Consultation response: children's online safety

About Defend Digital Me

Defend Digital Me is a non-profit call to action for safe, fair and transparent data processing, focused on the rights of learners in the digital environment in education, in England and beyond. More at https://defenddigitalme.org.

Sections covered: age gating measures and technology; the "digital age of consent" (Q8–Q11) and enforcement and compliance; and VPNs (Chapter 3)

The print-ready and HTML versions of the consultation use different numbers for the same questions; the question wording is reproduced below so the mapping is unambiguous.

The implications of age gating any access in the digital environment

Defend Digital Me has carried out assessment of the implications of the Australian social media minimum age restrictions for children's privacy and data protection, and has published findings in a report. This will be digital-only and updated with version-control on a rolling basis, as more information becomes available.

https://defenddigitalme.org/age-gating-the-internet-id-and-children/

Defend Digital Me. (2026). *Age Assurance Technology in the context of the Australian Social Media Ban and emerging European proposals: the implications for children's privacy and data protection rights*.

Australia and the UK have both adopted a restrictionist mentality without first being able to provide a clear or satisfactory definition of social media. While Australia has a narrower approach - banning particular services that fulfil certain criteria - the UK seems poised to take much more complex and far-reaching measures. This could include restricting certain functionalities and features with different age limits, which would create a complicated online landscape (CRIN, 2026b).

"Age of digital consent" (Q8–Q11)

Preliminary point. Article 8 of the UK GDPR is frequently, but wrongly, described as a "digital age of consent." It is neither a minimum age at which a child's data may be processed nor a minimum age for using social media. It is engaged only where both (a) the lawful basis is consent under Article 6(1)(a) and (b) the processing is by an information society service (ISS) offered directly to a child; in that narrow case it sets the age above which a child may consent for themselves rather than a parent authorising it — 13 in the UK (ICO, n.d.; Persson, 2026). Although a great deal of space is given over to this subject in the consultation, changing the age of consent would not affect online services that do not rely on consent as their legal basis for processing. Where a service relies on contract or legitimate interests instead, Article 8 never applies and no age gate is required by the GDPR

(Persson, 2026). Article 8 of the GDPR is the wrong instrument to use to attempt to facilitate change on any social media minimum age or restriction (“ SMMA”).

Q8. At what age do you think the age of digital consent in the UK should be set for information society services?

Answer: e. Other.

The question cannot be answered as framed. There is no “digital age of consent” to set. If forced to a number, we would retain 13, because raising it does not achieve the stated policy aim and actively worsens data protection outcomes (see Q9). The substantive position is that Article 8 should not be the instrument at all (Persson, 2026).

Q9. What risks or burdens may be associated with raising the minimum age of digital consent? (e.g. ensuring parental consent, costs to industry, access to services, volume of requests)

Raising the Article 8 age increases the processing of personal data rather than reducing it — the opposite of the consultation’s protective intent (Persson, 2026).

Parental consent — more data, for longer, from more services. Below the threshold a parent must authorise consent and supply their own personal data to verify it. Raising the age means more parents’ data is processed for more years, until each child reaches the higher limit, and across all consent-reliant ISS (search, gaming, edtech, marketplaces), not only social media where consent is the basis for data processing but everywhere. Parental tick-box authorisation is also a poor proxy for freely given, informed consent (Persson, 2026; ICO, n.d.).

Consent is invalid. The proposed powers (pp. 4–6) to alter Article 8 by regulation, without consultation or evidence, conflate compulsory data processing (ID/age checks bundled into a service) with a freely given consent process. Bundled or compulsory “consent” is not valid consent (Recitals 42–43; EDPB, 2020), so the mechanism is flawed at source (Persson, 2026). This also undermines the validity, both legal and ethical, of the argument that biometric data processing in age-verification obligations operate on a consent-based legal basis. The high bar required for children’s biometric data processing should not be lowered nor normalised in order to protect children for life into adulthood.

