Mozilla's response to the UK Department of Science, Innovation and Technology's Consultation "Growing up in the online world"

Executive Summary

Mozilla's mission is to keep the internet open, accessible, private and secure for everyone, including young people. VPNs and VPN-like features are essential privacy and security tools that protect all users, including children. Age-restricting them would undermine the very protections the Government seeks to strengthen.

The consultation's proposals on VPNs risk conflating circumvention tools with the privacy tools all users legitimately rely on. The evidence does not support the premise that young people are using VPNs primarily to bypass age assurance. Any age verification regime applied to internet services including VPN, email or cloud storage services access would affect every user, not only minors, and would introduce new data security risks at scale. Rather than restricting access to core internet services and privacy-preserving technologies, we believe that a holistic approach to online safety is needed.

About Mozilla

Mozilla is a non-profit-backed internet company with a mission to ensure the internet remains a global public resource that is open and accessible to all. Founded in 1998, Mozilla is best known for the Firefox browser, which serves more than 200 million users worldwide. The UK is a priority market for Mozilla, with over 4.25 million monthly active Firefox users on desktop and mobile, and approximately 7,000 Mozilla VPN subscribers. Mozilla's policy team is headquartered in London and has been pleased to engage with policymakers and regulators in the UK to ensure principles of safety, privacy and openness are at the heart of the internet and digital innovation.

Mozilla builds products that reflect its public interest mission. Unlike many large technology companies, Mozilla works to put people in control of their data and online experiences. Our data privacy principles are embedded into how our products are designed. This means we have a distinctive vantage point in this debate: we are a technology provider with direct experience of the trade-offs between privacy, security, access and choice online. We are grateful for the opportunity to contribute to the consultation and provide this experience.

Mozilla VPN, our standalone VPN product, launched in 2020 with the goal of providing device-level protection to help users control how their data is shared across their network. Separately, Firefox's built-in VPN feature, which launched in the UK on desktop in March 2026, routes users' web traffic through a secure proxy server. This free IP-protection feature helps users improve their privacy online as an easy-to-use tool directly embedded into the browser, demonstrating Mozilla's commitment to raising the bar for online privacy for all of our users. This feature is the latest addition to the suite of privacy protections offered by Firefox.

Firefox is built on the principle that not even Mozilla should know which websites users visit. This principle is extended to our VPN tools: we do not keep logs of the websites our users visit or the content of communications, and have limited visibility into how users engage with Mozilla VPN and Firefox's built-in VPN feature.

Firefox also offers a range of integrated privacy protections that are relevant to the safety and privacy of all our users, including young people:

- Enhanced Tracking Protection and Total Cookie Protection work together to block cross-site tracking, giving users more control over their data.
- Firefox also blocks fingerprinting, a type of online tracking that's more invasive than ordinary cookie-based tracking, consisting of profiling users based on their computer hardware, software, add-ons, and even preferences.
- HTTPS-Only Mode allows users to choose to only connect to websites via encrypted connections, enhancing user's privacy by protecting their data when connecting to a website.

These protections are available to all users without any account requirement, and they demonstrate that browsers can be designed to protect users by default rather than extracting data from them. Beyond specific features, we strive to empower our users by giving them choice and control, providing granular settings to opt into or out of using features, and processing data on devices where possible.

The Benefits of VPNs for Young People

VPNs are essential privacy and security tools for users of all ages. The consultation document itself acknowledges that "the main reason [minors use VPNs], as with adults, is to access the privacy and data protection benefits that VPNs offer." We welcome this recognition and urge the Government to treat it as determinative in its policy conclusions.

Based on user research Mozilla has conducted, we know that users engage with VPN products for core three reasons:

- Device-level protection: VPN services like Mozilla VPN create encrypted "tunnels" between a user's device and the internet, protecting all internet traffic from that device and concealing users' IP addresses.
- Added privacy: Over 50 percent of VPN users in the US and UK said that seeking protection when using public wi-fi was a top reason for choosing a VPN service. Students often use public or school wi-fi for homework.
- Enterprise use: Many employees, professionals and students rely on VPNs to connect remotely to networks owned by their employers, schools or universities.

