# Response by the Centre for Information Policy Leadership to the OAIC's Consultation on the Exposure Draft of the Children's Online Privacy Code

Submitted 5 June 2026

The Centre for Information Policy Leadership (CIPL)[1] welcomes the opportunity to respond to the consultation by the Office of the Australian Information Commissioner (OAIC) on the Exposure Draft of the Children's Online Privacy Code (the Draft Code).[2] CIPL's response builds on our detailed submission to the OAIC's Issues Paper consultation on 31 July 2025,[3] where we addressed the scope, the "likely to be accessed by children" threshold, age assurance, age-range guidance, and the substantive APP-specific provisions that should inform the Code.

CIPL recognises the importance of designing and delivering appropriate online environments for children. We have played an active role in advancing discussions on effective, practical, and proportionate measures that protect children online while preserving their ability to engage with and benefit from digital services.[4]

In particular, CIPL, together with WeProtect Global Alliance, has convened a series of multistakeholder dialogues on age assurance—one of the most consequential and contested questions in this area—with the aim of identifying the technical, practical, and legal challenges facing stakeholders and society and moving the policy conversation toward workable solutions.[5]

---

[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, 85+ 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 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 Australian Information Commissioner, "Official Exposure Draft of the Children's Online Privacy Code," available at: https://www.oaic.gov.au/privacy/privacy-for-kids/official-exposure-draft-of-the-childrens-online-privacy-code.

[3] Response by the Centre for Information Policy Leadership to the OAIC's Consultation on the Children's Online Privacy Code, 31 July 2025, 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/.

[4] In April 2021, CIPL launched a special global project on children's privacy and, in October 2022, published a detailed Policy Paper on international issues and compliance challenges. Among the issues identified for further exploration was the use of age assurance and its impact on children's privacy and safety. Please see: CIPL Policy Paper (2022) *International Issues and Compliance Challenges*, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_childrens_privacy_policy_paper_i_-_international_issues___compliance_challenges__21_oct_2022_.pdf.

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

CIPL commends the OAIC for its thoughtful and consultative approach to developing the Draft Code, characterised by extensive engagement with a broad range of stakeholders, including industry, civil society, academia, and children themselves. We also commend the OAIC's initiative to draw on analogous international instruments, in particular the Age Appropriate Design Code (AADC) developed by the UK Information Commissioner's Office. Global alignment ensures that children will be protected by uniform standards worldwide.

## I. Alignment with CIPL Recommendations

CIPL is pleased to see that a number of the positions raised in our earlier submission are reflected in the Draft Code:

- 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/.
- Research on age verification legislation identified technical, practical, and legal challenges. Please see: Takeaways from CIPL Roundtable: The State of Play in Age Assurance in the US, October 2024, available at https://www.informationpolicycentre.com/resources/the-state-of-play-in-age-assurance-in-the-united-states-key-takeaways/.

In November 2025, the CIPL/WeProtect Framework for Interoperable Age Assurance Solutions outlined relevant technologies and stakeholder roles; the project was later nominated for an Age Assurance Industry Award for its contribution to policy and regulation. Please see: Proposal for a Wallet Credential Manager Framework for Age Assurance Solutions, Centre for Information Policy Leadership, November 2025, available at: https://www.informationpolicycentre.com/resources/proposal-for-a-wallet-credential-manager-framework-for-age-assurance-solutions/.

### *A. The best interests of the child as a primary consideration*

CIPL recommended that the Code adopt a *best interests of the child* standard along the lines of the AADC, and we noted that this would also align with Proposals 16.4[6] and 16.5[7] of the 2023 Privacy Act Review Report.[8]

The Draft Code, however, gives effect to this recommendation not as an overarching guiding principle, but rather in three discrete ways:

- as a constraint on collection (section 10),
- as a precondition for use and disclosure (section 11), and
- as a required element of the privacy impact assessment (section 38(2)(d)).

While CIPL welcomes the acknowledgment of the *best interests of the child* as the north star for design decisions, we believe that this would be better served with a more flexible, principles-based approach as under the UK AADC. Such an approach would accommodate diverse services and business models, and it would take into account the 2023 Attorney-General's Privacy Act Review recommendation, which discourages regulatory fragmentation and seeks alignment with other international approaches, including the UK AADC.[9] Treating the *best interests of the child* as an overarching principle, rather than a mandatory requirement attached to each individual data-processing activity, better aligns with international consensus and preserves the flexibility needed to achieve meaningful privacy outcomes for children across a diverse range of services. [10] As an overarching principle, the *best interests of the child* is not the sole consideration for services covered by the Code, but it should serve as the primary consideration.

