

Submission on behalf of Monica Harding MP: Growing up in the online world

Executive Summary

This submission is based on an extensive consultation on online safety involving over 2,000 emails from constituents, conversations with Headteachers, educators, families, local campaign groups and a series of dedicated roundtables with students at schools across Esher and Walton and with parents in the community.

These conversations revealed widespread concern about the scale and urgency of online harms facing children today.

What emerged most clearly from these discussions was a sense of systemic failure - both from the Government, through inadequate policy and inaction, and from technology companies whose platforms continue to expose children and young people to harmful and addictive services. Young people spoke candidly about social media systems designed to capture and exploit their attention and vulnerabilities, while parents described the frustration of being left to manage harms they often feel powerless to prevent.

Notably, both students and parents demonstrated scepticism that regulation as it is currently enforced can constrain technology companies in any meaningful way, with current age restrictions deemed ineffective and easily bypassed. This submission outlines the key findings and makes clear recommendations in each section for stronger, faster and more enforceable action to protect children growing up in the online world.

Section One: Age Restrictions and Social Media Ban

This submission supports the introduction of a statutory under-16s social media ban for high-risk social media platforms and functionalities.

The evidence gathered throughout the consultation process demonstrated widespread concern that current age restrictions are ineffective, inconsistently enforced and easily circumvented. Students across all roundtables consistently reported that false dates of birth are routinely used to bypass platform restrictions and that children frequently bypass restrictions. In one roundtable, all students had some form of parental restriction on their phone, all students had at some point bypassed it.

One student asked, "Why call it a ban if you can get around it?". This reflected a broader sentiment among young people that existing safeguards are performative rather than thorough.

The failure of age verification systems is an incentive problem. Social media and technology companies have little commercial motivation to meaningfully prevent underage users from accessing platforms when engagement, advertising revenue and long-term platform loyalty all benefit from younger audiences joining earlier and remaining online for longer.

The [recent](#) US legal case involving Meta and YouTube is a significant example in this regard. Evidence presented during proceedings suggested that technology companies were aware underage users were accessing platforms despite public claims regarding minimum age protections. This raises serious questions regarding whether existing voluntary approaches to age restrictions, such as the [current](#) legal age of thirteen, are fundamentally incapable of delivering meaningful protection for children.

Parents participating in roundtables overwhelmingly supported stronger restrictions on under-16 access to social media. Participants repeatedly argued that current systems leave parents carry the responsibility while technology companies continue profiting from addictive and engagement-driven platform design. This leads to friction at home and parents often unable to enforce or monitor restrictions which children can bypass.

At the same time, this submission recognises that age restrictions alone will not fully resolve the wider structural issues driving online harms. Students themselves raised concerns that bans without broader reforms could push children towards less regulated or more hidden online spaces. This concern is also shared in reflections from organisations including the Online Safety Act Network.

For this reason, the Government should not treat an under-16 ban as a standalone solution or symbolic intervention. Students that we spoke to claimed that a sudden introduction of social media to 16- or 18-year-olds having not gradually been introduced would be harmful, especially during a period of already massive life changes and uncertainty.

Rather, it should form part of a broader package of reforms including meaningful age assurance systems, legally enforceable safety-by-design duties, restrictions on addictive platform features and much stronger enforcement powers against technology companies.

The Government should treat this as a public health crisis and must act with urgency on this basis. A year is too long to lay the regulations before Parliament.

This submission therefore supports:

- A statutory under-16 age ban for high-risk social media services.
- Stronger age assurance requirements.
- Legal accountability for technology companies that provide platforms that knowingly permit underage access.

Section Two: Functionalities and Persuasive Design

The strongest evidence gathered throughout this consultation concerned persuasive and addictive platform design. Across all schools and parent roundtables, participants consistently identified platform functionalities deliberately engineered to maximise engagement, prolong usage and encourage compulsive behaviour among children and young people.

Young people themselves repeatedly demonstrated an awareness that these systems are designed to retain attention. Students described losing track of time while scrolling, struggling to disengage from feeds and repeatedly returning to platforms despite recognising the negative effects on their wellbeing.

TikTok was consistently identified as the most addictive platform across all roundtables. During one of the school roundtables, a student described their friend spending 36 hours a week on TikTok. Students explained how algorithms increasingly tailored content based on watch time and interaction, making feeds progressively more difficult to disengage from over time.

Students described physical and emotional consequences associated with excessive scrolling, including tiredness, reduced alertness, irritability and shortened attention spans. One student described becoming increasingly pessimistic and emotionally drained while spending extended periods scrolling through social media content.

