Submission to the Office of the Australian Information Commissioner

regarding the

Children's Online Privacy Code

August 2025

Who we are

Digital Rights Watch is a charity founded in 2016 to promote and defend human rights as realised in the digital age. We stand for privacy, democracy, fairness, and freedom. Digital Rights Watch educates, campaigns, and advocates for a digital environment in which rights are respected, and connection and creativity can flourish. More information about our work is available on our website: www.digitalrightswatch.org.au

Acknowledgement of Country

Digital Rights Watch acknowledges the Traditional Owners of Country throughout Australia and their continuing connection to land and community. We acknowledge the Aboriginal and Torres Strait Islander peoples as the true custodians of this land that was never ceded and pay our respects to their cultures, and to elders past and present.

Contact

[redacted]

Contents

General Position

Digital Rights Watch welcomes the opportunity to provide feedback on the OAIC's *Phase 2 Consultation* on the *Children's Online Privacy Code*. We are aligned with the OAIC's objective of protecting children through strengthened privacy protections, rather than preventing children from engaging in the digital world. The Internet is a vital component of modern civil life and it is vital for the health of our democracy and of us as individuals that children are able to participate in the online world.

We strongly support the development of a comprehensive and enforceable code that prioritises the privacy rights of children in digital environments. If the current digital privacy landscape is not good enough for children, we must ask: *is it good enough for anyone*? Children are often the most vulnerable users of digital services. A code that upholds their rights must improve digital protections across the entire population.

Digital Rights Watch urges the OAIC to take a transparent approach to privacy. This means focusing not only on visible elements (such as pop-ups and targeted ads) but on how data is collected, managed, stored, shared, and profiled — often without the user's awareness. Algorithms and automated systems are frequently opaque, and the Code must shine a light on these hidden processes.

The COP code should continuously ask entities if their data practices are in the best interest of the child. Organisations must only collect children's data necessary for running a service. Such data should not be shared and must never be shared unless it undoubtedly benefits the child (for example, sharing of medical information between hospitals). Furthermore, cross-border data flow should only be allowed when expressly requested or a compelling case for the benefit of the child exists (ie. the sharing of educational records to the child's new international school).

The Code should apply to all digital services likely to be accessed by children, including but not limited to AI systems and EdTech platforms. A broad scope ensures no child falls through the cracks and raises the standard of privacy practices for all users.

We caution against siloed exemptions for emerging technologies. While AI may raise unique privacy concerns that require additional oversight, these concerns should supplement, not exempt, core obligations. As technology evolves, the Code should be principle-based, for example: *"Only data*

necessary for the service's core function may be collected." Additional safeguards and obligations should be implemented where the application of the COP code principles does not adequately address the privacy risks of the tech.

Threshold for the Code to apply:

Digital Rights Watch supports a default application model for the COP Code. The default application model reflects the reality that minors access almost every corner of the internet. The COP code should apply to social media, despite the 'Social Media Minimum Age' ban as it is likely children will continue to access these platforms. In other words, the Code should apply to all online services unless the provider proactively demonstrates that their service is not accessed by anyone under 18. To qualify for an exemption, a service must:

- Submit a written justification to the OAIC explaining why minors are unlikely to access the platform, and

- Implement robust access controls *that comply with the Code* (if applicable), rather than bypassing it.

Age and developmental stage protections:

We caution against stratifying protections based on children's age due to the complexity and inaccuracy involved in age estimation. Instead, the COP Code should be designed to protect all children under 18, without forcing platforms to make intrusive or unreliable guesses about age.

Instead, we recommend:

- Privacy notices and policies to be provided in accessible, plain language for users of all ages.
- Restrictions on using age-gating as a compliance workaround.
- A reminder that age-gating mechanisms themselves (such as age estimators or login walls) must also comply with the Code, as they are likely to be accessed by children.

Enforcement of breaches

We are aligned with the OAIC's civil penalty regime of introducing mid- and lower-tier thresholds for civil claims. Beyond compensation for claimants, the OAIC should be empowered to issue fines to entities in

breach, taking into account the entity's size and our expectation of their capability to protect children's privacy.

Our Views and Evidence

1 Scope of services covered by the Code

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.

The current proposed Code excludes health service providers by default. We think that this exemption is too broad and that health service providers should be covered by the Code, noting that there will need to be more specific exemptions or use cases. Health data is some of the most private data about a person[1] and it is vital that this is recognised as true for children, too.

Older children and teenagers in particular may require health services relating to their gender or sexuality[2]. It is vital that this vulnerable group is not discouraged from seeking help on account of fear of losing their privacy.[3]

Children are also "users" of many educational technology (EdTech) systems, imposed on them by schools and similar institutions.[4] As these entities hold the personal data of large numbers of children, they should

---

[1] Pew Research Center, "Americans Consider Certain Kinds of Data to Be More Sensitive than Others," Pew Research Center, November 12, 2014, https://www.pewresearch.org/internet/2014/11/12/americans-consider-certain-kinds-of-data-to-be-more-sensitive-than-others/.

[2] Minus18, "QUEER YOUTH NOW 2025 the National Survey of LGBTQIA+ Youth Voice in Australia," 2025, https://res.cloudinary.com/minus18/image/upload/v1749769528/Queer%20Youth%20Now/Queer_Youth_Now_Report_2025_fnz7rx.pdf.

