Children's Online Privacy Code: Issues Paper

Submission from elevenM

30 July 2025

Contents

Introduction

Children are entitled to more than just protection

As a society we hold few values more dearly than the protection of children. Our obligations to the next generation, however, go beyond simply protecting them from harm or from economic exploitation. Positive values of participation, autonomy and agency are key objectives alongside safety. Without the agency needed to participate and exercise rights, children can neither take advantage of the opportunities digital media afford, nor develop resilience when facing risks.[1] There is strong public support for this policy goal, with 82% of parents agreeing that 'children must be empowered to use the internet and online services, but their privacy must also be protected'.[2]

To date Australian law has done little to respond to children's vulnerability to privacy harms from online services. The Children's Online Privacy Code (**the Code**) is an opportunity to change that. The Code can be viewed as the continuation of an international trend towards implementing additional privacy protections for children. Australia has been slower than comparable jurisdictions but now enjoys a second mover advantage — the opportunity to learn from successful international approaches to regulating online services and develop them for the Australian context.

The development of the Code will involve a range of perspectives from interested stakeholders including, and most saliently, children. Consultation questions relating to children's lived experiences online and evidence of children's functionality requirements are, in our view, best addressed by children and advocates that directly represent them.

elevenM has been closely engaged in research and advocacy around children's privacy rights for many years. Our perspective is informed by our ongoing engagement in this space, combined with our deep expertise in industry, applying the Australian Privacy Principles (**APPs**) in practice, advising regulated entities on privacy risks and implementing privacy programs.

elevenM welcomes the opportunity to make this submission to the Office of Australian Information Commissioner's (**OAIC's**) Issues Paper on the Code.

Our submission in brief

We make the following submissions:

- The Code should be grounded in human rights and aligned to comparable international approaches which elevate the best interests of the child, balancing participatory rights with protective rights.
- The Code should adopt a harms-focused approach that allocates responsibility for preventing harm to the entities who are best placed to do so.

---

[1] Amanda Third et al, *Children's Rights in the Digital Age* (Unicef, September 2014).
[2] Office of the Australian Information Commissioner and Lonergan, *Australian Community Attitudes to Privacy Survey 2020* (September 2020), 94.

- The best way to introduce consideration of the best interests of the child into the existing APP framework is to incorporate those interests into the overall reasonableness requirement in APP 1.2, which is operationalised in several other APPs.
- There is a risk that limiting the application of the Code to online services likely to be accessed by children will not achieve the Code's stated policy objectives. We submit that a broader scope of entities who handle children's personal information in online services should be covered by the Code, including:
    - small businesses (consistent with the Government's commitment to remove the small business exemption)
    - entities with whom a child may not be likely to interact directly, but whose operations intrinsically involve the handling of children's personal information and provide or contribute to the provision of an online service.
- The Code should also clarify its interaction with the social media age restriction as complementary, and not mutually exclusive regulatory measures.
- We support measures to enhance the quality and accessibility of privacy policies and notices. However, we caution against an over-reliance on notice and privacy self-management, or any approach that places primary responsibility for understanding and engaging with privacy rights and responsibilities on a child or their parent.
- Notice requirements could be enhanced by:
    - Adopting the ACCC's 2019 recommendations for clearer, age-appropriate privacy notifications
    - Clarifying that the APP 5 obligation to provide notice is not discharged unless there are reasonable grounds for the organisation to believe that such notice is *effective*.
    - Elaborating on 'reasonable steps' for well-resourced organisations to include best practice design and accountability practices.
- Children's vulnerability to privacy harms from online services can materialise because, in comparison to adults, children are both:
    - more vulnerable to privacy harms, and
    - less able to effectively utilise security settings, such as passwords.
- The onus to keep children's personal information secure should be placed on organisations to develop age-appropriate controls, rather than on children or their parents.

About elevenM

elevenM is a specialist privacy, cyber security, AI and data risk consultancy. Our mission is to build trust in the online world.

Our team comprises deep experts in complementary digital risk disciplines such as privacy, cyber security, data governance, AI, strategy, and communications. We have a strong public policy focus, and many members of our team are personally motivated to create a safer and more inclusive online environment, particularly for children and the vulnerable.

Members of our team combine technical, business and legal qualifications with extensive experience in the field. We work hand in hand with our clients to understand their business strategies and priorities, and advise them on how to achieve these ambitions safely and responsibly, through pragmatic and effective digital risk solutions that are suitable for today and for the future.

Our work spans the public and private sector, and comprises strategic and operational activities – including strategic guidance in the areas of cyber security, privacy, data and AI, implementing programs, developing risk assessment frameworks, conducting impact assessments, incident planning and remediation, and training and awareness.

