CIPL's Response to the OPC Draft Guidance on "Assessing whether and how to use age assurance – Guidance for websites and online services"

Submitted 31 July 2026

The Centre for Information Policy Leadership (CIPL)[1] welcomes the opportunity to respond to the consultation by the Office of the Privacy Commissioner of Canada (OPC) on its Draft Guidance on "Assessing whether and how to use age assurance – Guidance for websites and online services" ("the Draft Guidance").[2]

CIPL recognizes the importance of designing and delivering appropriate online environments for children. We have continuously worked to identify effective and practical solutions that can ensure the protection of children online so they can participate and thrive in the digital space. Since launching our Children's Privacy Project in 2021, CIPL has worked extensively on advancing the global discussion on age assurance

[1] **The Centre for Information Policy Leadership (CIPL)** is a global privacy and data policy think tank within the Hunton law firm that is financially supported by the firm, 80+ member companies that are leaders in key sectors of the global economy, and other private and public sector stakeholders through consulting and advisory projects. CIPL's mission is to engage in thought leadership and develop best practices for the responsible and beneficial use of data in the modern information age. CIPL's work facilitates constructive engagement between business leaders, data governance and security professionals, regulators, and policymakers around the world. For more information, please see CIPL's website at https://www.informationpolicycentre.com/. Nothing in this document should be construed as representing the views of any individual CIPL member company or Hunton. This document is not designed to be and should not be taken as legal advice.

[2] Office of the Privacy Commissioner of Canada, *Assessing whether and how to use age assurance – Guidance for websites and online services*, May 4, 2026, available https://www.priv.gc.ca/en/privacy-topics/age-assurance/aa-gd-web/

by convening a series of Multistakeholder Dialogues on Age Assurance,[3] publishing relevant documents,[4] and engaging with numerous consultations globally. That work has produced, among other outputs, an award nominated Interoperable Framework for Age Assurance Solutions, which considers how interoperable, privacy-preserving credential architectures can support age assurance while safeguarding user autonomy.[5] We have also engaged directly with the OPC, having responded to the Exploratory Consultation on Privacy and Age Assurance (2024)[6] and the Exploratory Consultation on the Children's Privacy Code (2025).[7]

---

[3] The takeaways from these discussions are available on CIPL's website:

- Roundtable 1 (March 2024), available at https://www.informationpolicycentre.com/resources/a-multi-stakeholder-dialogue-on-age-assurance-key-takeaways/.
- Roundtable 2 (July 2024), available at https://www.informationpolicycentre.com/resources/key-takeaways-from-a-multi-stakeholder-dialogue-on-age-assurance-law-and-regulation/.
- Roundtable 3 (September 2024), available at https://www.informationpolicycentre.com/resources/a-multi-stakeholder-dialogue-on-age-assurance-working-group-on-risk-assessments-key-takeaways-next-steps/.
- Roundtable 4 (October 2024), available at https://www.informationpolicycentre.com/resources/key-takeaways-a-multi-stakeholder-dialogue-on-age-assurance-working-group-on-global-regional-perspectives/.
- Roundtables 5 & 6 (October–November 2024), available at https://www.informationpolicycentre.com/resources/key-takeaways-a-multi-stakeholder-dialogue-on-age-assurance-working-group-on-law-and-regulation/.
- Roundtable 7 (June 2025), available at https://www.informationpolicycentre.com/resources/a-multi-stakeholder-dialogue-on-age-assurance-considerations-towards-an-interoperable-age-assurance-framework/.

[4] Please see:

- CIPL Policy Paper (2022), *Protecting Children's Data Privacy: International Issues and Compliance Challenges*, October 2022, available at: https://www.informationpolicycentre.com/resources/protecting-childrens-data-privacy-policy-paper-i-international-issues-and-compliance-challenges/.
- Centre for Information Policy Leadership, Age Assurance & Age Verification Laws in the United States, September 2024, available at: https://www.informationpolicycentre.com/resources/age-assurance-age-verification-laws-in-the-united-states/.

Additional information about CIPL's extensive work on children's safety and privacy is available at https://www.informationpolicycentre.com/resources/.