[3] Power, Jennifer, Sylvia Kauer, Christopher Fisher, Roz Bellamy, and Adam Bourne. "The 7th National Survey of Australian Secondary School Students and Sexual Health." *Young People and Sexual Health Publications*. La Trobe University, 2021. Page 21. https://s3-ap-southeast-2.amazonaws.com/figshare-production-eu-latrobe-storage9079-ap-southeast-2/39488062/1217996_PowerJ_2022.pdf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIARRFKZQ25KW2DIYRU/20250731/ap-southeast-2/s3/aws4_request&X-Amz-Date=20250731T003653Z&X-Amz-Expires=10&X-Amz-SignedHeaders=host&X-Amz-Signature=b28c5fea63534d631b9c70594704830914d79616f32df8a27c1943f91e361685.

[4] Campion Education, "Digital Landscapes in Australian Schools," 2023, https://campion.com.au/wp-content/uploads/2023/10/Digital-Landscapes-in-Australian-Schools-2023.pdf.

be explicitly included in the Code regardless of the size of the entity running the system.[5]

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?

All entities that hold data belonging to, or about, children must be included in the Code by default. The OAIC is best placed to issue exclusions on an as-needed basis.

1.3 Are 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 above, any entity that handles children's data is appropriate to include in the Code.

In order for an entity to be excluded from the Code, it must demonstrate to the OAIC that either it is not handling children's data or that an exclusion from the code is in the best interests of the children whose data is being used.

2. When and how the Code should apply to APP entities

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

We do not believe that there exist digital systems that are unlikely to be accessed by a child aged 17 years and 11 months, yet likely to be accessed by the same person at 18 years of age. For this reason, Digital Rights Watch supports a default application model for the COP Code. The default application model reflects the reality that minors access almost every corner of the Internet.

The COP code must specifically apply to social media platforms, despite the 'Social Media Minimum Age' ban, for two reasons. Firstly, 16-17 year-old teenagers are legal minors who will be able to access social media and be

[5] Juliane Jarke and Andreas Breiter, "Editorial: The Datafication of Education," *Learning, Media and Technology* 44, no. 1 (January 2, 2019): 1–6, https://doi.org/10.1080/17439884.2019.1573833.

covered by the Code. Secondly, the likelihood of social media platforms successfully banning under-16s from their platforms is minimal. Children will continue to access these platforms and it is not acceptable for Internet platforms to use the social media ban as justification to put children's privacy at risk.

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

The Age Appropriate Design Code is very capable at identifying services that are predominantly used by or deliberately target children. However, it is poor at identifying services targeted at adults which are also likely to be accessed by children.[6]

The Age Appropriate Design Code exists as part of a system of legal frameworks and institutions, including GDPR, and ECHR, that are not present in Australia. Without the weight of these institutions and the legal requirements that they have of all organisations handling data, the Age Appropriate Design Code would fall short. We need to strengthen the OAIC and associated entities to better enforce and extend the COP Code.

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

As above: all services should be covered by the Code by default.

DRW accepts that there may be limited circumstances where services are demonstrably not accessed by minors (e.g. car registration portals, dating apps with verified age checks), these should be the exception not the rule. Entities need to prove to the OAIC not only that children are *unlikely* to use their services, but that they have made it *impossible* for them to do so.

---

[6] John Mootz and Kate Blocker, "UK Age-Appropriate Design Code Impact Assessment Age-Appropriate Design Code Impact Assessment" (Children and Screens: Institute of Digital Media and Child Development, 2024), https://www.childrenandscreens.org/wp-content/uploads/2024/03/Children-and-Screens-UK-AADC-Impact-Assessment.pdf.

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

Age-gating and similar mechanisms have no place in meeting an entity's obligations under the Code.

Age-estimation techniques such as behavioural profiling, device tracking, or inferred demographic data would need to meet the Code in their own right as they need to handle children's data in order to make an age estimation.[7][8] These systems are also privacy-invasive by their very nature and are contrary to the spirit of the Code.

Moreover, age-gating shifts the burden onto children to prove they are entitled to protection, rather than keeping the burden with the APP entity to prove they are not.

Finally, age-gating mechanisms are of dubious capability - no matter the claims of the platforms using them, there will always be "false positive" matches that allow children to access systems that they are gated out of.[9] Those children deserve their privacy to be upheld, even when they are in a space that attempts to exclude them.

---

[7] Jennifer Huddleston, "Online Age Verification Could Create More Problems than It Solves," Cato Institute, 2025, https://www.cato.org/commentary/online-age-verification-could-create-more-problems-it-solves.

[8] eSafety Commissioner, "Tech Trends Issues Paper: Age Assurance," *ESafety Commissioner* (Australian Government , 2024), page 10-16. https://www.esafety.gov.au/sites/default/files/2024-07/Age-Assurance-Issues-Paper-July2024_0.pdf?v=1753929939993.

[9] The Age Verification Providers Association, "INQUIRY into IMPACTS of HARMFUL PORNOGRAPHY on MENTAL, EMOTIONAL, and PHYSICAL HEALTH, Submission Number 9" (NSW Parliament, 2024), https://www.parliament.nsw.gov.au/lcdocs/submissions/88004/0009%20The%20Age%20Verification%20Providers%20Association.pdf.