We also have direct experience in children's privacy. In 2020, elevenM and Monash Law School conducted a major research project examining the privacy risks and harms that can arise for children and for other vulnerable groups online. Our research was commissioned by the OAIC and conducted in partnership with two leading academics from Monash Law School, Normann Witzleb and Moira Paterson.[3] Parts of this submission draw substantially on that work. Our submission to the Australian Government's Privacy Review also drew on that research in supporting enhancements to children's online privacy.[4] Most recently, we were proud to support the OAIC and Reset.Tech as privacy advisors at the consultation for academia, civil society and children's rights advocates on the Code in Sydney on 7 April 2025.

[3] The full report is accessible via the OAIC: https://www.oaic.gov.au/__data/assets/pdf_file/0012/11136/Report-Privacy-risks-and-harms-for-children-and-other-vulnerable-groups-online.pdf.
[4] Accessible via https://elevenm.com.au/blog/elevenms-submission-to-the-privacy-act-review/.

Submission

Our approach

Our approach in this submission is to address key thematic privacy issues surfaced in the Issues Paper. While the submission does not sequentially follow the order of the questions in the Issues Paper, we have mapped the sections in this submission to the corresponding sections and question numbers in the Issues Paper for ease of reference.

As noted above, we have taken this approach to focus on the issues aligned with our expertise, and from the perspective that, in our view, multiple questions relating to a consistent underlying issue could be addressed with one thematic response.

Our submission assumes that the steps outlined in the OAIC's regulatory guidance relating to compliance with the APPs and the *Privacy Act 1988* (**Privacy Act**) are an existing baseline upon which the Code will be built, and do not need to be cited.

Our view on the Code's overarching policy objectives

In summary	The Code should be grounded in human rights and aligned to comparable international approaches which elevate the best interests of the child, balancing participatory rights with protective rights. The Code should adopt a harms-focused approach that allocates responsibility for preventing harm to the entities who are best placed to do so.

Grounded in human rights

There is a clear policy mandate for the Code to adopt a rights-based framework with the best interests of the child as its underpinning rationale. This is evident in the Government's response to the Privacy Act Review Report, in which the Government recommended that the code align with relevant international approaches and made specific references to the best interests of the child in its agreed-in principle responses to other proposals relating to children's privacy.[5] This is reinforced by the Explanatory Memorandum to the *Privacy and Other Legislation Amendment Bill 2024*, which references the UN Convention on the Rights of the Child (**CRC**) and notes that the Code is intended to 'elevate' privacy protections and promote the right to privacy of a child by imposing specific enforceable obligations in the handling of children's personal information than would otherwise exist under prevailing law.[6]

[5] At p 13.
[6] At para 117.

Grounding the Code in human rights law is consistent with the objects of the Privacy Act,[7] provides greater certainty by adopting well established legal principles and will facilitate greater international interoperability.

Australia has recognised and committed to children's right to privacy through general human rights frameworks[8] as well as instruments specifically focused on children, such as the CRC. However international law is clear that the right to privacy is not absolute, and must be understood in context, balanced with other rights and legitimate competing interests. We submit that the Code should seek to implement Australia's international human rights obligations in relation to children's privacy in this broad and balanced sense, balancing protective rights[9] with enabling rights,[10] in line with the central obligation of the CRC to always act with the best interest of the child as a primary consideration (CRC art 3) and drawing on well-defined legal mechanisms (reasonableness, necessity, and proportionality) to resolve competing interests.

Finally, this approach would achieve the alignment with international approaches specified by the Government in its response to the Privacy Act Review Report. The application of this obligation to online services accessible is explained in detail in guidance from the UK Information Commissioner's Office and would be a suitable reference for a Code developer.[11]

Alignment to international approaches

The Government Response to the Attorney-General's Department's Privacy Act Review Report specifies that the development of the Code should align with international approaches, including the UK Age Appropriate Design Code (**UK Code**).[12] The Fundamentals for a Child Oriented Approach to Data Processing from the Irish Data Protection Commission[13] is another international approach the Australian Code could leverage.

This does not mean the Code should directly 'copy' standards from the UK or Ireland – provisions in the Code will need to be drafted to have effect in the unique context of Australian privacy law, as we explore further below. They are, nevertheless, a useful base

---

[7] Section 2A(1)(h) states that one of the objects of the Privacy Act is 'to implement Australia's international obligations in relation to privacy'. Australia's principal international obligations in relation to privacy arise from human rights law.
[8] Such as the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights.
[9] Such as the right to privacy (CRC art 16) and freedom from economic exploitation (CRC art 36).
[10] Such as the rights to freedom of expression (CRC art 13), access to information (CRC art 17), and participation in play, cultural life and the arts (CRC art 36).
[11] https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/how-to-use-our-guidance-for-standard-one-best-interests-of-the-child/the-united-nations-convention-on-the-rights-of-the-child/.
[12] 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/executive-summary/.
[13] https://www.dataprotection.ie/en/dpc-guidance/fundamentals-child-oriented-approach-data-processing#Fundamentals.

from which to draw inspiration (i.e., taking an approach to developing the Code that asks 'is there any reason why Australia *couldn't* adopt a similar standard or requirement?').