Young people benefit from VPNs for the same reasons as adults. A VPN protects users from surveillance by their internet service provider, from network information-based tracking, and from interception on unsecured public wi-fi. Noted above, more than 50% of VPN users in the UK cited privacy protection when using a public wi-fi network as a top reason for choosing a VPN service. Students regularly connect to public or school networks for homework and research; VPN protection is a proportionate response to the genuine security risks this can create. VPNs are also commonly used in educational settings for accessing private institutional networks, a purpose that is clearly legitimate.

Young people are particularly vulnerable to online tracking, targeted advertising, and the risks that flow from personal data being collected and processed for commercial purposes without adequate consent or transparency. These harms originate in platform design choices. Research has found that 80% of popular children's apps contain manipulative design features with children from lower socioeconomic backgrounds affected more so. A growing body of evidence, recognised by both the ICO and CMA in their joint work on harmful online choice architecture, also confirms that dark patterns engineered to maximise engagement cause concrete harm to users, with children particularly exposed given their developing capacity to recognise and resist manipulative design. The surveillance advertising business model, as noted by Global Action Plan, incentivises algorithmic systems that maximise time on platform to generate data and serve ads, to the detriment of all other considerations including user wellbeing.

VPNs and VPN-like features that limit the exposure of users' IP addresses and browsing behaviour to third parties are one of the strongest tools available to young people from the harms of indiscriminate, opaque or non-consensual data collection and processing. Restricting young people's access to these tools would therefore work directly against their privacy and safety online. It would remove a layer of protection from precisely the users the Government is seeking to protect, while doing nothing to address the platform conduct that generates harm in the first

place. The protections children need are protections from the platforms collecting their data, not restrictions on the tools they use to shield themselves from that collection.

The argument for VPN access also aligns with the Government's own stated ambitions around digital skills and preparing young people for a digital future. Understanding and using privacy tools is a key aspect of digital literacy. In a world in which young people are exposed to digital technologies as part of their realities from young ages onward, restricting young people's access to privacy-protecting technologies is in tension with the goal of equipping them to navigate the internet safely and competently. In order to be able to develop agency and responsible habits in engaging with digital technologies, it is crucial for young people to be exposed to best practices and key safety and privacy tools as they engage with the online world.

Circumvention is a marginal reason for using VPNs

Regarding the concern that VPNs are used for circumvention age restrictions, the data on why children use VPNs does not support this narrative. A study published by Internet Matters in December 2025 found that only 8% of children had used a VPN in the past twelve months, and of those, 66% did so to protect their personal data. Childnet found that 38% of child VPN users reported using one to stay safe online. Further evidence from the Australian eSafety Commissioner shows that less than 7% of those surveyed said that they believed their child still held an account across age-restricted social media platforms because of VPN use. This is corroborated by findings from a May 2026 study by Internet Matters that found that only 7% of children used a VPN to circumvent age restrictions. These figures suggest a user population motivated primarily by legitimate privacy and security concerns, with users relying on VPNs to circumvent age restrictions presenting as an edge case. The Government should be cautious about designing policy responses to edge cases that the evidence does not show to be the dominant use.

The recently published Compliance Update by the Australian eSafety Commissioner on the enforcement of the social media minimum age obligation emphasises this. The Compliance Update reports consistent strong signals of under 16 year-olds using age-restricted social media platforms. In reporting on the reasons underlying this trend, the Compliance Update notes that the most common explanation for why children still had access to social media platforms was that they had not been asked by the platform to prove their age. The Commissioner also found that platforms were offering users that had self-declared their age as under 16 the opportunity to undergo age assurance to "correct" their age in case a wrong age had been submitted, resulting in users passing low-confidence age assurance processes and gaining access to unrestricted accounts. The May 2026 study from Internet Matters provides additional insights, documenting that most young users circumvented age restrictions by entering a fake birthdate or using parents' or older siblings' log-ins or devices (8%). The same study also reports anecdotal evidence from children successfully circumventing age assurance systems by drawing facial hair on themselves.