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?

We are witnessing platforms' over-enthusiastic implementation of the UK's Online Safety Act lead to LGBT+ content being blocked to all users in the UK, regardless of age.[10][11][12]

It is no stretch to imagine that platforms keen to skirt their COP Code obligations will not hesitate to be similarly over-enthusiastic in their restrictions, leading to young people being unable to find and access useful and relevant information on those platforms.

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?

Health service providers are a class of entity for which the Code may require different requirements - noting the highly personal nature of healthcare information, and the need to use it in the best interests of the child, who may not be in a position to consent to this use.

The key consideration should always be the best interests of the child.

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

As above, the key consideration should always be the best interests of the child. By taking a child-centric rights-based approach, the various nuances

---

[10] LGBT Foundation (OSB0191), "Written Evidence," Parliament.uk, 2021, https://committees.parliament.uk/writtenevidence/39572/html/.
[11] Pride In Labour ' Is the Online Safety Act Blocking LGBTQ Resources?'. https://www.prideinlabour.org.uk/post/is-the-online-safety-act-blocking-lgbtq-resources
[12] Benjamin Butterworth, "Online Safety Bill Gives Legal Basis for LGBT Censorship, Warn Stephen Fry and Campaigners," The I Paper, September 2021, https://inews.co.uk/news/online-safety-bill-would-give-legal-basis-for-censorship-of-lgbt-people-stephen-fry-and-campaigners-warn-1178176?ref=wearequeeraf.com.

of the services provided by APP entities will be governed by general principles.

3. Age range-specific guidance

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

Yes, particularly in terms of shaping communications with children to help them manage their privacy in terms that are understandable and age-appropriate.

In terms of the mechanics of the Code, the requirements of entities to handle data in privacy-respecting fashion, and adherence to the APPs, there is no difference between the privacy rights of children of different ages.

However, the Code must take into account the fact that as children age, the extent to which it is appropriate for their guardians to speak for them decreases. This is especially relevant in the context of teenagers seeking support for their gender and sexuality, and doubly-so for those young people who do not have the support of their family while navigating their sexuality.[13] The Code must reflect that, in some circumstances and for some age groups, the wellbeing of the child means that their guardians may not be suited to acting on their behalf.

[13] Mathijs Lucassen et al., "How LGBT+ Young People Use the Internet in Relation to Their Mental Health and Envisage the Use of E-Therapy: Exploratory Study," *JMIR Serious Games* 6, no. 4 (December 21, 2018): e11249, https://doi.org/10.2196/11249.

Application of Australian Privacy Principles (APPs)

Application of APP1: Open & transparent management of personal information

4.1 What communication methods should APP entities use to ensure privacy policies are meaningfully understood by children of different ages, abilities and backgrounds?

DRW notes and strongly concurs with Reset.Tech's research showing that fewer than one third of young people understood online terms and conditions to any extent[14] and their 2025 polling data showing that 63% of young people want terms of service written in simple, easy-to-understand language.[15]

The Code must ensure that entities that collect data from or about children have proactive obligations to ensure transparency and accountability surrounding data use.[16]

Privacy policies must be written in language accessible to children, including those of non-English speaking backgrounds. To ensure that privacy policies are understood, entities must present collection notices in accessible, age-appropriate language, such as having it explained through videos or audio.

Entities should be responsible for demonstrating that their communications are understood by children.

---

[14] Reset Tech Australia, "The APPs and Children's Best Interests," Reset Tech Australia, April 2025, https://au.reset.tech/uploads/app-childrens-rights-briefing-paper.pdf.
[15] Reset Tech Australia, "Results from a Survey with Young People about the Children's Online Privacy Code," Reset Tech Australia, March 2025, https://au.reset.tech/uploads/copc-survey-of-young-people.pdf.
[16] Committee on the Rights of the Child 2021 General comment No. 25 (2021) on children's rights in relation to the digital environment.Paragraph 39, https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021

4.2 How should APP entities ensure APP1 obligations are met when their services are used by both adults and children, particularly when children are not the intended primary users?

DRW strongly believes that APP entities should treat all data on their services as belonging to a child unless the entity is able to prove otherwise.

It is far safer for both adults and children for adults to be accidentally afforded extra privacy protections than it is for children to have them accidentally removed.

4.3 What should be considered under the 'reasonable steps' test when implementing internal practices, procedures and systems for managing children's personal information?

In terms of handling the data of a child: better than a "reasonable steps" test is a "best interests of the child" test.
In terms of identifying data as that belonging to a child, the reasonable step is for an APP entity to overcome the burden of proving that the data does not belong to a child, with the margin of error clearly falling on the side of treating more data as that of a child than not.

4.4 What steps should APP entities take to ensure children, and their parents, can easily make privacy-related inquiries or complaints, and how should APP entities respond in a child-appropriate way?

This is up to APP entities. However, DRW believes that the community would be best served by entities working with civil society and regulatory bodies such as the OAIC to determine common standards and processes that are transparent.
The Code must define minimum standards of timeliness, accessibility, and accountability for complaints and inquiries.

4.5 Do you have any specific views on how APP 1 should be applied or complied with in relation to the privacy of children?