The consistent principle underpinning both the UK and Irish approaches is that the 'best interests of the child' is the lens through which all other requirements in the codes should be viewed. The UK and Irish approaches can be distinguished from other notable international regulations applying to children and online services on the basis that, as the Executive Summary to the UK Code explains, they seek to protect children within the digital world, not protect them from it. The US Children's Online Privacy Protection Act and Rule,[14] by comparison, places a much greater emphasis on controlling access to online services through age restriction and consent mechanisms.

Efficient allocation of accountability for preventing harm

Regulation should balance self-management and organisational accountability in the best interests of the child. That balance should reflect children's varying capabilities and development needs (including the need for agency) and allocate responsibility for the protection of children's rights and interests appropriately between organisations, parents and children themselves based on which party is best placed and most capable to efficiently manage the relevant risks. Responsibility for protecting a child's rights and interests should never lie with the child alone.

Can the Code achieve the best interests of the child?

Issues Paper reference(s)	Section 4; Question 4.5 Refer also to Attachment A (below)
In summary	The best way to introduce consideration of the best interests of the child into the existing APP framework is to incorporate those interests into the overall reasonableness requirement in APP 1.2, which is operationalised in several other APPs.

The code-making power in the Privacy Act provides that an APP code may impose additional requirements to those imposed by one or more of the APPs, so long as the additional requirements are not contrary to, or inconsistent with, those principles.[15] This procedural requirement complicates the integration of the best interests of the child principle into the design of Code for a couple of reasons:

- the requirements in the UK and Irish codes were developed by reference to the European General Data Protection Regulation (GDPR), which generally provides a higher standard of privacy protection and greater individual privacy rights than the Privacy Act, and provides a stronger foundation for enhanced privacy rights in a Code

[14] Refer generally to https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa.
[15] Section 26C(3)(a).

- the Privacy Act is currently subject to a review process, with the Government agreeing in-principle and committing to further consultation on a raft of proposals to amend the Privacy Act in ways that could materially alter the application of the APPs in their current form, with the potential impact that any Code requirements that are closely tied to current APP requirements may be inconsistent with future amendments.

Notwithstanding these complexities, in our view it is possible for the APPs, in their current form, to be interpreted in such a way that enlivens the best interests of the child principle. Indeed, in our view it is desirable for the Code to take a reasonably expansive approach to the way in which the APPs can be interpreted to support the adoption of as many elements of the comparable international approaches as possible that have applied the best interests of the child in a privacy context. Taking this approach also has the advantage of 'future proofing' the Code in anticipation of a reformed Privacy Act.

The primary provision in the APPs that the Code could leverage for this purpose is the requirement in APP 1.2(a) that an APP entity must take such steps as are reasonable in the circumstances to implement practices, procedures and systems relating to the entity's functions or activities that will ensure that the entity complies with the APPs and a registered APP code (if any) that binds the entity. The Code could specify, for the purposes of APP 1.2(a), that the steps that are reasonable in the circumstances to implement practices, procedures and systems relating to an entity's functions of providing an online service that handles the personal information of children are those which apply the best interests of the children whose personal information is being handled, above any competing considerations.

An overarching obligation in the Code under APP 1.2 to apply the best interests of the child while implementing practices, procedures and systems relating to privacy compliance in providing an online service that handles children's personal information would then need to be supported by an articulation of how this obligation applies in the context of the other APPs. In our view, the APPs can be interpreted in a way that enlivens most, if not all, of the features of the comparable international approaches, including UK and Irish Codes. We have set out high-level mapping of the APPs, with emphasis added to particular elements of the APPs that could be leveraged in the development of the Code, to corresponding features in these international approaches at Attachment A.

When, to whom and how the Code should apply

Issues Paper reference(s)	Section 1; Questions 1.1, 1.2, 1.3. Section 2; Questions 2.1, 2.3, 2.4 Section 5; Question 5.3
In summary	There is a risk that limiting the application of the Code to online services likely to be accessed by children will not achieve the Code's stated policy objectives. We submit that a broader scope of entities who handle children's personal information in online services should be covered by the Code, including: • small businesses (consistent with the Government's commitment to remove the small business exemption)

- entities with whom a child may not be likely to interact directly, but whose operations intrinsically involve the handling of children's personal information and provide or contribute to the provision of an online service.

The Code should also clarify its interaction with the social media age restriction as complementary, and not mutually exclusive regulatory measures.

Section 26GC(5) of the Privacy Act specifies that the Code will bind APP entities which provide a social media service, relevant electronic service or designated internet service (all within the meaning of the *Online Safety Act 2021*), the service provided by the APP entity is likely to be accessed by children, and it is not a health service. As is noted in the Issues Paper, this is the same applicability threshold as in the UK Code.