These are just some examples that show that circumventing age restrictions does not require access to tools like VPNs, and that restricting VPN access would likely not be a meaningful mitigation to age gate circumventions.

The consultation itself notes that the spike in VPN usage following age assurance requirements "does not suggest the peak in VPN use was driven by children seeking to bypass age assurance

processes." This suggests that VPN spikes are driven by legitimate users uneasy about providing identity documents to platform providers they did not fully trust to properly protect that sensitive information, rather than children seeking to bypass age checks. Restricting VPNs would therefore do little to prevent circumvention, while reducing access to privacy and security tools for users of all ages who rely on them for entirely just purposes.

The Consequences of Age-Restricting VPNs

Age restrictions would undermine the privacy and security of all users

The central problem with age-restricting VPN access is structural. Any age assurance system applied to a VPN service would affect every user, not only minors. There is no mechanism by which a VPN provider can determine which users are minors without verifying the age of all users. Requiring age verification for VPN access therefore means requiring every user, regardless of age, to provide sensitive personal data before accessing baseline privacy protections. Depending on a user's situation, this may leak age-related information beyond the VPN provider or a third-party age assurance provider. Especially in enterprise contexts, including schools, universities and workplaces, a user's IT environment might include software that logs or inspects traffic and would therefore be in a position to have unintended access to age-assurance related information.

This creates a fundamental tension with the Government's own objectives. The consultation is concerned with protecting young people online; age-restricting VPNs would remove a tool that children use primarily for privacy and safety. It would also harm adults for whom privacy is an operational necessity: journalists protecting sources, public servants requiring high levels of online privacy and security, domestic abuse survivors concealing their location, and others for whom submitting identity documents and other sensitive data to a VPN provider would directly defeat the purpose of using one.

The risk of data exposure created by mandatory age verification is concrete. The 2023 Discord data breach, which leaked the ID photos of 70,000 users, illustrates what happens when age assurance obligations require the collection of sensitive identity documents at scale. Age estimation using biometrics carries additional risks: facial estimation systems often underperform for people with darker skin tones, women, and those with non-binary or non-normative facial features due to biased or limited training datasets. The technology is thus error-prone and introduces new vectors for discrimination and miscategorisation.

Age restrictions would be technically unenforceable and counterproductive

Age-restricting VPNs through a regulatory mandate would face significant challenges in practice. As mentioned, VPN traffic resembles normal encrypted internet traffic, and it is extremely difficult for government or network-level authorities to distinguish between compliant and non-compliant VPN providers, or to block access to unregulated services without affecting legitimate traffic. Any regime that successfully restricts regulated VPN providers would therefore create a competitive advantage for unregulated, non-compliant services, which are far more likely to expose users to privacy and security risks.

The evidence from comparable policy interventions bears this out. Research on age verification in gaming found that 77% of minors surveyed evaded restrictions by registering under the names of older relatives or friends, and that enforcement attempts themselves created new vulnerabilities including a black market in accounts resulting in significant financial harm to minors. Separate research on social media platforms found that 82% of parents of ten-year-olds on one major platform had actively helped their children to create accounts, and that more than half believed age limits were advisory rather than legally binding. The lesson is that technical age restrictions alone, without changes to platform design and practices, and societal norms, do not achieve the underlying policy goal.

Age restrictions risk creating a two-tier internet

Setting aside the privacy implications of data collection or age verification purposes for all users, age gating VPN access would in practice create a two-tier internet: one in which adults retain access to privacy-preserving technologies, and one in which minors are excluded from those same protections. As we have noted, this undermines a growing body of evidence that young people are particularly vulnerable to online tracking, targeted advertising and risks from their personal data being collected, processed and shared for commercial purposes without sufficient consent – harms VPNs and VPN like features can protect against. Stripping young people from safe ways to access credible and legitimate privacy tools is contrary to the spirit of the consultation's own stated goal of enriching children's digital lives. It would disproportionately affect children from households without the resources to access alternative privacy tools, and children in circumstances where online privacy is particularly important, such as those in care, those experiencing domestic abuse, or those in communities facing discrimination.

