VPN Industry Statement
on VPNs and Age Verification in the UK

For the UK Government consultation on "Growing up in the online world" and interested stakeholders

The goal of protecting children online is shared across industry, government and wider society. Achieving that goal requires solutions grounded in how the Internet actually works.

Regulating VPNs as an enforcement mechanism risks severe and damaging unintended consequences. It would undermine cybersecurity, create new privacy risks, result in the overblocking of legitimate content, and fail to prevent the circumvention of harmful content. Closing perceived loopholes by regulating VPNs would undermine widely-used security tools while failing to deliver any meaningful enforcement.

The VPN Trust Initiative (VTI) and the undersigned members of the VPN industry fully support evidence-based approaches to improving online safety for children. We share the goal of reducing underage access to harmful content and recognise the importance of effective measures to address this

Discussions about age assurance and new regulatory powers are ongoing, including the Government's consultation on "Growing up in the online world." It is therefore important to distinguish clearly between effective approaches to online safety and those that risk undermining core Internet security tools without delivering any real benefits.

The VPN Trust Initiative and its members will engage constructively in this consultation process to help ensure that future measures are grounded in technical reality. We also encourage stakeholders across industry and wider society to participate in the consultation.

VPNs are core security infrastructure, not circumvention tools

VPN technology is widely used across society to secure communications and protect sensitive data. Businesses rely on VPNs to protect trade secrets and customer information. Universities and schools depend on them to provide secure access to learning resources and internal

systems. Journalists, lawyers, healthcare professionals, government officials, legislators, and other public servants regularly use VPNs to protect confidential communications, and are often required to do so.

Families and young people also rely on VPNs. Students use them to access university networks safely from home and on public Wi-Fi. Young people use VPNs to reduce their exposure to tracking, scams, and harassment. Vulnerable teenagers, including LGBTQ+ youth, children experiencing domestic abuse, and those seeking sensitive health or counselling information, often rely on privacy tools to explore the Internet safely.

Treating VPNs primarily as a “loophole” is a complete misunderstanding of their role. The same encrypted technology used to protect corporate and government networks helps individuals protect their own privacy and security. Policies that weaken or restrict VPNs risk reducing online safety for the very users these proposals are intended to protect, without delivering commensurate benefits.

Regulating VPNs risks unintended consequences

The policy goal behind the proposals is clear and well-intentioned: lawmakers want to prevent children from bypassing age-verification measures. However, there is limited evidence that children are using VPNs at scale to bypass age-verification measures, including in jurisdictions where such systems have been introduced. Available research suggests that increases in VPN usage following the introduction of age checks are not primarily driven by children, and that children are not adopting VPNs in significant numbers for this purpose. (See, for example, research by Childnet and Internet Matters on children’s use of VPNs.)

At the same time, we of course recognise that the current evidence base is still developing. The VPN industry is committed to working with researchers and policymakers to better understand patterns of use and to contribute data where appropriate to inform future policymaking.

A VPN connection prevents services from reliably determining a user’s physical location by design, because the service sees the VPN server rather than the user’s underlying network. Any requirement to block “UK VPN users” would therefore force services into one of two outcomes: blocking *all* VPN traffic globally, despite the fact that services cannot reliably identify all VPN traffic, or withdrawing services from the UK entirely. Neither outcome improves child safety.

Requiring VPN providers to conduct age verification themselves raises a different but equally serious issue. Consumers use VPNs for privacy and security, and reputable VPN services are intentionally designed to minimise data collection and avoid storing personal information. This is a core cybersecurity and privacy principle which allows customers to reduce the risk of data breaches, prevent misuse of sensitive data, and ensure the service itself cannot be turned into a tool for surveillance: the less sensitive data a service holds, the less data can be stolen, leaked, compelled or misused.

Mandating age verification would require VPN providers to fundamentally change how their services operate and introduce identity verification mechanisms into services that are intentionally designed to minimise data collection and avoid linking user identity to network activity. Even where age verification is performed by a third-party provider and identity documents are not retained, VPN services would still be required to collect personal information, integrate with verification systems, or associate age credentials with accounts. These changes would undermine the vital privacy-preserving architecture of VPN services while introducing new cybersecurity and data protection risks.

Adults have legitimate reasons to use VPNs; including protecting themselves on public Wi-Fi, safeguarding sensitive communications, and reducing exposure to tracking and cybercrime. If reputable VPN providers are required to implement intrusive verification systems, some users will inevitably seek alternatives that promise anonymity without verification. These services often operate in the “Wild West” outside regulatory frameworks, and may rely on aggressive data collection, malware, or deceptive practices. The result is not the elimination of VPN use, but a shift toward less trustworthy and harder-to-regulate services. In this way, broad restrictions risk weakening rather than strengthening the cybersecurity of ordinary Internet users.

Even if commercial VPN providers were age-regulated, determined users would still be able to bypass age-verification systems using widely available tools. VPN functionality can be created using common cloud and hosting services or through remote-access and tunnelling capabilities already built into mainstream software. Other widely-available privacy networks such as Tor can also provide similar functionality.

It is entirely right that legislators should want to reduce childrens’ access to inappropriate content. However, regulating commercial VPN providers would primarily affect ordinary users and reputable security services, leaving the most determined users able to bypass restrictions using general-purpose technology or migrating to untrustworthy services. The result would be significant collateral damage without achieving the intended policy goal.

As policymakers consider future measures through the current consultation process, it is important that any approach to age assurance remains focused on effectiveness, proportionality, and technical feasibility. Measures that extend to general-purpose Internet infrastructure risk introducing broad unintended consequences without addressing the underlying policy objective.

Age verification is most effective at the content and platform layer

International experience shows that governments can pursue age assurance without targeting Internet infrastructure. For example, Australia’s online safety regime places responsibility on platforms and content providers to take reasonable steps to implement age-assurance measures. Policymakers there acknowledge that circumvention tools may exist, but treat this as a risk to manage rather than a reason to regulate encryption or infrastructure providers.

This approach recognises an important distinction. Measures aimed at the content and platform layer can be adapted and improved over time. Extending enforcement to content-neutral

security infrastructure risks destabilizing the technical foundations that support the digital economy. If the scope of services subject to age verification were nonetheless considered for expansion, a single, centralised mechanism at the services distribution layer, such as app stores, would be the most proportionate approach, enabling age assurance to occur once rather than being replicated across individual services.

A constructive path forward

The VPN Trust Initiative and members of the VPN industry stand ready to work with policymakers on effective approaches that improve child safety without undermining essential security tools. Evidence-based approaches include platform and app-store accountability, device-level parental controls, age-appropriate service design, and digital literacy and family support measures. We intend to provide further input through the consultation process and welcome continued engagement with policymakers and stakeholders.

As the Government considers next steps through its ongoing consultation, we encourage policymakers, industry participants, and civil society organisations to engage in this process and help ensure that future measures are evidence-based, proportionate, and effective; rather than promoting unintended and damaging consequences.

Sincerely,

The VPN Trust Initiative (VTI)