[5] Centre for Information Policy Leadership, *Considerations Towards an Interoperable Age Assurance Framework: Key Takeaways*, November 2025, available at: https://www.informationpolicycentre.com/resources/a-multi-stakeholder-dialogue-on-age-assurance-considerations-towards-an-interoperable-age-assurance-framework/.

[6] Centre for Information Policy Leadership, *Response to the Office of the Privacy Commissioner of Canada's (OPC) Exploratory Consultation on Privacy and Age Assurance*, September 2024, available at: https://www.informationpolicycentre.com/resources/cipl-response-to-office-of-the-privacy-commissioner-of-canadas-opc-exploratory-consultation-on-privacy-age-assurance/.

[7] Centre for Information Policy Leadership, *Response to the Office of the Privacy Commissioner of Canada's (OPC) Exploratory Consultation on the Children's Privacy Code*, August 2025, available at:

Rather than responding to each section of the Draft Guidance, CIPL has organized this response around the core principles and considerations that we believe should inform the finalization of an effective and proportionate framework, guided by the *best interests of the child* principle. We hope that these cross-cutting observations will be useful to the OPC in refining the Draft Guidance as a whole.

CIPL commends the OPC for a thoughtful, evidence-informed, and privacy-centred draft. In particular, we welcome:

- the recognition that "age assurance should not be the default condition for accessing the Internet," but rather one of multiple approaches to the protection of children online, to be used, where appropriate, in a risk-based manner, proportionate to the potential harm being addressed;
- the requirement that organizations first consider whether potential harms can reasonably be addressed through alternative, less privacy-invasive approaches before deploying age assurance;
- the strong emphasis on the data minimization principle;
- the clear preference for privacy-preserving architectures, including reusable credentials, selective disclosure, and double anonymity; and
- the attention to fairness and to the impact of age assurance on "equity-deserving" groups.

These positions are closely aligned with the Joint Statement on a Common International Approach to Age Assurance, co-signed by the OPC,[8] the European Data Protection Board's Statement 1/2025 on Age Assurance,[9] and CIPL's own extensive body of work on children's data privacy and age assurance.

1. There is no one size fits all solution

CIPL has consistently held that there is no single, universally correct approach to age assurance. Where age assurance is warranted, the appropriate mechanism and the point in the user journey at which it is applied should depend on the nature of the service, the features and functionalities offered, and the likelihood and severity of the risks to children associated with that service.[10] We therefore strongly welcome the Draft Guidance's framing that age assurance can be a useful mechanism in a broader protective ecosystem, and its two-step structure requiring organizations first to establish whether there is

https://www.informationpolicycentre.com/resources/cipl-response-to-canada-opc-exploratory-consultation-on-the-childrens-privacy-code/.

[8] International Age Assurance Working Group, *Joint Statement on a Common International Approach to Age Assurance*, September 19, 2024, available at https://www.priv.gc.ca/en/opc-news/speeches-and-statements/2024/js-dc_20240919/.

[9] European Data Protection Board, *Statement 1/2025 on Age Assurance*, adopted February 12, 2025, available at https://www.edpb.europa.eu/our-work-tools/our-documents/statements/statement-12025-age-assurance_en

[10] Centre for Information Policy Leadership, Response by the Centre for Information Policy Leadership to the OPC's Exploratory Consultation on the Children's Privacy Code, August 1, 2025, available at https://www.informationpolicycentre.com/project/childrens-privacy/.

a legitimate need for age assurance, and only then to determine the nature and extent of the age assurance to be deployed.

It is also worth mentioning that a binary approach— determining only whether an individual is above or below a particular age threshold – does not take full account of children's evolving autonomy. Safety measures, including age assurance, should take into account children's evolving capacities. CIPL would welcome further engagement on safeguards, default settings, and user experiences to reflect children's progressive autonomy and differing levels of maturity.

2. A risk-based and proportionate approach

CIPL supports the Draft Guidance's express recognition that individuals should not be required to provide more, or more sensitive, personal information than is necessary to adequately address the identified risk. Not all processing presents the same level of risk, and the level of age assurance should therefore be calibrated to the likelihood and severity of the specific risk, taking into account both the nature of the processing and the benefits it delivers. This requires careful balancing between two extremes:

- **Overly intrusive age assurance.** Requiring full age or identity verification for all users across routine services, without regard to the level of risk, may impose disproportionate privacy and data protection burdens that also exceed those typically encountered in offline environments, without commensurate evidence of improved child safety.
- **Insufficient age assurance.** Relying on an age assurance method that is not sufficiently robust in higher-risk contexts may fail to provide appropriate protection for children.

