Submission to the
Office of the Australian Information Commissioner [OAIC]
Children's Online Privacy Code

By the Australian Research Council Centre of Excellence for the Digital Child

This submission is made by the Australian Research Council (ARC) Centre of Excellence for the Digital Child with thanks to Centre members who contributed to this submission, including [redacted]

About the Australian Research Council Centre of Excellence for the Digital Child

The ARC Centre of Excellence for the Digital Child ('Digital Child') plays a key role in leading national and global research, policy and practice to ensure that all Australian children are healthy, educated and connected in a rapidly expanding digital world.

The Digital Child positively shapes an environment with children and families, and with educational contexts and communities to support their navigation of their digital worlds. We know that children's daily experiences are rapidly changing, and that every childhood is now fundamentally digital. Our mission is to build positive digital childhoods for every child in Australia.

We do this by focusing on:

- Healthy digital lives, understanding how digital technology intersects children's lived experiences and providing guidance to families, educators, and policymakers as they navigate this space.
- Educational empowerment, equipping children with the skills they need to live their best digital lives.
- Safe digital spaces, making online engagement safer while promoting healthy digital relationships.

This submission provides a brief response to the Children's Online Privacy Code Exposure Draft. We would be pleased to provide further information, including an oral submission.

Contact information

[redacted]

Position Statement

The ARC Centre of Excellence for the Digital Child welcomes this opportunity to respond to the Office of the Australian Information Commissioner's Children's Online Privacy Code 2026 Exposure Draft. The national Centre is a team of over 200 multidisciplinary researchers across Australia and internationally, with disciplines including education, media and communication, health, psychology, sociology, law and computer science. We recognise, through this feedback on the Exposure Draft of the Children's Online Privacy Code (the Code), children of all ages interact online in various ways. We emphasise the importance of protecting the rights of **children who are growing up in a rapidly changing digital age** [1]**.**

The Centre upholds the work of the OAIC to genuinely engage with children to inform the design and feedback on the Code. **It is particularly pleasing to see the uplift to privacy protections for Australian Children** outlined in the Code and the clear alignment with United Nations Conventions on the Rights of the Child (UNCRC). Importantly the comments and recommendations in this submission **are intended to illustrate the ways that the Code can go further in strengthening these protections,** recognising that privacy is a foundational and enabling human right. For children, privacy is especially important as they develop autonomy and independence, form their identity, and exercise freedom of thought. For this submission, a 'child' is defined as any person under the age of 18 years as per Article 1 of the UNCRC.

Key recommendations

- Include that the collection of information be **fair and reasonable** in the circumstances and list those circumstances. Draw from the Privacy Act Review Report (2022) to inform the objective assessment as to whether the collection, use and disclosure is fair and reasonable (see Proposals 12.1 and 12.2). *These factors include, but go beyond* whether the collection, use (etc.) is in the child's best interests.
- **Detailed definition of personal information**. Be more explicit in the definition than outlined in the APPs. List all data collection, generation, inferrence, observation, processing or storage by an entity that might reasonably identify a child, regardless of whether that data meets the statutory threshold for personal information.
- Reframe the **definition of 'parental responsibility' for** better alignment with legal decision-making responsibility as per the *Family Law Act 1975* (Cth).
- Application of the Code to adult end-users of online services primarily concerned with the activities of children requires consideration and further detail. **Protections should be explicitly extended to the adult end users of online services that are primarily concerned with the activities of children** (see Division 1, Sections 8-11) to curtail the deceptive structuring of family accounts as a proxy for the collection, use and disclosure of children's data.
- We note **the significant need for the expansion of resourcing** to ensure the OAIC are able to fulfill their enforcement obligations under the Code.
- Further consideration is to be given to the ways that children's personal information, where it may be integrated into an LLM, may be shared with third-parties or used to train LLMs when the service is likely to be accessed by children or primarily concerned with the activities of children.

This submission outlines **24 Recommendations** in total.

[1] https://digitalchild.org.au/

Response to Exposure Draft Privacy (Children's Online Privacy) Code 2026

Part 1—Preliminary

Clear and robust definitions [4]. This is pertinent given the OAIC's ambition to put Australian children at the centre of privacy protections and highlights the opportunity for the Code to provide clarity for Entities and serve as an educative standard for all Australians.

Age-appropriate. We support the Code's recognition that age-appropriate information must be assessed by reference to the youngest child likely to access or use the service. In particular, where a service is directed to a specified age range, information should be suitable for the youngest child within that range; and where no specific age range is identified, the default standard of appropriateness for children aged 10 to 12 years provides a clear and workable compliance benchmark for regulated entities. In terms of the drafting of the definition the word 'if' is repeated unnecessarily in sub-clauses (a) and (b).