### *B. Age-appropriate communications and child-directed transparency*

CIPL recommended that transparency requirements for children be delivered in formats tailored to the child's developmental stage, including through simpler language, visuals, storytelling, and other user-design-driven tools. The Draft Code reflects this recommendation in several places:

- the requirement for a child-directed APP privacy policy (section 23(2)),
- the expectation of "non-text material to engage children effectively" (sections 23(3)(c), 24(2)(d), 26(2)(d)),

---

[6] This requires entities "to have regard to the best interests of the child as part of considering whether a collection, use or disclosure is fair and reasonable in the circumstances."

[7] It recommends that "the substantive requirements of the [Children's Online Privacy] Code could address how the best interests of child users should be supported in the design of an online service."

[8] Attorney-General's Department (Australia), *Privacy Act Review – Report 2022*, published 16 Feb. 2023, pp. 153 and 157, available at https://www.ag.gov.au/rights-and-protections/publications/privacy-act-review-report.

[9] Id., p. 10.

[10] The ICO's March 2025 progress update found that, under the UK AADC's principles-based framework, platforms had implemented significant improvements to children's privacy protections, including stronger default privacy settings, enhanced geolocation safeguards, and changes to advertising practices. Please see: Information Commissioner's Office, "Children's Code Strategy Progress Update – March 2025", March 3 2025, available at: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/protecting-childrens-privacy-online-our-childrens-code-strategy/children-s-code-strategy-progress-update-march-2025/.

- the prohibition on complex or technical expressions or specialist legal language (section 23(5)), and
- the requirement that information provided to a child in response to access or correction requests be "simple, easy to understand and age appropriate" (sections 27(1), 28(6)).

### *C. Recognition of older children's autonomy*

CIPL emphasised that older children should not be treated as lacking capacity, and that doing so could incentivise teens to seek workarounds to protections in place. The Draft Code recognises this in two ways:

- Section 13(1) permits children aged 15 and over to consent to the collection, use, or disclosure of their own personal information.
- The assent mechanism in section 20 ensures that even where parental consent is required, the child's own views are sought before sensitive collection, secondary use, or direct marketing occurs.

These are meaningful recognitions of children's evolving capacities and reflect Article 12 of the UN Convention on the Rights of the Child (UNCRC),[11] which guarantees that children have the right to express their views freely in all matters affecting them, according to their age and maturity.

That said, and as further explained below in Section II K, the assent mechanism creates supplementary obligations over and above those already required for consent from the person with parental responsibility, which ultimately governs the processing of the child's personal information.

### *D. Mandatory privacy impact assessments and staff training*

CIPL has long advocated for accountability-driven approaches to data protection, and our Accountability Framework identifies risk assessment, training, and awareness as among the core elements of any meaningful organisational programme.[12] The Draft Code reflects these elements:

- privacy impact assessments are required for entities proposing to provide a new service or proposing to adopt a new or changed way of processing personal information (section 38)
- persons employed or otherwise engaged by a covered entity and who have regular or frequent access to children's personal information must receive education and training as soon as practicable after engagement and at least annually thereafter (section 40).

CIPL welcomes these requirements, though we have specific concerns regarding the scope, scalability, and publication of the assessments, which we note below in Section II M.

### *E. Notification of monitoring as a recognition of child autonomy*

The notification requirement in section 33 reflects CIPL's view that children's autonomy must be considered alongside parental and platform safety mechanisms. In particular, the provision requires

---

[11] Convention on the Rights of the Child, Article 12, United Nations Office of the High Commissioner for Human Rights, available at: https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child.

[12] CIPL Accountability Framework. See CIPL's resources and papers on organizational accountability at https://www.informationpolicycentre.com/organizational-accountability.html, and CIPL Accountability Discussion Paper 1, *The Case for Accountability: How it Enables Effective Data Protection and Trust in the Digital Society*, 23 July 2018.

children to be informed where such mechanisms are used to monitor or control their use or track their geolocation. CIPL welcomes this principle, while noting that the operational design of the provision—particularly the obligation to provide ongoing, prominent notifications in a manner that ensures the child's awareness—raises practical and safety concerns that warrant further consideration (as noted below in Section II_L).

Moreover, guidance on the scope of the notification obligation under section 33(2) would be welcome. Would compliance require a constantly visible notification, or would periodic reminders at defined points in time (e.g., once a week) be sufficient? Clarity on these and related questions would assist entities in implementing the provision in a manner that is both workable and consistent with the Code's objectives.