The best way for entities to comply with APP1 is to not collect and store information that they do not need. In line with European policy, companies

should be required to submit a statement to the OAIC accurately describing their harvesting, use, retention, or transfer of children's data and justifying that this use is beneficial to the child. [17]

Application of APP 2: Anonymity and pseudonymity

DRW notes and agrees with the Reset.Tech findings that anonymity and pseudonymity are largely under-utilised privacy tools.[18] We also note that they are especially important in creating a safe environment to encourage students to seek sexual health help. Two thirds of secondary school students turn to the internet for sexual health advice.[19]

5.1 How can APP entities provide children with meaningful options to use services anonymously or under pseudonyms, considering their developmental stages at different ages?

APP entities must offer to children the ability to create pseudonymous accounts, and/or interact with the service anonymously, unless it is in the best interest of the child to have a named account. They must do this in a manner that is easily understood by the child.

5.2 In what scenarios would it be justifiable to require children to identify themselves in order to access an APP entity's service? How can these instances be minimised to protect their privacy?

There are instances where a child may need to be identified - classroom management systems, healthcare providers, learners' driving licences. DRW believes that APP entities should be required to justify their identity requirements to the OAIC as being in the child's best interest before restricting access to only identifiable children.

---

[17] Information Commissioner's Office, "2. Data Protection Impact Assessments," Ico.org.uk (ICO, May 19, 2023), 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/2-data-protection-impact-assessments/.

[18] Reset Tech Australia, "The APPs and Children's Best Interests," Reset Tech Australia, April 2025, https://au.reset.tech/uploads/app-childrens-rights-briefing-paper.pdf.

[19] Jennifer Power, Sylvia Kauer, Christopher Fisher, Roz Bellamy & Adam Bourne 2022 The 7th National Survey of Australian Secondary Students and Sexual Health 2021 https://ssashsurvey.org.au/wp-content/uploads/2023/10/2021_SSASH_Report.pdf

5.3 Are there instances where age assurance technologies conflict with an individual's right to remain anonymous or pseudonymous, and what evidence supports this, or suggests otherwise?

Age-assurance technologies are antithetical to privacy and deleterious to the ability to remain anonymous.[20] They all, to a greater or lesser extent, require an individual to compromise some aspects of their privacy in order to validate their age, whether that's in a facial recognition age estimate, details of an ID card, or patterns of behaviour or speech.[21]

Age assurance technologies have no place in protecting children's privacy or providing excuses for entities to neglect their APP duties.

5.4 Do you have any specific views on how APP 2 should be applied or complied with in relation to the privacy of children?

Entities must not attempt to de-anonymise users other than in instances where real-world harms may result (eg: self-harm or harm to others).

Application of APP 3: Collection of solicited personal information

The easiest way to ensure children's privacy is preserved is to not collect their data in the first place.
Reducing the amount of children's data reduces the need for data to be processed, secured, and safely destroyed.
Reducing the amount of data collected about a child also reduces the impact should that data be leaked.

---

[20] Jason Kelley, "Age Verification Mandates Would Undermine Anonymity Online," Electronic Frontier Foundation, March 10, 2023, https://www.eff.org/deeplinks/2023/03/age-verification-mandates-would-undermine-anonymity-online?.
[21] CNIL, "Online Age Verification: Balancing Privacy and the Protection of Minors | CNIL," www.cnil.fr, September 22, 2022, https://www.cnil.fr/en/online-age-verification-balancing-privacy-and-protection-minors.

6.1 What criteria should define what is ‘reasonably necessary’ for an APP entity’s functions or activities when collecting children’s personal information, and how can APP entities ensure they adhere to this?

The existing APP3 criteria are excellent and should apply to the COP Code. The code should prohibit the collection of children’s data other than that required to run a service. This collection should extend to data ingested from data brokers.

6.2 What does ‘lawful ‘and ‘fair’ mean in the context of children’s personal information? How should these terms be applied specifically for children, given their evolving developmental and digital engagement stages?

There need to be additional criteria for children’s data: notably that the functions for which the data is collected are operated in the child’s best interest and that consent must be gathered in a manner that is understood by the child and can be removed by them.

6.3 Are there cases in which the collection of children’s personal information would not be considered fair in any circumstances?

It would not be fair to collect children’s person information under the following circumstances:

- The child has not been able to grant meaningful informed consent
- The data is not required for the operation of the service
- It is not in the child’s best interest to share this data.

6.4 How can APP entities obtain genuine consent from children, or their parents or guardians, for the collection of sensitive information?

The current APP assumes that a user has the ability to consent. However, a child may not be capable of giving informed consent. The code must account for this, and not allow children to consent to uses of their data that are not in their best interest.

Consent must be informed, explicit, and time-bound. Entities should be required to regularly update consent for their services.

6.5 Do you have any specific views on how APP 3 should be applied, or complied with, in relation to the privacy of children?

Children's data is increasingly being collected by EdTech, something that increased in popularity during the COVID19 Pandemic[22], and apps designed for kids[23]. Currently, the legislation does not account for this.

All practices that obtain a child's data must be justified in a statement to OAIC explaining how the collection of this data directly benefits the child.

Application of APP 4: Dealing with unsolicited personal information

The requirements of APP 4 are good and commendable. They should be supported by the Code.