Definition of 'person with parental responsibility'. The definition is important because, in the Code, a person with parental responsibility is able to provide consent to the collection, use or disclosure of information whenever consent is required and where the child is under 15 (or otherwise lacks capacity). The definition of parental responsibility in the draft Code states that a parent of the child, a guardian of the child or a person who is legally responsible for the child's day-to-day care, welfare and development has parental responsibility. However, for family law purposes, there will be situations where court orders provide that only one parent should have parental responsibility (or decision making responsibility). Alternatively, the court may grant decision making responsibility to a person (such as a guardian) who is not a parent.

Reconsider the definition of parental responsibility. It is not appropriate to allow a parent (or other person) without legal decision-making responsibility in relation to a particular child, to make decisions in relation to the child's personal information.

We recommend:

1. **Provide a detailed definition of personal information.** The Code operationalises the definition of personal information set out in section 6 of the Privacy Act 1988. Given the central role of the personal information definition, we recommend the Code (Part 1) should *include a clear definition of personal information.* The definition should include details from APP (B88-92) ***and*** explicitly reference behaviour and engagement data that can be collated and combined to reasonably identify children.
2. **Refine wording of age appropriate.** Remove the word 'if' which is repeated unnecessarily in sub-clauses (a) and (b).
3. **Reframe the definition of 'person with parental responsibility'** so that it better aligns with legal decision-making responsibility as per the *Family Law Act 1975* (Cth). For example, the definition *person with parental responsibility*, in relation to a child, means, the person or persons with legal decision-making responsibility in relation to the child as per the *Family Law Act 1975* (Cth). However, parental responsibility is complex and advice from family law experts should be sought to further refine this definition.

Part 2—Application of this Code

We particularly **welcome the inclusion of online services that are primarily concerned with the activities of children (Section 7(b))**. This is an important protection for children, as many online services that are primarily concerned with the activities of children in particular, are designed with parent or adult accounts[2].

We note that the draft exposure and explanatory statement are **currently unclear in how the Code applies to adult end-users of online services primarily concerned with the activities of children**. Evidence shows that data collection about children is facilitated through an adult proxy, through connecting children's or family data with the adult end-users personal information[3]. This type of account set up is increasingly popular in EdTech products, which facilitates deceptive data collection and commercially exploitative profiling of families and children[4].

We acknowledge that the application of the Code **requires further consideration for entities that are a provider of online services using Large Language Models (LLMs)**. In conventional data systems, records are discrete and traceable, enabling deletion or correction upon request. By contrast, LLMs do not store data as retrievable entries but rather encode information. Therefore, entities that use LLMs to collect, use and process children's personal information will not be able to comply with **Divisions 2, 4 and 5** of the Code.

We recommend:

4. **Clarification on how the Code applies to adult end-users of online services primarily concerned with the activities of children** is required in both the Code and explanatory materials.
5. **Protections be explicitly extended to the adult end users of online services that are primarily concerned with the activities of children** to curtail the structuring of family accounts as a proxy for the collection, use and disclosure of children's data, along with deceptive and commercially exploitative profiling of families and children.

Part 3—The Australian Privacy Principles and the privacy of children

Division 1 - General Requirements

Sections 8-11 set out the necessary foundations for entities to enact protections of children's personal information set out in all other divisions of the code. We **welcome the inclusion of the privacy by default mechanism.** We welcome the reduction of compliance burden associated with ascertaining the age of end users for entities in circumstances where the Code's divisions are applied for *all users* of applicable online services [section 8] and acknowledge the broad uplift to Australian privacy that this clause invites.

We acknowledge the need for an entity's services to ascertain the age of end users as a necessary step to enacting a Children's Code. The OAIC already provides sound guidance on age assurance technologies and privacy obligations to entities, even outside of the specific context of the Children's Code[5]. However, **we**

[2] Langton, K., & Ng, R. (2025). "Tracking the Trackers" of children's first personal data in mobile applications: Using static analysis and privacy policy evaluation to explore the data-sharing capabilities and practices of baby apps. Proceedings of the 37th Australian Conference on Human-Computer Interaction, 845–859. https://doi.org/10.1145/3764687.3769936

[3] Kemp, K. (2023). *Your body our data—Unfair and unsafe privacy practices of popular fertility apps*. UNSW Sydney. https://dx.doi.org/10.2139/ssrn.4396029

[4] Apps, T., Beckman, K., & Howard, S. K. (2023). Valuable data? Using walkthrough methods to understand the impact of digital reading platforms in Australian primary schools. *Learning, Media and Technology, 48*(2), 294–309. https://doi.org/10.1080/17439884.2022.2160458