## II. Additional Considerations

While the Draft Code reflects significant progress, some of CIPL's recommendations remain unaddressed, and the Draft Code's introduction of new concepts raises additional concerns. CIPL respectfully sets these out below.

### *A. The Draft Code relies on Online Safety Act 2021 definitions*

The Draft Code's scope is anchored in the categorical service definitions of the Online Safety Act 2021,[13] such as social media service, relevant electronic service, and designated internet service. CIPL had noted that these definitions are likely to prove problematic over time because services and business models evolve.

This concern is particularly relevant with respect to the designated internet services category, which encompasses a wide range of services without further distinction. Other instruments under the Online Safety Act—including the Phase 1 DIS Standard[14] and the Phase 2 DIS Code[15]—have approached this through more granular classifications, recognising that different types of services pose different levels of privacy risk to children.

That said, the Report of the Statutory Review of the Online Safety Act 2021,[16] published in February 2025, explicitly described the existing service definitions as "narrow," "inflexible," "complicated," and "confusing," recommending reform. Reform, however, should not come at the expense of meaningful

[13] Government of Australia, *Online Safety Act 2021* (Cth), December 11, 2024), available at: https://www.legislation.gov.au/C2021A00076/latest/text.

[14] eSafety Commissioner, *Online Safety (Designated Internet Services — Class 1A and Class 1B Material) Industry Standard 2024*, 21 June 2024, available at: https://www.legislation.gov.au/F2024L00710/asmade/text.

[15] eSafety Commissioner, *Designated Internet Services Online Safety Code (Class 1C and Class 2 Material)*, registered 9 September 2025, available at: https://www.esafety.gov.au/industry/codes/register-online-industry-codes-standards.

[16] Department of Infrastructure, Transport, Regional Development, Communications and the Arts (Australia), Report of the Statutory Review of the Online Safety Act 2021, 4 February 2025, available at https://www.infrastructure.gov.au/have-your-say/statutory-review-online-safety-act-2021.

risk distinctions. Indeed, the Report itself noted that "a more simplified approach" should still provide "for a flexible and proportionate application in risk assessment obligations and codes."[17]

Should Parliament follow the Report's recommendation and amend the definitions, the scope of the Children's Online Privacy Code will shift correspondingly—without further public consultation and without an opportunity for affected entities to assess the implications. Conversely, if the definitions remain unchanged, CIPL's earlier observation that they may not adequately capture services that are appropriately regulated by the Code (or, conversely, may capture services that are not) continues to apply.

Regardless of how the definitions are ultimately restructured, they should be sufficiently differentiated based on risk and aligned with the proportionality principles that underpin the broader Online Safety framework.

### *B. "Likely to be accessed by children" lacks a significance or risk threshold*

CIPL recommended that the "likely to be accessed by children" threshold be aligned with the AADC's approach, which links the threshold to clear evidence of meaningful risk to children.[18] The Draft Code, however, does not define or qualify this threshold.

This creates two main issues. First, an unqualified threshold may capture services where children's access is incidental or minimal, or where the processing poses little or no risk to children's rights or wellbeing—such as B2B platforms or enterprise tools—leading to disproportionate compliance burdens. Second, the lack of a clear standard creates uncertainty for organisations seeking to assess whether the Code applies.

The Privacy and Other Legislation Amendment Act 2024 expressly authorises the Commissioner to issue guidelines on this question.[19] CIPL therefore reiterates its recommendation that the OAIC issue guidance alongside the Code, introducing a ***significance*** qualifier so that the framework applies only where children's access is ***more than minimal*** and where processing presents a ***meaningful risk*** to their rights.

### *C. "Concerned with the activities of children" threshold is broad and undefined*

The Draft Code introduces a new threshold concept—services that are "primarily concerned with the activities of children." While the OAIC's Explanatory Statement offers, by way of example, "applications that track early childhood development, family photo sharing applications, online school management systems that monitor student performance and internet-connected baby monitors," the undefined term could include services that do not process the personal information of children or pose any privacy risk to children. For example, a website that discourages underage drinking could be

---

[17] Id., p. 26.

[18] Information Commissioner's Office, *Age Appropriate Design: A Code of Practice for Online Services* — "About this Code", available at https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/about-this-code/.