Concern was raised regarding functions such as location-sharing functionalities, large group chat messaging systems, infinite scrolling capabilities, algorithmic “For You” pages (TikTok function), push notifications and “disappearing messages”.

Other students described Snap Maps and location-sharing features as increasing feelings of exclusion and “fear of missing out”. One student explained that “the less you have it, the more you want it” in relation to tracking friends through location services, demonstrating the compulsive and psychologically reinforcing nature of these systems.

Snapchat’s disappearing message system was repeatedly identified as enabling bullying and abusive behaviour by removing accountability and evidence trails. Students argued that messages disappearing after viewing allowed peers to “get away” with abusive behaviour in ways that would not occur offline.

WhatsApp group chats were also repeatedly identified as harmful environments where children could be targeted, isolated or exposed to inappropriate content. Students described whole-year-group chats where inappropriate images were shared, and children became vulnerable to bullying or exclusion. Parents similarly raised concerns regarding group chats involving primary-age children sharing harmful or sexualised content.

The consultation correctly identifies many of these functionalities as risks. However, this submission shares concerns raised by the Online Safety Act Network that the Government’s current approach risks regulating individual features in isolation without confronting the deeper commercial incentives driving harmful design.

The central issue is that many business models are deliberately engineered to exploit children’s psychology for profit. As demonstrated in the recent US court case involving Meta and YouTube, major technology companies have built platforms that monetise attention by maximising emotional intensity, compulsive engagement and time spent online, despite growing evidence that these systems can damage children’s wellbeing. Children’s attention, behaviour and personal data have become commercial assets traded for advertising revenue at enormous scale.

The incentives underpinning advertising-driven platform models are fundamentally incompatible with child wellbeing because the safest and healthiest outcomes for children are often directly opposed to the commercial interests of the companies designing these systems.

Participants repeatedly argued that the national conversation around social media must fundamentally change. Parents involved in the consultation consistently described social media as harmful for children and argued that Government policy should begin from a clearer recognition that many current platforms are simply not suitable environments for young adolescents.

There was widespread agreement among parents that technology companies are knowingly incentivised to keep children on platforms for commercial gain. Participants repeatedly argued that major technology companies continue profiting from addictive systems while avoiding meaningful accountability for the harms caused to children and young people.

Parents also stressed that an under-16 social media ban should be viewed as a first step rather than a complete solution. Participants argued that broader cultural and political change is required to “claw back childhood” from platforms designed around addictive engagement and behavioural dependency.

Technology companies should not be permitted to deploy products at scale before demonstrating they are safe for children and young people.

This submission therefore supports:

- Legally enforceable safety-by-design duties.

- Greater user control over algorithmic feeds.
- Transparency requirements regarding recommendation systems.
- Stronger safeguards around disappearing messages and group chats.
- Restrictions on autoplay, infinite scroll and compulsive engagement features for children.
- Independent auditing of recommender algorithms used on children.

Section Three: AI Chatbots and Tools

The consultation process revealed widespread and rapidly normalising use of AI chatbots among children and young people, often with very limited understanding of the associated risks, highlighting its widespread unregulated use.

The evidence collection process revealed that AI chatbots and tools are often utilised as an advisory tool. Students across multiple schools reported using AI systems such as Snap AI and Microsoft Copilot for emotional support, such as dealing with homesickness, health and fitness advice, homework assistance and general life advice.

Students described using AI tools for emotional reassurance and stress management, including breathing exercises and wellbeing advice. Students generally expressed confidence that they could distinguish AI-generated content from reality and showed little concern regarding the absence of meaningful regulation surrounding these systems.

However, this submission believes that confidence is misplaced.

AI systems, especially chatbots, are increasingly functioning as emotionally responsive conversational companions and perceived authority figures for young users. Unlike traditional search engines, modern AI chatbots simulate human interaction, emotional understanding and personalised responses in ways that create entirely new safeguarding concerns.

The risks associated with these systems extend beyond misinformation alone and include growing concerns regarding emotional dependency, synthetic intimacy, manipulative conversational systems, data harvesting, harmful advice, deepfakes and AI-enabled abuse.

Students described AI-generated manipulated images being used as a tool for bullying and humiliation. This represents a rapidly evolving safeguarding challenge that existing anti-bullying frameworks are poorly equipped to address.

There are also serious concerns regarding the regulatory gaps currently surrounding chatbot technologies. Evidence provided during the consultation process highlighted that many AI chatbot systems remain outside the effective scope of the Online Safety Act where they are not classified as user-to-user services or search platforms.