[5] OAIC. (2026). *Privacy guidance on age assurance technologies.* https://www.oaic.gov.au/__data/assets/pdf_file/0017/262043/OAIC-privacy-guidance-on-age-assurance-technologies.pdf

recommend additional guidance be provided to entities in the form of a typology of specific approaches and options for age assurance. We also highlight the utility of this guidance as education material to increase digital, data and privacy literacy of end-users. For instance, depending on the purpose and nature of the service, and the sensitivity of the personal information collected, a range of example approaches or acceptable technologies could be provided to entities, oriented on the three primary categories of age assurance referred to by the European Data Protection Board[6]: age estimation, age verification and self-declaration, which may be supplemented by parental attestation, as outlined in the current OAIC guidance. Where services are planning to integrate age assurance technologies from an external provider, the introduction of certification based on the specific rules outlined in the Code could be considered, similar to the UK's Age Check Certification Scheme[7].

Section 9 stipulates that entities may collect, use or disclose personal information about a child by default only if strictly necessary. We strongly support the principle of data minimisation, particularly in relation to children. However, **while this requirement is welcome, we wonder whether it is open to challenge on the basis that it goes beyond the legislative scope of the Online Privacy Code as provided for in the *Privacy Act 1988*?**

Section 26C(3)(a) of that Act provides that the code may impose additional requirements if they are 'not contrary to or inconsistent with the Australian Privacy Principles (APPs).' The effect of APP 3.1 and 3.2 is to permit the collection of personal information (other than sensitive information) without consent where that is 'reasonably necessary for or directly related to one of the entity's functions or activities'.

The effect of the proposed section 9 would be to *prohibit* automatic collection of personal information, unless that information is strictly necessary (even if it was reasonably necessary). As such, there is a risk that section 9 is contrary to or inconsistent with APP 3.2.

The draft Explanatory Statement suggests that section 9 does not narrow and restrict the operation of APP 3.1 or 3.2 because it is 'directed to the default design of services'. Making the object of the section the design of services (such that the design prevents automatic collection of information that is not strictly necessary), rather than a prohibition on collecting non necessary information per se, could be a successful device here to achieve data minimisation. However, we suggest that there is still a risk that section 9 could be challenged on the basis that its *effect* does limit the right to collect information (other than sensitive information) where collection is reasonably necessary (not strictly necessary).

It may be worth considering, then, whether an alternative to Section 9 could be **the inclusion of a fair and reasonable test (as suggested in Recommendation 7 below)** which would specify as one of the factors informing the question as to whether collection was fair and reasonable 'whether the collection, use or disclosure is necessary to achieve the functions and activities of the entity'.

Section 10 posits that collection of Personal Information of a child must be consistent with the best interests of the child. Reference to the best interests of the child in relation to the collection and use of personal information is welcome. However, the current drafting of the code misses an opportunity to go even further (as explained below).

Opportunity to go further

The Privacy Act Review Report (2022) recommended the introduction of a fair and reasonable test in relation to information handling practices. The recommendation would introduce a requirement that the collection (as well as the use and disclosure) of information be fair and reasonable in the circumstances (see Privacy Act Review Report, Proposal 12.1). It would also set out a range of considerations to be factored into determining whether, objectively, information handling was fair and reasonable. One of these factors (set out in Proposal 12.2) is whether the collection (use, and disclosure) is in the best interests of the child.

[6] European Data Protection Board. *Statement 1/2025 on Age Assurance.* https://www.edpb.europa.eu/system/files/2025-04/edpb_statement_20250211ageassurance_v1-2_en.pdf

[7] Age Check Certification Scheme. (2026). *Age Check Certification Scheme*. https://accscheme.com/

While the recommendation to introduce a fair and reasonable test was accepted in principle by the Government (see Australian Government Response to Review) it has not (as yet) been introduced into the *Privacy Act*. As such, the APPs do not currently require either fair or reasonable information handling (except to the extent that APP 3.5 provides that an APP entity must 'collect personal information only by lawful and fair means').

The introduction of a fair and reasonable test would, arguably, not be contrary to or inconsistent with the current APPs but would *extend* the APPs. As such, it is arguably open to include this test in the code itself.

The fair and reasonable test for information collection, use and disclosure, if introduced into the Online Privacy Code, could adopt all of the factors listed in Proposal 12.2 of the Privacy Act Review Report that go to determining whether collection, use and disclosure is fair and reasonable. One of those factors is 'whether the collection, use or disclosure is reasonably necessary for the functions and activities of the organisation or is reasonably necessary or directly related to the functions or activities of the agency'. That particular consideration could be slightly amended to read 'the collection, use or disclosure is necessary' (not *reasonably* necessary).

Section 10(1) refers to compliance with APP 3.2, but not to APP 3.1. Is the intention then, that the requirement to consider the best interests of the child when collecting non-sensitive personal information apply *only* to organisations and not to agencies? The other sub-sections of section 10 appear to apply to all APP entities (i.e. both agencies and organisations), so it is unclear why the first sub-section should not.

