

a. Yes – minimum age requirements for AI chatbots

b. Yes – restrict access to certain features and functionalities

c. Yes – both minimum age requirements and restricting access to certain features and functionalities

d. No

e. Don’t know/ Prefer not to answer

Please explain the reasoning behind your answer

I would support both minimum-age requirements and age-based restrictions on specific features and functionalities. Very young children interacting heavily with AI chatbots, without parental supervision, especially where the system is conversational, personalised, emotionally responsive or capable of generating persuasive or inappropriate content, is concerning. However, I am not sure that a single blanket age threshold is sufficient, because risks vary significantly depending on the design of the chatbot and the context. A general-purpose chatbot used for homework support is different from an AI companion, an image-generation tool, a chatbot that simulates intimacy, or a system that gives advice on health, wellbeing or relationships. The better approach would be a minimum age floor, combined with stricter controls on higher-risk features: emotional companionship, private one-to-one conversations, image / video generation, memory / personalisation, profiling, commercial nudges and advice on sensitive topics.

Many major AI chatbot services use 13+ with parental consent for under-18s; for example, OpenAI says ChatGPT is not for children under 13 and that users aged 13-18 need parent or guardian permission. In the EU, lawmakers are pushing for a stricter model: no access under 13, parental consent from 13-16, and 16+ as the default minimum age for social media, video-sharing sites and AI chatbots. In China, the law requires providers to identify appropriate user groups and uses, guide responsible use, and take effective measures to prevent minors becoming over-reliant on or addicted to generative AI services, including identity / age checks, time limits, spending controls, platform duties and anti-addiction design obligations.

What do you think the impact would be of introducing age restrictions on AI chatbots or certain features and functions? 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.

Introducing age restrictions on AI chatbots, especially on higher-risk features, could improve children's safety and wellbeing by reducing very young children's exposure to systems that are persuasive, emotionally responsive, personalised, or capable of producing inappropriate advice or content. I would be particularly concerned about young children forming dependent relationships with AI companions, disclosing sensitive personal information, receiving misleading guidance, or engaging with systems that simulate intimacy, authority or friendship. Restrictions could therefore be useful where chatbots provide emotional companionship, advice on sensitive topics, image / video generation, memory and profiling, or private one-to-one interaction without meaningful oversight.

However, the impact will depend heavily on implementation. A blanket ban could be difficult for parents to manage and could restrict beneficial uses of AI, such as supported learning, accessibility, creativity and language practice. A better approach

would be age-appropriate design: minimum-age floors for general access, stricter controls for high-risk functions, child-safe versions of AI tools, clear parental settings, strong transparency requirements, and limits on data collection and profiling. This would create costs for businesses, but these are reasonable where services are being offered to children. It could also support innovation by encouraging safer, more trustworthy AI products rather than systems designed primarily around engagement, dependency or data extraction.

I think the hard truth is that parents need to be doing much more, and responsibility for children's wellbeing cannot simply be outsourced to platforms, schools or governments. At the same time, parents also need to be informed, empowered and properly equipped to fulfil that role effectively. This requires clear and robust regulatory frameworks that place meaningful responsibilities on technology companies to design safer systems by default, provide understandable tools and controls, and avoid features that are intentionally manipulative, addictive or exploitative. The goal should not be to replace parental responsibility, but to create digital environments where parents are realistically able to exercise it.

To what extent do you agree with this statement: "Adults should complete age checks more often, if it means children are safer online"?

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

In favour of proportionate, feature-based, risk-based regulation and strong emphasis on parental responsibility plus safer design, rather than heavy-handed surveillance or universal identity checks.

What should be considered to make minimum age restrictions effective and workable? This could mean either age restrictions for access to whole services, or for specific risky or 'addictive' features or functionalities.

Minimum age restrictions will only be effective and workable if they are proportionate, privacy-preserving, and targeted at the highest-risk features, rather than imposed as blunt access bans across whole categories of services. The video games sector shows both the value and limits of age assurance. Age verification in games is still often based on self-declaration, sometimes cross-checked through app stores or digital distribution platforms, but the industry has raised concerns about the limited availability of trusted ID verification tools and the additional privacy risks they may create. For this reason, the combination of parental controls, age ratings, privacy tools, spending controls, time limits, communication restrictions, reporting systems and media education campaigns are often preferred as complementary or alternative safeguards[39].

China provides a much stricter comparison. In online games, China uses real-name registration and age verification, with minors limited to one hour of play between 8-9pm on Fridays, weekends and public holidays[40]. This shows that age verification can be made technically enforceable, but it also illustrates the trade-off: effective enforcement may require much more intrusive identity checking and state / platform monitoring. The UK should be cautious about adopting age verification as the default answer to every online safety concern. Age checks should be used where the risk justifies them, but they should be designed to minimise data collection, avoid creating new privacy harms, and sit alongside safer design duties, parental tools, transparency, education and strong enforcement against harmful platform features.

What do you think the impacts might be from requiring age assurance across a greater number of online platforms? 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.

Age assurance also has practical limits. At present, there is no universally reliable, privacy-preserving and low-friction technology that can confidently distinguish between closely grouped ages, such as whether a young person is 14, 15 or 16. The more precise the age check needs to be, the more likely it is to rely on intrusive identity documents, biometric estimation, third-party verification, or additional data processing. This creates a difficult trade-off: stronger enforcement may improve child protection in some contexts, but it may also increase privacy risks for both children and adults.

It could also increase business costs and make compliance harder for smaller companies, while large platforms may absorb the costs more easily.

[39] Ibid.

[40] 'Stricter limits on minors' online gaming' (The State Council of the PRC, August 31, 2021) https://english.www.gov.cn/statecouncil/ministries/202108/31/content_WS612da2a2c6d0df57f98df6bd.html

Chapter 3: Effective compliance and enforcement of online safety rules

Enforcement is too often treated within technology regulation as a technical problem awaiting a technical solution. It is not. Age assurance, anti-circumvention systems, restrictions on privacy-enhancing technologies, and mandatory schooling rules are forms of regulation by design. They do not simply implement substantive rules; they reorganise the conditions under which access, identity and lawful conduct become possible in the digital environment. The objective of protecting children online is unquestionable. What is genuinely in question is the architecture chosen to pursue that objective. A regulatory system that protects children by normalising routine identity presentation across the open internet, by conditioning lawful adult access on biometric assurance, or by treating privacy-enhancing technologies themselves as suspect, would secure one set of values at the price of others. The values displaced — legality, proportionality, transparency, privacy, fairness, dignity, equality of access, and the rule of law itself — are the conditions of its legitimacy. The architecture that follows from these commitments is risk-tiered, design-targeted and rights-respecting. The primary regulatory burden should sit on platforms, because platforms design the systems, control the interfaces, hold the data, capture the engagement and reap the commercial rewards. Children, parents and schools are not the appropriate locus of enforcement responsibility for failures embedded in commercial digital architectures. Where age assurance is required, it should be required in the contexts where the risk justifies it, calibrated to the severity of that risk, and constrained by independent audit and meaningful redress. Where privacy-enhancing technologies are at stake, the default should be protective, not suspicious. The state's role is to insist on platform duties of design, not to recruit families to enforce those duties.

To what extent do you agree with this statement: “Adults should complete age checks more often, if it means children are safer online”?

Answer: Somewhat agree.

The question conceals a category mistake. "More often" can mean two very different things. It can mean more rigorous age assurance in contexts where the risks to children are serious, foreseeable and disproportionately tied to age — pornography, content promoting suicide, self-harm or eating disorders, sexualised contact functionalities, and other high-risk environments. In those contexts, more demanding age assurance is justifiable and necessary, and the design-based intervention should be expected to do real protective work; to that proposition, we agree.