Evidence from Australia indicates the 'ban' policy is failing on its own terms: 61% of 12–15-year-olds who previously had accounts retain access, 70% of those still using restricted sites found it "easy" to circumvent, and half report no difference to their safety (Molly Rose Foundation, 2026), echoing a comparable Korean night-time gaming curfew that researchers found increased young people's online hours (Lee et al., 2017). What such a regime reliably produces is the normalised, lifelong biometric processing of children at scale, removing their adult autonomy to refuse later.

Children’s privacy. Age-Gating younger children specifically expands state data access**.** The Australian Age Check Certification Scheme Trial found that exact age verification for children is “constrained by limited access to hard data,” and that improving precision would require government-backed blind-access APIs to records such as schools and healthcare (Age Check

Certification Scheme, 2025). Raising the age and gating younger children therefore drives expansion of commercial access to children's ID and verifiable records, another data-expansion not minimisation for protection.

Volume of requests. Each additional cohort year pulled below the threshold multiplies parental-authorisation and verification events across every consent-reliant service a child uses — repeated checks per service, per child, per year — a large, recurring processing and administrative load with no corresponding protective benefit.

Access to services. A service cannot apply an age threshold without first processing data that reveals age, so raising it compels more identification, not less. This is the opposite of data minimisation, required for children in Recital 38, and Recital 57. In practice it pushes toward "robust" age verification requiring a state-authorised identity credential, which not everyone in the UK holds, risking exclusion from ordinary services (Persson, 2026).

Necessity and proportionality. Restrictions on children's rights (privacy, expression, access to information) are lawful only where necessary and proportionate — effective at the aim and the least restrictive means. Raising the Article 8 age fails both: it does not reduce most processing and is more intrusive than alternatives such as enforcing the Age Appropriate Design Code (CRIN, 2026b).

Liable to backfire. In 2026, 438 experts from over 30 countries warned that social-media bans and age checks can backfire, citing easy circumvention, migration to riskier fringe sites and years-long infrastructure hurdles, and called for a moratorium pending clearer evidence (438 Signatories: Joint statement, 2026).

Q10. What should be considered to make raising the digital age of consent effective and workable?

The approach needs reframing rather than tuning, because Article 8 is the wrong vehicle. We recommend replacing Q8–Q11 with the following (Persson, 2026):

Do not use Article 8 to restrict social media access. Data protection law regulates how controllers process data; it does not govern who may access content. Where a platform relies on contract or legitimate interests rather than consent, Article 8 is never engaged, so changing the age has no effect on most processing.

Separate any platform-access restriction from data protection law entirely. As in Australia, place any age-based account restriction as an obligation on designated platforms, not on the child or parent, and not via Article 8 (Persson, 2026; CRIN, 2026c).

Enforce the existing regime through the Age Appropriate Design Code: prohibit personalised targeted advertising and real-time bidding (RTB) for children's data — RTB is structurally difficult to reconcile with the GDPR's requirements for a lawful basis, transparency and security, and regulatory intervention is necessary (Veale & Zuiderveen Borgesius, 2022); strictly limit retention of data collected from or about children, and resolve whether the "child's data" label persists after 18; and require algorithmic impact assessments for youth-facing services as part of the existing DPIA duty (Persson, 2026).

Avoid the cliff edge. Age-threshold approaches create a sudden jump from a sanitised environment to full access with no graduated development of capacity, contrary to the CRC's "evolving capacities" principle — a further reason to favour design-and-enforcement duties over a raised consent age (CRIN, 2026b).

Avoid the paradox of processing more data (age verification plus linked parental ID) in order to protect children from data processing. Favour attribute-based, minimal-disclosure age assurance over hard identifiers, consistent with data protection by design and the ICO's stated preference for attribute systems (ICO, n.d.; Persson, 2026).

Q11. To what extent do you agree or disagree: "There is a case for changing the digital age of consent for some online services but not others"?

Answer: d. Somewhat disagree — as to mechanism.