As currently worded, section 10, seeks to require entities to ensure that the collection, use and disclosure of information is 'consistent with' the best interests of the child. It is clear from the draft Explanatory Statement that this is a deliberate choice to signify that the collection of information need not be in the child's best interests, provided it is not inconsistent with them. There is a risk that entities will fail to *actively* consider what is in the best interests of the child (in order to determine whether the collection is consistent with them); instead making assumptions that there is no incompatibility between the child's best interests and their own. If **Recommendation 7** below is adopted, this will become a moot point.

In **Section 11**, again, there is a risk that the use of the words 'consistent with the best interests' of the child will result in entities failing to actively consider what is in the best interests of the child.

We also suggest that **there is an opportunity to go further and include a fair and reasonable test** that would apply to the use and disclosure of information, along with the collection of information (see **Recommendation 7** below).

Subsection 11(1), the draft Explanatory Statement states that 'the introduction of this requirement will mean that entities will not be able to rely on APP 6.1(b) as a basis for the use and disclosure of a child's personal information. There is an argument that excluding 6.1(b) will be considered inconsistent and therefore open to challenge. Section 26C(3)(a) of the *Privacy Act* provides that the code may impose *additional* requirements if they are 'not contrary to or inconsistent with the Australian Privacy Principles'. There is no apparent power to exclude operation of any of the APPs. **This issue could be avoided if there is introduction of a fair and reasonable test that applies to the use and disclosure of information.**

Section 11(3)*,* the note to this sub-section explains that its effect is that the exception in APP 7.3 does not apply at all. The exception in APP 7.3 allows for the use of non-sensitive personal information in certain circumstances, including where the individual has consented or where gaining consent is impracticable (and other conditions are met). As such, there is an argument that excluding this is contrary to or inconsistent with the APPs and is, as such, open to challenge. Section 26C(3)(a) of the *Privacy Act* provides that the code may impose *additional* requirements if they are 'not contrary to or inconsistent with the Australian Privacy Principles'. There is no apparent power to exclude operation of any of the APPs. This issue could be avoided if

there is introduction of a fair and reasonable test that applies to the use and disclosure of information.

To minimise or prevent the disclosure of personal information about a child through their interactions with LLMs as outlined in **Section 11**, we recommend further consideration be given to how children's personal data, where it may be integrated into an LLM may be shared with third-parties or used to train LLMs when the service is likely to be accessed by children or primarily concerned with the activities of children.

We recommend:

6. Additional guidance be provided to entities in the form of **a typology of specific approaches and options for age assurance.** We also highlight the utility of this guidance as education material to increase digital, data and privacy literacy of end-users.
7. **A requirement be included in the Code that the collection of information be fair and reasonable** in the circumstances and list those circumstances. This should be drawn from the Privacy Act Review Report (2022) to inform the objective assessment as to whether the collection, use and disclosure is fair and reasonable (see Proposals 12.1 and 12.2).
   These factors include, but go beyond whether the collection, use etc is in the child's best interests as outlined in **Sections 10** and **11**.
   If included in the Code, factor (c) as per Proposal 12.2 could be amended to *omit the word* 'reasonably' so that the relevant consideration is whether collection, use or disclosure is 'necessary'.
8. **Further consideration to how children's personal information, where it may be integrated into an LLM,** may be shared with third-parties or used to train LLMs when the service is likely to be accessed by children or primarily concerned with the activities of children.

Division 2 - Consent

The requirements relating to giving and obtaining consent to the collection, use or disclosure of personal information about a child are generally well considered, and meaningfully oriented to similar international standards.

Section 13(1) suggests that a child may *only* have capacity to consent to handling of their personal information if they are 15 or over. However, children younger than 15 may be considered to have capacity on an individual basis if they have sufficient maturity to understand the consequences of giving or withholding consent. We prefer that – where practicable – the entity assesses capacity on an individual basis: this is consistent with the idea of children's evolving capacities in the Convention on the Rights of the Child. However, we support a broad statement that a child of 15 and above should *generally* be considered to have capacity (in line with current OAIC guidance).

Nevertheless, the code should reflect that some children of 15 and over do not have capacity to consent. In these cases, consent of the person with parental responsibility still must be sought.
We are concerned that this section provides that a child aged 15 and over *may* give consent for personal information handling. We suggest that if a child has capacity, they *must* give consent (rather than a person with parental responsibility).