7.1 What processes should APP entities implement to identify and appropriately handle unsolicited personal information related to children?

This is up to entities to decide. However, the Code should enforce additional reasonable timelines and expectations for unsolicited personal information about children.

It is reasonable to expect entities to have some basic protections to prevent children from accidentally providing their personal information - eg: "You've put your home address in a comment. We don't allow that so we've hidden it"

[22] Human Rights Watch 2022, 'How dare they peep into my private life!' https://www.hrw.org/report/2022/05/25/how-dare-they-peep-my-private-life/childrens-rights-violations-governments
[23] Children & Media Australia 2022, 'Apps can track' https://childrenandmedia.org.au/app-reviews/apps-can-trap-tracking

7.2 Do you have any specific views on how APP 4 should be applied, or complied with, in relation to the privacy of children?

The COP Code must be adhered to regardless of how an entity came into possession of the data it holds. Entities must not put children's privacy at risk behind the excuse of their ingestion of data from unknown sources.

Application of APP 5: Notification of the collection of personal information

APP 5.2 is clear that entities cannot treat the notification of users about data collection as a mere tick-box exercise. To meet the threshold of genuine awareness for children, organisations must present collection notices in accessible, age-appropriate language and communicate them directly to the child in a clear and understandable way.
We note Reset Tech's findings that 76% of 16-17 year olds found privacy policies to be 'too long' and a further 46% found that the information was hard to read[24] and would like shorter Privacy Policies.[25]

8.1 What methods can be employed by APP entities to effectively notify or ensure children are aware of data collection practices in a manner that is age-appropriate and can be easily understood by children?

To ensure that privacy policies are understood, entities must present collection notices in accessible, age-appropriate language, such as having it explained through videos or audio.
Entities should re-notify users on a regular basis

8.2 How can APP entities ensure that notifications are accessible to children with diverse needs, including those from culturally and linguistically diverse backgrounds, or living with disability?

[24] Reset Tech Australia, 'Did we really consent to this?', 2021 https://au.reset.tech/uploads/l01_resettechaustralia_policymemo_t_c_report_final-july.pdf
[25] Reset Tech Australia, "Results from a Survey with Young People about the Children's Online Privacy Code," Reset Tech Australia, March 2025, https://au.reset.tech/uploads/copc-survey-of-young-people.pdf.

DRW believes that the OAIC should issue guidance in this matter with expertise from civil society organisations working with young people in diverse communities.

8.3 Are there circumstances in which an APP entity would be justified in taking no steps to notify or ensure children are aware about data collection practices? How can we minimise these instances to ensure that APP entities are adopting a best practice approach when it comes to notification and awareness?

If the APP entity is not collecting children's data, there would be no need for them to do notifications and gather consent. While this seems glib, it is DRW's position that entities tend to collect more data than they need for the operation of a service and that they should be incentivised to collect less.

If children's data is collected, it is in the child's best interest that there must be notification and consent. We are unable to imagine circumstances in which this might not be the case. We can envisage cases, particularly around sexual health and identity, where it is not appropriate for an entity to notify a child's guardian, however.

Application of APP6: Use or disclosure of personal information

9.1 How can APP entities obtain genuine consent from children, or their parents or guardians, for the use or disclosure of their personal information, while ensuring that they comprehend the implications of such use or disclosure?

The replacement of the vague "reasonable expectation" standard with a stricter "best interests of the child" test will allow for better comprehension of terms and conditions.

Privacy policies should include a statement on how automated decision-making will be used in relation to children. This will enable children and guardians to provide informed consent regarding us and disclosure of personal information.

9.2 What safeguards should APP entities put in place to prevent the misuse of children's personal information for secondary purposes without appropriate consent or where other exceptions apply?

APP entities should be subject to maximum data retention periods requiring them to automatically delete children's data after a certain time unless retaining the data has a clear benefit to the child.

APP entities should face a prohibition on secondary use without explicit consent to disallow secondary uses of children's data without informed age-appropriate consent from the child or their guardian.

APP entities could make use of a "nightly algorithmic reset" of content recommendation algorithms for a child user's profile to remove any personal information gathered over the previous 24 hours. This will ensure that the information gathered remains as small as required to run the service, but that secondary purposes such as the creation of advertising profiles won't be able to build up longitudinal data on a child.

9.4 Do you have any specific views on how APP 6 should be applied or complied with in relation to the privacy of children?

Young people have expressed a desire to curb the overcollection of data and its subsequent sharing: 87% of 16-17 year olds surveyed noted they did not wish for their data to be shared beyond what they had consented to.[26] The Children's Online Privacy Code should reflect this.

Young people have a high level of distrust and generally low expectations regarding the use of their personal information by companies.[27]

---

[26] Reset Tech Australia, 'Response to the draft Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021, reflecting the views of children and young people', 2021 https://consultations.ag.gov.au/rights-and-protections/online-privacy-bill-exposure-draft/consultation/ view_respondent?_b_index=60&uuId=1044012677

[27] Reset Tech Australia, "The APPs and Children's Best Interests," Reset Tech Australia, April 2025, page 20 https://au.reset.tech/uploads/app-childrens-rights-briefing-paper.pdf.