The Government must therefore move much more quickly to establish a regulatory framework capable of responding to emerging AI harms, rather than kicking timelines for action down the road as set out in the Children's Wellbeing and Schools Bill. Children should not become the testing ground for emotionally manipulative or insufficiently regulated AI technologies.

As per our conversations, this submission supports:

- Require meaningful age assurance for AI chatbot services accessed by children and young people.
- Mandate clear disclosure when users are interacting with AI systems and what personal data is being collected, stored or used.

- Require robust moderation standards for AI-generated advice, particularly relating to mental health, wellbeing, self-harm, body image and medical issues.
- Introduce mandatory digital literacy and AI education focused on misinformation, synthetic media, privacy risks and the limitations of generative AI systems.
- Establish clear legal liability for companies whose AI tools are used to generate manipulated images, deepfakes or other abusive content targeting children.

Section Four: Enforcement, Ofcom and Age Assurance

A recurring theme throughout the consultation process was widespread scepticism regarding the effectiveness of existing online safety enforcement and deep frustration at what many participants viewed as a failure to hold technology companies meaningfully accountable.

Students repeatedly expressed little confidence that either Ofcom or current online safety legislation can constrain platform behaviour in practice. During one of the roundtables, students described Ofcom's current approach as consisting largely of "empty words and promises", arguing that the regulator appears reactive, slow and unable to impose meaningful consequences on major technology companies. Students consistently questioned whether existing penalties have any real deterrent effect on global platforms generating vast profits from engagement-driven business models.

Young people repeatedly argued that fines imposed on social media companies should be significantly heavier and more punitive. Several students also raised concerns that technology companies are effectively able to absorb financial penalties as a manageable operational cost while continuing to profit from harmful platform design. There was a strong feeling among participants that current enforcement mechanisms simply lack teeth.

A further recurring concern was that regulation currently focuses too heavily on headline restrictions while failing to address weak implementation and enforcement. Students questioned the effectiveness of bans or minimum age rules when existing verification systems are so easy to bypass. This reflects a broader sentiment that ineffective enforcement risks undermining confidence in online safety regulation altogether.

Participants repeatedly described children using false dates of birth, parents' details and other workarounds to circumvent age restrictions. Students also highlighted inconsistencies between different platforms and services, arguing that uneven standards create gaps that children quickly learn to exploit.

Several participants specifically raised concerns that streaming services and adjacent digital platforms are often held to lower standards than traditional social media platforms despite featuring livestreaming, recommendation systems, algorithmic feeds and interactive functionalities capable of creating similar harms.

The evidence gathered throughout this consultation strongly suggests that current age assurance systems are insufficiently robust and inconsistently applied. Voluntary or lightly enforced verification systems are no longer adequate for platforms knowingly accessed by large numbers of children.

This submission therefore supports:

- Meaningful and enforceable age assurance requirements for high-risk services.
- Substantially larger financial penalties for companies that fail to prevent underage access.
- Stronger enforcement powers for Ofcom.
- Escalating sanctions for repeat breaches.
- Significantly greater transparency regarding how platforms enforce age restrictions in practice.

However, participants also repeatedly stressed that better enforcement must be accompanied by better regulation. Young people consistently argued that online safety cannot rely solely on restrictions or bans while leaving harmful platform architecture fundamentally unchanged.

This submission therefore agrees with concerns raised by the Online Safety Act Network that many harmful functionalities currently under discussion had already been identified by Ofcom as potential risks under the Online Safety Act framework, yet decisive intervention has been limited. The issue is no longer a lack of evidence regarding harm. The issue is a lack of meaningful consequences for companies that fail to prevent foreseeable harms to children.

Several students also raised broader concerns regarding accountability and access to justice. Participants argued that young people and families should have stronger routes to challenge platforms directly where companies fail to protect users from harm, bullying or exploitation. This submission believes the Government should explore stronger legal mechanisms allowing individuals to hold technology companies accountable where systemic failures in safeguarding can be demonstrated.

The Government must therefore move beyond symbolic enforcement and create a genuinely credible regulatory framework capable of imposing meaningful consequences on technology companies that fail to protect children online. Without stronger enforcement, stronger age assurance and meaningful accountability, public confidence in online safety regulation will continue to deteriorate.

Section Five: Schools, Digital/Media Literacy and Family Support

Schools, parents and safeguarding professionals repeatedly described feeling overwhelmed and outpaced by the pace of technological change. Participants consistently raised concerns that responsibility for managing online harms is increasingly falling on families and schools while technology companies continue operating with insufficient accountability.

