



Department for
Science, Innovation
& Technology

Rt Hon Liz Kendall MP
Secretary of State for Science, Innovation and
Technology
22-26 Whitehall
London SW1A 2EG

www.gov.uk/dsit

15 July 2026

To: All MPs
House of Commons
London SW1A 0AA

Government Response to Consultation on “Growing up in the online world”

Dear Colleague,

Last month I announced a landmark package of measures to better protect children online. We announced that social media companies will no longer be able to offer their services to under-16s, introduced new restrictions on livestreaming and communications with strangers, and became the first country in the world to ban chatbots that offer sexualised content to children. We took these steps for a simple reason – to give children the best start in life, ensure their safety and wellbeing, and put power back in parents’ hands.

I said then that the announcement was not ‘one and done’, that further measures would be needed, and that I would set those out in July. Today I am writing to update you on the second part of the government’s formal response to the questions posed in the consultation. This is, however, far from the end of the story on online safety; technology is ever-evolving and we must and will continue to ensure that the safety of UK citizens comes first.

Protections for 16-and 17-year-olds

We recognise, and heard clearly through the consultation and national conversation, that the risks young people face online do not stop on their 16th birthday. We are particularly aware that at 16 and 17 young people should be especially focused on their futures, and on exams.

Ofcom evidence shows that 15- to 17-year-olds are among the heaviest users of online service. They spend on average 6 hours and 20 minutes online each day, and the time children spend online between 11pm and 5am increases with age. However, it is also important to recognise that, as they get older, young people rightly have more responsibility and agency. We need a graduated approach that both avoids a cliff edge at 16 and supports older children in making safe, informed choices about their experience online.

I can announce today that we will therefore require social media services to apply sensible default protections for 16- and 17-year-olds.



Overnight curfews

This includes default overnight restrictions between midnight and 6am, with push notifications muted during the curfew period. These measures will create natural stopping points, reduce engagement-maximising design, and help teenagers log off, sleep, study and spend time offline.

The pilots of different possible social media restrictions, which have now concluded, showed that nighttime curfews on apps helped some young people to establish healthier routines, improve sleep and time management, and spend more time offline. They also showed why the approach must be proportionate: effects were not uniform, some young people moved to other apps or activities, and older teenagers were more likely to see restrictions as socially disruptive. This is not a blanket curfew for 16- and 17-year-olds, but age-appropriate defaults that support healthier choices while preserving their ability to change their own settings.

Personalised feeds and autoplay

We have also listened to long-standing concerns about the risks of autoplay and personalised content recommender feeds. We know that these features encourage children to be online for longer. Autoplay means videos start or continue playing automatically without breaks or input from the user. Personalised feeds work by serving up content tailored to a specific user, often based on their individual activity and data, which is designed to capture and hold their attention. We are already tackling these harms for under 16s by restricting the ability for social media companies to offer their services to children of this age group.

Today, I am pleased to announce that we will go further on this to break the pattern of addictive recommended content for 16- and 17-year-olds by requiring autoplay and personalisation in recommender feeds to be turned off by default. These restrictions will extend to personalised advertisements which appear in a user's feed.

Whilst 16- and 17-year-olds can choose to turn these features back on, by making this a default setting, the government's aim is to give older teenagers more control on their social media experience without some of the most intense elements of persuasive design. This builds on existing protections under the Online Safety Act, which protect children from harmful content.

AI chatbots

The government is also taking further action on AI chatbots and their impact on children and young people. We heard through the consultation that chatbots can offer children benefits, particularly around education and creativity. But we also heard concerns about the novel risk emotional dependency can pose. We will therefore require mandatory breaks for under-18s using chatbots and will work with experts on how frequently, and for how long, these should happen.

I have said previously that there are serious concerns with other chatbots, including therapy chatbots. We will work with Department for Health and Social Care and the Medicines and Healthcare products Regulatory Agency (MHRA) to take stronger action on chatbots that may pose risks to children, through harmful, inaccurate or unverified mental health advice. We can

commit today to consider a full range of options, including, if necessary, banning certain services that present a threat to children where other regulatory and safety mechanisms are insufficient. We will ensure the regulatory system for AI medical devices supports children to access trusted, evidence-based support. This will ensure that, where children seek medical advice, they and their parents can be sure this advice meets certain standards and is safe.

We have always been clear that children should be able to benefit from the opportunities AI offers while being protected from harm and threats to wellbeing. We recognise that there is public appetite to do more on AI chatbots and how children use these, and the government reserves the right to take further action in this area.

