AUSTRALIAN CHILD RIGHTS TASKFORCE

31 July 2025

Office of the Australian Information Commissioner

Email: copc@oaic.gov.au

Children's Online Privacy Code – Issues Paper

Thank you for the opportunity for the Australian Child Rights Taskforce ('the Taskforce') to make a submission to this consultation process to inform the development of the Children's Online Privacy Code. The Taskforce is a coalition of over a hundred organisations, networks and individuals committed to the protection of the rights of children and young people in Australia.[1]

One of the key roles of the Taskforce is to monitor and report on the implementation of the *United Nations Convention on the Rights of the Child* ('the Convention'). When Australia ratified the Convention in 1990, this was a commitment that every child in Australia should enjoy the rights set out in the Convention. This includes monitoring and providing advice around children's right to privacy and now includes their rights in relation to the digital world.

The Taskforce has already contributed to this process through previous submissions including to the Attorney General's Department consultation in late 2021, to the Privacy Act Review in 2023 and more recent consultation conducted by the Office of the Australian Information Commissioner ('OAIC' or 'the Office'). We will briefly review the key principles for context and design from these previous submissions before addressing the questions raised the Issues Paper released by the Office as the latest stage in the development of the Code. We have given particular attention to Question 4 – Open and Transparent Management of Personal Information and the steps to support children and young people to complain.

We have been assisted considerably by the efforts of our members and partners including Reset. Tech Australia, UNICEF Australia, Child Fund Australia, Bravehearts, Project Rockit, Reach Out, your town / Kids Helpline and the Alannah and Madeline Foundation. Crucially many of these efforts have included consultations with children and young people whose insights and experiences have been invaluable in guiding us to understand the issues and opportunities presented by the development of the Code to enhance the experiences and protection of children and young people online.

We welcome the work of the OAIC so far in the development of the Code and as set out in the Issues Paper. We applaud and endorse the care and time taken to consult with children and young people and the insights drawn from this approach. We look forward to the further stages in the development of the Code.

These are the key principles drawn from our previous work that should continue to apply in the further development of the Code.

[1] For more information about the Taskforce, please see https://childrightstaskforce.org.au/

Key Principles for Context

Realising children's rights requires aligning international, national and regional laws, policy, regulation, as well as learning from best practice globally. The development of the Code should continue to bring Australia's privacy framework into closer alignment with:

International child rights principles, including the rights provided by the *UN Convention on the Rights of the Child 1989*, the UN Committee on the Rights of the Child's ('CRC Committee') General Comment on the appropriate application of the 'best interests' principle,[2] the Committee's more recent General Comment on children's rights in relation to the digital world,[3] the UN Special Rapporteur on the Right to Privacy's comment on the right to privacy with regards to children[4] and UNICEF's *Children's Rights and Business Principles.*[5]

Emerging best practice internationally, including equivalent Codes from the UK,[6] Ireland,[7] Europe[8] and the United States.[9]

Recent national policy and practice developments across a range of initiatives that support better outcomes for children and young people, which should not be separated from the guidance, regulation and protection of children's online privacy rights. We recommend reviewing the proposals for alignment with the following national policies:

- the *National Strategy to Prevent and Respond to Child Sexual Abuse*
- the ongoing implementation of the recommendations of the *Royal Commission into Institutional Response to Child Sexual Abuse*
- the *National Plan to End Violence Against Women and Children 2022-2032*
- the *National Children's Mental Health and Wellbeing Strategy*
- *Safe and Supported: The National Framework for Protecting Australia's Children 2021-2031*
- the *National Principles for Child Safe Organisations*

Current proposals for and future reform of privacy law in Australia, and the need to ensure these reforms enhance respect and protection for privacy rights for children and young people. We note the importance of extending protections to advertising[10] and EdTech [11]. We note the guidance provided by the CRC Committee's definition of personal data to include "information about, inter alia, children's identities, activities, location, communication, emotions, health and relationships".[12]

[2] UN Committee on the Rights of the Child 2013 *General comment No. 14 (2013) on the right of the child to have his or her best interests taken as a primary consideration* https://www2.ohchr.org/english/bodies/crc/docs/gc/crc_c_gc_14_eng.pdf
[3] UN Committee on the Rights of the Child 2021 General comment No. 25 (2021) on children's rights in relation to the digital environment
[4] UN Special Rapporteur on the Right to Privacy 2021 *Comment on Artificial intelligence and privacy, and children's privacy* (UN Doc A/HRC/46/37, 25 January 2021)
https://www.ohchr.org/sites/default/files/HRBodies/HRC/RegularSessions/Session46/Documents/A_HRC_46_37_Add_6.docx
[5] UNICEF, Save the Children & the UN Global Compact 2021 Children's Rights and Business Principles | UNICEF
[6] UK - https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/
[7] Data Protection Commission https://www.dataprotection.ie/en/dpc-guidance/childrens-data-protection-rights
[8] https://digital-strategy.ec.europa.eu/en/policies/group-age-appropriate-design
[9] https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa
[10] Holloway, D. 2019 'Surveillance Capitalism and Children's Data: The Internet of Toys and Things for Children' *Media International Australia, Incorporating Culture and Policy* 170(1), pp. 27-36
[11] Human Rights Watch 2022 *How Dare They Peep into My Private Life* https://www.hrw.org/report/2022/05/25/how-dare-they-peep-my-private-life/childrens-rights-violations-governments
[12] UN Committee on the Rights of the Child 2021 *General comment No. 25 (2021), Para 68*