In our view this is one suitable threshold that will capture many online services. We suggest that the Code adopts the 'common sense' approach outlined in the UK Code[16] and in the Explanatory Memorandum to the *Privacy and Other Legislation Amendment Bill 2024*[17] in guiding APP entities on whether this threshold covers their operations. That is, an approach which balances an assessment of whether the nature and content of a service is likely to appeal to children with any measures to increase friction in the way children access the service. Consistent with the policy objective of the Code encouraging online participation rather than preventing children's online engagement through age-gating measures, there should not be reliance or over-emphasis on age-assurance mechanisms as an indicator of whether a service is likely to be accessed by children.

We also submit that 'likely to be accessed by children' should not be the only threshold that is used to determine the entities that the Code will apply to. In our view there are two further issues regarding the application of the Code that require consideration.

Overcoming the small business exemption

As noted above, a key difference between the UK Code and the Australian Code is their enabling legislation. The Privacy Act applies to APP entities, which, in the context of organisations, means that it applies to businesses with an annual turnover of more than $3 million. This contrasts with the GDPR and privacy law in most other developed countries, which do not have exceptions for businesses based on their size or financial status.

The removal of the 'small business exemption' in the Privacy Act[18] was agreed in-principle by the Government in its response to the Privacy Act Review Report, citing overwhelming community support.[19] As it stands, the Code is being developed in tandem with further consultation on the removal of this exemption. Without clarity on the continued application of the small business exemption there is a real risk that the Code, if it is scoped as applying to

[16] https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/services-covered-by-this-code/.
[17] At 85.
[18] Section 6D.
[19] Refer to p 6.

APP entities as they are currently defined, is misaligned with both community expectations and a reformed Privacy Act.

It would be consistent with a harms-focused approach to the design of the Code that prioritises the mitigation of potential privacy harms in the best interests of children for all entities that handle children's personal information in the provision of an online service to be captured within the scope of the Code. Privacy harms for children can arise from an online service irrespective of the status of the entity providing it. Further, we think it is reasonable to suggest that smaller entities have the greater potential to be the source of privacy harms because they are otherwise unregulated by the Privacy Act. In this regard we note the growing cohort of small 'start-up' entities whose business proposition relies on the large-scale collection and use of data, and potentially personal information, for Artificial Intelligence model development and training.[20]

Our reading of the enabling provisions for the Code and the small business exemption provisions in the Privacy Act is that they do not appear to contain a mechanism for small businesses to be brought within the scope of the Code. That is, an entity must already be an APP entity before it can be deemed as being within the scope of the Code. Further legal analysis could interrogate this question.

It would be unfortunate for the Code's policy objectives to be frustrated by a limitation in the Privacy Act that is out of step with community expectations and, importantly, that the Government has indicated support for removing. In tandem with the development of the Code, the OAIC could seek advice on and consider potential avenues overcome this limitation, for example by prescribing certain small business operators to be organisations for particular acts or practices through regulation[21] or by amending the Privacy Act with limited and specific reference to the application of the Code to all organisations irrespective of their size or annual turnover.

Children accessing online services is not the only way privacy harms to children can materialise

It has been acknowledged consistently in the Issues Paper,[22] the Government's Response to the Privacy Act Review Report[23] and in the then Attorney-General's second reading speech for the *Privacy and Other Legislation Amendment Bill 2024*[24] that the problem the Code is seeking to solve is the potential privacy harms which can arise from the 'datafication' of children and their childhoods.

These materials cite the statistic that it is estimated that by the time a child turns 13, up to 72 million data points may have been gathered about them. Many of these datapoints will have been captured from a child accessing an online service, such as an educational program at school or an online game. Many others will not, such as:

---

[20] See https://www.hrw.org/news/2024/07/03/australia-childrens-personal-photos-misused-power-ai-tools.
[21] Pursuant to section 6E(1) or (2) of the *Privacy Act 1988* (Cth).
[22] Refer to p 6.
[23] Refer to p 13.
[24] https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22chamber%2Fhansardr%2F28033%2F0046%2.

- images and information about children published on adults' social media accounts
- images and information about children published on portals managed by childcare and educational facilities
- online-enabled child safety monitoring tools such as webcams, location trackers and health monitors controlled by adults
- online enabled voice assistants and 'internet of things' devices in a child's household.

The collection of personal information about a child by one of these tools in each individual instance is not, of itself, indicative of privacy harm. The issue is potential for harms to arise, unintended or otherwise, from the sheer volume of the data that is collected.