There may be a case for regulating a designated set of high-risk platforms differently from the wider web, but this cannot be achieved by "changing the digital age of consent." Article 8 is horizontal: it applies uniformly to every ISS that relies on consent and cannot be switched on or off service-by-service. Attempting service-specific outcomes through it would either fail (because many services do not rely on consent) or sweep in vast numbers of unrelated services. Service-specific restriction, if pursued, should be done through a platform-obligation framework, not data protection law (Persson, 2026; CRIN, 2026c).

Virtual Private Networks "VPNs"

Which option should the government prioritise to reduce circumvention of online safety rules in the UK?

Answer: More education for children.

Restricting access to VPNs would not meaningfully reduce circumvention — a May 2026 UK study found only 7% of children use VPNs to get around age checks, and the methods above mostly do not involve a VPN at all (CRIN, 2026a). It would also be technically futile: VPNs are core internet infrastructure used by governments and businesses, and cannot be fully banned, because skilled users (or anyone willing to provide a service to children) can self-host one on a cheap rented cloud server in minutes, so users simply migrate to smaller, less trustworthy providers (CRIN, 2026a). Education, alongside genuine conversations with children about appropriate VPN use and enforcement of existing data protection duties (RTB/targeted-advertising prohibition, data minimisation, the Age Appropriate Design Code), addresses harms directly without building circumvention-driving identity infrastructure (CRIN, 2026a; Veale & Zuiderveen Borgesius, 2022).

VPN bans and platform blocking are overwhelmingly the tools of authoritarian states that promote censorship and surveillance. The more restrictive and ID-dependent the gate, the stronger the incentive to migrate to smaller, less-moderated spaces. Circumvention does not make children safe; it tends to move them somewhere worse while removing platforms' incentive to make mainstream services safe for the children who remain (CRIN, 2026a; CRIN, 2026b).

To what extent do you agree or disagree: "Everyone should go through age checks to access a VPN if it would prevent children using them"?

Answer: Strongly disagree.

See CRIN. (2026d). *VPNs for children: Villains, Predators, Nastiness? More like Visibility, Privately Negotiated.* https://home.crin.org/the-big-debates/vpns-for-children

The conditional ("if it would prevent") is false. It would not, given non-VPN circumvention routes and the availability of offshore and self-hosted VPNs outside any UK regime. The statement therefore asks the entire adult population to surrender anonymity on a basic security tool for a measure that is both disproportionate and ineffective. VPNs are a fundamental cybersecurity technology — protecting data on public Wi-Fi, securing remote corporate access, and shielding journalists, activists and at-risk users, children among them. Gating them behind state-ID-linked age checks attaches a verified legal identity to precisely the traffic people use VPNs to keep private.

It is notable that the countries which heavily restrict VPNs — including Belarus, China, Iran, Russia and the UAE — do so to control what citizens can see, not to protect children (CRIN, 2026d).

What do you think the impacts would be if VPNs were age-restricted?

Privacy and data for all users. Age-restricting VPNs requires identifying everyone who uses one, attaching a verified identity to the very tool meant to prevent that linkage and creating a high-value "who uses privacy tools" dataset — inverting the technology's purpose.

Children's safety and wellbeing. Minimal protective benefit (children have many non-VPN routes and would migrate), while children who legitimately rely on VPNs lose real protection: safety on public Wi-Fi against location/identity exposure and "evil twin" networks, reduced risk of targeted attacks, protection from ISP tracking and data-selling, and — for some — access to support, sexual-health or LGBT+ information and freedom from surveillance. Some VPNs also bundle parental filters, so a restriction could remove a tool parents use.

Parents and carers. Another verification burden and another identity dataset to manage, with no offsetting reduction in the methods children actually use.

Business costs, revenue and innovation. Age-assurance compliance and liability fall on providers; legitimate corporate, security-research, journalistic and remote-working uses are caught; UK providers are disadvantaged against offshore and open-source alternatives outside the regime, pushing usage to less accountable services.

Security, population-wide. Discouraging or gating VPN use weakens everyday security hygiene (public Wi-Fi, secure remote access) for adults and children alike.

