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

Submitted 31 July 2025

The Centre for Information Policy Leadership (CIPL)[1] welcomes the opportunity to respond to the Consultation[2] by the Office of the Australian Information Commissioner (OAIC) on the Issues Paper[3] addressing the development of the Children's Online Privacy Code (the Code).[4]

CIPL recognises the importance of designing and delivering appropriate online environments for children. We have worked for many years to identify effective and practical solutions that can ensure the protection of children online so that they can participate and thrive in the digital space. 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.[5] Among the issues identified for further exploration was the use of age assurance and its impact on children's privacy and safety.

Consequently, CIPL, together with WeProtect Global Alliance, initiated a series of Multistakeholder Dialogues to examine the issue more deeply and provide an environment for fostering solutions.[6]

---

[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] Children's Online Privacy Code (consultation for industry, civil society, academia and other interested stakeholders), available at https://www.oaic.gov.au/engage-with-us/consultations/childrens-online-privacy-code-consultation-for-industry,-civil-society,-academia-and-other-interested-stakeholders.

[3] Children's Online Privacy Code – Issues Paper, available at https://www.oaic.gov.au/__data/assets/pdf_file/0031/253795/Childrens-Online-Privacy-Code-Issues-Paper-2025.pdf.

[4] Children's Online Privacy Code, available at https://www.oaic.gov.au/privacy/privacy-registers/privacy-codes/childrens-online-privacy-code.

[5] 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.

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

- Roundtable 1 (March 2024), available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/key_takeaways_from_a_multi-stakeholder_dialogue_on_age_assurance.pdf.
- Roundtable 2 (July 2024), available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_weprotectglobalalliance_key_takeaways_age_assurance_law_and_regulation.pdf.

These Multistakeholder Dialogues are ongoing, and we welcome the OAIC's participation at future meetings.

In September 2024, CIPL issued a discussion paper focusing on U.S. state legislation requiring the use of age verification measures, with the goal of identifying technical, practical, and legal challenges affecting stakeholders and society more broadly.[7] We followed up with a Roundtable held in San Francisco that addressed these challenges, and we published our takeaways from that discussion.[8]

CIPL is a member of the European Commission's special group informing the Guidelines for Article 28 of the EU Digital Services Act and have been engaging through consultations and workshops.

In light of our research and our work in this space, CIPL supports strong protections for the privacy, safety, and security of minors online. We support robust privacy-by-design requirements and the use of a balanced, risk-based approach that takes the best interest of the child into account. CIPL seeks to foster the development of context-specific risk taxonomies to assist companies in employing measures that are proportionate and appropriate to potential harms and do not restrict minors' access to beneficial, age-appropriate content and services.

We commend the OAIC for their effort to provide clarity on these issues in the form of a Code. Clear and concise regulatory guidance creates the necessary legal certainty for online platforms and services to deliver safe online spaces for children and promote best practices. CIPL has provided extensive comments and recommendations to similar codes, and we incorporate by reference our responses to the initial consultation on the Draft Age Appropriate Design Code (AADC) by the UK Information Commissioner's Office (ICO)[9] and the Draft Guidance on Fundamentals for a Child-Oriented Approach to Data Processing by the Irish Data Protection Commissioner (DPC).[10]

- Roundtable 3 (September 2024), available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_weprotectglobalalliance_keytakeaways_multistakeholderdialogue_sep24.pdf.
- Roundtable 4 (October 2024), available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/oct_22_key_takeaways_final.pdf.
- Roundtables 5 & 6 (October–November 2024), available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_weprotect_a_multistakeholder_dialogue_on_age_assurance_law_and_regulation_apr25.pdf.

[7] CIPL Discussion Paper: *Age Assurance & Age Verification Laws in the United States*, September 24, 2024, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_age_assurance_in_the_us_sept24.pdf.

[8] *Takeaways from CIPL Roundtable: The State of Play in Age Assurance in the US*, October 2024, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/the_state_of_play_in_age_assurance_in_the_us_-_key_takeaways_oct24.pdf.

[9] CIPL Response to the UK ICO's Consultation on Age Appropriate Design - A Code of Practice for Online Services, May 31, 2019, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_response_to_ico_consultation_on_age_appropriate_design_-_a_code_of_practice_for_online_services.pdf.

[10] CIPL Response to the Ireland Data Protection Commissioner's Draft Guidance on Fundamentals for a Child-Oriented Approach to Data Processing, March 26, 2021, available at

In particular, CIPL would like to praise the OAIC's initiative to inform elements of the Code by soliciting **input directly from children** regarding their lived experiences in the online world. CIPL believes that incorporating children's perspectives and views in the development of the Code will ensure that recommendations are practical, trustworthy, and aligned with the needs of real users.

CIPL would like to stress the importance of embedding a **risk-based approach** in the Code to ensure an effective and proportionate approach to children's privacy and safety online. Not all data processing involving children presents the same level of risk, and regulatory frameworks must account for this variance. Measures such as age assurance requirements, default settings, and design elements should be calibrated not only to the different nature of online services and platforms, but also to the nature, context, and severity of risk posed by the specific processing activity, as identified through tools such as Data Protection Impact Assessments (DPIAs). These risk assessments must be structured to assess any potential harms to the development, autonomy, and safety of children, while also recognising the potential benefits of data processing, such as access to educational content, social connectivity, and digital literacy. Overly rigid or uniform approaches can undermine these benefits and may lead to unintended exclusion or friction in service delivery.