In applying the principle of proportionality, the OPC should also take into account an organization's actual processing practices. Where a service has adopted privacy-by-design principles to minimize data collection and retention, the level of risk is arguably lower, and the proportionality assessment should be reflective of this. Indeed, requiring an age assurance process that is more data-intensive than the service itself would not align with the Draft Guidance's commitment to privacy by design and data minimization.

CIPL would also welcome additional clarification to ensure that the principle of proportionality is applied consistently across all scenarios. In particular, Section 2.1 appears to suggest that where a legal obligation exists to prevent access by children, a high level of assurance—such as government issued identification or biometric age estimation—will generally be required. In line with the proportionality principle, CIPL encourages the OPC to clarify that the existence of a legal age restriction should not, in and of itself, predetermine the level of age assurance required. While CIPL agrees that the examples given — adult entertainment content, gambling, and the sale of age-restricted products — are clear cases where robust age verification measures are warranted, a legal age restriction does not always equate to a high risk arising from mere access to a service. Some products or services are restricted to 18+ for contracting or transactional reasons alone— for example, where account creation is limited to adults because of legal capacity to contract or where a vehicle rental platform restricts reservations to adults. Automatically equating an age restriction of 18+ with a requirement for the most robust and data-intensive verification

methods, without a contextual assessment of the actual risk arising from access as opposed to participation or purchase, runs the risk of overlooking the broader set of factors. The nature of the service, existing safeguards, and the maturity of the user should be folded into a risk-based response. CIPL would encourage the OPC to clarify that, even where a legal requirement applies, the choice of method remains subject to a proportionality assessment.

Any age assurance solution will inevitably present tradeoffs between high levels of accuracy, as contemplated by the Draft Guidance, and privacy, security, equity of access, civil rights, or user experience. CIPL therefore encourages the OPC to acknowledge these trade-offs expressly so that they remain an integral part of the proportionality assessment as age assurance technologies continue to evolve.

CIPL would also welcome clarification that organizations demonstrating only a "trivial likelihood of access" by children under Section 2.2.2 are not, in practice, expected to satisfy documentation or technical requirements comparable to those applicable in higher-risk contexts. We encourage the OPC to clarify what a "trivial likelihood of access" means and provide guidance on whether the term is intended to carry the same meaning here as in the forthcoming Children's Code. In this regard, CIPL would encourage the OPC to provide illustrative examples or identify specific categories of services, such as B2B software and other enterprise tools, as examples of services that would generally meet the "trivial likelihood of access" standard because children are highly unlikely to use them.

CIPL raised a similar point in its response to the OPC's Exploratory Consultation on the Children's Privacy Code. There, in the context of the "likely to be accessed by children" standard, we urged that the standard should be limited to situations where access would be significant, so that the Code would not apply where access is merely incidental or arises only because parents share devices with their children. "Significant" in this context should not mean a large number of children or that children must be a substantial proportion of users; rather, it means *more than de minimis*, and the measure of significance should relate to how children's access may affect their rights, interests, and well-being.[11] Therefore, we would encourage the OPC to apply the same understanding to the "non-trivial number of children" standard in Section 2.2.2 of this Draft Guidance, so that the two instruments are read consistently.

Finally, CIPL would also welcome clarification on the interplay, for example, with Quebec's Act[12] respecting the protection of personal information in the private sector where biometric information is processed solely for age estimation, rather than for identification. Such clarification on the interplay with privacy laws would provide greater legal certainty and support the use of privacy-preserving age assurance methods consistent with the Draft Guidance's data minimization objectives. CIPL looks forward to engaging further

[11] Centre for Information Policy Leadership, Response by the Centre for Information Policy Leadership to the OPC's Exploratory Consultation on the Children's Privacy Code, August 1, 2025, available at https://www.informationpolicycentre.com/project/childrens-privacy/.