[19] Government of Australia, *Privacy and Other Legislation Amendment Act 2024*, Section 32: "The Commissioner may make written guidelines to assist entities to determine if a service is likely to be accessed by children," available at: https://www6.austlii.edu.au/cgi-bin/viewdoc/au/legis/cth/num_act/paolaa2024377/sch1.html.

viewed as one "primarily concerned with the activities of children." Accordingly, CIPL recommends a narrowing of the scope of this threshold to ensure that it applies only to those services intended to be covered.

### *D. The absence of clear out-of-scope categories*

CIPL recommended that certain entities should be excluded from the Code's application due to their inherent nature, including (but not limited to) banking, travel, hospitality, everyday retail, grocery services, and enterprise/B2B services, as such services do not realistically meet a properly framed "likely to be accessed by children" threshold. The Draft Code does not adopt this recommendation. Section 6 specifies only carriage service providers as excluded entities under section 26GC(7) of the Act.

CIPL acknowledges that the OAIC may prefer to address out-of-scope categories through guidance rather than in the Code itself. In that case, CIPL strongly recommends that such guidance be issued alongside the Code's commencement and include a non-exhaustive list of service categories that are presumptively out of scope, subject to rebuttal where there is specific evidence of child access (meeting the significance threshold mentioned above in Section II B). Without this clarity, organisations would still need to undertake full access assessments and risk evaluations even in uncontroversial cases, creating unnecessary compliance burden.

### *E. The "health service" exclusion remains unclarified*

CIPL highlighted the need for clarity in the definition of a health service, especially in the context of wellness, athletic, or caloric-tracking apps. While the Draft Code (section 5) maintains the exclusion for health services, it does not yet provide specific guidance for wellness apps. Without clarification, organisations operating wellness, mindfulness, fitness, and self-care applications face substantial uncertainty about whether the Code will apply to them.

### *F. The Draft Code lacks a risk-based framework*

The Draft Code as a whole fails to adopt a risk-based and outcomes-focused approach. Generally speaking, obligations appear to apply at the entity level, without an initial assessment of the type of service, the risks presented, and the mitigation measures in place.

Taking into account the age and capacity of the child, the nature of the service, the nature of the data, the potential harms of the processing—and, importantly, the benefits—is essential. The Draft Code reflects risk considerations in some places, notably in section 8(2), which ties the reasonableness of age-ascertainment steps to the risk of harm, and in section 38(2)(f), which requires risk assessment as part of the privacy impact assessment. However, the operative obligations themselves apply uniformly once the "likely to be accessed" or "primarily concerned with the activities of children" threshold is met, without being proportionate to the level of risk involved.

This means that a low-risk service that incidentally meets either threshold has the same obligations as a high-risk service. These obligations may include the implementation of measures to ensure that any collection of children's personal information by default is strictly necessary or the preparation of a mandatory privacy impact assessment. Without a risk-based approach, compliance obligations would apply regardless of the level of harm posed by the underlying activity.

CIPL reiterates its earlier recommendation that the Code move away from a one-size-fits-all approach and adopt a risk-based framework. Under this model, baseline obligations would apply to all services

meeting the applicable threshold, with additional requirements calibrated to the nature, context, and severity of the risks involved. This approach should be supported by clear risk categories, examples, and guidance to aid assessment, and CIPL points to Australia's Online Safety Codes as a useful model for proportional, risk-based regulation.

### *G. Age assessment obligation should be tailored and risk-based*

Section 8 of the Draft Code requires entities to ascertain the age of end users, without regard to the risks presented by the underlying service. While the Draft Code does not mandate the use of age assurance technologies—instead requiring only the use of "steps that are reasonable in the circumstances to ascertain the age of the end-user"—the age assessment appears to apply to all end users (children and adults). CIPL does not believe that adults should be required to present proof of age to access non-restricted services.

Moreover, as drafted, the age assessment requirement does not appear to permit the detection of an age range (such as over 18), but the actual age of each user.

In light of these concerns, and consistent with CIPL's broader work on age assurance, CIPL encourages the OAIC to redraft section 8 to tailor its applicability and scope, ensuring that age assessment obligations are calibrated to the nature and risk level of the underlying service, that detection of an age range is expressly permitted where sufficient, and that adults are not required to verify their age to access non-restricted services.[20]

### *H. The default rule in section 9 risks operating as a uniform strict-necessity test*

Section 9 requires entities to implement technical and organisational measures so that, by default, they only collect, use, or disclose personal information about a child that is "strictly necessary" to provide the service. The provision then requires entities to give children a control mechanism over any non-strictly-necessary processing.