A risk-based approach must be embedded not only in legal compliance, but also within product design, governance structures, the use of privacy enhancing technologies, and the implementation of age assurance and other tools. It must take into account the **perspectives of all stakeholders**, thereby enabling a layered approach that is supported by clear, service-specific risk taxonomies and ongoing participatory testing involving children and other key stakeholders. Co-design, transparency, and accountability must form the basis of any risk-based model to ensure that children's best interests are meaningfully protected in practice and not only in principle.

Finally, CIPL would like to stress the importance of **regulatory convergence and coordination**, not just nationally, but internationally. Many of the most popular online platforms and services operate globally with diverging requirements and obligations. Working toward greater convergence especially where similar concepts such as "likely to be accessed by children" are deployed, ensures greater legal clarity and protects children's access to beneficial digital services. We commend the OAIC's reference to the UK's AADC in that regard, which has become a de facto baseline for many organizations operating internationally.

Please find below CIPL's submissions to the OAIC's individual consultation questions.

---

https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_response_idpc_consultation_children_data_fundamentals_26_march_2021.pdf.

TABLE OF CONTENTS

1. SCOPE OF SERVICES COVERED BY THE CODE

The Act sets out that the Code will apply to APP entities if they provide a:

- *Social media service: online services where users connect, share content and interact (e.g. social networks, media-sharing sites, forums, review platforms)*
- *Relevant electronic service: online services that facilitate communication (e.g. messaging apps, email, video calling platforms, online games with chat)*
- *Designated internet service: online services that allow users to access or receive material over the internet. (e.g. cloud storage, websites that let users receive/access content, streaming platforms, consumer IoT devices).*

In each case, the service must be likely to be accessed by children and must not be a health service provider. However, the OAIC may specify in the Code additional APP entities, or a class of entities to which the Code applies or does not apply. For example, the Code may specify that:

- *A provider of a designated internet service may be excluded*
- *A health service provider may be included*
- *An APP entity that doesn't fall under the three service types listed above may still be included.*

1.1 Are there additional APP entities, or a class of entities, that should be covered by the Code? Please provide reasons or evidence to support your view.

Australia's *Privacy Act 1988*, as amended by the *Privacy and Other Legislation Amendment Act 2024*, provides that an APP entity[11] is bound by the Code ***if all of the following apply***:

> (i) the entity is a provider of a social media service, relevant electronic service or designated internet service (all within the meaning of the Online Safety Act 2021);
>
> (ii) the service is likely to be accessed by children; and
>
> (iii) the entity is not providing a health service.[12]

The Act also permits the Code to specify whether additional APP entities should fall within the scope of coverage.[13] CIPL therefore interprets the OAIC's question as asking whether entities that do not satisfy all three of the above criteria should be covered.

(i) Provider of a social media service, relevant electronic service or designated internet service

As for the first criterion—"a provider of a social media service, relevant electronic service or designated internet service"—the Online Safety Act 2021 defines those terms as follows:

> **Sec. 13 Social media service**
>
> (1) For the purposes of this Act, social media service means:
>
> (a) an electronic service that satisfies the following conditions:
>
> (i) the sole or primary purpose of the service is to enable online social interaction between 2 or more end-users;
>
> (ii) the service allows end-users to link to, or interact with, some or all of the other end-users;
>
> (iii) the service allows end-users to post material on the service;

[11] Defined as "an agency or organization." *Privacy Act*, Section 6(1).

[12] *Privacy Act*, Section 26GC(5)(a).

[13] *Privacy Act*, Section 26GC(5)(b).

(iv) such other conditions (if any) as are set out in the legislative rules; or

(b) an electronic service specified in the legislative rules; but does not include an exempt service (as defined by subsection (4)).

(2) For the purposes of subparagraph (1)(a)(i), online social interaction includes online interaction that enables end-users to share material for social purposes.

(3) In determining whether the condition set out in subparagraph (1)(a)(i) is satisfied, disregard any of the following purposes:

(a) the provision of advertising material on the service;

(b) the generation of revenue from the provision of advertising material on the service.

(4) For the purposes of this section, a service is an ***exempt service*** if:

(a) none of the material on the service is accessible to, or delivered to, one or more end-users in Australia; or

(b) the service is specified in the legislative rules.

Sec. 13A Relevant electronic service

(1) For the purposes of this Act, relevant electronic service means any of the following electronic services:

(a) a service that enables end-users to communicate, by means of email, with other end-users;

(b) an instant messaging service that enables end-users to communicate with other end-users;

(c) an SMS [short message service] service that enables end-users to communicate with other end-users;

(d) an MMS [multimedia message service] service that enables end-users to communicate with other end-users;

(e) a chat service that enables end-users to communicate with other end-users;

(f) a service that enables end-users to play online games with other end-users;

(g) an electronic service specified in the legislative rules;

but does not include an exempt service (as defined by subsection (2)).