Section 14 and **Section 15** detail that consent must be voluntary and informed, respectively. These requirements warrant further consideration in the context of school use of education technologies (EdTech). Schools expect children to engage with a range of commercial education technologies, including productivity platforms such as Microsoft 365, and a range of Learning Platforms and Learning Management Systems (LMS). These tools routinely collect a wide range of personal information about children, often stored in locations

outside of Australia (e.g., cloud servers in the United States)[8]. While many schools provide information about their use of these technologies to parents, it is often unclear whether the provided information includes alternative choices and options for families to opt-out of their children's use of these platforms. It is therefore equally unclear whether consent here can be deemed voluntary, and whether families have alternatives provided for the use of particular education technologies, to ensure children are not disadvantaged in their access to resources for education. For consent to be voluntary, schools must provide meaningful alternatives to the use of EdTech services where parents or children identify an unreasonable data privacy risk.

The implications of the collection, use or disclosure of personal information about children through education technologies used in Australian schools are often unclear, and poorly understood by schools[9]. Due to the inconsistent use of reliable evaluation practices regarding the safeguarding of children's data privacy by education technologies used in Australian schools, but an understanding that these are "vital to modern education systems"[13], schools are likely to simply trust, rather than comprehensively assess, tech providers' practices[12]. Parents, in turn, tend to trust schools to use education technologies that have been vetted and therefore are 'safe' to use[13]. In these contexts, it is unclear how consent is meaningfully informed. The responsibility should be on the APP entities covered by the Code to facilitate informed consent from parents and/or young people.

In the context of schools' use of education technologies that collect, use and disclose children's personal information, for consent to be voluntary and informed, example 'best practice' processes and mechanisms must be developed. These will guide entities covered by the code, as well as schools, on how to ensure parents and children are meaningfully informed, and have choices to allow them to retain control over children's personal information.

With online services that use LLMs, Division 2 may be applied at the commencement of use, and importantly, there is **currently no feasible mechanism to prevent or regulate the voluntary inputting of personal information or other types of children's data**. The nature of LLMs allow conversational engagement using natural language, and because children are more likely to 'trust' and over-share personal information with conversational AI[10] [11] a child may input personal information in their prompts and use of the LLM over time that is impossible to reasonably anticipate and consent to in the application of Division 2.

Section 20 requires assent of a child under 15 if that child is an end-user of the service. Make clear that the entity should not collect additional personal information about the child in order to obtain their assent.

The code must include special considerations that allow for a range of alternative consent mechanisms for children under 15 years of age, in circumstances where they may not have ready access to a person with clear parental responsibility. Examples include children in care whose parents may no longer have legal permission to access or manage information about them, where parents are deceased, or guardianship may be otherwise transitory. To effectively uphold children's right for participation in online spaces and activities that align with and promote their rights, these circumstances must not exclude children from being able to request a 'person with parental responsibility' giving consent, especially when they have already given their own assent. We

[8] Pangrazio, L., & Bunn, A. (2024). Assessing the privacy of digital products in Australian schools: Protecting the digital rights of children and young people. *Computers and Education Open*, *6*, 100187. https://doi.org/10.1016/j.caeo.2024.100187

[9] Pangrazio, L., Duffy, G., & Zomer, C. (2026). The power of the norm: How schools interpret, use and disclose education data. *Cambridge Journal of Education*, *56*(1), 1–18. https://doi.org/10.1080/0305764X.2025.2590450

[10] Addae, D., Rogachova, D., Kahani, N., Barati, M., Christensen, M., & Zhou, C. (2026). *A Privacy by Design Framework for Large Language Model-Based Applications for Children* (Version 1). arXiv. https://doi.org/10.48550/ARXIV.2602.17418

[11] Neugnot-Cerioli, M. (2026). *Adolescents & Anthropomorphic AI*. https://everyone.ai/wp-content/uploads/2026/02/Adolescents-Anthropomorphic-AI-Rethinking-Design-for-Wellbeing-.pdf

propose that the definition of 'person with parental responsibility' be refined as proposed under Part 1 of this document, in consultation with Family Law experts.

For entities to confirm who holds this responsibility, we acknowledge that principles of data minimisation should be followed as much as possible, and that any unnecessary linking of data sets that should remain separate should be avoided. Example approaches to ascertain who may be an appropriate adult from whom consent for access to a digital service could be obtained, could orient themselves on approaches from health and medical contexts that typically rely on digital mechanisms to confirm who holds legal decision-making responsibility; for instance, consent to a child's medical treatment[12] or mechanisms used in digital welfare service records regarding the current custody status[13].

We recommend:

9. **Section 13** to specify that, where a child has capacity (i.e. generally >15), they *must* give consent (rather than a person with parental responsibility).

10. To ensure **sections 14 & 15** can be operationalised in education settings, example 'best practice' processes and mechanisms must be developed to guide entities covered by the code and schools, on how to ensure parents and children are meaningfully informed, and have choices to allow them to retain control over children's personal information.