But "more often" can also mean the routinisation of age and identity checks across ordinary digital activity — the conditioning of access to lawful information, services and communication on repeated identity presentations. To that proposition, we do not agree and would not agree even if a measurable safety benefit could be demonstrated. The reason is not that child safety lacks weight. It is that the architecture under consideration carries consequences that the question does not surface. Generalised age assurance reshapes the relationship between citizen and digital infrastructure. It accustoms users — adults and children alike — to identifying themselves as a precondition of lawful access. It builds a substrate that other public and commercial

interests can draw upon later. And it does so in a way that bypasses the deliberative and constitutional checks that more visible forms of identification have historically had to satisfy.

The answer is therefore conditional. Adults should be subject to age assurance when the risk to children is serious enough to justify the intrusion, when less intrusive alternatives have been shown inadequate, and when the design of the assurance system itself meets independent standards of privacy, accuracy, fairness, and redress. They should not be subjected to age assurance as a default condition of digital participation. The strength of the case for age assurance varies directly with the seriousness of the risk; the weight of the case against intrusive assurance varies directly with the ordinariness of the activity in question. Any policy that loses sight of that gradient is not proportionate.

What should be considered to make minimum age restrictions effective and workable? This could mean either age restrictions for access to whole services, or for specific risky or 'addictive' features or functionalities.

Minimum age restrictions are not self-executing rules. They are design-based regulatory instruments whose practical operation depends on the architecture chosen to implement them, the parties on whom the burden falls, the assumptions about family and household life that the architecture quietly imports, and the redress available when the architecture fails. Effectiveness and workability are functions of those choices, not of the rule itself.

The first consideration is the target of regulation. The question is rarely whether children should have access to a service as such. It is the features within services that generate the risks that minimum age rules are intended to address. Livestreaming, stranger-contact functionalities, ephemeral or disappearing content, location sharing, image-based sharing involving nudity, algorithmically curated recommendation systems, and engagement-maximising design patterns are not equivalent risks and are not equally amenable to redesign. Where features can be turned off, redesigned or rendered age-appropriate without removing children from the service entirely, feature-specific regulation is more proportionate, less prone to displacement, and more administrable than service-wide bans. Where features cannot be made age-appropriate, age-based exclusion from those features (rather than from the whole service) is the more precise instrument.

The second consideration is responsibility. The primary duty must fall on platforms, in the form of duties of design rather than duties of conduct. A regime that treats age restrictions as a matter of consistent enforcement of self-declared minimum ages — under which a child who enters a false date of birth is treated as a compliance success — is not a regime of age restriction at all. It is a regime of regulatory theatre. Platforms must be required to demonstrate, against an independently auditable standard, that their age restrictions function in practice: that systems are designed to detect and disrupt foreseeable circumvention; that account creation, recovery and inheritance pathways do not provide ready routes around the rule; and that recommendation systems and design patterns are not configured in ways that contradict the stated age policy.

The third consideration is proportionality. The required assurance threshold must correspond to the severity of the risk being addressed. The assurance regime appropriate for excluding children from pornographic material is not the regime appropriate for distinguishing a 13-year-old from a 15-year-old on a service whose principal risk is excessive use. Calibration is not a technical detail. It is the difference between a proportionate regulatory architecture and an indiscriminate one.

The fourth consideration is inclusion. Any age-assurance regime that presupposes documented identity, private devices, reliable internet access, digitally confident adults and unobstructed access to formal verification infrastructure will exclude children who lack one or more of these conditions. Children in care, children experiencing domestic abuse, disabled children, children with special educational needs, children from low-income households, and children whose family circumstances do not match the assumed model will be systematically disadvantaged. A regime whose effectiveness depends on conditions not equally available to all children is not a workable regime; it quietly redistributes the burden of compliance onto those least able to bear it.

The fifth consideration is redress. All classification systems err. Age assurance systems will misclassify some children, exclude some adults, fail for some households, and produce outcomes that cannot be reconciled with users' lived realities. A workable regime must provide accessible, prompt and human-mediated routes to challenge decisions, and must not leave users trapped in automated loops with no exit. The presence of meaningful redress is the test of whether the system treats users as rights-bearing persons or as data subjects to be sorted.

The final consideration concerns the locus of enforcement. The consultation rightly recognises that no child, parent or carer should be punished where a child circumvents safeguards. That principle should be made structural. Enforcement attention should be directed at platform design, audit findings and demonstrable failure to discharge duties of design — not at family life, not at children's choices, and not at the configuration of the household.

What do you think the impacts might be from requiring age assurance across a greater number of online platforms? For example, impacts on the safety and well-being of children, on parents and carers, and on other users. You could also comment on the impact on all users' privacy and data or on business costs, revenue, and innovation.

The impacts depend on whether the expansion is targeted or generalised. Targeted expansion — extending rigorous age assurance to services and functionalities whose risk profile justifies it — can deliver real protective effect, render existing duties operational, and equip regulators to test substantive compliance rather than relying on platforms' written policies. Generalised expansion is a different matter, and the question is not only whether it would deliver marginal safety gains but what kind of digital environment it would produce. Six categories of impact should be considered.

The first is the impact on privacy and informational self-determination. If age assurance becomes a routine condition of digital participation, users must present certain information about themselves before accessing ordinary lawful content. This bears most heavily on activity that lawful adults have substantive reasons to keep

unrecorded: information about health, sexuality, religion, domestic abuse, immigration, mental health, political activity and other sensitive subjects. It also bears on children, whose ability to seek confidential information about their own lives is a recognised dimension of their rights, not a regrettable side-effect of access to digital services.

The second risk is function creep. Data infrastructures established for one purpose rarely remain confined to that purpose. Age and identity signals collected for child protection — whether held by platforms, by third-party vendors or by an emergent class of "trusted" intermediaries — will exert downstream pull toward advertising, personalisation, fraud scoring, behavioural profiling, commercial analytics and law enforcement uses, unless those uses are foreclosed by clear and enforceable legal prohibitions at the point of collection. The pattern is consistent across the history of data infrastructures: today's narrowly justified collection becomes tomorrow's foundational dataset. The presumption should run against such drift, and the prohibitions should be specified at the front end, not promised at the back.

The third is the impact on equality of access. Age assurance methods that rely on official documents, biometric capture, smartphone ownership, stable connectivity, or device-level signals do not perform uniformly across the population. They disadvantage users without ID, users with disabilities, users in unstable housing, users in low-income households, and users who depend on shared or borrowed devices. Where age assurance becomes a precondition of access, these performance gaps translate directly into gaps in digital participation. That is an equality concern of constitutional dimension, not a usability problem to be addressed by better interfaces.

The fourth is the structural impact on the digital market. Compliance costs fall disproportionately on smaller services — educational platforms, civic infrastructure, community forums, niche creative spaces, charitable services — while the largest commercial platforms can absorb them with relative ease and, in some cases, monetise the resulting infrastructure. A regulatory architecture that incidentally concentrates digital activity on the largest platforms is not neutral with respect to the harms the regulation is intended to address; many of those harms are themselves products of platform scale, design and business model.

The fifth is the displacement effect. Children excluded from regulated mainstream platforms do not cease to be online. They move — to smaller services, to less visible spaces, to overseas platforms, to peer-to-peer arrangements, to encrypted alternatives. The consultation acknowledges this risk. It should be treated not as a minor caveat but as a determinant of whether the regime improves child safety overall.