(2) For the purposes of this section, a service is an exempt service if none of the material on the service is accessible to, or delivered to, one or more end-users in Australia.

Sec. 14 Designated internet service

(1) For the purposes of this Act, designated internet service means:

(a) a service that allows end-users to access material using an internet carriage service; or

(b) a service that delivers material to persons having equipment appropriate for receiving that material, where the delivery of the service is by means of an internet carriage service;

but does not include:

(c) a social media service; or

(d) a relevant electronic service; or

(e) an on-demand program service; or

(f) a service specified under subsection (2); or

(g) an exempt service (as defined by subsection (3)).

(2) The Minister may, by legislative instrument, specify one or more services for the purposes of paragraph (1)(f).

(3) For the purposes of this section, a service is an exempt service if none of the material on the service is accessible to, or delivered to, one or more end-users in Australia.

Given the very detailed definitions set forth above, it is possible that entities may not meet the statutory elements but nevertheless should fall within the scope of the Code because they are likely to be accessed by children. That said, CIPL would recommend excluding certain entities from the Code's application due to their very nature—such as banking, travel, hospitality, and enterprise/B2B services—as such services intrinsically would not meet the "likely to be accessed by children" threshold.

To ensure that Australia's Code "will apply to online services likely to be accessed by children,"[14] CIPL encourages the OAIC to prioritize the "likely to be accessed by children" criterion (as more fully explained below), and not to limit the Code's coverage to certain business models, i.e., "a provider of a social media service, relevant electronic service or designated internet service"—as defined by the Online Safety Act 2021.

Indeed, it is important to note that the Online Safety Act 2021 recently underwent a statutory review to ensure that Australia's online safety laws keep pace with the evolving online environment. The review, as detailed in a Report published in February 2025,[15] explicitly found that the existing definitions of service categories within the Act—i.e., social media services, relevant electronic services, and designated internet services—are "narrow," "inflexible," "complex," and "confusing." Given that assessment and given the Report's recommendation to simplify those definitions, CIPL notes that the Code's reliance on definitions found in another legal instrument could be problematic, as definitions may change via subsequent amendments and business models may fall within or outside scope over time.

(ii) Likely to be accessed by children

As mentioned above, CIPL views the "likely to be accessed by children" criterion to be the principal factor when deciding the applicability of the Code.

That said, the Code should ***only*** *apply, where the likelihood of access is* ***significant***. In other words, the Code should not apply where access is merely incidental or where access is likely because parents are sharing devices with their children, for example. We note, however, that "significant" in this context does not mean a large number of children or that children must be a substantial proportion of users; rather, "significant" would mean more than de minimis, and the measure of significance should be related to how children's access may affect their rights, interests, and well-being.

A risk-based approach is critical in this context. The Code should enable an assessment of risks based on context, taking into account a matrix of issues to reach balanced judgments. In the context of children's data processing, these include, for instance (i) the age and capacity of the child (e.g., recognising that a 17-year-old has very different capacity, interests, and needs than a seven-year-old) and (ii) the nature of the service offered. CIPL provides additional criteria to consider below.

---

[14] Issues Paper, OAIC Children's Online Privacy Code, p. 3, available at https://www.oaic.gov.au/__data/assets/pdf_file/0025/254662/Childrens-Online-Privacy-Code-Issues-Paper-2025-2-7-2025.pdf.

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

The Code should provide organizations with a clear methodology, specific examples, or criteria for assessing the likelihood of minors accessing the platform or service. Of course, the nature of a service, the content, and the presentation can be factors in determining the "platform appeal" and, in turn, the likelihood of children accessing the platform. The Code should therefore permit a certain degree of flexibility for entities to perform an initial assessment of these factors to conclude that children are not likely to access their platform or service. For example, websites focused on professional, business-to-business (B2B), or technical topics (such as CIPL's)[16] would clearly not fall within scope.

This will not always be the case, however. Organizations often face practical barriers in identifying whether children visit their platforms, especially where a user is not required to sign in via an account. Clear guidance is therefore crucial. The *Privacy and Other Legislation Amendment Act 2024* authorizes the OAIC to provide guidance on how the "likely access" standard would be met.[17] CIPL encourages the OAIC to develop such guidance in a timely manner to ensure that organizations have a clear comprehension of the threshold for likelihood of children to access their services (amongst other things).

Where the initial assessment indicates that children are likely to access the service, the Code would apply and a more formal risk assessment should come into play to evaluate potential risks. As with the ICO's AADC, however, the risk assessment (i.e., DPIA) process should be flexible and scalable. We would encourage the OAIC to follow the AADC's lead in this regard. For example, where an online recruitment platform posts part-time jobs for teens, or where a company that employs teens offers staff discounts via an employee portal, such benefits could be accounted for in a flexible and scalable assessment.

(iii) Not providing a health service

CIPL views the third criterion in need of clarification. Although the *Privacy Act 1988* defines "health service" in Section 6FB,[18] the Code should at the very least include a reference "as defined in Section

---

[16] See https://www.informationpolicycentre.com/.

[17] "The Commissioner *may* make written guidelines to assist entities to determine if a service is likely to be accessed by children …"*Privacy and Other Legislation Amendment Act 2024,* Section 32 (emphasis added).