Application of APP 7: Direct marketing

10.1 Can an APP entity ensure that it creates a 'reasonable expectation' that it may use or disclose children's personal information for the purposes of direct marketing? And if so, how?

The Code must also include strong transparency requirements of entities on how they use data to target advertising at users.

10.2 How can APP entities ensure mechanisms are in place for children to opt-out of receiving direct marketing communications, in a simple and accessible way?

The Code should clearly and unequivocally ban targeted advertising to children. Ireland's privacy rules offer a useful example of how this could work.[28][29]

10.3 Do you have any specific views on how APP 7 should be applied or complied with in relation to the privacy of children?

The Code should remove exemptions which allow for the aggressive ad targeting of children and instead replace them with a simple test asking if the exemption is in the child's best interest. Currently, children are targeted with different ads depending on characteristics such as gender, religion or ethnicity, infringing the child's right to be free from discrimination. 52% of young people surveyed believe that young people should not be targeted with direct advertising. 48% believe that platforms should not use their sensitive data for advertising purposes.[30]Removing the exemptions protects children from discrimination, unfair targeting and better reflects the wishes of young people.

---

[28] Data Protection Commission, "Data Protection Legislation | Data Protection Commission," Data Protection Legislation | Data Protection Commission, January 31, 2019, https://www.dataprotection.ie/en/who-we-are/data-protection-legislation.
[29] DLA Piper, "Law in Ireland - DLA Piper Global Data Protection Laws of the World," Dlapiperdataprotection.com, 2016, https://www.dlapiperdataprotection.com/index.html?t=law&c=IE.
[30] Reset Tech Australia, "Results from a Survey with Young People about the Children's Online Privacy Code", March 2025, https://au.reset.tech/uploads/copc-survey-of-young-people.pdf.

Application of APP8: Cross-border disclosure of personal information

11.1 How can APP entities ensure that cross-border transfers of children's personal information are conducted in a way that protects children's privacy rights, especially when laws in other countries may not offer equivalent protections?

The Code should explicitly state that children's privacy, and the code, applies to data processed outside Australia when transferred there by an Australian entity.

11.2 What steps should APP entities take to communicate with children (or their parents or guardians) about the risks of cross-border data transfers?

The Code should state that APP entities transferring data across borders, where legal privacy protections are less than those afforded by the APPs, must inform users not only that their data is being transferred offshore, but also of the legal protections that it may no long be afforded.

11.3 Do you have any specific views on how APP 8 should be applied or complied with in relation to the privacy of children?

Cross-border data transfers jeopardise the privacy of a child, as the recipient nations may have poorer privacy standards than Australia or may have contradicting privacy laws eg. retaining data for long periods of time. Storing child data in a different jurisdiction may provide loopholes around data retention laws in Australia.

Furthermore, nations have differing levels of legal majority - Australian teenagers could qualify as adults in other nations, and would not be afforded the extra protections due children.

Application of APP 10: Quality of personal information

12.1 What does ‘accurate’, ‘up-to-date’, ‘complete’ and ‘relevant’ mean in the context of children’s personal information? How should these terms be applied specifically for children, given their evolving developmental and digital engagement stages?

‘Accurate’, ‘up-to-date’, ‘complete’ and ‘relevant’ in the context of children’s personal information means a proactive approach to deletion of information that does not fit this criteria, including upon request by individuals. This accords with recommendations such as the capability for nightly algorithmic resets referenced above in relation to APP6.

12.2 How can APP entities effectively ensure that the personal information they collect from children remains accurate and up-to-date, considering the dynamic nature of a child’s life and the potential challenges in maintaining this data?

The current APP lacks sufficient support in correction and deletion rights. Children aren’t guaranteed the right to access or alter their recorded data, and there is no right to erasure, which has been recommended by the Attorney General’s department.

Entities should offer more options for more frequent deletion of a child’s data in recognition of their dynamic life stages - consider default deletions of mutable data on a “new school” basis with more frequent opt-in options yearly or similar.

12.3 Do you have any specific views on how APP 10 should be applied or complied with in relation to the privacy of children?

As we set above, there is no justification for the collection of data for marketing to children. APP entities must be vigilant to not collecting children’s data for marketing purposes.

The code must guarantee children and their guardians the right to access, change, or delete their recorded data (by default and with elective options) to ensure it remains accurate, up-to-date, complete and relevant

Application of APP 11: Security of personal information

13.1 Are there any additional or specific technical measures that APP entities should adopt to safeguard children's personal information from security risks, considering their heightened vulnerability?

Encryption is a vital tool in privacy protection, Efforts to weaken encryption to aid detection of child sexual abuse material (CSAM) weaken children's safety. Children's privacy and safety relies on their right to access securely-encrypted systems.[31]APP entities should not be able to break into children's end-to-end encrypted data where used. The Code should explicitly reassert that children have the right to use encrypted systems to keep their information secure.

For datasets containing both children and adult individual's data, the presumptions should be that the Children's Online Privacy Code applies to the entire dataset.

13.2 Are there any additional or specific organisational measures that APP entities should adopt to safeguard children's personal information from security risks, considering their heightened vulnerability?

APP entities need to have policies in place to ensure that a child's guardians are able to access a child's data only when it is in the best interests of the child. APP entities should ensure that relevant employees are aware of Children's Online Privacy Code obligations and best practices.