Equity. Restriction would disrupt democratising uses — accessing educational and other resources from anywhere — that help bridge socioeconomic divides.

What should be considered to make age-restricting VPNs effective and workable?

We do not consider it can be made effective or proportionate, for the technical and rights reasons above, and recommend it not be pursued. The evidence on access-gating of this kind is poor: South Korea's 2011 midnight–to–6am gaming shutdown for children produced negligible effects on time online, academic performance or sleep, and was repealed (CRIN, 2026c). If the government nonetheless proceeds, it must address:

Legitimate uses. Robust carve-outs for corporate, security, journalistic, research and at-risk-user contexts — though these are very hard to operationalise without defeating the privacy purpose, which itself argues against the measure.

Technical futility. Self-hosted, open-source and offshore VPNs, and operating-system-level VPN features, sit outside any UK gate; a measure this easily circumvented cannot satisfy a proportionality test.

Accessibility and equity of age assurance. Methods must not exclude the substantial population without state ID, and must not standardise on hard identifiers; attribute-based, minimal-disclosure assurance (a yes/no over-age signal) should be the ceiling, consistent with data protection by design and the ICO's preference for attribute systems over passport/credit-card collection (ICO, n.d.).

Public trust and engagement. Extending age assurance into general-purpose privacy and security tools is likely to erode trust and push adoption toward less safe alternatives; the chilling effect on legitimate privacy-protective behaviour should be assessed first (CRIN, 2026a).

Data protection law. Any scheme must satisfy data minimisation (Recital 38) and Recital 57 — controllers should not acquire additional identifying data solely to comply — and avoid the paradox of processing more identity data to protect people from data processing (Persson, 2026).

References

438 Signatories: Joint statement of security and privacy scientists and researchers on Age Assurance (March 2026) https://csa-scientist-open-letter.org/ageverif-Feb2026

CRIN. (2026a). *To ban or not to ban?: That should not be the question*. https://home.crin.org/the-big-debates/to-ban-or-not-to-ban-that-should-not-be-the-question

CRIN. (2026b). *Banning what exactly? The quicksands of defining social media*. Child Rights International Network. https://home.crin.org/the-big-debates/banning-what-exactly-the-quicksands-of-defining-social-media

CRIN. (2026c). *Letting kids on social media is like sending them to Mars (and other bizarre analogies).* https://home.crin.org/the-big-debates/letting-kids-on-social-media-is-like-sending-them-to-mars-and-other-bizarre-analogies

CRIN. (2026d). *VPNs for children: Villains, Predators, Nastiness? More like Visibility, Privately Negotiated.* https://home.crin.org/the-big-debates/vpns-for-children

EDPB (2020). *Guidelines 05/2020 on consent under Regulation 2016/679*. European Data Protection Board, 4 May 2020.

ICO (n.d.). *What are the rules about an ISS and consent?* Children and the UK GDPR. Information Commissioner's Office. https://web.archive.org/web/20260526214348/https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/children-and-the-uk-gdpr-old/what-are-the-rules-about-an-iss-and-consent/

Molly Rose Foundation. (2026). *Australia's social media ban – is it working?* Molly Rose Foundation. https://mollyrosefoundation.org/wp-content/uploads/2026/04/MRF_Australia-Social-Media-Ban-Research_Briefing-April-26.pdf

Persson, J. (2026). *There is no such thing as "the Digital Age of Consent". The national consultation: kids online and UK government powers (1)*. 5 March 2026.

Veale, M. & Zuiderveen Borgesius, F. (2022). Adtech and Real-Time Bidding under European Data Protection Law. *German Law Journal*, 23, 226–256. https://doi.org/10.1017/glj.2022.18

Legislative references

UK GDPR, Article 6(1)(a) (consent), Article 8 (conditions applicable to a child's consent in relation to information society services), and Recitals 38, 42, 43, 57 and 58.

Data Protection Act 2018, s.9.

Directive (EU) 2015/1535, Article 1(1)(b) (definition of an information society service).

Defend Digital Me

May 26, 2026