[18] 6FB Meaning of health service

"(1) An activity performed in relation to an individual is a health service if the activity is intended or claimed (expressly or otherwise) by the individual or the person performing it:

"(a) to assess, maintain or improve the individual's health; or

"(b) where the individual's health cannot be maintained or improved—to manage the individual's health; or

"(c) to diagnose the individual's illness, disability or injury; or

"(d) to treat the individual's illness, disability or injury or suspected illness, disability or injury; or

"(e) to record the individual's health for the purposes of assessing, maintaining, improving or managing the individual's health.

"(2) The dispensing on prescription of a drug or medicinal preparation by a pharmacist is a health service.

"(3) To avoid doubt:

6FB." It should also provide further guidance to entities to help them assess whether this criterion is met. For example, if an entity develops an app that records a child's daily caloric intake, would the app be viewed as "providing a health service"? Entities, especially those providing products in juvenile athletics and exercise, will need further guidance on this topic. Moreover, given that "an individual's health includes the individual's … psychological health," apps providing daily encouragement or spiritual reflections could arguably fall within the meaning of a health service.

1.2 Are there any APP entities, or a class of entities, that should be excluded from the Code's application? If so, on what basis?

As mentioned above, CIPL would recommend considering whether certain entities can be excluded from the Code's application due to their very nature, such as banking, travel, hospitality, and enterprise/B2B services. An initial assessment of nature, content, and presentation of a given service should be sufficient to exclude an entity from the Code's application. This primary assessment should focus on whether the platform or service is designed to be attractive or relevant to children. That said, the Code should provide a detailed list of non-exhaustive factors—such as market research or current evidence of user bases of similar services—for entities to consider when the initial assessment leaves ambiguity regarding potential child access or potential risks to young users. However, requiring all entities to assess these detailed factors would be disproportionate and impose an unjustifiable burden on many companies.[19]

1.3 Is there criteria that should be used to determine whether a particular APP entity, or class of entities, is appropriately included or excluded from the scope of the Code?

As mentioned above, a clear and common understanding of what constitutes a service likely to be accessed by children is paramount. Additional criteria for including or excluding an APP entity from application of the Code could include, but would not be limited to, the following:

- **Service Directed to or Intended for Children**: Entities that provide services specifically targeted at children, or are likely to be accessed by children, should be included. This includes assessing elements like subject matter, terms and services, visual content, use of animated characters, child-oriented activities, music, child-specific language, internal policies or strategies including child users.
- **Risk-Based Approach**: As emphasized above, the Code should reflect a risk-based approach, considering the levels of risk associated with children's privacy and safety. Not all data

---

"(a) a reference in this section to an individual's health includes the individual's physical or psychological health; and

"(b) an activity mentioned in subsection (1) or (2) that takes place in the course of providing aged care, palliative care or care for a person with a disability is a health service."

"(4) The regulations may prescribe an activity that, despite subsections (1) and (2) is not to be treated as a health service for the purposes of this Act."

[19] Centre for Information Policy Leadership (CIPL), *CIPL Submission to the ICO Consultation on the Draft Guidance on Services Likely to be Accessed by Children*, May 18, 2023, https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/final_cipl_submission_ico_consultation_likely_to_be_accessed_by_children_18may2023.pdf.

processing activities related to children pose the same risks, and this should be accounted for. In the reverse, some services will expressly not be intended for children but would likely to be accessed by children due to their nature (such as pornography sites), and would therefore fall under the Code.

- **Best Interests of the Child**: In conjunction with the risk-based approach, the Code should adopt a Best Interests of the Child standard, similarly to the ICO's AADC,[20] so as to capture services that may pose a significant risk of harm to children or are otherwise detrimental to their best interests. Adopting the "best interests of the child" principle would also align with Proposal 16.4 from the 2022 Privacy Act Review Report, which 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," as well as Proposal 16.5, which 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."[21]

- **Proportionality:** Proportionality should also be considered when determining whether an entity should be included or excluded from the Code. For example, if a service is likely to be accessed by children, but poses no or low risk, this could justify its exclusion. This means that the Code should also include a clear taxonomy of risks to support such assessments, with practical examples for organizations.

2. When and How the Code Should Apply to APP Entities

The Act states that the OAIC may issue written guidelines to assist APP entities in determining whether a service is likely to be accessed by children.

2.1 What threshold should determine when a service is considered 'likely to be accessed by children'?

As mentioned above in response to Question 1.1, CIPL views "likely to be accessed by children" as a critical consideration when deciding the applicability of the Code. But again, the Code should ***only*** *apply, where the likelihood of access is* ***significant***. (Please see our earlier discussion on this topic.)

Determining whether a service is considered "likely to be accessed by children" should be risk-based, looking initially at the nature and content of the service and whether it has special appeal to children. Among the factors to assess:

- **Content and Features:** The nature, content, language, and features either directed at or appealing to children can indicate likelihood of access. This includes child-oriented activities, visuals, characters, and music that attract children's attention. Additionally, taking into

[20] Information Commissioner's Office, *Age Appropriate Design: A Code of Practice for Online Services – Code Standards*, 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/code-standards/

[21] Attorney-General's Department (Australia), *Privacy Act Review – Report 2022*, pp. 153 and 157, available at https://www.ag.gov.au/sites/default/files/2023-02/privacy-act-review-report_0.pdf.

account factors like spikes in access to specific sites by children driven by social media posts or access during particular times (e.g., outside school hours, weekends, school holidays) could be an important criterion to determine the likelihood of a service to be accessed by children.