At the extreme end of directly impactful harms, the proliferation of AI powered tools to biometrically identify individuals and manipulate images into deepfake content has demonstrated that seriously invasive privacy harms can materialise for a child of any age, and without a child directly accessing an online platform themselves.[25]

There are also a broader, indirect harms that arise from the large-scale collection of children's personal information by online services. While there is limited empirical evidence on the psychosocial impacts of digital surveillance on children's development, it is generally accepted that the omnipresence of technology for supervision and monitoring can have a 'chilling effect' on behaviour, causing individuals to suppress genuine behaviours in favour of convergence to expected norms.[26] A recent Office of the e-Safety Commissioner has demonstrated a link between parental surveillance through location tracking apps and children's acceptance of behaviour from their peers that is consistent with coercive control.[27]

Limiting the scope of the Code to online services that are likely to be accessed by children obscures a range of privacy harms to children that can arise without a child ever having accessed an online service. To fully achieve its stated policy objective of addressing the 'datafication' of children, in our view it is necessary for the Code to apply on a broader, information ecosystem basis, to entities that handle children's personal information in a way that enables, directly or indirectly, children to be monitored and profiled in ways that are not consistent with their best interests, regardless of whether the entity provides a service that is likely to be accessed by children. The OAIC could investigate utilising the deeming provision in s26GC(5)(b) of the Privacy Act to specify that the Code will apply to all APP entities whose operations, for example, intrinsically involve the handling of children's personal information and provide or contribute to the provision of an online service.

As an example of this approach in practice, we are suggesting that the Code not only applies to a website that contains content that is designed to be accessed by children and may contain advertisements, but also to any entities that are involved in any downstream processes involved in serving those advertisements and tracking user engagement. We note that this approach would be consistent with the Government's in-principle support for a prohibition on targeted advertising and trading in personal information where these activities relate to children, except where it can be demonstrated that they are in the child's best

---

[25] https://www.esafety.gov.au/newsroom/blogs/addressing-deepfake-image-based-abuse.
[26] The Chilling Effects of Digital Dataveillance: A Theoretical Model and an Empirical Research Agenda - Moritz Büchi, Noemi Festic, Michael Latzer, 2022; Internet surveillance, regulation, and chilling effects online: a comparative case study | Internet Policy Review.
[27] https://www.abc.net.au/news/2025-05-15/location-sharing-apps-esafety-commission-coercive-control/105289994.

interests.[28] This approach would also be aligned with the anticipated 'fair and reasonable' test in the reformed Privacy Act.

Interaction with the Social Media Minimum Age

Finally, we note the concurrent design and implementation of the Government's age restrictions for children under the age of 16 for social media services under the *Online Safety Amendment (Social Media Minimum Age) Act 2024*. While we recognise this is a separate Government initiative that is outside of the scope of the Issues Paper, we also note the potential for the age restrictions to undermine or cause confusion about the scope of entities that the Code will apply to.

If it is expected that a child under the age of 16 will be prevented from accessing a social media service under the mandatory age restrictions, does this mean that the service operator is entitled to consider that it is not 'likely to be accessed by children' for the purposes of the Code? There appears to be a risk that the implementation of the social media age restriction will have an unintended and perverse policy outcome of placing these services outside the scope of the Code, undermining the opportunity for the Code to improve the privacy settings within these services for when children are old enough to access them. In our view, there would be a benefit in clarifying that the Code and the social media age restriction are complementary, and not mutually exclusive regulatory measures.

Providing age-range specific privacy notice and guidance

Issues Paper reference(s)	Section 3; Questions 3.1, 3.3 Section 4, Questions 4.1, 4.4 Section 8; Questions 8.1, 8.2, 8.3, 8.4
In summary	We support measures to enhance the quality and accessibility of privacy policies and notices. However, we caution against an over-reliance on notice and privacy self-management, or any approach that places primary responsibility for understanding and engaging with privacy rights and responsibilities on a child or their parent. Notice requirements could be enhanced by: • Adopting the ACCC's 2019 recommendations for clearer, age-appropriate privacy notifications • Clarifying that the APP 5 obligation to provide notice is not discharged unless there are reasonable grounds for the organisation to believe that such notice is *effective*. • Elaborating on 'reasonable steps' for well-resourced organisations to include best practice design and accountability practices.

[28] Proposals 20.6 and 20.7 in the Government Response to the Privacy Act Review Report.

Note – this section draws on analysis and recommendations we made in this report.

In general, we support measures to enhance the quality and content of privacy policies and notices, but we do not believe that the current notice paradigm in the Privacy Act can ever be effective in informing or empowering children (or their parents) in relation to their privacy. Children are not equipped to bear responsibility for reading and understanding uses and disclosures (however simply drafted) of personal information, nor is it reasonable to expect them to have the cognitive ability and background knowledge to understand how a disclosed act or practice is likely to impact them, particularly in the context of complex online data and advertising ecosystems. Indeed, evidence suggests that their parents are similarly unable to interpret lengthy and legalistic privacy policies and notices.[29] Any approach that places primary responsibility for understanding and engaging with privacy rights and responsibilities on a child does not strike the right balance between organisational accountability and privacy self-management.

A greater onus should be on organisations — to be accountable for managing personal information in the interests of children, to provide information about their practices in an accessible way, and to go beyond providing mere notice of relevant facts by providing ongoing support and guidance and designing their services in such a way that people of all ages and abilities can use them safely.