CIPL has consistently argued, in this and other contexts, that data minimisation should be applied in a contextual and flexible manner rather than as a strict quantitative limit, focusing on the necessity and proportionality of data use in relation to a legitimate purpose.[21] An overly narrow interpretation of strict necessity could limit consumer-facing services where personalisation is integral to delivering the very features a user has signed up for—such as specifically tailored content—and where such

---

[20] Please see:

- Centre for Information Policy Leadership (CIPL), A Multistakeholder Dialogue on Age Assurance – Working Group on Law and Regulation, 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/.
- Centre for Information Policy Leadership (CIPL), CIPL Response to the Office of the Australian Information Commissioner's (OAIC) Consultation on the Children's Online Privacy Code, July 2025, 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/.

[21] CIPL, *Reconciling AI with the Data Minimization Principle: Bridging the Innovation,* December 2025, available at: https://www.informationpolicycentre.com/resources/reconciling-ai-with-the-data-minimization-principle-bridging-the-innovation-and-privacy-gap/.

processing is, therefore, reasonably anticipated by the child and the person with parental responsibility.

CIPL recommends that section 9 be reframed so that the default rule operates as a baseline of contextually-appropriate minimisation, supported by a control mechanism for non-baseline processing, rather than a strict-necessity gate. This would preserve the protective purpose of the provision while enabling beneficial processing where it serves the child's interests.

### *I. The consent architecture in Division 2 is highly prescriptive*

CIPL's earlier submission cautioned against prescriptive design and consent requirements on the basis that such requirements (a) tend to become obsolete as technology and user-interface conventions evolve, (b) fail to reflect the wide variety of architectures of online services, and (c) constrain the ability of organisations to design solutions that are most effective for their users. The Draft Code's Division 2 contains a number of highly prescriptive consent rules that should be reconsidered:

- **The 12-month consent expiry (section 15(4)(b)).** A uniform 12-month maximum expiration for all consent, regardless of the processing's risk level or the nature of the service does not align with the fact that there is no one-size-fits-all solution. The appropriate consent period varies significantly with the nature of the processing, the relationship between the child and the service, and the risk profile of the data. Mandatory re-consent every 12 months runs the risk of creating a certain level of consent fatigue that might ultimately undermine meaningful engagement with privacy choices. Periodic reminders—e.g., prompting children to review and reconsider their privacy settings without requiring active re-consent each time as a default—may better balance the goals of child safety and operational practicality.
- **The written-notice-only formality (section 15(2)).** Requiring a written notice as the basis of informed consent does not sit comfortably with the Code's broader emphasis on age-appropriate, non-textual communications including video, audio, and graphics (sections 23(3)(c), 24(2)(d), 26(2)(d)). A child-friendly notice may communicate the relevant information more effectively than a written one. Ultimately, notices should meet children where they are and be reflective of the manner in which they engage most meaningfully with content.
- **The prescribed notice contents (sections 13(3), 15(3), 20(5)(b)).** The Draft Code lists specific items that must appear in every notice. While each item is sensible in principle, the cumulative effect runs the risk of producing notices that resemble adult privacy policies in length and density, undermining the very intelligibility the Code seeks to promote.
- **The bundled-consent prohibition (section 14(3)(b) and (4)).** CIPL agrees that genuine consent requires the ability to make granular choices. However, an absolute prohibition on any "request [that] seeks the individual's consent to multiple collections, uses or disclosures of the information; and […] does not allow the individual to consent, or not consent, to each individual collection, use or disclosure" runs the risk of creating long consent screens for children, similar to those widely criticised in the context of cookie consent.

Accordingly, CIPL recommends that the consent provisions in Division 2 be redrafted to focus on outcomes (consent must be voluntary, informed, specific, current, and unambiguous) and to provide non-prescriptive guidance on how those outcomes may be achieved across different service types and user interfaces.

### J. A risk-based approach to the 15-year-old self-consent threshold

Section 13 of the Draft Code establishes age 15 as the threshold for self-consent; children below that age must secure parental consent to any collection, use, or disclosure of their personal information (save the narrow exceptions in section 13(4) for legal or health-related issues). The 15-year-old blanket threshold for consent is inconsistent with the more nuanced age assessment requirement of section 8, which expressly requires entities to ascertain the age of end users with "reasonable" steps, described as those that take into account "the risk of harm that may arise from any collection, use or disclosure of an individual's personal information." Section 13 applies no equivalent calibration to the consent threshold.