- **Nature of the Service:** The inherent nature of the service, such as gaming, educational, or entertainment platforms, can be a factor for attracting child users.
- **User Demographics:** To the extent certain entities have access to user demographic information showing that children are attracted to their service, even if such users are not expected or welcome, such information could support a "likely to be accessed by children" finding.
- **Similar Services:** Information regarding children's access to similar services could also support such a finding.

Where appropriate, a platform's use of reasonable measures to age-gate or restrict access to all or part of a service could also be a relevant factor in determining whether a service (or a portion thereof) is likely to be accessed by children. In light of the amendment to Part 4A of the Online Safety Act 2021—which introduces an obligation on age-restricted social media platforms to prevent children under 16 years from having accounts on their services—OAIC must consider to what extent "reasonable steps to prevent age-restricted users having accounts"[22] impacts whether a service is "likely to be accessed" by that age group. This is in line with the UK ICO's AADC guidance, which recognises that the way in which a service is accessed and any measures put in place to restrict access are key factors in assessing whether a service is likely to be accessed by children.[23]

2.2 'Likely to be accessed by children' is the same standard as the UK's Age Assurance Design Code. Is there any evidence as to the practical effectiveness of the threshold in that context?

We commend the OAIC's efforts to promote convergence with the ICO's AADC. CIPL notes, however, that the AADC's "likely to be accessed by children" threshold is tied to "clear evidence of ***significant risk*** arising from the use of children's data."[24] CIPL encourages the OAIC to further align to the AADC's "likely to be accessed by children" threshold by uniting it to the concept of "significant risk."

While the AADC also interprets the "likely to be accessed" standard as encompassing "a ***significant number*** of children … accessing your service,"[25] we note that "significant number" in this context does

---

[22] Online Safety Act 2021, Section 63D, available at https://www.legislation.gov.au/C2021A00076/latest/text.

[23] UK's Age Assurance Design Code, "When are services 'likely to be accessed by children'?," 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/services-covered-by-this-code/#code4.

[24] *Id.*. "About this Code" (emphasis added), 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/.

[25] See UK's Age Assurance Design Code, Services covered by this Code (emphasis added), 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/services-covered-by-this-code/#code4

not mean a large number of children or that children must be a substantial proportion of users, but simply more than a de minimis amount.[26]

2.3 What steps should APP entities reasonably be expected to take to assess whether children are likely to access their services?

Please see our responses to Questions 2.1 and 2.4, especially with respect to the privacy costs that may be associated with some age assurance approaches. As discussed below, higher-risk scenarios may merit incurring such costs, while they can be reasonably avoided in lower-risk ones.

Some jurisdictions have adopted an "actual knowledge" standard. The U.S. FTC, for example, applies such a standard to the COPPA Rule, which is based on the text of the underlying statute.[27] Any consideration of a knowledge-based standard, however, should ensure that entities do not remain willfully ignorant.

2.4 What role, if any, should age gating or other access control mechanisms play in meeting obligations under the Code?

To the extent the Code contemplates the deployment of age assurance measures, CIPL would endorse an approach that is risk-based, context-specific, and takes into account the wide variety of architectures of online services. It is important, for example, not to automatically assume that an 18+ age restriction in the terms and services of a given platform implies an identified risk to minors, as many transactional services may pose lower risks when simply accessing the site, for example. Age assurance may not be necessary at all where other measures, such as the provision of parental control tools or a high level of content curation, reduce the assessed risk sufficiently. This is particularly important as age assurance can be an exclusionary technology, keeping children away from certain online content. The deployment of age assurance must therefore carefully consider the **best interests of the child** as enshrined in the UN Convention on the Rights of the Child, and take into account the rights of children "to seek, receive and impart information, to be protected from harm and to have their views given due weight."[28]

While age assurance aims to keep children safe online, there is a lack of consensus among global regulators regarding the effectiveness, appropriateness, and adequacy of age assurance methods vis-à-vis data protection laws. Specifically in Australia, the ongoing Age Assurance Technology Trial (AATT)

---

[26] Centre for Information Policy Leadership (CIPL), *CIPL Submission to the ICO Consultation on the Draft Guidance on Services Likely to be Accessed by Children*, May 18, 2023, https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/final_cipl_submission_ico_consultation_likely_to_be_accessed_by_children_18may2023.pdf.

[27] 15 USC § 6502(a)(1) (providing that "[i]t is unlawful for an operator of a website or online service directed to children, or any operator that has *actual knowledge* that it is collecting personal information from a child, to collect personal information from a child in a manner that violates the regulations prescribed under subsection (b)"). Emphasis added.