    The Centre is well-placed to facilitate and support consultation processes with education (across sector and jurisdiction) and industry stakeholders to inform the development of such guidance.

11. **Section 20** be amended to clearly state that entities should not collect additional personal information about the child in order to obtain their assent.

    Special considerations to be included to allow for a range of alternative consent mechanisms for children under 15 years of age, in circumstances where they may not have ready access to a person with clear parental responsibility.

Division 3 - Transparency

We welcome this division as transparency is essential to support children and those with parental responsibilities to understand how entities collect, use, disclose, access and manage personal information.

APP privacy policies [**Section 23**] 'directed specifically at children' is appropriate; presently, APP privacy policies are purposefully vague. This requirement does not encourage APP entities to be more transparent. The few age-appropriate privacy policies currently implemented, in particular by EdTech, are equally vague even when using 'age-appropriate language'.

For more transparency, broaden this section to consider different dimensions of value and financial exchange regarding data. Entities should be required to differentiate between and be clear about 'selling' data to and 'sharing' data with third parties. Notably, current privacy policies may mention they do not 'sell' data to third parties, obscuring the fact that they do indeed share data even though there is no obvious financial exchange[14].

We support the recognition that privacy policies are required to be accessible for all children; in particular,

[12] Cincinnati Children's. (2026). *IDENTITY Software.* https://www.cincinnatichildrens.org/research/support/innovation-ventures/successes/identity

[13] Cannon, M., Herrera, S., & Mechael, P. (2020). Case Protection Child Management Information System. *MEASURE Evaluation.* https://www.measureevaluation.org/resources/publications/ms-20-186/at_download/document

[14] (Cyphers, 2020). Google Says It Doesn't 'Sell' Your Data. Here's How the Company Shares, Monetizes, and Exploits It.

accessibility should be supported by the integration of visual elements. It is desirable to develop and share a series of **default images or graphics** that could be used by different entities regarding communication with children[15]. Visual consistency, especially for younger children, could assist in building digital literacy about what types of information are being kept, used, disclosed and managed if they are visually represented (not just described) consistently. At the very least, we expect **parameters or guidelines for entities** regarding formatting of such accessible information to support the transparency and accessibility of the information for children.

The draft Code requires entities to provide children with information about cross-border disclosures and the location of overseas recipients **[Sections 26 and 28],** but does not provide children with a meaningful understanding of how personal information is being used, analysed, shared, retained, or acted upon. We welcome further guidance on supporting children to understand and have knowledge of what occurs with their private information once acquired by entities.

Section 28(3) relates to the period of time that an organisation has to respond to a request for information regarding the handling of personal information. The section seeks to modify APP 12.4(a)(ii), which provides that an entity that is an organisation must respond to the request within a reasonable period following the request. In effect, it provides a long-stop date of 30 days to respond to requests unless Section 28(4) applies, in which case there is a long-stop date of 60 days. We consider that these provisions risk being considered inconsistent with APP12.4(a)(ii) in that the stipulated periods (30 days or 60 days) may not be objectively reasonable in the circumstances.

We recommend:

12. Revise Section 28(3 & 4) to clearly state that, generally, a reasonable period of time *will be no more than 30 days and no longer than 60 days in relation to more complex requests.*

Division 4 - Access to, and correction of, personal information about children

We welcome the specificity regarding the 'reasonable period' to respond to access or correct their personal information. We recommend a new section be added to the Code: that a request for access to or correction of personal information about a child can be made by a child **or by a person with parental responsibility** (but the latter only where the child is under 15 or otherwise lacks capacity to make the request). When requests are made by those with parental responsibility, the entity is to take reasonable steps to ensure this person has parental responsibility.

Section 30 sets out timelines for responding to a request. For reasons provided above (in relation to **Section 28(3)**) we query whether this may be considered inconsistent with APP12.4(a)(ii) and might better be dealt with by way of guidance. However, it is unclear why these timelines would not apply to all requests for personal information of a child: whether made by the child or a person with parental responsibility.

Section 31 sets out timelines for correcting the personal information of a child in response to a request. We query whether this may be considered inconsistent with APP13.5(a)(ii) for similar reasons provided above (in relation to **Section 28(3)**). It is unclear why these timelines do not apply to all requests for correction of the personal information of a child, whether made by the child or a person with parental responsibility. We recommend providing guidance on reasonable timelines for organisations to respond to requests for access or correction.

[15] McKnight, L., & Read, J. C. (2009, June). Designing the'record'button: using children's understanding of icons to inform the design of a musical interface. In Proceedings of the 8th International Conference on Interaction Design and Children (pp. 258-261).