The sixth, and most fundamental, is the impact on the relationship between citizen and digital infrastructure. Routine identity presentation as a condition of lawful access alters that relationship in ways that privacy law alone does not adequately capture. It accustoms users to a posture of permission-seeking before engaging with information and communication in ordinary ways. It builds infrastructures whose subsequent uses are difficult to constrain. And it does so without the deliberative and constitutional checks that have historically accompanied state-mandated identification regimes. This is a rule-of-law concern, properly understood, and it deserves to be named as such.

It is not that age assurance should be confined to narrow cases. It is the case that any given expansion should be made on its own terms, against the specific risk it is intended to address, with independent evidence of necessity, demonstrable consideration of less intrusive alternatives, and explicit acknowledgement of the architectural consequences of generalisation.

How, if at all, could age assurance be made more effective?

Effectiveness is a property of the regulatory architecture in which the product operates. The most effective single intervention is therefore not technical but institutional: age assurance should be repositioned in regulatory thinking as accountable public infrastructure, not as a procurement category. Several features follow from that repositioning.

It should be risk-tiered. Assurance designed for the highest-risk contexts — pornographic content, suicide and self-harm material, eating-disorder content, high-risk contact functionalities — should be demonstrably robust, even at the cost of intrusiveness. Assurance designed for lower-risk distinctions — for example, distinguishing among adolescent age cohorts on services whose principal risk is excessive use — should be calibrated accordingly. A uniform standard applied across categories of risk is not a sign of rigour; it is a sign of indiscrimination.

It should be privacy-preserving by design. The proper informational output of age assurance is a yes-or-no signal as to a relevant age threshold, not a record of identity, not a behavioural profile, and not a token usable for cross-service tracking. Reusable age credentials and trusted third-party architectures may have a role, but only where they are designed to prevent the very correlation and tracking that the system is supposed to avoid. The technical possibility of such architectures is well established; the regulatory will to require them is the variable.

It should be independently audited. Platform self-attestation and vendor self-attestation are not adequate substitutes for external accountability. Accuracy at the relevant threshold, demographic performance, false-positive and false-negative rates, security posture, data retention practices, and accessibility outcomes should all be tested by bodies independent of the platforms and vendors whose systems are under review. The auditing function is not optional; it is the mechanism through which the system becomes trustworthy in fact rather than in claim.

It should be explainable to ordinary people. Parents, children and adult users should be able to understand, in non-technical terms, what is being checked, what data is used, who receives it, how long it is kept and how its conclusions can be challenged. Explanation is not a transparency virtue alone; it is the condition under which redress becomes practically available.

It should incorporate human redress. Wrongly classified users — adults misread as children, children excluded by malfunction, households whose configuration confounds the system — must have access to prompt, human-mediated review. Automated loops in which the only recourse is to resubmit to the system that failed are not a redress mechanism.

Above all, age assurance must not be permitted to function as a substitute for substantive duties of design. A platform that has assured its users has not thereby discharged its responsibilities with respect to recommendation systems, contact features, engagement-maximising design or commercial incentives. The risk is that procedural compliance with age assurance comes to occupy the conceptual space that substantive design duties should occupy — a pattern observable in other regulatory regimes, in which an auditable input substitutes for a contested outcome. Age assurance is one layer among several. It is not the work itself.

What should be considered when assessing the effectiveness of age-verification and age-assurance technologies?

Effectiveness cannot be assessed solely by technical accuracy. A system may perform impressively on accuracy metrics and still be unacceptable on legal, social or constitutional grounds. The assessment framework must include the following dimensions.

Accuracy at the relevant threshold. The distinction between an adult and a young child is a simpler classification problem than the distinction between a fourteen-year-old and a sixteen-year-old. The closer the boundary, the greater the inherent uncertainty, and the greater the importance of acknowledging that uncertainty in the design of the regulatory consequences attached to misclassification.

Fairness across demographic groups. Performance should be tested across gender, ethnicity, skin tone, disability, age, device quality, socio-economic background and household configuration. Differential performance is not a curiosity to be reported in an appendix; it is the operational shape of the regime's equality consequences, and the duties of public-sector equality law, data protection law, and human rights law attach directly to it.

Privacy and data minimisation. The system should collect only the information necessary to answer the question, retain it for the shortest period consistent with the answer, and produce no by-product datasets that exceed the specific purpose. Where the system produces identity tokens or biometric records that outlive the moment of verification, the question of whether the system is privacy-preserving has effectively been answered in the negative.

Security. Any system that aggregates identity, biometric or behavioural data becomes a target. The security posture of age assurance infrastructure should be assessed in its own right, with recognition that the consequences of compromise extend well beyond the individual platform.

Accessibility. A system that works for users with passports, smartphones, reliable connectivity and digital literacy, but not for users without those resources, is not workable; it is a system of exclusion by design. Accessibility is a primary design criterion, not a downstream accommodation.

Resistance to circumvention. The system should reduce foreseeable evasion. It should not be evaluated against an unrealistic standard of perfect enforcement. No

system will prevent every shared device, every borrowed account, every household arrangement that defeats the model the regulator assumed.

Transparency. Users should understand the process. Regulators should be able to inspect the system. Vendors should not be permitted to treat the operating logic of an age-assurance system as a commercial secret immune to oversight.

Redress. There must be a practicable, accessible and human-mediated route to challenge incorrect decisions. The presence or absence of meaningful redress is a primary, not a secondary, criterion of effectiveness.

The framework that emerges is a framework of democratic technology regulation as it applies to any consequential classification system operated at scale: not "does it work?" but "does it work lawfully, fairly, proportionately, and on terms that the persons subject to it can understand and contest?"

What methods to circumvent online safety rules do you think children in the UK use, beyond Virtual Private Networks (VPNs), or similar technologies?

Children use the accounts of parents, siblings, older friends or partners. They enter false dates of birth. They create multiple accounts under varied identifiers. They share devices within the household — a shared family tablet, a parent's phone, a sibling's console. They access content via browsers rather than apps, where age signals are weaker. They screenshot, repost and circulate via private groups, links and direct messages. They obtain content from peers rather than from the source.

What these methods share is that they are not principally technical. They are social, behavioural and architectural. Children circumvent rules because their friends are on the service, because age gates are weak, because services bundle beneficial and harmful features together, because the design of the digital environment makes circumvention easy, and because the social cost of compliance is high. The corollary is that responses focused narrowly on a single circumvention vector — for example, restrictions on VPNs — will not address the phenomenon. Effective response requires attention to the underlying conditions: platform design, incentive architecture, the social environment in which digital activity is embedded, and the educational support available to children navigating that environment. Blame directed at children for circumvention is misdirected, because circumvention is a predictable response to a system whose design invites it.

Which of the options below do you think the government should prioritise to reduce circumvention of online safety rules in the UK?

Answer: **Other — a combined model of platform responsibility, audit-backed enforcement, accountable age assurance and age-appropriate education.**

The choice posed in the consultation — between further restricting VPNs and providing additional education for children — is a mis-framing of the problem. The dominant cause of circumvention is not the availability of privacy tools or education alone; while necessary, education alone cannot bear the weight of an enforcement

strategy. The right priority is a combined model in which the primary load falls on platforms.