[12] Act Respecting the Protection of Personal Information in the Private Sector, CQLR c P-39.1, Government of Québec, available at: https://www.legisquebec.gouv.qc.ca/fr/document/lc/p-39.1?langCont=en.

with the OPC on these issues and, in the near future, sharing its forthcoming research on AI-supported age estimation.

3. A clear, evidence-based risk taxonomy is crucial

A clear, evidence-based risk taxonomy, supported by practical examples and case studies, is essential to promote consistent and proportionate implementation of age assurance. Such guidance would help organizations distinguish between higher and lower risk processing activities, thereby averting both under-protection and over-protection. In CIPL's multistakeholder dialogues, we have consistently observed that there is no common understanding—either across jurisdictions or among stakeholders—of how risk should be categorized, or which factors should inform a risk-based age assurance assessment. Providing greater clarity in this area would represent a valuable contribution that would support consistent, risk-based implementation.

Further, CIPL would welcome the inclusion of practical examples illustrating what constitutes low, medium, and high-risk processing under the proposed framework. Examples could also include considerations for safe harbors that would help give entities a sense of—and incentive for—reasonable compliance options. This would provide organizations with a clearer basis for assessing risk and selecting proportionate age assurance measures.

This is particularly important for the medium-risk category, which, in the absence of further guidance, runs the risk of becoming an overly broad classification encompassing services and processing activities with materially different risk profiles. Without clearer parameters, organizations may interpret medium risk in different ways, leading to inconsistent classifications across comparable services. Moreover, not all processing activities falling within the medium-risk category will necessarily present the same nature, likelihood, or severity of risk to children. Services organized around different architectures will present a different profile in terms of nature and likelihood of the risks in question. CIPL therefore believes that more granularity may be needed to help organizations assess different levels of medium-risk and calibrate age assurance measures accordingly.

In sum, a risk-based approach, underpinned by a clear, evidence-based risk taxonomy and supported by sufficiently nuanced examples, provides a consistent basis for implementation while helping to avoid both over-protection and under-protection. Enabling a more accurate assessment of when age assurance measures are warranted will ultimately strengthen legal certainty, facilitate effective regulatory oversight, and better advance the Draft Guidance's objective of establishing a predictable, proportionate, and risk-based framework for age assurance.

4. The limited but legitimate role of self-declaration

CIPL strongly welcomes Section 2.2.3 of the Draft Guidance, which requires organizations to consider whether reasonable, less privacy-invasive measures would suffice to prevent potential harm before resorting to age assurance. As discussed, not all types of services carry the same level of risk. Platforms

and services also have a wide range of options to reduce risk, including privacy-by-design and default settings, parental controls and consent mechanisms, age-appropriate user interface design, educational initiatives, monitoring and reporting tools, and content curation and service features that steer young users away from harmful material.[13] Strict age assurance may not be necessary where other measures reduce the assessed risk sufficiently. Each entity should be able to choose the most appropriate and effective method based on the type of service and the assessed risk.

While CIPL does not consider self-declaration to be appropriate where the nature or level of risk requires robust age assurance methods, it may nevertheless still have a legitimate role within a graduated, risk-based framework where it is commensurate with a (low) level of risk. This approach is consistent with the position taken by leading international data protection and online safety authorities,[14] which recognize the inherent limitations of self-declaration while acknowledging that it may be an appropriate age assurance method in low-risk contexts where its use may be proportionate to the risks presented by the service.

5. The risk assessment should be continuous

CIPL believes that risk assessment must be continuous, and it must be able to evolve over time based on evidence. What constitutes a risk — including a high risk — and what constitutes appropriate mitigation should be assessed on the basis of developing evidence and re-evaluated over time, as services evolve and as new risks and benefits emerge. Reliance on a static assessment can produce both over- and under-protective outcomes. It may lead to disproportionate verification requirements that restrict access to beneficial services, encourage children to migrate to less-regulated platforms, or necessitate the collection of additional personal data—including from adults—with attendant privacy implications. At the same time, it may fail to capture newly emerging risks that warrant additional safeguards. We therefore welcome the Draft Guidance's expectation that organizations regularly revisit their choice of age assurance method as the field develops.