The Government should also consider the international dimension. Restricting VPN access in the UK would set a precedent that other jurisdictions could use to justify their own restrictions on VPN access. The UK has a strong tradition of supporting a free and open internet; a policy that restricts access to privacy tools for a category of users is at odds with this and could have potentially drastic effects.

Overall, policy should be calibrated to the predominant use case, not the marginal one. Where the evidence shows that the overwhelming majority of young VPN users are motivated by privacy and security, designing restrictions around the minority who may be circumventing age gates is a disproportionate response that harms the many to address the behaviour of the few.

Alternative Policy Directions

Mozilla supports the Government's ambition to improve children's safety online and recognises the complexities this consultation addresses. Our concern is that proposals relating to VPN access restrictions would not achieve this ambition, and would instead create significant new harms. We have therefore set out below three alternatives which ensure more proportionality, are more technically workable, and are more likely to achieve the Government's stated objectives.

Stronger enforcement of existing platform obligations

The evidence consistently shows that the harms this consultation is concerned with, including exposure to harmful or age-inappropriate content, contact with strangers, and compulsive use driven by algorithmic design, originate in platform choices, not in VPN access. Addressing these harms therefore requires enforcement action targeted at the platforms and business models generating them, rather than blanket requirements imposed across all online services.

The Online Safety Act already provides for this. It imposes significant obligations on services in scope, including requirements to assess and mitigate risks from harmful content, addictive design features, and inadequate moderation, whilst also affording platforms the proportionality and space for innovation needed to address the specific risks that stem from their own services. Mozilla urges the Government and Ofcom to use the enforcement powers available under the Act to hold platforms accountable for meeting these obligations.

Encourage the use of parental controls

The most proportionate and technically workable protections for children online are those that operate at the point of use, on the devices children actually use, rather than at the level of network infrastructure. Device-level parental control allows parents or guardians to block specific websites and downloads in ways that children cannot override themselves.

This approach is better targeted, focusing protective measures on the child's own device rather than imposing blanket requirements on infrastructure used by millions of adults for legitimate privacy and security purposes. Parental controls come with their own challenges, particularly in situations in which parents seek to control their children's access to critical resources, for example on political, identity or sexual health related issues. However, parental controls can be an important tool to give parents agency to calibrate their child's online experiences depending on their child's age, maturity, and circumstances.

Despite the flexibility they offer families in managing access to content and media, parental controls remain underutilised. According to a 2025 study by FOSI, adoption of parental controls varied widely. The Government should invest in raising awareness of existing parental control tools, ensure that device manufacturers and browser providers are required to make these tools accessible and easy to use, and consider whether current defaults, particularly on devices marketed to or commonly used by children, adequately reflect child safety objectives. Relying on on-device parental controls also tend to be safer than third-party parental control apps which have experienced data breaches and often entail features that facilitate the granular surveillance of children, risking their privacy and security. Investing in awareness training and education on parental controls would deliver meaningful, targeted protection without the disproportionate collateral harms that age restricting services like VPNs would produce.

Investment in digital skills and a whole-society approach

Sustainable improvements in children's safety online require more than technical restrictions on individual technologies. Circumvention follows restriction, and enforcement races against ingenuity. Without a broader foundation of digital resilience, piecemeal technical interventions will not deliver lasting change.

Mozilla supports significant investment in digital literacy as part of a whole-society approach. This means more than adding media literacy modules to school curricula: it means equipping parents and educators with practical tools and guidance, investing in mental health support and social infrastructure for young people experiencing harm online, and enabling meaningful conversations between young people and trusted adults about the risks and opportunities of the digital world.

Building resilience across society rather than attempting to restrict access to particular technologies is the approach most likely to achieve lasting improvements in children's wellbeing online.