In our view, this model has the following elements. Platforms should be subject to a duty to prevent foreseeable circumvention as a matter of design, not as a matter of post-hoc enforcement. Where children's services exhibit repeated failed age checks, rapid account recreation patterns, suspicious account-switching behaviour, evident age inconsistencies, or design choices that facilitate the persistence of underage users, the regulatory response should focus on the platform's design choices, not on the children whose behaviour those choices invite. Age assurance should be deployed at the scale and intensity that the risk justifies, with the privacy-preserving and audit-backed architecture set out above. Regulators should have the legal and technical capacity to audit actual compliance—not the platform's written policies, but its operating practices. Children should receive age-appropriate education that explains why safety rules exist, how platforms are designed to capture and hold attention, and what is at stake when children circumvent restrictions or share accounts. Parents and carers should receive clear, practical guidance, not be expected to negotiate the architecture of the digital environment unaided. The priority is platform accountability, supported by education, calibrated by risk, and audited independently. Children should be educated and supported. They should not be conscripted as the enforcement mechanism for design failures.

To what extent do you agree or disagree with the following statement: “Everyone should go through age checks to access a VPN if it would prevent children using them”

Answer: Strongly disagree.

The proposition contains a contradiction that deserves to be made explicit. A virtual private network is, by design, a privacy-enhancing technology. Conditioning access to a privacy tool on identity-bearing verification is not a refinement of the technology; it is its inversion. A regime in which a user must first identify themselves to obtain a tool whose purpose is to limit identification is no longer providing the protection the tool is designed to provide.

The case against generalised age assurance for VPNs rests on three further grounds. The first is the breadth of legitimate use: VPNs are used by employees, students, researchers, journalists, lawyers, activists, abuse survivors, and ordinary users of public Wi-Fi for purposes ranging from corporate security to personal safety. Children themselves use VPNs for legitimate privacy reasons, as the consultation's own evidence-based records. A universal age-checking requirement would impose friction on lawful, often safety-critical, activity for a population whose use of VPNs is not the principal driver of child-safety failures.

The second is the misdirection of regulatory effort. If children are using VPNs to bypass platform restrictions, the appropriate response is to strengthen platform enforcement so that the bypass is less consequential — not to restrict the privacy infrastructure

used by the population at large. The asymmetry between cause and remedy is striking: the failure occurs at the platform layer, while the proposed remedy lies at the network-privacy layer.

The third is the precedent the measure would set. Age-restricting VPNs would mark a transition from regulating substantive harms toward regulating the privacy posture of digital activity itself. Once the principle is established that a privacy tool may be conditioned on identity verification because of its capacity to enable circumvention, the principle applies to other privacy and security technologies — secure messaging, encrypted email, anonymising browsers — whose facilitation of lawful activity vastly exceeds their facilitation of child circumvention. This route should not be followed.

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.

The potential safety gains are limited; the costs are extensive. The consultation's own evidence does not establish the empirical premise on which the measure would have to rest. The doubling of UK VPN use following the introduction of highly effective age assurance is recorded, but the consultation also records that the evidence does not suggest the peak was driven by children seeking to bypass age assurance. The consultation further records that a substantial proportion of children who use VPNs do so to protect their personal data and to stay safe online. A regulatory measure whose stated rationale is child safety, but whose effect would be to remove privacy and safety infrastructure from children themselves, has not made out its case under any test of necessity or proportionality.

For children, the likely impact is mixed at best and counterproductive at worst. Age-restricting VPNs would reduce children's ability to protect their data on public Wi-Fi, access secure communications, maintain privacy in family or social circumstances where privacy itself is a safety condition, and use the same tools that adults are encouraged to use for the same protective purposes. It may also push children toward less reputable VPNs, proxy tools or workarounds whose security and privacy properties are worse than those of the regulated alternatives they replace.

For adults, the impact is uniformly negative. The measure would impose identity-presentation requirements on lawful privacy-protective activity, require VPN providers to collect information they would otherwise not need, and create new data protection and cybersecurity risks at the verification infrastructure level itself. Compliance burdens would fall disproportionately on smaller providers, with market-structure consequences that mirror those identified in earlier answers.

For public trust, the consequences may be the most significant of all. Many users will read age verification for privacy tools as a step toward the normalisation of identity-based access to ordinary digital infrastructure. That perception is well-founded, and it will affect the political and social environment in which subsequent regulatory measures are received.

What should be considered to make age-restricting VPNs effective and workable? For example, public trust and engagement with increased age assurance requirements, accessibility of age assurance methods and variations of age assurance approaches across services, interaction with legitimate uses of VPNs.

The preferable answer is that VPNs should not be the subject of generalised age restrictions. If the question is nevertheless to be considered, the threshold inquiry is whether the measure could satisfy the legal tests of necessity and proportionality — tests rooted in domestic public law and in human rights law, not in policy preference. The government would need to demonstrate that children's VPN use is a material cause of online-safety enforcement failure; that less intrusive alternatives, including stronger platform duties, have been considered and shown to be inadequate; and that the benefits expected from the measure exceed the costs to privacy, security, lawful access and market structure. The current evidence base, including the evidence in the consultation document itself, does not support that demonstration.

If the inquiry proceeds despite those reservations, several further considerations apply.
The definition of what constitutes a VPN for regulatory purposes must be precise. VPNs are one category of privacy-enhancing technology among many. A narrow rule will be circumvented by adjacent tools. A broad rule will sweep in legitimate cybersecurity infrastructure, including infrastructure on which businesses, schools, public bodies and critical services rely. Neither outcome is acceptable.

Legitimate uses must be protected explicitly, not merely acknowledged. The categories include remote work, secure access to corporate networks, public Wi-Fi protection, journalism, legal practice, security research, and personal safety — all of which depend on the technology functioning unimpaired.

Any age assurance for a privacy tool would need to satisfy exceptional standards of privacy preservation. The default conclusion is that this is not feasible without contradiction, which is itself a reason against the measure.

The likely operational effectiveness of the measure should not be overstated. Children may move to proxies, browser extensions, overseas tools, shared devices or peer-mediated workarounds. The displacement effect cannot be assumed away.

Better alternatives exist and should be exhausted first: stronger platform duties of design, audit-backed compliance regimes, app-store-level safeguards, public education, support for parents, and enforcement actions targeting services specifically marketed to children as tools to evade online-safety rules. These alternatives operate at the layer where the failure occurs, without dismantling the privacy infrastructure used by the wider population.

For these reasons, generalised age restrictions on VPNs should not be the choice.

To what extent do you agree or disagree with the following statement: “To address some of the challenges schools face with mobile phones, the

Department for Education's (DfE) non-statutory guidance on 'mobile phones in schools' should be made statutory." This would mean schools have a legal duty to follow the guidance, which explains to individual schools and trusts how to implement a policy that prohibits the use of mobile phones throughout the school day, they have good reasons not to. This includes during lessons, the time between lessons, breaktimes and lunchtime.

Answer: Somewhat agree.

There is a defensible case for placing the guidance on a statutory footing, but the case is for a statutory duty to have regard to guidance, not for an inflexible national prohibition administered from the centre. The distinction matters.

The conditions to which the guidance is addressed are real. Mobile phones in lessons are a source of distraction, a vector for bullying, harassment and unauthorised image-sharing, and an obstacle to the kind of attention that the work of school requires. The data in the consultation document, showing the gap between the existence of school policies and the persistence of in-lesson use, indicate that policy alone is not converting into changed practice. A statutory duty to have regard to guidance could provide a clearer national baseline, support headteachers in conversations with parents and pupils, and reduce the cost of locally re-litigating the same battle in every school.

The case for flexibility is equally strong. Children with medical needs, children with disabilities or special educational needs requiring assistive technology, children with safeguarding concerns specific to their family circumstances, children with caring responsibilities, and children whose journey to and from school raises genuine safety issues are not abstract exceptions. They are children whose particular circumstances are not well served by a rule that treats all pupils identically.