---

[13] See CIPL's Response to the OAIC's Consultation on the Children's Online Privacy Code, available at: https://www.informationpolicycentre.com/resources/cipl-response-to-the-office-of-the-australian-information-commissioners-office-oaic-consultation-on-the-childrens-online-privacy-code/.

[14] Please see:

- UK Information Commissioner's Office, Age Assurance, Data Protection Audit Framework: Age-Appropriate Design Toolkit, available at: https://ico.org.uk/for-organisations/advice-and-services/audits/data-protection-audit-framework/toolkits/age-appropriate-design/age-assurance/.
- International Age Assurance Working Group, *Joint Statement on a Common International Approach to Age Assurance*, September 19, 2024, available at https://www.priv.gc.ca/en/opc-news/speeches-and-statements/2024/js-dc_20240919/.

Relatedly, the Draft Guidance contemplates harm evaluations.[15] To the extent such evaluations are required, to promote efficiency and consistency, organizations should be able to satisfy these requirements as part of comparable assessments under other requirements, such as Privacy Impact Assessments more generally and any assessment expectations under the OPC's forthcoming Children's Privacy Code.

Additionally, CIPL believes that risk assessments should be holistic—weighing both risks and benefits—to strike an appropriate balance between privacy and children's other rights and interests, including access to information, participation in the digital environment, and the opportunity to benefit from richer and more relevant user experiences.[16]

For example, while CIPL understands and supports the objective of ensuring that features be configured in a privacy- and safety-protective manner by default, a blanket "off-by-default" expectation for certain features may overlook an important role such features may play in promoting children's safety and well-being. CIPL therefore encourages the OPC to adopt a nuanced, holistic, risk-based approach to assessing individual features and functionalities, recognizing that features which may appear problematic in isolation can provide significant protective benefits when evaluated in context, given their design, default settings, user controls, transparency, and the age of the user.

For instance, geolocation features may serve as important child safety mechanisms, enabling parents or guardians to locate a child in an emergency. A presumption that such features should be disabled by default could inadvertently limit these beneficial uses. The guidance should therefore preserve organizations' ability to rebut the presumption with appropriate evidence and supporting documentation, evaluated within the broader context of how a feature contributes to a child's overall online safety and well-being.

CIPL therefore encourages the OPC to clarify that organizations may rely on evidence, including contextual design evidence, to show how a feature operates in practice and how it promotes safety or provides other benefits in conjunction with other safeguards. This would support a contextual, evidence-based assessment, rather than creating a de facto expectation that all organizations must adopt the same design approach.

---

[15] The Draft Guidance requires organizations to undertake, and be able to demonstrate, a number of distinct harm- and risk-related evaluations at different stages of the decision-making process. These include evaluating whether age assurance is justified, whether children are likely to access the service, whether less privacy-invasive alternatives are available, and how the level of risk should inform the choice of an appropriate age assurance method. However, the Draft Guidance does not clarify how these evaluations relate to the assessments that will be required under the forthcoming Children's Privacy Code, or whether they are intended to constitute separate assessment requirements.

[16] Centre for Information Policy Leadership, Response by the Centre for Information Policy Leadership to the OPC's Exploratory Consultation on the Children's Privacy Code, August 1, 2025, available at https://www.informationpolicycentre.com/project/childrens-privacy/.

6. The best interests of the child should guide age assurance

Age assurance serves an objective beyond mere data protection; where appropriate, it can support the comprehensive protection of children and adolescents in the digital environment. It can advance not only their rights to privacy and safety but can also affect their right to participate and express themselves through access to information, culture, digital participation, and the progressive development of autonomy. Policy makers must therefore be mindful that age assurance does not merely become an exclusionary technology that blocks children from the benefits of the digital world. The deployment of age assurance must be guided by the *best interests of the child* as the overarching North Star, including the child's right to seek, receive, and impart information as guaranteed by the UN Convention on the Rights of the Child[17] and elaborated in General Comment No. 25 on children's rights in relation to the digital environment.[18] Where necessary, age assurance should be understood as a gateway to age-appropriate experiences, not solely as a barrier to entry.