13.3 How can APP entities ensure their data retention policies are appropriate for children's data, including timely deletion or de-identification when the information is no longer needed?

[31] CRIN 2023 A children's rights approach to encryption https://home.crin.org/readlistenwatch/stories/privacy-and-protection

The Children's Online Privacy Code ensures that children have the right to remedy and address, as outlined in the general comment.[32]Enshrining a general approach of data minimisation, can limit the impact of cybersecurity breaches when they occur. APP entities must not rely on de-identifying data as too often it is trivially simple to re-identify this data. It is not safe to apply this technique for children's safety. [33]

As per our comments above in respect of APP 10, entities need to allow for more frequent default deletions of children's data.

13.4 Do you have any specific views on how APP 11 should be applied, or complied with, in relation to the privacy of children?

"States parties should protect children from cyber aggression and threats, censorship, data breaches and digital surveillance."[34]

APP 11's reasonable steps test doesn't outline how it applies to children's privacy specifically

Cyberattacks and leaks pose a uniquely dangerous risk to children, especially where location data, contact information, or behavioural data are involved. Data breach notification systems and support remedies may not be accessible to children. APP entities have a duty to ensure that breach notifications are accessible and responsible. This could include learning materials for both children and guardians and must be conducted in a manner that is in the best interest of the child (including who is the appropriate person to notify if the child's personal information is compromised). [35]

---

[32] United Nations, "General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment," OHCHR, 2021, https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation.

[33] Office for the Victorian Information Comissioner, 'The Limits of De-Identification - Protecting Unit Level Personal Information' https://ovic.vic.gov.au/privacy/resources-for-organisations/the-limitations-of-de-identification-protecting-unit-record-level-personal-information/

[34] United Nations, "General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment," OHCHR, 2021, https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation.

[35] Normann Witzleb, Moira Paterson, Jordan Wilson-Otto, Gabby Tolkin-Rosen and Melanie Marks 'Privacy risks and harms for children and other vulnerable groups in the online environment' page 22-28. https://www.oaic.gov.au/__data/assets/pdf_file/0012/11136/Report-Privacy-risks-and-harms-for-children-and-other-vulnerable-groups-online.pdf

Application of APP 12 : Access to personal information

14.1 What mechanisms are needed to ensure children can easily access their own personal information?

With the exception of particular circumstances that might arise under 14.2 below, in general, personal information should be able to be easily accessed by children themselves, without the need to take multiple steps or navigate complex request systems, and should be provided in a format that can be easily understood by children.

14.2 In what circumstances might providing a child access not be in their best interests? What would help entities navigate these situations responsibly?

As a general principle, children must be able to access their personal information unless it is not in their best interest to do so. Entities should consult with expert groups for their specific data use cases to help determine when it may not be in their best interest. The same applies to providing access to a guardian.

14.3 In what circumstances should a parent or guardian be able to make an access request on their child's behalf and receive a copy of their child's personal information? How should the balance be struck between a parent's right to protect the best interests of their child and the child's right to privacy, when APP entities are dealing with access requests for a child's personal information?

As above, guardians should only be granted access when it is in the best interests of the child. For most use cases, and for most ages, it would be appropriate. As children age into teenagers and young adults, and access more adult-like services, it will become less appropriate.

14.4 What timeframe should be considered a 'reasonable period' for responding to a child's access request?

Default mechanisms for data access referred to in 14.1 above should be available instantly. There may be particular scenarios (referred to in 14.2 and 14.3 above) where consultation with experts about the disclosure may be appropriate, which would require a longer period for a response.

14.5 In what manner or format should personal information be provided to a child when an access request is made, so that it is both practicable for APP entities and developmentally appropriate for children of different ages and capacities?

The OAIC should engage with child development experts to determine standards for the manner and formats in which children should receive their access requests.

14.6 Do you have any specific views on how APP 12 should be applied or complied with in relation to the privacy of children?

The General comment emphasises the importance of children and caretakers to be able to access data relating to themselves. [36]

The code must compel platforms to allow users to view, correct, and delete any data that entities keep about them. In line with this, children and guardians must be able to easily access a correction system.

Application of APP 13 : Correction of personal information

[36] United Nations, "General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment," OHCHR, 2021, https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation.

15.1 What does ‘accurate, ‘up-to-date’, ‘complete’, ‘relevant’ and ‘not misleading’ mean, in the context of children’s personal information, given their evolving developmental and digital engagement stages?

The Code should recognise that children’s developmental stages change very rapidly and therefore entities must ensure that they offer children a path to correct and update their information that is straightforward.

15.2 What processes or mechanisms should be established to allow children to request corrections of their personal information easily?

This is up to APP entities to implement based on guidance and requirements in the code. Processes should be automated, simple, and rapid.

15.3 In what circumstances should a parent or guardian be able to make a correction request on their child’s behalf?

Guardians should always be able to request a correction but entities should only action it when it is in the best interest of the child.

15.4 What timeframe should be considered a ‘reasonable period’ for responding to a child’s correction request?

We refer to our response at 14.4 above.

15.5 Do you have any specific views on how APP 13 should be applied or complied with in relation to the privacy of children?