The right architecture is therefore a statutory duty to have regard to the guidance, accompanied by clear, named exception categories, support for school-level implementation, and explicit recognition of headteacher discretion within the framework set by the guidance. That is consistent with how proportionate regulation operates in adjacent areas and with what the consultation appears to propose.

What impacts would there be if this guidance was made statutory and why? For example, on disruption in lessons, bullying or harassment, parental views on mobile phone policies, staff, etc.

The potential positive impacts are real. A statutory baseline can reduce in-lesson disruption, support teacher authority, reduce opportunities for in-school bullying and image-based harassment, create clearer expectations for parents and pupils, and lower the political cost to individual schools of maintaining a mobile-phone-free environment. Where the underlying problem reflects a wider digital culture rather than the practice of any individual school, a national baseline can do work that no individual school is well placed to do.

There may also be safety benefits beyond academic concentration. During the school day, phones can become instruments of unauthorised recording, image-based abuse,

cyberbullying, coercive messaging, sexualised peer pressure and the rapid circulation of harmful content. A school environment in which phones are unavailable during the school day reduces those risks at their source.

The implementation has to be done with care. Storage and confiscation policies can generate disputes if not clearly designed. Some parents will be anxious about the loss of direct, in-day contact with their children, and that anxiety has to be addressed through reliable alternative contact arrangements. Some pupils — those with medical, disability-related, safeguarding or caring needs — will be disproportionately affected by a rigid policy, and the exception architecture has to be designed accordingly. Staff time will be drawn into managing the policy at the margin, and that has to be supported rather than treated as a costless externality.

The statutory framework should therefore be accompanied by model policies, named exception categories, practical guidance on storage and confiscation, communication templates for parents, alternative arrangements for emergency contact, and recognition that headteacher judgement is the operating layer through which the policy works in practice. The purpose is to make schools calmer and safer, not to add a bureaucratic burden to environments already carrying many.

Are there specific circumstances where you think children should be permitted to have or use a mobile phone during the school day?

Answer: Yes — specifically: medical needs; SEND requirements (including assistive technology); individual safeguarding concerns; caring responsibilities; authorised educational use; travel to and from school (subject to the phone being inaccessible during the school day unless otherwise authorised); and exceptional family circumstances, subject to school approval.

The default should be that phones are not in use during the school day. The exceptions should be specified, authorised, recorded and periodically reviewed at the school level. They are not concessions to inconvenience; they are recognitions that a phone is, for some children, a medical device, an assistive technology, a safeguarding device, or a coordination tool without which the child's safety or family functioning is compromised. A policy that fails to accommodate those uses is not strict; it is inattentive to the children whose circumstances differ from the assumed model.

A good policy is firm enough to change the school environment, and humane enough to recognise that the children most likely to need exceptions are often the children whose needs are most easily overlooked.

It is our view that the government is right to address compliance and enforcement. Substantive online-safety duties have limited effect if they can be evaded at scale, and the credibility of the regulatory system depends on its capacity to convert duties into outcomes. The question is not whether to enforce but how, and the answer is constitutional as much as it is technical. The architecture proposed in this response is principled and practicable. The primary regulatory burden belongs on platforms, in the form of duties of design subject to independent audit. Age assurance should be calibrated to the seriousness of the risk, structured to preserve privacy, accessible to all the users it classifies, and accompanied by meaningful redress. Privacy-enhancing

technologies should not be conscripted into a compliance architecture they were designed to resist. Schools should be supported by a statutory framework that is firm in default and humane in exception. Children should be treated throughout as rights-bearing persons navigating systems designed by powerful institutions, not as the residual locus of enforcement responsibility for failures that occur elsewhere. It is the architecture that protects children without dismantling the conditions that make a digital environment worth protecting in the first place.

What methods do children use to circumvent safety measures, beyond VPNs?

- Children use:
  • Proxy websites
  • Tor and anonymous browsers
  • Shared accounts or devices
  • Alternative platforms and mirror sites
  • Encrypted messaging apps
  • DNS-based workarounds

What should be prioritized to reduce circumvention?

- Education should be the priority.
- Children need better digital literacy, stronger critical thinking skills, and clearer understanding of online risks.
- Building resilience and informed decision-making is more sustainable than attempting to block every circumvention tool.

Do you agree with requiring age checks for VPN use?

- Strongly disagree.

- The focus should instead remain on platform accountability and effective safeguards on regulated services.

What would be the impacts of age-restricting VPNs?

- Any safety gains are likely to be limited, while the downsides are significant.
- Restrictions could weaken privacy protections, encourage alternative circumvention methods, and create unnecessary surveillance concerns.

How could VPN restrictions be made effective?

- If any restrictions are considered, they must be tightly limited, proportionate, and privacy-preserving.
- Government should engage closely with cybersecurity experts, civil society organisations, privacy advocates, and industry before introducing any measures in this area.

Chapter 4: Preparing children for a digital future

Media and digital literacy for children / Media literacy – support for families

Media literacy is about understanding, questioning, and making sense of the content you see online. It helps children tell the difference between fact and opinion, check sources and assess their trustworthiness, and recognise how online content can affect thoughts, feelings and behaviour.

Digital literacy means having the practical skills to use devices and online services safely, confidently and independently. This includes knowing how to set up and use devices, recognising scams, protecting personal information, and managing everyday digital tasks.

Which areas of media or digital literacy do children and families most need additional help with?

(Please select all that apply)

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

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)

- **Schools or childcare settings**
- Community or youth spaces (for example libraries, youth clubs or local charities)
- Parent or carer groups or networks
- **Public services (such as family hubs, GP surgeries or community centres)**
- Faith or cultural groups
- **Non-governmental online sources (such as websites, platforms or online communities)**
- **Government websites**

- Don’t know/ Prefer not to answer
- None of the above/I would not use these to find help
- Other (please specify):

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)

- **By providing clear guidance that children can use on their own**
- By supporting parents and carers to support children online
- **By working with online platforms and services that children already use**
- By supporting youth organisations and community groups to help children online
- **By making help or advice easy to access when something goes wrong online**
- **By involving children and young people in designing support**
- Don’t know/ Prefer not to answer
- None of the above

What types of support would help children with additional needs stay safe online and build digital skills?

By 'additional needs', we mean children who may need extra support for a range of reasons (such as learning, communication, health or access needs).
(Please select all that apply)

- **Clear, simple information using plain language**
- **Content adapted for different ages, abilities or needs**
- **Visual, audio or interactive formats**
- Support delivered through trusted local or community services
- Flexible or on-demand support that can be accessed when needed
- **Support that helps parents or carers guide children online**
- Don’t know/ Prefer not to answer
- None of the above
- Other (please specify):

91%

Promoting high quality content

We know that access to high quality content can be beneficial for children. By ‘high quality’ online content, we mean content that can have positive impacts on children’s learning and development.

Who would you trust to determine what is meant by 'high quality online content' for children 13-16?

(Please select all that apply)

- Government
- Online platform trust and safety teams
- Parents, carers or trusted adults
- **Children**
- **Developmental experts**
- **Educators**
- Youth workers
- **Child advocacy charities and organisations**
- Don’t know/ Prefer not to answer
- None of the above
- Other (please specify):

What further action should be prioritised to support positive online spaces for young people?

(Please select all that apply)

- **Develop best practice principles for industry**
- **Develop guidance for parents and carers**
- **Develop guidance for children**
- **Reviewing international approaches**
- Industry voluntarily promoting high quality content for children
- Don’t know/ Prefer not to answer
- None of the above
- Other (please specify):

What should be considered when taking further action to support positive online spaces and content for young people?