The *best interests of the child* principle finds meaningful expression in the Draft Guidance. CIPL welcomes the recognition in Section 1 that age assurance should not be the default condition for accessing the Internet. Section 2.2.1, in turn, directs attention to established child-rights tools, including the UNICEF Child Rights Impact Assessment,[19] the UN Convention on the Rights of the Child, General Comment No. 25, and the Federal, Provincial and Territorial resolution on the best interests of young people.[20] CIPL particularly welcomes the Draft Guidance's recognition that a child may be harmed by a *lack of access* to a website or service—such as losing access to important community or informational resources—and its requirement that organizations document why potentially harmful practices cannot instead be adjusted to accommodate children's access.

In line with *the best interests of the child* principle, CIPL would also encourage the OPC to recognize the importance of anonymous and pseudonymous access to information, which matters particularly for young people seeking, for example, safety information or resources related to sensitive topics. In that regard, we

---

[17] United Nations General Assembly, *Convention on the Rights of the Child*, November 20, 1989, United Nations, Treaty Series, available at https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child.

[18] UN Committee on the Rights of the Child, *General comment No. 25 (2021) on children's rights in relation to the digital environment*, CRC/C/GC/25, available at https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation.

[19] UNICEF, Assessing Child Rights Impacts in Relation to the Digital Environment, UNICEF Child Rights and Business, available at: https://www.unicef.org/childrightsandbusiness/workstreams/responsible-technology/D-CRIA.

[20] Office of the Privacy Commissioner of Canada, Putting Best Interests of Young People at the Forefront of Privacy and Access to Personal Information: Resolution of the Federal, Provincial and Territorial Privacy Commissioners and Ombuds with Responsibility for Privacy Oversight, October 5, 2023, available at: https://www.priv.gc.ca/en/about-the-opc/what-we-do/provincial-and-territorial-collaboration/joint-resolutions-with-provinces-and-territories/res_231005_01/.

would welcome confirmation that age assurance is not expected at the level of search and general-purpose information retrieval services, for example.

7. Interoperability, international convergence, and clarity across the value chain

Interoperability remains a key enabler of a privacy-protective ecosystem. For interoperability to be effective in practice, organizations should be able to rely on multiple, interoperable age assurance signals, and users should be able to choose which signal they wish to use.

CIPL has supported interoperable approaches, including cross-recognition of credentials and convergence around international standards in its multistakeholder dialogues and in its Interoperable Framework for Age Assurance Solutions, as a means to reduce the need for repeated verification, lower compliance costs, narrow the surface area for breaches, and improve the experience for users, parents, and adults alike. To that end, we welcome the reference to ISO/IEC 27566[21] and would further encourage alignment with recognized technical standards such as IEEE 2089.1[22] and with comparable international approaches, including the ICO's Opinion on Age Assurance for the Children's Code.[23]

As CIPL has emphasized in its multistakeholder dialogues, age assurance often operates within multi-party ecosystems involving operating systems, app stores, identity and credential providers, and online services. The Draft Guidance should recognize these ecosystems by supporting a proportionate, risk-based approach that clarifies the respective roles of different actors and, where appropriate, avoids unnecessary duplication of personal data collection and verification, thereby promoting data minimization, legal certainty, and effective implementation.

More broadly, CIPL would like to expressly commend the OPC's leadership within the International Age Assurance Working Group and its express reliance on the Joint Statement on a Common International Approach to Age Assurance.[24] Given the inherently global nature of digital services, organizations are increasingly required to navigate multiple jurisdictions with differing legal and regulatory expectations. Greater convergence around common principles and risk-based approaches can enhance legal certainty, reduce unnecessary fragmentation, and support the development of privacy-protective, effective age assurance solutions. Continued regulatory cooperation also helps promote consistent protections for

---

[21] International Organization for Standardization and International Electrotechnical Commission, ISO/IEC 27566-1:2025, *Information Security, Cybersecurity and Privacy Protection — Age Assurance Systems — Part 1: Framework* (Geneva: ISO, 2025), available at https://www.iso.org/standard/88143.html.

[22] IEEE 2089.1-2024, *IEEE Standard for Online Age Verification*, available at https://standards.ieee.org/ieee/2089.1/10700/.