Circumvention and Virtual Private Networks (VPNs)

As I said in June, we need to be clear-eyed about the fact that some children will get around the new rules banning social media platforms from providing their services to under 16s. Circumvention is a real and enduring challenge, and no single intervention will remove it altogether. Children may use a range of routes, from seeking help from parents or older friends, using someone else's account to more technical tools such as VPNs.

The evidence shows that VPNs are not the only or most common route for bypassing age checks. DSIT-commissioned research found that around 7% of 11- to 17-year-olds use VPNs primarily to access age-restricted websites, apps and games. The most common reason for children using VPNs was privacy, and many children said VPNs made them feel safer online. DSIT's research builds on the existing evidence base. Internet Matters, for example, found that the most common methods children had used to bypass age checks were entering a fake birthdate (13% of 9-16yos), compared to only 7% of children using a VPN.

Having considered the evidence and consultation responses, the government will not require VPN providers to age-assure users. VPNs are widely used for legitimate privacy and security purposes, including secure access to public WiFi, online banking, business systems and protection from tracking or fraud. There are also many technical and enforcement challenges specifically related to regulating VPNs.

We will put an onus on platforms in scope of the new restrictions to take robust steps to detect and prevent attempts by underage users to circumvent age assurance measures. I have already asked Ofcom to report by October on what highly effective age assurance looks like for determining whether someone is over 16 which will include an assessment of the robustness of age assurance methods at service-level. To build on this, I will ask Ofcom, with input from the Information Commissioner's Office as necessary, to conduct research into what more services can do to detect and prevent VPN use on their platforms, while protecting privacy and rights.

We will also engage VPN providers on voluntary action and strengthen guidance for parents through the Kids Online Safety Hub.

We will keep this area under close review and reserve the right to take further action on this, should evidence show that it is needed.

Support for children

Regulation must be backed by practical support that helps children develop the confidence, judgement and resilience they need to thrive online. The consultation showed strong support for media literacy as a core part of children's online safety, alongside stronger regulation and safer platform design.

We will work with the Department for Education to strengthen children's digital resilience and online safety as wider curriculum reforms are taken forward. The DfE will conduct a full consultation this year on what teachers, parents and pupils want from the curriculum and the support required as the curriculum is implemented from September 2028. Online safety is also a critical component of Relationships, Sex and Health Education where the curriculum has already been strengthened for first teaching from September 2026.

Work in schools will be complemented by government support for work delivered through youth organisations, libraries, community groups and civil society partners to help children build media literacy, critical thinking and online safety skills in trusted settings.

A safer online world should not only reduce harm; it should also help children find trusted, educational and age-appropriate content that supports their development, wellbeing and creativity. Consultation responses showed strong support for improving access to positive online experiences, with parents, carers, teachers and developmental experts viewed as the most trusted groups to help determine what constitutes high-quality online content. We will develop a package of non-legislative measures to promote positive online experiences for children which could include working with industry, experts and civil society to improve access to trusted, educational and age-appropriate content and make it easier for children and young people to discover. This work will be taken forward alongside wider government activity, including DCMS work on trusted news and high-quality media content in the digital age.

Support for parents

Parents and carers remain one of the most trusted influences on children's online behaviour and wellbeing. The consultation showed strong support for parental controls, with respondents calling for controls to be clearer, simpler, more consistent and easier to use across platforms and devices, alongside safer-by-default design.

We are building on initiatives such as the '*You Won't Know Until You Ask*' campaign and the [Kids Online Safety Hub](#), adding subjects including AI and healthy screen use, helping parents to build critical thinking skills and identify harmful content, as they prepare for the transition to more independent online participation.

We will work closely with the Department for Education and the Department of Health and Social Care as they develop guidance on the safe and positive use of devices for parents of children aged 5 to 16. We will also support adults to develop the digital skills and confidence they need through DSIT's wider digital inclusion work and updates to the Essential Digital Skills Framework.

Today's announcement completes the second part of the government's formal response to the consultation. We will now move at pace to implement our proposals, including laying the first regulations on the ban by the end of this year, with a view to them coming into effect in early 2027. I will deposit a copy of this letter in the Libraries of the House.

Yours sincerely,

A handwritten signature in black ink, reading 'Liz Kendall', written in a cursive style.

Rt Hon Liz Kendall MP
Secretary of State for Science, Innovation and Technology