For example, how would this work in practice for services, taking into account existing best practice across industry, and who should feed into future guidance.

Supporting and fostering positive, safe online spaces for young people in the UK requires a comprehensive approach that balances robust systemic regulation with creative user empowerment. Under the regulatory landscape shaped by the **Online Safety Act 2023 (OSA)** and the Information Commissioner's Office (ICO) **Age Appropriate Design Code (Children's Code)**, creating these environments moves away from a purely reactive "content takedown" approach toward a structural, proactive, and holistic framework (Law, 2025; NYU Stern, 2025).

The following elements detail what must be considered, how these principles work in practice for service providers, and who should feed into future guidance.

---

1. Key Considerations for Supporting Positive Online Spaces

When taking further action to support young people online, several interconnected dimensions must be addressed:

- **The Shift from "Rules and Tools" to Digital Resilience:** Historically, online safety relied heavily on static internet filters and parental locks (Ambitious

about Autism, 2012). Modern best practice recognizes the "mosaic effect"—the fact that a young person's offline vulnerabilities and fluid movements across various platforms mean risks cannot be completely isolated (Nominet, 2019). Focus must therefore balance mitigating risk with proactively building a child's critical thinking skills, emotional well-being, and digital resilience (Nominet, 2019; PMC, 2024).

- **Systemic Risk and "Safety by Design":** Rather than merely responding to user reports, services must evaluate how their platform architectures—such as optimization algorithms, infinite scroll features, and push notifications—afford or amplify risks like compulsive usage, cyberbullying, or exposure to content promoting disordered eating and self-harm (NYU Stern, 2025; PMC, 2024; ICO, 2018).
- **Bridging the Generational Disconnect:** Academic research indicates a steep disconnect between how adults and young people view online spaces. While caregivers primarily focus on potential harms (e.g., violent or inappropriate content), young people frequently cite the immense mental health benefits of online spaces, including community validation, learning new skills, and reducing loneliness (PMC, 2024; ICO, 2018). Guidance must support positive engagement without chilling these vital spaces for connection.
- **Proportionality, Privacy, and Fundamental Rights:** Measures implemented to protect children (such as age verification or proactive content scanning) must be carefully balanced against users' fundamental rights to privacy and freedom of expression (Law, 2025; BILETA, 2025).

---

2. Implementation in Practice for Service Providers

For user-to-user platforms, search engines, and Information Society Services (ISS), translating these expectations into practice involves robust internal governance (Law, 2025; ICO, 2018):

A. Comprehensive, Age-Distinct Risk Assessments

Services must explicitly map out how their products affect different age groups. Data from the ICO highlights that parental anxiety peaks during the transitional ages of 10–13, which is when children move from highly supervised environments to independent social networking (ICO, 2018). Risk assessments must also be intersectional—for instance, recognizing how online gender-based violence or misogyny disproportionately impacts young girls (BILETA, 2025).

B. Architectural Alterations (Safer by Design)

- **Algorithmic Transparency and Control:** Services are increasingly expected to modify their recommender systems (University of Hertfordshire, 2024). Platforms should allow young users to customize safety settings and opt out of profiling or aggressive algorithmic recommendation loops that draw them into "rabbit holes" of harmful content (NYU Stern, 2025).
- **Proactive Technologies:** Where applicable, services utilize technical measures such as automated fraud detection and hash-matching databases to detect and prevent severe harms (like Child Sexual Abuse Material) before they reach young users (University of Hertfordshire, 2024).

- **Friction-by-Design:** Implementing design features that interrupt impulsive behaviors—such as prompts asking, *"Are you sure you want to post this?"* or preventing notifications late at night—can mitigate online harassment and support sleep hygiene.

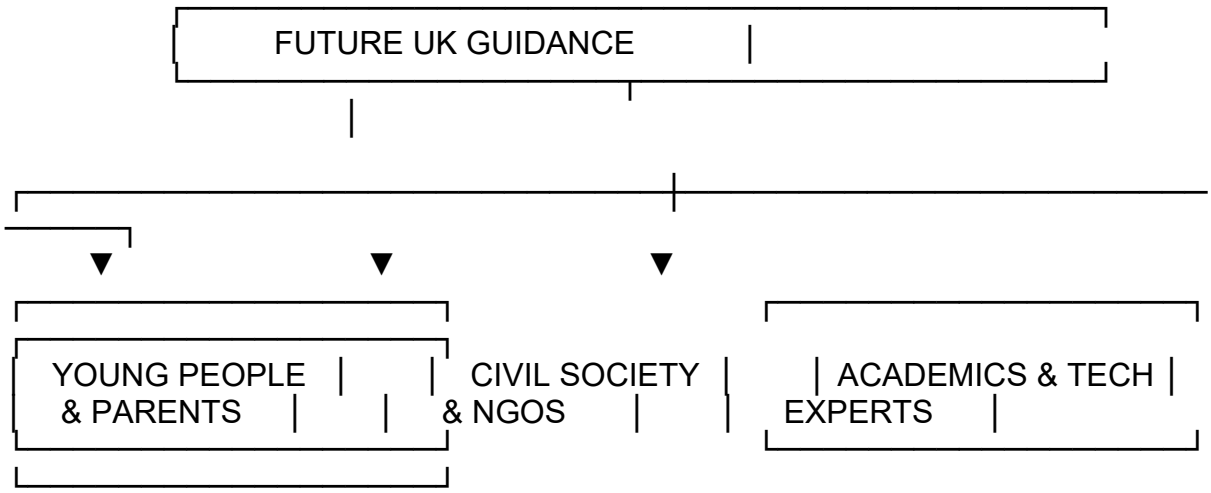
C. Accessible Terms and Transparent Redress

Terms of service must be written in simplified, age-appropriate language (Ambitious about Autism, 2012). Content moderation systems must also avoid a strict "tick-box" approach; platforms should employ trained staff capable of understanding complex contextual harms (such as coercive abuse or eating disorders) and provide transparent, independent appeals mechanisms for mistakenly removed content or user sanctions (University of Hertfordshire, 2024; BILETA, 2025).

---

3. Stakeholders Who Should Feed into Future Guidance

To ensure regulatory codes and industry practices remain agile and effective, an ongoing, multi-stakeholder co-design approach is vital:



- **Young People and Caregivers:** Regulators must actively consult children of varying ages, backgrounds, and neurodivergent profiles to co-design guidance (Ambitious about Autism, 2012; ICO, 2018). Forums like youth parliaments or digital co-design labs ensure guidelines reflect how young people *actually* experience the internet, rather than operating on adult assumptions.
- **Civil Society, Charities, and NGOs:** Civil society organizations are uniquely positioned to translate real-world vulnerabilities into policy arenas (Nominet, 2019). Input must specifically come from children's rights organizations, youth mental health charities, and specialized safety advocates (such as women's safety NGOs) to ensure niche or emerging threat patterns are captured (BILETA, 2025).
- **Academic Researchers and Subject-Matter Experts:** Empirical research from child development psychologists, tech ethicists, and human rights legal scholars must anchor any highly prescriptive design mandates (NYU Stern,

2025; ICO, 2018). Experts in algorithmic auditing and content moderation play a key role in verifying that the safety solutions proposed by tech platforms are technically viable, transparent, and legally sound (Law, 2025; NYU Stern, 2025).

- **Industry and Technical Trade Associations:** Small and medium-sized enterprises (SMEs) alongside major technology providers should feed into guidance to ensure that "safer by design" expectations are technically feasible, scalable, and do not inadvertently entrench market monopolies by making compliance impossible for smaller innovators (ICO, 2018).