[28] UN Committee on the Rights of the Child (CRC). (2021). *General comment No. 25 (2021) on children's rights in relation to the digital environment*, CRC/C/GC/25, Section III, B. Best Interests of the Child, p. 3, https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation.

aims to address these questions.[29] Simple self-declaration (e.g., checking a box or providing proof of age via credit card/ID) is often unreliable, as children can easily circumvent these checks.

More rigorous methods, while offering greater assurance, raise concerns about the collection of large amounts of or sensitive types of data. For example, accessing reliable data like a child's date of birth, family, school, and online activity could verify age, but it comes with significant practical difficulties and privacy implications, especially concerning data storage. Many young people also may not possess official identification documents, which could exclude them from age-appropriate content if such methods are the sole means of verification. These concerns are amplified when age verification data includes biometric data (e.g., facial images, voice imprints, keystroke dynamics, facial dimensions). Hence, the solutions need to balance the pursuit of precision in age-gating with privacy concerns, tailoring the rigor of verification and the potential collection of additional information to the risks posed.[30]

CIPL believes that a lack of a common understanding of risk levels could result in either under-protection, where providers underestimate a risk and apply insufficient safeguards, or overprotection. Overprotection, in this context, would encompass providers who implement disproportionate restrictions that might unduly limit minors' access to beneficial digital content or services. Overprotection would also potentially encompass providers who collect personal data from adults for age assurance purposes. In scenarios where the actual risk to children is low, such collection could be viewed as being disproportionate. A clearly articulated risk taxonomy is required, with illustrative examples and case studies, especially for medium- and low-risk scenarios in a variety of contexts. CIPL would also like to point out that assessment of what constitutes a risk, including a high risk, needs to be based on evidence and may change as research continues to develop. Risks can change over time as services develop and new threats or benefits emerge in the online environment. This must be continuously evaluated.

The discussion on appropriate and reliable age assurance methodologies and tools is ongoing, and there is no one-size-fits-all approach to age assurance.[31] As mentioned earlier, CIPL has set up a Multistakeholder Dialogue with WeProtect Global Alliance in order to explore a holistic and principles-based approach to age assurance that carefully balances risks and rights.[32]

---

[29] See https://ageassurance.com.au/.

[30] 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.

[31] See supra, n. 27. AATT's Press Release says: "We found a **plethora of approaches** that fit different use cases in different ways, but we did not find a single **ubiquitous solution** that would suit all use cases, nor did we find solutions that were guaranteed to be effective in all deployments." [Bold in original.]

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

- Roundtable 1 (March 2024), available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/key_takeaways_from_a_multi-stakeholder_dialogue_on_age_assurance.pdf.
- Roundtable 2 (July 2024), available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_weprotectglobalalliance_key_takeaways_age_assurance_law_and_regulation.pdf.

Concretely, in addition to establishing a common risk taxonomy framework for age assurance, CIPL considers it important to work towards further standardisation, such as through a centralised interoperable age assurance solution that streamlines the process and reduces the burden of repeated checks across multiple services for platforms and users. An interoperable system, where age information established in one trusted context could be shared or reused, could simplify the process for all stakeholders significantly. CIPL recognises that such a solution must carefully balance a number of challenges, including privacy, security, competition concerns, cost, and liability.[33] This discussion forms part of the Multistakeholder Dialogue on Age Assurance. We would welcome the OAIC's participation at future meetings.

2.5 Are there alternative approaches APP entities could take to meet their obligations under the Code, beyond age gating or age verification methods? If so, is there any evidence on the impact of such approaches on children's access to services or privacy outcomes?

As mentioned above, age assurance measures should primarily play a role that is risk-based and context-specific. Beyond age gating or age verification methods, platforms and services have a range of possibilities:

- **Privacy by Design and Default**: Implementing privacy by design principles ensures that children's privacy and the best interests of the child are integrated into the development of services from the outset. This includes minimizing data collection, ensuring data security, and providing clear privacy notices. It may also encompass privacy default settings for children (e.g., geolocation tracking and sharing being turned off by default, children's friend/follower lists being private by default, and non-public profiles for children by default).
- **Parental Controls and Consent Mechanisms**: Offering robust parental controls and consent mechanisms allows parents to manage their children's access to services. This empowers parents to make informed decisions about their children's online activities.
- **Service Features**: Certain service features such as recommender systems can also play a positive and proactive role in protecting children if they are tailored to prioritize and promote age-appropriate, educational, and enriching content, effectively steering young users away from harmful material. They can act as risk-minimizing measures, ensuring children receive suitable content and facilitate access to beneficial information.

- Roundtable 3 (September 2024), available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_weprotectglobalalliance_keytakeaways_multistakeholderdialogue_sep24.pdf.
- Roundtable 4 (October 2024), available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/oct_22_key_takeaways_final.pdf.
- Roundtables 5 & 6 (October–November 2024), available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_weprotect_a_multistakeholder_dialogue_on_age_assurance_law_and_regulation_apr25.pdf.

Takeaways from our latest roundtable, held June 13, 2025, are forthcoming.