Entities that use Large Language Models to process children's personal information will likely not be able to comply with **Divisions 4 or 5** of the code. LLMs do not store data as retrievable entries but rather encode information. Consequently, in the LLMs an entity may not be able to provide access to, "permanently delete" or "accurately correct" specific data elements as this is technically misaligned with how LLMs represent and process information. Existing techniques to remove or correct data used to train LLMs are not able to guarantee complete and permanent correction or deletion of specific data and its influence within the model.

Though likely beyond the scope of the Code to adequately address, we highlight the collective need for advances in machine unlearning, improved data governance practices prior to training, and clearer standards for what constitutes meaningful access to, correction or deletion (Division 5) of personal information in AI systems.

We recommend:

13. Requests for access to information about a child, or correction of a child's personal information, can be made by the child or (only if the child is under 15 or otherwise lacks capacity) a person with parental responsibility.

14. Entities should take reasonable steps to establish whether a person seeking to access or correct a child's personal information on the basis of having parental responsibility does indeed have parental responsibility.

15. Provide guidance on what 'reasonable timelines' are generally going to be for organisations to respond to requests for access or correction rather than including in the Code (where they could be subject to challenge on the basis of inconsistency).

Division 5 - Destruction of personal information about children

We welcome **Section 32,** which provides the right for the deletion of children's personal information upon request. This significant inclusion aligns with international standards, such as the GDPR's "right to erasure"[16], which recognises children's rights to control and erase their personal data. It reflects the principle of evolving autonomy by enabling individuals to revisit and revoke decisions made about their data during childhood, thereby addressing the long-term persistence of digital information. Additionally, it strengthens accountability for entities by requiring systems that support deletion and correction, reinforcing a rights-based approach to children's privacy in digital environments. We acknowledge the process for locating and making requests should be clearly available in an age-appropriate format (see comments in Section 36).

We recommend that the wording of Section 32(1) be clarified to include the provision for requests being made by children under 15 years without accompanying parental consent. We support the right of children under the age of 15 years to request deletion of their personal information without parental consent.

Section 32 does not specify if the provision applies to all activities outlined in the Code in Section 7. Specifically, will children and/or a person with parental responsibility have the ability to request for access to, correction and destruction of their personal information in instances where the data was provided by others (e.g. others' use of online services primarily concerned with the activities of children)?

There is ambiguity regarding whether Section 32 permits the deletion of personal information while allowing a child to continue accessing and using the online service, or whether such a request would necessarily limit or terminate functionality. Additionally, the Section 32 does not specify whether users may request the

[16] Art. 17 GDPR Right to erasure ('right to be forgotten') https://gdpr-info.eu/art-17-gdpr/

destruction of specific or partial categories of data, rather than requiring complete erasure, thereby creating uncertainty as to the practical scope of these rights.

Section 31 references the APPs requirement for entities to make reasonable steps to notify other entities in relation to the correction of personal information. We propose the same requirement be applied to Section 32 regarding the destruction of personal information about children. Entities responsible for the collection of the data increasingly may rely on external processors (e.g., such as analytics services or other data intermediaries) to host, process, or retain user data. In such a scenario, deletion obligations may be rendered less effective in practice, as data would persist within third-party systems beyond the reach of the entity's compliance with the Code. This outcome would undermine the intended protective function of Section 31 by shifting, rather than eliminating, risks associated with children's personal information.

Section 32(3-5) outlines that, inevitably there will be situations in which information cannot/should not be destroyed. We recommend that, in some situations where information cannot/should not be destroyed, there be an option to ensure that the information is not further disclosed or used. The Code should provide that, when a request for destruction of information has been made but is not able to be actioned for a reason specified in Section 32(3), the entity must take reasonable steps to cease using or disclosing the information in question, where it is possible and practicable to do so (bearing in mind the factors set out in Section 32(3)).

There may also be implications for university-based researchers where universities are entities bound by the Code. The National Statement on Ethical Conduct in Human Research (2025), section 3.1.31, requires participants be informed of their right to withdraw, any consequences of withdrawal, and whether their data can be withdrawn. However, withdrawal does not automatically require deletion of data already collected, particularly where data was de-identified, aggregated, analysed, published, or deposited in research repositories with consent. While we recognise the risks of re-identification, especially through data linkage, the Code must account for lawful and ethically approved research practices where limits on withdrawal, retention, and future data use may affect compliance with Sections 31 and 32.

We recommend:

16. Revise the wording of Section 3(1) to include the provision for requests to be made by children under 15 years without accompanying parental consent.
17. Additional requirements for the partial destruction of personal information consequences for the continued use of online service if the users' personal information is partially or completely destroyed.
18. An additional requirement for entities to make reasonable steps to notify other entities in relation to the destruction of personal information, as outlined in Section 31 in regard to correction.
19. An additional requirement that where a request for destruction of information has been made but is not able to be actioned for a reason specified in Section 32(3), the entity must take reasonable steps to cease using or disclosing the information in question where it is possible and practicable to do so (bearing in mind the factors set out in Section 32(3)).