References

- Ambitious about Autism. (2012). *Learning disabilities, autism and internet safety: A parent's guide.* Ambitious about Autism / Cerebra. URL Cited by: N/A
- BILETA. (2025). *BILETA's response to Ofcom's draft guidance: 'A safer life online for women and girls'.* University of Hertfordshire Research Archive. URL Cited by: N/A
- Information Commissioner's Office (ICO). (2018). *Age appropriate design: Call for evidence.* Internet Matters. URL Cited by: N/A
- Law, S. (2025). Effective enforcement of the Online Safety Act and Digital Services Act: Unpacking the compliance and enforcement regimes of the UK and EU's online safety legislation. *Journal of Media Law*, 1-38. URL Cited by: 17
- Nominet. (2019). *Keeping children safe online report.* Nominet / Cliff Manning. URL Cited by: N/A
- NYU Stern Center for Business & Human Rights. (2025). *Online safety regulations around the world.* NYU Stern. URL Cited by: N/A
- PMC. (2024). Social media and youth mental health: Scoping review of platform and policy recommendations. *PubMed Central*. URL Cited by: N/A
- University of Hertfordshire. (2024). *BILETA response to Ofcom's additional safety measures consultation.* University of Hertfordshire Research Profiles. URL Cited by: N/A

Chapter 5: Supporting families

97%

Parental controls

Many online platforms provide parental control tools which allow parents and carers to oversee and place parameters around children's online activity, including content, time and functionality-based restrictions.

To what extent do you agree or disagree with the following statement:

"Parents should have control over the online experiences of their children"

- Strongly agree
- **Somewhat agree**
- Neither agree nor disagree
- Somewhat disagree
- Strongly disagree
- Don't know/ Prefer not to answer

Please explain the reasoning behind your answer:

When addressing the statement, **"Parents should have control over the online experiences of their children,"** a comprehensive analysis across UK policy, industry standards, and academic research generally aligns with a position of **Somewhat agree**.

While parental involvement is vital for safeguarding, an overreliance on absolute "control" can conflict with a child's developmental needs, privacy rights, and digital literacy.

The reasoning below outlines the balance required in practice, drawing on current regulatory frameworks and industry best practices.

---

1. Why Parental Involvement is Crucial (The Argument for "Agree")

There is a consensus among regulators, charities, and industry leaders that parents play an indispensable role in navigating a child's early digital life:

- **Developmental Safeguarding:** Younger children often lack the cognitive maturity to identify online risks, such as grooming, commercial exploitation, or radicalization. Parental controls (e.g., content filters, screen-time limits) act as necessary training wheels (ICO, 2018).
- **Mitigating "The Mosaic Effect":** Because children frequently move between different platforms, apps, and physical environments, technical safety measures on a single platform are rarely foolproof. Active parental mediation helps bridge these gaps by providing immediate, real-world context and emotional support when a child encounters distressing content (Nominet, 2019).
- **Accountability:** Legally and socially, parents bear the primary responsibility for their children's well-being. Giving them technical tools to monitor and manage access aligns with this existing responsibility.

---

2. The Risks of Absolute "Control" (The Argument for "Disagree")

The reason a blanket "Strongly Agree" is often contested by legal scholars and child rights advocates stems from the unintended consequences of total surveillance and restriction:

- **Undermining Digital Resilience:** Research shows that overly restrictive parental control (e.g., strict blocking software) can stifle a child's ability to develop critical thinking and online coping mechanisms. When children

encounter inevitable risks without having developed "digital resilience," they are often less equipped to handle them safely (Nominet, 2019; PMC, 2024).

- **Chilling the Benefits of Online Spaces:** For many young people—particularly marginalized groups, such as LGBTQ+ youth or neurodivergent individuals—the internet is a vital lifeline for finding supportive communities, expression, and mental health validation (PMC, 2024; Ambitious about Autism, 2012). Rigid parental control can inadvertently cut off these positive networks.
- **The "Safety by Design" Responsibility Shift:** Historically, technology companies relied on parental controls to shift the entire burden of online safety onto families. The UK's **Online Safety Act 2023** and the **Age Appropriate Design Code (Children's Code)** explicitly reject this stance. They mandate that the digital environment must be *inherently* safe by design, reducing the need for parents to act as constant content moderators (Law, 2025; ICO, 2018).
- **Children's Rights to Privacy:** Under article 16 of the UN Convention on the Rights of the Child (UNCRC), children have a right to privacy. As a child grows older, absolute parental control can infringe upon their autonomy and can drive risky online behaviors underground, making teenagers less likely to disclose online harms to their parents out of fear of losing device access (ICO, 2018; BILETA, 2025).

---

3. Conclusion: Moving from "Control" to "Mediation"

In practice, the ideal model is not absolute control, but a sliding scale of **parental mediation** that evolves as the child matures. For a 7-year-old, strict technological control is appropriate. For a 15-year-old, "control" should transition into collaborative oversight, transparent boundaries, and open dialogue.

Ultimately, parental tools should complement, rather than replace, a tech platform's foundational duty to provide a safe, transparent, and age-appropriate user interface (Law, 2025; NYU Stern, 2025).

References

- Ambitious about Autism. (2012). *Learning disabilities, autism and internet safety: A parent's guide.* Ambitious about Autism / Cerebra. URL
- BILETA. (2025). *BILETA's response to Ofcom's draft guidance: 'A safer life online for women and girls'.* University of Hertfordshire Research Archive. URL
- Information Commissioner's Office (ICO). (2018). *Age appropriate design: Call for evidence.* Internet Matters. URL
- Law, S. (2025). Effective enforcement of the Online Safety Act and Digital Services Act: Unpacking the compliance and enforcement regimes of the UK and EU's online safety legislation. *Journal of Media Law*, 1-38. URL
- Nominet. (2019). *Keeping children safe online report.* Nominet / Cliff Manning. URL

- NYU Stern Center for Business & Human Rights. (2025). *Online safety regulations around the world.* NYU Stern. URL
- PMC. (2024). Social media and youth mental health: Scoping review of platform and policy recommendations. *PubMed Central*. URL

How should this level of control change for children of different ages?

For example, a 16-year-old and an 11-year-old.
When considering how parental control should adapt to a child's age, regulatory frameworks and child development research suggest a clear transition from **active technological restriction** for younger children to **collaborative oversight and guidance** for older adolescents.

This approach aligns with the legal concept of *Gillick* competence in the UK and international standards like the UN Convention on the Rights of the Child, which recognize that a child's right to autonomy and privacy increases as they mature.

---

1. The 11-Year-Old: A Foundation of Structure and Direct Protection

An 11-year-old is at a critical developmental intersection. In the UK, this age typically marks the transition from primary to secondary school—a period where independent device ownership and peer pressure sharply increase, yet cognitive skills like long-term risk assessment are still developing (ICO, 2018).

- **Approach: Active Technological Control & Scaffolding.**
- **Technical Implementation:**
    - **Default Restrictive Profiles:** Strict age-gating should be enforced. Accounts on platforms should be set to maximum privacy by default (e.g., hidden profiles, direct messaging limited to approved contacts or disabled entirely) (ICO, 2018).
    - **Curated Ecosystems:** Content access should be restricted via robust whitelisting or strict age filters rather than open search, protecting them from structural algorithmic risks like radicalization or content promoting self-harm (NYU Stern, 2025).
    - **Friction and Boundaries:** Strict screen-time parameters, bedtime lockouts, and mandatory parental approval for app downloads are appropriate at this stage to establish healthy digital hygiene boundaries.
- **Underlying Logic:** At 11, the primary focus is on minimizing exposure to severe contextual and behavioral risks while the child begins to understand basic digital literacy rules (Nominet, 2019).