CIPL believes that establishing a fixed age limit, combined with the broad range of activities it covers, may lead to outcomes that do not serve the *best interests of the child*. This does not necessarily mean that the threshold should be abolished, but rather suggests that a more graduated approach—one that takes into account the risk profile of the service and the maturity of the child—would better serve both child safety and the practical realities of implementation. Rigid binary thresholds create compliance fragmentation without delivering proportionately better outcomes for children.

### K. Assent obligations are superfluous

In section 20, the consent framework introduces a new concept—"assent of a child under 15 years." CIPL welcomes OAIC's engagement with children to receive their input, and we suspect that this provision was included in response to that engagement to increase transparency, digital literacy, and a level of autonomy, albeit limited, over the handling of the child's personal information. Notwithstanding these aspirations, the provisions create supplementary obligations over and above those already required for consent from the person with parental responsibility, which still applies and ultimately governs the processing of the child's personal information.

### L. The notification requirement in section 33 warrants careful refinement

CIPL welcomes the principle underlying section 33—i.e., that children should be aware of mechanisms that monitor or control their use of a service—as a meaningful recognition of a child's growing autonomy as they mature. The broad scope, however, captures a wide range of legitimate safety tools used by families, including location-sharing, parental controls, and content restrictions designed to protect children. There may be concerns that the requirement for ongoing and visible notification of monitoring may also, in some cases, undermine the protective purpose. It is important to ensure a functionality that will not, in some sensitive situations, lead to avoidance behaviours such as hiding activity, switching accounts, or moving to less-regulated services.

### M. The mandatory public PIA register raises concerns

Section 39 requires entities to maintain a register of their privacy impact assessments and to publish that register online. It also obliges entities to provide their assessments to the Commissioner upon request.

CIPL strongly supports the use of privacy impact assessments as a core accountability tool. However, the requirement to publish the registry online—coupled with the implicit expectation that the underlying assessments may need to be made public—raises concerns.

First, while transparency is a core element of CIPL's accountability framework, it is intended to support effective risk management rather than rigid disclosure obligations. CIPL's work on data protection impact assessments favours flexible and context-sensitive approaches and cautions against overly

prescriptive transparency requirements that may shift the focus from meaningful internal analysis to defensive documentation. Privacy impact assessments often contain sensitive information about data flows, processors, and security measures. Public disclosure of such details could create security risks, particularly in services used by children, where systems may be targeted by malicious actors. Mandatory public disclosure may therefore weaken the quality of the assessments and reduce their value as practical risk-management tools.

### *N. The age-appropriate default in section 4 may not reflect the developmental realities of older children*

The Draft Code defines "age appropriate" by reference to (a) the youngest age in the targeted age range, or (b) where there is no targeted age range, a child aged between 10 and 12 years old.

CIPL contends that age-based guidance should be advisory rather than prescriptive, given the diversity of children's developmental needs, including neurodiversity and learning differences. As drafted, the 10–12 default could require content directed at older minors (e.g., 17-year-olds) to be presented at a much lower comprehension level.

This may be operationally difficult and risk producing communications that older children perceive as inappropriate, potentially undermining the effectiveness of the protective measures. CIPL therefore recommends allowing age-appropriate communications to be tailored to known age cohorts, with the 10–12 benchmark serving only as a fallback where age information is not available.

### *O. The Draft Code does not sufficiently take benefits into consideration*

CIPL's earlier submission emphasised that risk assessment should balance harms as well as benefits. However, the Draft Code pays limited attention to the benefits of children's engagement with digital services—including the ways in which children learn, play, develop socially, and express themselves online. Children's best interests are not served exclusively by restricting the processing of their personal information; in many cases, they are served equally by enabling meaningful, age-appropriate digital participation.

CIPL recommends that the OAIC clarify that the best interests of the child include access to beneficial digital experiences, and that any processing supporting such experiences may still be consistent with those interests, even where the processing goes beyond that which is strictly necessary.

## III. Conclusion

Overall, CIPL appreciates the OAIC's continued engagement with stakeholders in the development of the Code. The Draft Code reflects considerable progress and incorporates a number of recommendations from CIPL's earlier submission and from the wider consultation. The concerns identified in this response are offered in a spirit of constructive engagement and with the shared objective of producing a Code that delivers meaningful protection for children online while supporting their access to beneficial, age-appropriate digital services.

CIPL stands ready to engage further with the OAIC on any of the issues raised in this response, including through bilateral discussion, participation in workshops, or contribution to subsequent consultations on the implementation guidance that will accompany the Code.