There may be narrow justifications for entities refusing to comply with APP13 (for instance, in healthcare settings) but a refusal can only be justified when it is in the best interests of the child.

Further comment on relevant issues

Alignment with international standards

Article 16 of the *Convention on the Rights of the Child* affirms that "no child shall be subjected to arbitrary or unlawful interference with their privacy."[37] This right extends to the digital environment through the UN Committee's *General Comment on Children's Rights in Relation to the Digital Environment*, which clarifies how privacy protections must be applied online[38].

The General Comment states that to uphold children's right to privacy, governments must prohibit profiling and targeting children for commercial purposes based on any digital record of their actual or inferred characteristics—including group data, affinity profiling, or behavioural traits[39].

UNICEF further distinguishes between general advertising and targeted advertising, warning that targeted advertising often violates children's rights, as much of the data collection involved occurs without meaningful consent or even knowledge. These practices undermine children's autonomy and repeatedly breach their privacy[40].

The OAIC has already named the UK as a point of reference in their development of the Children's Privacy Code.[41] The UK standards would represent a step forward for Australian privacy codes. However, we believe that they can be built upon to better protect the privacy of children.

Modelling the Children's Privacy Code entirely off the UK Code risks replicating the same weak spots. One critical weakness in the UK Code is its treatment of targeted advertising and profiling. While the Code

---

[37] United Nations, "Article 16, Convention on the Rights of the Child," OHCHR (United Nations, November 20, 1989), https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child.
[38] United Nations, "General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment," OHCHR, 2021, https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation.
[39] ibid
[40] UNICEF, "Children and Digital Marketing," Unicef.org, 2018, https://www.unicef.org/childrightsandbusiness/workstreams/responsible-technology/digital-marketing.
[41] OAIC, "Better Privacy Protections for Children Are Coming," OAIC, September 16, 2024, https://www.oaic.gov.au/news/blog/better-privacy-protections-for-children-are-coming?.

discourages profiling and mandates that such features be switched off by default, it does not prohibit them outright.[42] This leaves room for commercial exploitation of children's data through opt-ins, "dark patterns," or parental waivers. Moreover, the standard does not require platforms to justify profiling or advertising on a best interests basis, meaning enforcement depends heavily on corporate discretion.

Ireland offers a more protective model. Under the *Irish Fundamentals* for children's data processing, the Data Protection Commission takes a presumptive stance against targeted advertising to children[43]. Profiling is explicitly disallowed unless the controller can demonstrate that the processing is in the best interests of the child, a test grounded in Article 3 of the CRC[44]. This reversal of the burden of proof places accountability squarely on entities seeking to process children's data and aligns more closely with the *General Comment No. 25*.[45]

A key feature of both UK and Irish legislation is child privacy impact assessments which must be submitted to the information commissioner explaining how an entity's data collection, retention, & use is benefitting the child. Australia could adopt a similar process that is straightforward and accessible, yet thorough and child-centric.

Australia's delayed adoption of a dedicated children's privacy code creates a unique opportunity: to learn from existing international models. By integrating the UK's best design principles while adopting Ireland's stronger stance on targeted advertising and profiling, the OAIC can set the COP Code as a global benchmark.

---

[42] ICO, "Age Appropriate Design: A Code of Practice for Online Services," ico.org.uk, May 19, 2023, 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/.

[43] Data Protection Commission, "CHILDREN FRONT and CENTRE for a CHILD-ORIENTED APPROACH to DATA PROCESSING FUNDAMENTALS," 2021, https://www.dataprotection.ie/sites/default/files/uploads/2021-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_FINAL_EN.pdf.

[44] United Nations, "Article 3, Convention on the Rights of the Child," OHCHR (United Nations, November 20, 1989), https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child.

[45] Reset Australia, "The Children's Online Privacy Code and Targeted Advertising," 2025, https://au.reset.tech/uploads/copc-target-advertising-roundtable.pdf.

Recommendations

General Principles

- The Code should adopt a child-first, transparent approach, regulating not just user-facing content but the data flows, profiling, and storage practices that underpin them.

- The Code should include a “best interests of the child” test as its governing standard, aligning with Article 3 of the Convention on the Rights of the Child.

- The Code should apply to all services likely to be accessed by children, with a default inclusion model and limited, justified exemptions determined by the OAIC.

Age-Based Protections

- Avoid issuing exemptions to entities using age-estimation and age-gating, which are privacy-invasive and easily bypassed.

- Ban age-gating as a compliance workaround; require any age verification tools to comply with the Code.

- Provide all privacy messaging in accessible, age-neutral formats.

Technology-Specific Safeguards

- COP Code principles should apply across all entities handling children’s data, including AI, healthcare, and EdTech.

- AI and emerging tech presents unique risks (e.g. training data, inference models). The Code should err on the side of children’s right to privacy. This might include:

    - Complete ban on the use of children’s data for AI model training. AI providers to demonstrate and certify that their systems are not trained on children’s data.
    - AI models found to have been trained on children’s data are in breach and subject to penalty.

    - AI tools that are used by children to require child-specific DPIAs.

Good Practices

- Do not replicate the UK's weaknesses, especially around opt-outs for targeted advertising.

- Adopt the Irish model: prohibit profiling unless it meets the best interests of the child, and shift the burden of proof to data processors.