As a starting point, the code could consider implementing the ACCC's 2019 recommendations (which were directed economy-wide) that:

- notifications be concise, transparent, intelligible and easily accessible, written in clear and plain language, and provided free of charge
- notifications clearly set out how the APP entity will collect, use and disclose the consumer's personal information, and
- notifications be written at a level that can be readily understood by the minimum age of the permitted digital platform user[30]
- notifications be layered, and that the Code set out a baseline requirement for the content of each layer
- standard language be defined and mandated for describing key matters, such as the types of third parties to whom information might be provided, and types of purposes for which information might be used or disclosed.[31]

[29] https://www.abc.net.au/news/2024-05-21/accc-digital-services-data-report/103872726.
[30] Ibid 461.
[31] Ibid 485.

Additionally, we would encourage the Commissioner to explore whether the Code could expand APP 5 to require platforms providing notice under APP 5 to take steps to ensure that notice is *effective*. That is, the obligation to provide notice should require attention to the *outcome* (is there reason to believe users are in fact informed of the relevant matters) in addition to the form (was a complete, clear and accessible statement of the relevant matters made available). This would require an organisation to consider whether individuals are, in practice, likely to read the notice, and possibly to adopt additional measures (e.g.: through user experience design) as required to effectively convey the relevant information. This amounts to a strengthening of the existing expectation that 'reasonable steps' to provide notice include steps to ensure notices are clear, accessible and considerate of individuals' special needs and is consistent with the obligation on organisations to ensure awareness under APP 5.1(b).[32]

Requiring a focus on the outcome rather than the form would shift focus away from one-off, text-based notifications on sign-up for a service that are unlikely to be effective in bringing key matters to a user's attention, however clearly worded or structured, and would be consistent with a harm-focussed regulatory approach. Organisations would be required to adopt a more wholistic approach to conveying privacy information to children. Rather than exhaustively covering everything up front, children will benefit from platform providers providing privacy information in bite-sized chunks, embedded into the experience of the service itself. Alternative timings and modes of delivery for privacy information are important to enable understanding and engagement, particularly in younger children. Importantly, privacy information can be conveyed through user experience design, such as a light or icon to indicate a camera or microphone is active, or the look and feel of the interface itself — a button or section of a site coloured red warrants more caution than one coloured green. The growing prevalence of Internet of Things devices, including smart toys and home assistants, further underscores the need for ongoing transparency about data handling that is built into the product experience itself.

Further, in view of the vulnerability and need for special protection of children, the standard of 'reasonable steps' to ensure effective 'notice' or awareness', as expected under APP 5, would generally be high. The Code could codify best practice design and accountability practices for the largest organisations or most high risk contexts, including an expectation that in these contexts reasonable steps would include:

- adopting appropriate design practices for privacy transparency measures, which take into account the needs, capabilities and behaviours of children of varying ages who may use their service, and which include consultation and testing to ensure effectiveness
- tailoring notification content, style, mode of delivery and timing to be effective for all users, and offer a version or versions of the notification that are appropriate for the variety of ages and abilities of individuals whose information will be collected, including the ability for these devices to resurface age-adjusted content as children progress through developmental stages
- considering significance of the collection in terms of the possible adverse consequences for children at various stages of development, and present privacy

[32] See APP Guidelines 5.4-5.6.

notifications in a manner that reflects that significance (i.e. by emphasising higher risk or unexpected practices), and

- demonstrating why the organisation considers the steps taken were reasonable in the circumstances (including by measuring and reporting on how many users review privacy information or access privacy settings).

Finally, though it may not be achievable through the Code, we would like to see APP 5 expanded for the online context to include how users can report concerns, exercise their rights, or use any other privacy self-management tools available to them (such as how to use account privacy settings or turn off profiling, targeted advertising or location tracking).

Securing children's personal information

Issues Paper reference(s)	Section 13; Questions 13.2, 13.3, 13.4
In summary	Children's vulnerability to privacy harms from online services can materialise because, in comparison to adults, children are both: • more vulnerable to privacy harms, and • less able to effectively utilise security settings, such as passwords. The onus to keep children's personal information secure should be placed on organisations to develop age-appropriate controls, rather than on children or their parents.

Reasonable steps to secure personal information

The 'reasonable steps' that an APP entity should take to ensure the security of the personal information it holds will depend upon circumstances that include the amount and sensitivity of the personal information and the potential adverse consequences in the event of a breach.[33]

Children's personal information is not, of itself, considered sensitive information for the purpose of s 6 of the Privacy Act. Just as for adults, the potential privacy harms to a child arising from a breach are generally contingent on the volume and nature of the personal information involved. However, children are typically more vulnerable to privacy harms, due to limitations in their basic and digital literacy, their cognitive abilities and their capacity for mature decision-making, as well as their more limited capacity to take remedial actions in the event their personal information is involved in a breach.

Another distinction that can be drawn between children and adults is the extent to which children in different age groups will have the capability and contextual understanding to

[33] *APP Guidelines* Chapter 11 – Security of personal information at 11.7.

utilise security settings made available to them in an online service to protect their personal information from compromise.