[23] Information Commissioner's Office, *Age Assurance for the Children's Code*, Information Commissioner's Opinion, available at https://ico.org.uk/about-the-ico/what-we-do/information-commissioners-opinions/age-assurance-for-the-children-s-code/.

[24] International Age Assurance Working Group, *Joint Statement on a Common International Approach to Age Assurance*, September 19, 2024, available at https://www.priv.gc.ca/en/opc-news/speeches-and-statements/2024/js-dc_20240919/.

children while preserving access to beneficial digital services and enabling organizations to implement scalable compliance measures across markets.

8. Privacy enhancing technologies play a key role in age assurance solutions

CIPL has long encouraged the application of privacy-enhancing technologies (PETs) in the age assurance context and has consistently placed them at the centre of its policy engagement.[25] PETs can enable verification of a user's age without access to excessive personal data, thereby upholding the principles of data minimization and privacy by design and by default. Verifiable credentials, cryptographic age tokens, zero-knowledge proofs, on-device processing, and double-blind architectures allow a relying party to establish that a user is above a given age without accessing—or being able to retain, repurpose, or link—the underlying personal information. CIPL therefore welcomes the Draft Guidance's recognition of PETs as trusted mechanisms for future age assurance.

CIPL also commends the Draft Guidance for embedding data minimization throughout the age assurance process. In particular, the Guidance promotes the collection of personal information only where necessary, limiting collection to situations where age-based differentiation is either required or otherwise needed to provide access to non-restricted content. CIPL further supports the prohibition on repurposing of age assurance-related data, the requirement for its timely deletion, and the minimization of repeated authentications. However, the OPC should confirm that the deletion and purpose-limitation requirements are to be applied in a contextual, risk-based, and proportionate manner. In particular, the requirement to destroy information as soon as possible should be read coherently with the Guidance's own recognition that, in higher-risk scenarios, a relying party may periodically re-confirm that a previously received age signal remains valid. Moreover, an organization may need to retain certain records to demonstrate compliance—provided any such retention remains strictly limited, instrumental to the protective purpose of the system, and subject to appropriate governance and oversight.[26]

At the same time, consistent with CIPL's long-standing position, the guidance should remain technology-neutral overall and not prescribe or implicitly favour any particular technical solution, provided the mechanism chosen meets the applicable standards of effectiveness, proportionality, and data protection. An outcomes-based approach will accommodate technological innovation and allow relying parties to select solutions best suited to the specific risks of their services.

CIPL further encourages the OPC to consider the use of regulatory sandboxes as an opportunity for interested organizations and regulators to co-develop and test privacy-preserving age assurance models—including double-anonymity architectures and reusable credentials—for accuracy and effectiveness before

---

[25] Please see CIPL's work on age assurance here: https://www.informationpolicycentre.com/resources/.

[26] CIPL Policy Paper (2022), Protecting Children's Data Privacy: International Issues and Compliance Challenges, available at: https://www.informationpolicycentre.com/resources/protecting-childrens-data-privacy-policy-paper-i-international-issues-and-compliance-challenges/.

wider deployment.[27] Sandboxes are particularly valuable in a field as fast-moving as age assurance, where the Draft Guidance itself anticipates that the available privacy-protective options will continue to evolve.

Conclusion

Overall, CIPL supports the OPC's approach and appreciates the continued, consultative engagement with stakeholders. CIPL encourages the OPC to continue work towards an approach that:

- is risk-based and proportionate,
- focuses on a clear and example-driven risk taxonomy;
- prioritizes privacy-preserving methods and privacy-enhancing technologies, while remaining technology-neutral and outcomes-based;
- promotes interoperability and international convergence, including alignment with recognized technical standards and coherence with the forthcoming Children's Privacy Code; and
- treats the *best interests of the child* as encompassing the benefits of digital participation, not solely protection from harm.

CIPL stands ready to engage further with the OPC on any of the issues raised in this response, including through bilateral discussions, workshops, or participation in CIPL's ongoing Multistakeholder Dialogue on Age Assurance.

[27] Centre for Information Policy Leadership, "Learning from Practice: Designing Effective Regulatory Sandboxes," October 2025, available at: https://www.informationpolicycentre.com/resources/learning-frompractice-designing-effective-regulatory-sandboxes/.