---

2. The 16-Year-Old: Fostering Digital Resilience and Autonomy

By age 16, young people are approaching legal adulthood in many contexts, navigating employment, independent study, and complex social identities. Absolute

technical blocking at this stage is not only largely ineffective—as tech-savvy teenagers easily bypass local device filters—but it can also actively backfire by driving online vulnerabilities underground (Nominet, 2019).

- **Approach: Collaborative Oversight, Trust, and Open Mediation.**
- **Technical Implementation:**
    - **Autonomy by Design:** Platforms should offer full structural features, but with persistent safety reminders and transparent, accessible reporting mechanisms rather than parental intervention blocks (University of Hertfordshire, 2024).
    - **Privacy and Data Controls:** Technical settings should shift from parental locks to empowering the 16-year-old to control their own data footprint, such as opting out of behavioural tracking, algorithmic profiling, or targeted advertising (ICO, 2018; NYU Stern, 2025).
    - **Open Access with Safety Nets:** Restrictive firewalls should be replaced with open access to information, supported by underlying background protections (e.g., automated platform-level hashing to block severe harms like CSAM or illegal content) (Law, 2025).
- **Underlying Logic:** For a 16-year-old, the focus must shift entirely toward cultivating **digital resilience** (Nominet, 2019). The internet serves as an essential space for peer connection, mental health support, and identity exploration (PMC, 2024). Parental involvement should function as a supportive safety net based on dialogue rather than surveillance, ensuring the teenager feels safe disclosing online harms or cyberbullying without fearing the loss of digital access (BILETA, 2025).

Summary of the Age-Based Shift in Practice

Feature / Dimension	The 11-Year-Old	The 16-Year-Old
Primary Safety Mechanism	Strict parental filters and device-level restrictions.	Platform-level safety by design and personal critical thinking.
Account Privacy	Maximum privacy by default; fully closed network.	Custom user-controlled privacy; open social engagement.
Content Discovery	Whitelisted or highly curated content streams.	Unrestricted access with proactive platform safeguards.
Parental Role	**Gatekeeper:** Setting structural, non-negotiable boundaries.	**Advisor:** Open dialogue, mentoring, and support on structural risks.

References

- BILETA. (2025). *BILETA's response to Ofcom's draft guidance: 'A safer life online for women and girls'.* University of Hertfordshire Research Archive. URL
- Information Commissioner's Office (ICO). (2018). *Age appropriate design: Call for evidence.* Internet Matters. URL

- Law, S. (2025). Effective enforcement of the Online Safety Act and Digital Services Act: Unpacking the compliance and enforcement regimes of the UK and EU's online safety legislation. *Journal of Media Law*, 1-38. URL
- Nominet. (2019). *Keeping children safe online report.* Nominet / Cliff Manning. URL
- NYU Stern Center for Business & Human Rights. (2025). *Online safety regulations around the world.* NYU Stern. URL
- PMC. (2024). Social media and youth mental health: Scoping review of platform and policy recommendations. *PubMed Central*. URL
- University of Hertfordshire. (2024). *BILETA response to Ofcom's additional safety measures consultation.* University of Hertfordshire Research Profiles. URL

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.

To enable parents and carers to use parental controls effectively, the current UK regulatory and digital literacy landscape—highlighted by Ofcom's Media Literacy research and the Department for Science, Innovation and Technology (DSIT)—emphasizes that the solution requires a mixture of **point-of-purchase friction**, **platform simplicity**, and **cross-industry standardization**.

Rather than treating parental controls as an optional "add-on," best practices dictate that safety setup must be seamlessly woven into the consumer journey.

---

1. Mandating "Safety at Point of Sale" (The Retail Intervention)

A major hurdle for parents is that the procurement of a device and its safety configuration are completely decoupled. By the time a child receives a smartphone, the momentum is focused on immediate use rather than secure setup.

- **Mandatory Setup Guidance on Purchase:** Telecom operators (e.g., EE, Vodafone, O2) and device retailers should be legally or contractually obligated to provide an explicit, step-by-step "Set Up Safe" protocol at the exact point of sale—whether in-store or during digital checkout (DSIT, 2026).
- **Pre-Activated Frameworks:** Hardware manufacturers could incorporate an initial device boot-up sequence that explicitly asks, *"Is this device for a child?"* If selected, the device would automatically prompt the parent to link an administrative account (e.g., Google Family Link or Apple Family Sharing) before the home screen can even be accessed.

---

2. Radical Platform Simplification and "Layering"

Data from Ofcom's *Children and Parents: Media Use and Attitudes* reports consistently demonstrate a widening gap between parental concern and technical execution; many

parents want to implement restrictions but find the fragmented app settings overwhelming (Ofcom, 2025; DSIT, 2026).

- **In-App Onboarding and Triggers:** Platforms should provide clear, context-aware prompts for parents. For instance, when an account detects it is linked to a minor, or when a child approaches the age of digital consent, platforms should send simplified, visual walkthrough videos directly to the caregiver's linked account (Alan Mackenzie, 2026).
- **The "Layering" Concept:** Rather than presenting parents with dozens of toggles for privacy, mature content, cookies, and screen time, platforms should adopt a simplified "layered" or tier-based approach (e.g., *Highly Restrictive*, *Moderate Exploration*, *Open with Safeguards*) that maps cleanly to the child's developmental age (Alan Mackenzie, 2026).

---

3. Greater Standardization Across the Industry

Currently, a parent must learn an entirely different user interface and vocabulary to set controls on an iPhone, an Android tablet, a PlayStation 5, Netflix, and TikTok. This fragmentation causes compliance fatigue.

- **Unified Terminology:** The Information Commissioner's Office (ICO) and Ofcom should drive industry standards to ensure safety vocabulary is uniform. Terms like "Restricted Mode," "Supervised Experience," and "Family Pairing" should be standardized across the market so parents intuitively know what a setting does regardless of the brand.
- **Interoperable Central Dashboards:** Future technical guidance should encourage interoperability, allowing third-party safety aggregators or OS-level dashboards to manage app-specific permissions centrally. A parent should ideally be able to adjust content parameters for multiple independent apps from a single, centralized operating system hub.

---

4. Shifting from "Surveillance" to "Co-Regulation" Tools

Finally, tools need to evolve from invisible surveillance software into transparent communication bridges.

- **Shared Safety Alerts:** Instead of tools that secretly spy on a child’s activity—which breaks parental trust and stops adolescents from reporting genuine harms—tools should feature transparent, shared dashboards.
- **Collaborative Settings:** For older children, systems should allow the child to request modifications (e.g., asking for an extra 15 minutes of educational screen time or requesting access to an app), turning the software into a tool for active family negotiation and digital literacy rather than unilateral policing (Alan Mackenzie, 2026; DSIT, 2026).

References

- Department for Science, Innovation and Technology (DSIT). (2026). *Growing up in the online world: A national conversation (Consultation Document).* GOV.UK. URL

- Mackenzie, A. (2026). *Important e-safety updates and platform-level parental supervision alterations.* Online Safety UK / Castleview Portal. URL
- Ofcom. (2025). *Children and parents: Media use and attitudes report 2025.* Ofcom Research Archive / Kids Online World. URL
- Ofcom. (2026). *Children and parents' media literacy tracker 2025-26: Technical framework report.* Ofcom. URL