[33] *Id.*

- **Educational Initiatives**: Providing educational resources and guidance to children and parents about online privacy risks and safe practices can enhance awareness and encourage responsible digital behavior.
- **User Interface Design**: Designing user interfaces that are intuitive and age-appropriate can help children navigate services safely. This includes simplifying privacy settings and making them easily accessible.
- **Monitoring and Reporting Tools**: Implementing easily identifiable and user adapted tools to identify and address inappropriate access or behavior can help maintain a safe environment for children. Reporting mechanisms allow users to flag content or interactions that may pose risks.

It is important to note that APP entities vary greatly in technical set-up, features and risk profiles. Therefore, any measures under the Code should allow each entity to choose the method(s) most appropriate and effective based on the type of service and the assessed risk. As mentioned above, a holistic, risk-based approach must ensure that any measures implemented are proportionate to the level of risk, avoid over-restriction of children's access to age-appropriate content, and curtail excessive obligations on service providers.

2.6 Are there classes of APP entities, personal information, or activities of entities, for which different requirements under the Code may be appropriate? If so, what considerations should inform that approach?

Please see our responses to Questions 1.1, 1.2, and 1.3. In sum, a flexible, risk-based approach is best suited to address when and to what extent different measures may be warranted.

Additionally, to improve clarity and reduce operational burden, OAIC may consider notional classification of certain services across specific risk-tiers, similar to an approach adopted by Australia's Online Safety Codes and Standards.[34] However, any such categorization should be rebuttable on a case-by-case basis.

2.7 How should the Code accommodate for the varying roles, functions and risk profiles of different kinds of services, activities or personal information?

Again, a risk-based approach can accommodate the varying roles, functions, and risk profiles of different kinds of services, activities, or personal information. The Code should consider requirements only based on the actual risk profile of a service, taking into account the age of the user, type of service, and mitigation measures. This aligns with the general objective to protect children without preventing their engagement online. This ensures that privacy policies and collection practices, including what is deemed 'reasonably necessary' for data collection, are tailored to actual risks.

[34] eSafety Commissioner, *Fact Sheet: Registration of the Designated Internet Services Standard* (June 2024), https://www.esafety.gov.au/sites/default/files/2024-06/Fact-sheet-registration-DIS-Standard.pdf

3. AGE RANGE-SPECIFIC GUIDANCE

The OAIC may provide age range-specific guidance, aligning with the UK Information Commissioner's Office's Age Appropriate Design Code, to ensure the development needs of children at different ages are taken into account when drafting the Code.

It is noted that any age-based guidance will not be a 'one size fits all' approach, given the variance of development needs among children, not just due to age but due to other factors, including neurodiversity or learning differences.

The proposed age ranges are as follows:

- *0-5: pre-literate and early literacy*
- *6-9: core primary school years*
- *10-12: transitional years*
- *13-15: early teens*
- *16-17: approaching adulthood*

Questions:

3.1 Would age-based guidance be appropriate and assist APP entities in tailoring protections and interfaces appropriately and effectively?

While age-based guidance would be helpful for tailoring protections and interfaces, the OAIC's suggested age ranges—0-5, 6-9, 10-12, 13-15, 16-17—should be regarded as advisory only, and not prescriptive or mandatory, given the variety on online platforms, the wide age-range of young users, and the developmental realities of those with special needs. Moreover, existing regulatory frameworks define alternative age ranges.[35]

That said, the suggested age ranges comport with the ICO's AADC, and we again commend the OAIC for its efforts to advance regulatory convergence and coordination.

3.2 In terms of providing guidance for the processing of children's personal information by APP entities covered by the Code, how appropriate do you consider the above age ranges would be?

See our response to the preceding question.

3.3 Please provide any views or evidence you have on children's development needs, in an online context in each or any of the above age ranges.

CIPL defers to the research conducted by the ICO on this topic.

[35] See, for example, the National Classification Act (available at https://www.classification.gov.au/about-us/legislation) and the Online Safety Act (available at https://www.legislation.gov.au/C2021A00076/latest/text).

APP SPECIFIC QUESTIONS

With respect to the APP specific questions, CIPL strongly recommends that the OAIC adopt a risk-based and outcomes-focused approach guided by the Best Interest of the Child.[36] Not all processing of children's personal data has the same level of risk, and, in assessing the level of risk, organizations in their data processing impact assessments should take into account a matrix of issues to reach balanced outcomes.

In the context of children's data processing, these include, for instance (i) the age and capacity of the child (e.g., recognising that a 17-year-old has very different capacity and needs than a seven-year-old), (ii) the nature of the service offered and the processing of children's data in the context of that service and for what purpose, and (iii) the appropriate balance between various aspects of children's rights and welfare, including their privacy, their right to express themselves and have access to information, and relevant user experiences. Treating older children as lacking capacity may ultimately encourage teens to look for workarounds to the protections in place.

Risk assessment must be holistic. For example, when considering anonymous account settings, entities should consider the potential impact on peer users in the context of cyberbullying. Moreover, a holistic risk assessment must weigh harms against potential benefits. For example, when assessing personalisation, entities should consider how personalisation may enable platforms to offer content that matches a child's age, developmental stage, and interests, and how it can steer young users away from inappropriate content.[37] In that instance, personalisation can make the user experience more relevant and safe for children. Geolocation can also serve practical purposes, such as helping a child locate relevant emergency services quickly.[38]

A risk-based approach ensures that measures are proportionate to the level of risk, avoids over-restriction of children's access to age-appropriate content, and curtails excessive obligations on service providers. As mentioned above, a risk-based approach will require a clearly defined and commonly understood risk taxonomy, which must be centred around the likelihood and severity of a risk occurring as well as the potential benefits for the child.