The underpinning rationale for our comments on age-specific privacy notices and communications, above, can be equally applied in relation to securing children's personal information. That is, wherever possible, the onus of designing and implementing reasonable security controls to protect children's personal information should be on organisations rather than on child users. The use of passwords and passphrases appears to be an example of a security control where children have heightened vulnerability in comparison to adults. It is unlikely, in our view, that young children will have the capability to create and manage passwords and passphrases that are sufficiently complex to protect against an external threat of compromise. Recognising this vulnerability, the Code could:

- de-emphasise or recommend against online services relying on using passwords and passphrases for user accounts as a substantial means of satisfying the requirement to take reasonable steps to secure children's personal information
- consider whether, particularly in the context of online services aimed at younger children and online services that are likely to be used in group educational settings on a shared device, having individualised accounts that contain a user's personal information should be actively discouraged (consistent with the principle of 'collection limitation' in APP 3) unless it is demonstrably in the child's best interests for the online service to be configured with an individualised account
- indicate that, if an individualised account is required, in the same way that the Code is expected to recognise that online services will need to take differential approaches to communicating privacy information based on a child's age and capabilities, the online service will be required to take an approach to setting or facilitating the use of passwords or passphrases as a control that is developmentally appropriate and may require parental assistance
- ensure that parents or caregivers are included in any response to a breach involving a child's personal information to ensure that a person with suitable capabilities can take remedial action to prevent privacy harms.

Destruction or de-identification of personal information

The threshold for the destruction or de-identification of personal information under APP 11.2 is relatively broad – APP entities are required to take reasonable steps to destroy personal information or ensure it is de-identified if it no longer needs the information for *any* purpose for which it may be used or disclosed under the APPs (our emphasis).

Just as children are generally more limited in their capacities and contextual understanding in relation to information security controls, we submit that they are likely to be unaware of whether online services are retaining their personal information, let alone being aware of how long their personal information is being retained. Recognising this, and consistent with the position that the onus of designing and implementing reasonable security controls to protect children's personal information should be on organisations rather than on child users, we submit that the purpose for which personal information may be used or disclosed under the APPs to support the retention of personal information under APP 11.2 is limited only to purposes which can be demonstrated as being in the child's best interests, subject to any legislative information retention requirements.

Attachment A

How the Code could read the best interests of the child into the APPs

Issues Paper reference(s)	Section 4; Question 4.5	Section 12; Questions 12.1, 12.3
	Section 5; Question 5.4	Section 13; Questions 13.1, 13.4
	Section 6; Questions 6.1, 6.2, 6.5	Section 14; Question 14.6
	Section 9; Questions 9.3, 9.4	Section 15; Question 15.5
	Section 10; Questions 10.1, 10.3	

APP	Provision (emphasis added)	Applied in the best interests of the child looks like…	This aligns with…
APP 1	APP 1.3 An APP entity must have a clearly expressed and up-to-date policy about the management of personal information by the entity. APP 1.5(b) An APP entity must take such steps as are reasonable in the circumstances to make its APP privacy policy available in such form as is appropriate.	A privacy policy published by an online service handling children's information is accessible and easily interpretable by children, having regard to the potential for the children to comprise a range of ages and developmental stages, and noting that, in our view, in many instances, the practical limitations of making privacy policies and notifications easily interpretable by some cohorts of children should mean there is very limited reliance on these mechanisms as 'authorising' the collection, use or disclosure of children's personal information (refer to page 12 in the body of this submission).	UK AADC Standards 3 – Age appropriate application; 4 – Transparency Irish Fundamentals 5 – Information in every instance; 6 – Child-oriented transparency
APP 2	APP 2.1 Individuals must have the option of not identifying themselves, or of using a	The circumstances in which it will be impracticable for an APP entity providing an online service to not allow a child to deal with	UK AADC Standards 7 – Default settings; 8 – Data minimisation

	pseudonym, when dealing with an APP entity in relation to a particular matter. APP 2.2(b) Subclause 2.1 does not apply if, in relation to that matter it is impracticable for the APP entity to deal with individuals who have not identified themselves or who have used a pseudonym.	them anonymously or by using a pseudonym should be strictly limited. An available exception could apply where identifying a child in the context of an online service (such as through a login or recurring technical identifier) is necessary for the service to provide a longitudinal benefit across multiple sessions or uses of the service that is in the child's best interests. An APP entity identifying a child user of an online service for the purposes of accessing that service should not be conflated with the child's identity being made accessible to all other users of that service. A child's presence in the context of an online service accessible by others should be set to be anonymous by default, unless there is a purpose for the child's presence to be automatically identifiable to others that is consistent with their best interests, such as a clinical or educational requirement.	Irish Fundamental 14 – Bake it in
APP 3	APP 3.3 If an APP entity is an organisation, the entity must not collect personal information (other than sensitive information) unless the information is reasonably necessary for one or more of the entity's functions or activities. APP 3.5 An APP entity must collect personal information only by lawful and fair means.	The concepts of reasonably necessary and fairness in the context of the collection of personal information in APP 3 should be construed as narrowly as possible for the purposes of the Code, consistent with existing regulatory guidance and recent determinations which have read a consideration of proportionality into APP 3.[34] That is, there will be limited and specified circumstances in which the collection of personal information is reasonably necessary or fair where the collection is not consistent with the child's best interests.	UK AADC Standards 7 – Default settings; 8 – Data minimisation Irish Fundamental 14 – Bake it in

[34] Commissioner initiated investigation into 7-Eleven Stores Pty Ltd (Privacy) [2021] AICmr 50; at 105.