Division 6 - Notification requirements for control or monitoring mechanisms

Section 33 addresses the need for child users of digital devices to be notified about any mechanisms that may be used to monitor or control service use or monitor geolocation. Section 33(1) and (2) specify the division is limited to persons with responsibilities and other end-users. We recommend an additional item be included to broaden the scope of Section 33 to include the provision of notifications when monitoring or control of services

or monitoring of geolocation is conducted by entities. For example, research shows that schools monitor children's activities and location through school-owned devices[17] and/or edtech platforms[18]. Many platforms provide teachers and school administrators insight into when and how often children log into school systems and track their activities on these systems; often these types of data are not necessary and do not give additional insight into students' learning.

There is a presumption that services that monitor children's data, including location data, are screen-based or equipped with another mechanism to notify a child that data is being tracked. Many tracking devices (e.g. fitness trackers, air tags, etc.), though, do not have screens. **We recommend that guidance on providing notifications be provided for services that do not have obvious ways of providing a notification to a child through the service/device.**

We recommend:

20. **An additional requirement be included to broaden the scope of Section 33** to include the provision of notifications when monitoring or control of services or monitoring of geolocation is conducted by entities.

Division 7 - Making inquiries and complaints

We support the purpose of this division to notify users about the use and disclosure of their personal data, and the process of making inquiries, complaints, corrections to and deletion of their personal data.

Guidance on universal principles, terminology and imagery for use by entities in the provision of their online services and information provided to users, including children, would enhance the user's understanding of the Code. One example are the privacy icons advised in the GDPR[19].

We recommend:

21. Guidance be provided that sets out how entities should provide clear, concise, transparent and age appropriate information.

Division 8 - Privacy impact assessments and privacy education and training

We welcome the inclusion of guidance on internal governance and compliance structures, and include several recommendations to support their efficacy.

Section 38 sets out the circumstances under which an entity needs to conduct a Privacy Impact Assessment (PIA). Section 38(1)(b) limits PIAs to apply to new or changed ways of handling personal information where they are likely to have a significant impact on the privacy of children. As outlined in the exposure draft, the omission of a definition of 'significant' creates ambiguity and could be subject to challenge. We recommend that the caveat of "significant impact" be removed and a PIA be required for all new and changed ways of handling

[17] Selwyn, N., & Cumbo, B. (2024). "We've Tried to Keep the Beast on a Leash": The Domestication of Digital Classroom Surveillance. *Surveillance & Society*, *22*(2), 88-103.
[18] Zomer, C. (2026). How 'much' engaged are you? A case-study of the datafication of student engagement. *Learning, Media and Technology*, *51*(1), 166-180.
[19] von Grafenstein, M., Kiefaber, I., Heumüller, J., Rupp, V., Graßl, P., Kolless, O., & Puzst, Z. (2024). Privacy icons as a component of effective transparency and controls under the GDPR: effective data protection by design based on art. 25 GDPR. *Computer Law & Security Review, 52*, 105924.

personal information in relation to an existing service or activity.

Section 40 mandates privacy education and training as a mechanism to uphold key components of the Code in the conduct of entities and organisations. We recommend **Section 40** mandate privacy education and training for *any* person employed or otherwise engaged by entities covered by the Code who access children's personal information in the course of performing their duties, even if access is not 'regular' or frequent', and to include some basic guiding principles to ensure data privacy education is of appropriate quality. Additional guidance or detail would reduce the likelihood that education on children's data privacy may be understood as being rolled into, or covered by, existing training options (e.g. associated with online safety or cybersecurity[20]).

We **advocate for a sustainable long-term funding structure and resourcing** to support strategic compliance auditing of entities under the Code, by the regulatory body, at regular intervals. This step is essential to demonstrate commitment to the enforcement of the Code, and provides a necessary incentive for entities to keep adapting their procedures to maintain compliance. It signals the mechanisms by which poor compliance or breaches can be identified, and refers to what consequences may result.

We recommend:

22. An additional requirement for the publication of a summary of the key details relating to the use of children's personal information from the PIA be made publicly available under Section 39.

23. Additional detail or guidance on the basic guiding principles to underpin a quality framework for data-privacy-focussed education and training programs, against which entities need to evaluate the education and training provided to persons employed or otherwise engaged by them.

24. The provision of adequate funding to ensure the OAIC are able to fulfill their enforcement obligations under the Code.

[20] Pangrazio, L., & Mavoa, J. (2025). Studying the datafication of Australian childhoods: learning from a survey of digital technologies in homes with young children. *Media International Australia, 194*(1), 53-68.