Parents participating in roundtables frequently described difficulties understanding emerging platforms, setting effective boundaries and monitoring children's online activity. Students reported that most parents placed very few meaningful restrictions on children's phone use or social media access. One Year 7 student explained that they would likely be "grounded" if they misbehaved online, but that there were no formal rules around phone usage, no screen-time monitoring and little active oversight of what platforms were being used or what content was being viewed.

At the same time, the evidence collection process also demonstrated that overly heavy-handed or purely surveillance-based approaches are often ineffective. Students repeatedly suggested that trust-based approaches and open communication between parents and children work better than excessive monitoring or punitive restrictions. Young people expressed particular concern that overly strict controls often simply encourage children to hide online behaviour or move onto less visible platforms.

Parents themselves acknowledged that broader social anxieties are contributing to increased screen time among children. Several participants discussed fears around "stranger danger", reduced outdoor independence and concerns regarding children socialising offline, all of which contribute to greater reliance on phones and online entertainment within the home. Many parents recognised that social media and smartphones are increasingly filling social and recreational gaps that previous generations experienced differently.

The evidence gathered also demonstrated significant shortcomings in current online safety education. Students repeatedly argued that education often comes too early, before children are actively engaging with social media or understanding the risks being discussed.

Online safety lessons were noted by students to be delivered years before many children begin actively using social media platforms, limiting their practical relevance and impact. Effective education must therefore be timely and delivered when students are actively navigating online spaces rather than years in advance.

There was also strong agreement that online safety education cannot remain a one-off intervention. Students repeatedly emphasised that platforms, technologies and online behaviours evolve too quickly for single assemblies or isolated PSHE lessons to remain effective over time. Education and safeguarding guidance must therefore be ongoing, regularly refreshed and responsive to rapidly changing technologies and risks.

Schools also described increasing pressures associated with safeguarding harms originating online but manifesting within educational settings. Participants discussed cyberbullying, manipulated images, harmful group chats and social exclusion linked to algorithm-driven trends. At one of the roundtables, every student participating stated that they knew someone who had experienced online bullying. Students also described hesitation around reporting abuse online due to fears that reporting would worsen bullying or increase social isolation.

Parents repeatedly stressed that they need clearer guidance and greater support. Many participants expressed uncertainty regarding which platforms present the greatest risks, how algorithms influence children's behaviour and how to set effective boundaries without resorting to constant surveillance.

Several parents specifically requested more practical guidance around approaches such as removing phones overnight, delaying smartphone access to 14-years-old, enabling parent-child co-viewing and establishing clearer family expectations around social media use.

This submission therefore supports:

- Stronger and more practical digital literacy education.
- Ongoing online safety education delivered at age-appropriate stages.
- Greater focus on harmful algorithms, AI systems and manipulative platform design.
- Clearer guidance and support for parents.
- Stronger support for schools managing online safeguarding issues.

It's important to note that digital literacy and parental support cannot substitute for meaningful regulation of technology companies themselves. Children should not bear sole responsibility for safely navigating systems deliberately engineered to maximise engagement and behavioural dependency. The burden of online safety must not continue falling disproportionately on families and schools while technology companies continue profiting from harmful platform design.

Conclusion

The evidence gathered throughout this consultation demonstrates that online harms affecting children and young people are systemic, widespread and deeply embedded within the design and commercial incentives of many online platforms. Students, parents and teachers consistently described a sense that regulation has failed to keep pace with technology companies whose business models are built around maximising engagement, attention and behavioural dependency.

Young people are growing up in an online environment shaped by addictive design, weak safeguards and insufficient accountability. Families and schools are increasingly being left to manage harms that they did not create and often feel powerless to prevent. While digital literacy, parental support and education all have an important role to play, they cannot substitute for meaningful regulation and enforcement.

The Government must now move beyond piecemeal interventions and recognise online safety as a public health and safeguarding issue requiring urgent action. This means stronger age assurance, enforceable safety-by-design duties, meaningful accountability for technology companies and a regulatory framework capable of responding to rapidly evolving technologies, including AI systems.

Children should not be expected to navigate systems deliberately engineered to exploit their attention and vulnerabilities without far greater protections in place. Nor should parents be expected to carry the responsibility of restrictions they are powerless to enforce. The burden of online safety must shift back towards the companies designing and profiting from these platforms, and the Government must legislate and ensure regulation – in short, acting with far greater urgency ensures children can grow up safely in the online world.

A handwritten signature in blue ink that reads "Monica Harding". The signature is written in a cursive style and is positioned above a thin vertical line.

Monica Harding MP

Liberal Democrat MP for Esher and Walton