Additionally, while the privacy protections applied to children may differ from those applied to adult users (in order to account for children's special vulnerabilities), they may not necessarily be uniformly "higher" protections. For example, transparency requirements may be delivered in a different and specific way to a child through the use of simpler language, visuals, storytelling, videos, games, and

---

[36] See also Information Commissioner's Office. *Age Appropriate Design: A Code of Practice for Online Services.* Wilmslow: ICO, September 2020. Available at: https://ico.org.uk/for-organisations/childrens-code/

[37] Centre for Information Policy Leadership. Protecting Children's Data Privacy: International Issues and Compliance Challenges. October 2022. https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_protecting_childrens_data_privacy_paper1_oct22.pdf.

[38] Centre for Information Policy Leadership (CIPL), *CIPL Response to the ICO Consultation on Age Appropriate Design: A Code of Practice for Online Services*, May 2019, https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_ico_age_appropriate_design_may2019.pdf.

other user-design-driven tools. ICO's AADC,[39] EU's GDPR,[40] and Brazil's LGPD[41] require organizations to communicate information about the processing of children's data in a simple, clear, and accessible way, tailored to the child's maturity level and using audio-visual resources where appropriate. This does not necessarily result in a higher level of protection, but it fulfils the requirement in a way that is more specifically tailored to children.

The Code should be outcome-driven and should avoid mandating prescriptive or granular requirements with respect to design and transparency obligations. Such requirements would risk becoming obsolete quickly and would hinder the development of more innovative solutions from emerging technology. A prescriptive approach would also fail to account for evolving technical development for new services and new risk profiles, and it would hamper the ability of organizations to determine what solutions work best for them and their users. Any design or default measures proposed by the Code should be illustrative and accompanied by case studies.

CIPL's research shows significant developments in terms of privacy and safety by design across industry. Online platforms have developed a wide variety of tools to ensure not only that children are protected online, but also that they have positive online experiences and develop healthy online habits. Organizations often work closely with external expert partners such as academics, NGOs, and survivors across jurisdictions on significant topics—such as suicide prevention, online bullying, and eating disorders—to develop and regularly evaluate effective policies and tools. In addition, organizations have recognised the need to include children as well as parents and care-takers to understand their unique challenges and experiences and translate them into usable policies and online tools.

Some of the industry's best practices include:

- Setting child-user accounts to private by default, only becoming public if the child intentionally changes the setting. Where a child opts to make the account public, periodic notifications are sent reminding the child of the ability to return to private settings.
- Setting teen accounts with strict default controls over user interactions, ensuring that teens automatically receive age-appropriate experiences and are not exposed to inappropriate content.
- Integrating proactive well-being features, such as the activation of "sleep mode," which mutes notifications at night.
- Integrating parental supervision controls, which give parents flexibility to set daily time limits or block specific usage periods.
- Labelling content as made for children, with machine learning tools trained to detect and override incorrect settings.

---

[39] *Id*.

[40] European Union. *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation).* Official Journal of the European Union L 119/1 (May 4, 2016). Available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

[41] Centre for Information Policy Leadership. Protecting Children's Data Privacy: International Issues and Compliance Challenges. October 2022. https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_protecting_childrens_data_privacy_paper1_oct22.pdf.

- Disabling public news feeds that allow for unmonitored broadcasts, creating safer and more restricted environments.
- Restricting certain communications features.
- Disabling live features such as livestreaming, commenting, live chats, and content uploading.
- Developing robust parental tools to allow parents or guardians to set up individual profiles for each child, lock content, set screen time limits, control access to search functions, and restrict messaging applications.

In addition, CIPL notes that delivering effective privacy and safety protections for children and teens online requires more than mere compliance with the letter of the law. For more than a decade, CIPL has pioneered organizational accountability as a key building block of effective data privacy regulation and its corresponding implementation within companies. Indeed, **CIPL's Accountability Framework**[42] (see Figure 1 below) is a recognized standard for the development of best-in-class data privacy protections and responsible business practices. It identifies seven essential elements of organizational accountability and can serve as a starting point for setting up a meaningful accountability programme within an organization.

Figure 1

CIPL strongly believes that accountability is a modern and future-proof concept that can be applied to all digital regulation and corporate compliance. Meaningful and demonstrable accountability will ensure effective governance within an organization, placing the responsibility and discretion of how to operationalise legal obligations directly on organizations, with risk-based controls, policies, procedures, and tools commensurate with their business models and internal set-up.[43]

---

[42] See CIPL resources and papers on organizational accountability: https://www.informationpolicycentre.com/organizational-accountability.html.

[43] CIPL Accountability Discussion Paper 1 - The Case for Accountability: How it Enables Effective Data Protection and Trust in the Digital Society, July 23, 2018 https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_paper_1_-_the_case_for_accountability_-_how_it_enables_effective_data_protection_and_trust_in_the_digital_society.pdf