APP 4	No specific comments		
APP 5	Refer to page 12 in the body of this submission.		
APP 6	APP 6.1 If an APP entity holds personal information about an individual that was collected for a particular purpose (the primary purpose), the entity must not use or disclose the information for another purpose (the secondary purpose) unless… APP 6.2 …the individual would reasonably expect the APP entity to use or disclose the information for the secondary purpose.	The reasonable expectations of a child, or, more relevantly, a child's lack of a reasonable expectation about the use or disclosure of their personal information (for a primary or secondary purpose) could form the basis for several default requirements and restrictions on the use or disclosure of children's personal information in the Code unless the use or disclosure is in the child's best interests (such as those in the UK Code). We suggest this approach from the perspective that it is unlikely that children, especially younger children, will have an awareness about the potential for their personal information to be used or disclosed in ways other than are immediate apparent to them in their use of an online service. We also submit that, in the context of many online services which will collect and handle the personal information of children indirectly, there is no opportunity for the child to have formed any kind of expectation about the use or disclosure of their personal information because they are not aware of it having been collected (refer to page 9 in the body of this submission where we list common examples of children's information being collected indirectly or without their awareness) .	UK AADC Standards 5 – Detrimental use of data; 7 – Default settings; 9 – Data sharing; 10 – Geolocation; 12 – Profiling; 14 – Connected toys and devices Irish Fundamentals 3 – Zero Interference; 9 – Your Platform, Your Responsibility; 12 – A Precautionary Approach to Profiling
APP 7	APP 7.2 an organisation may use or disclose personal information (other than sensitive information) about an individual for the purpose of direct marketing if:	Per the comments in relation to APP 6, above, in our view it is very unlikely that most children will have a reasonable expectation that their personal information will be used for a secondary direct marketing purpose. Further, it is consistent with the stated policy intent of the Code that direct marketing to	UK AADC Standards 5 – Detrimental use of data; 9 – Data sharing; 12 – Profiling Irish Fundamentals 9 – Your Platform, Your

	(a) the organisation collected the information from the individual; and (b) the individual would reasonably expect the organisation to use or disclose the information for that purpose; and (c) the organisation provides a simple means by which the individual may easily request not to receive direct marketing communications from the organisation; and (d) the individual has not made such a request to the organisation	children is prohibited unless it is demonstrably in their best interest.	Responsibility; 12 – A Precautionary Approach to Profiling
APP 8		No specific comments	
APP 10	APP 10.1 An APP entity must take such steps (if any) as are reasonable in the circumstances to ensure that the personal information that the entity collects is accurate, up-to-date and complete. APP 10.2 An APP entity must take such steps (if any) as are reasonable in the circumstances to ensure that the personal information that the entity uses or discloses is, having regard to the purpose of the use or disclosure,	The concept of 'reasonable in the circumstances' in APP 10 should be construed as narrowly as possible in the Code, consistent with interpretations applied to APPs 3 and 6, to limit the collection, use and disclosure of personal information for purposes which are consistent with the best interests of the child. Reasonableness for the purpose of applying APP 10 in the Code, particularly in relation to the accuracy and relevance of children's personal information, should also be closely linked to the way the Code could interpret and apply APPs 1 and 5 to the differential approaches to communicating privacy information based on the range of children's ages and developmental stages (notwithstanding our comments about the limitations of the current notice paradigm). If, for example, the Code takes an approach that varies baseline expectations in relation to privacy notices and communications	UK AADC Standards 3 – Age appropriate application Irish Fundamentals 4 – Know your audience; 11 – Minimum user ages aren't an excuse

	accurate, up-to-date, complete and relevant.	for children aged 7-10 compared to children aged 11-13, it would be consistent for a differential approach to inform the way that the Code seeks to apply APP 10. That is, behavioural or personal information beyond strictly biographical personal information collected from children between the ages of 7-10 should not be considered continually accurate or relevant once a child progresses beyond that age and developmental stage to the ages of 11-13, or older.
APP 11	Refer to comments on page 15 in the body of this submission.	
APP 12	No specific comments, noting that the observations in relation to age specific privacy notice and guidance can and should be applied with equal effect to the design of any mechanisms provided to children to access their personal information.	
APP 13	No specific comments, noting that the observations in relation to age specific privacy notice and guidance can and should be applied with equal effect to the design of any mechanisms provided to children to correct their personal information.