Key Principles for Design

The Code and its supporting materials should be clear and understandable and provide all required explanatory information and background

Informed consent regarding the collection and use of private information is a necessary part of realising children's right to privacy.[13] As the CRC Committee outlines, "where consent is sought to process a child's data, States parties should ensure that consent is informed and freely given by the child".[14] This is confirmed in UNICEF's *Principles for responsible handling of children's data*.[15] A fundamentally more transparent approach is required for privacy policy. [16]

The Code should be guided by child rights principles and practice

While meaningful consent is necessary, it is not sufficient to fully realise children's right to privacy.[17] Children should not be asked to consent to data practices that violate their rights without additional safeguards. The 'best interests of the child' is central to the child rights framework. It is embodied in Article 3 of the Convention, of which Australia is a signatory, and it underpins the CRC Committee's *General Comment No. 25: Children's Rights in Relation to the Digital Environment*.[18]

It calls for consideration of the full circumstances of a child's experience and circumstances, and ongoing assessment and attention to the most effective protection for each child. It allows for balancing the child's rights under the Convention. These rights include the right to privacy (Article 16), to right to access information (Article 17), the right to express views and be heard (Article 12), the right to freedom of expression (Article 13), the right to identity (Article 8), and the rights to be protected from harm from violence, abuse and neglect (Article 19) and from sexual abuse and exploitation (Article 34). The Convention calls for recognition of a child's 'evolving capacities' (Article 5) across the stages of development in childhood and adolescence. It also calls for measures to protect children affected by disadvantage (Article 3) and discrimination (Article 2).

Continuous Improvement

The Code will not be perfect, but a commitment to ongoing monitoring and improvement will be critical to realise children's rights online. A focus on rights, alongside the creation of duties to mitigate risks, should help prevent harms from occurring.

Broad application

The Code should seek to use a generously interpreted 'likely to be accessed' test to achieve the most effective protection and to develop a rights-respecting online environment. The Code should seek to cover broadly including Ed Tech and newer and emerging markets. It should challenge the harmful practices of Ad Tech that use direct marketing to children, direct targeting of children and trading children's personal data in violation of their privacy rights.[19]

[13] Simone van der Hof, 'I Agree, or Do I: A Rights-Based Analysis of the Law on Children's Consent in the Digital World' *Wisconsin International Law Journa*l 34, no. 2 (Winter 2016): 409-445

[14] UN Committee on the Rights of the Child 2021 *General comment No. 25 (2021) on children's rights in relation to the digital environment*

[15] UNICEF 2021 *Responsible Data for Children* https://rd4c.org/principles/

[16] Williams, D. & Farthing, R. 2021 *Did We Really Consent to This?* https://au.reset.tech/uploads/l01_resettechaustralia_policymemo_t_c_report_final-july.pdf.

[17] Lawford, J., Taheri, M., & Public Interest Advocacy Centre (Canada). (2008). *All in the data family: Children's privacy online.* https://epe.lac-bac.gc.ca/100/200/300/public_interest_advocacy/children_final/children_final_small_fixed.pdf

[18] UN Committee on the Rights of the Child 2021 *General comment No. 25 (2021) on children's rights in relation to the digital environment*

[19] As the UN Committee on the Rights of the Child outline "The digital environment includes businesses that rely financially on processing personal data to target revenue-generating or paid-for content, and such processes intentionally and unintentionally affect the digital

Response to Issues Paper Questions

We support responses provided by our Taskforce partners, particularly Reset.Tech Australia, which provides rights-respecting guidance in a global context. We offer the following additional comments.

1.1 Are there additional APP entities, or a class of entities, that should be covered by the Code?

We endorse a broad approach to coverage to assist in building a rights-respecting online environment for all, especially children and young people. The online environment has developed with inadequate attention to the privacy rights of children and young people. Where applied, the approach of providing complicated and unclear notice of intended use and inviting formulaic and token indications of consent has rarely resulted in meaningful engagement and active and informed decision-making about privacy rights.

We also note the growing evidence of risk and exploitation in online products, services and practices with inadequate protections provided particularly for children and young people. We hope that the development of the Code can play a strategic role in addressing these deficits.

Given the broad and targeted use of EdTech products by schools, families and governments for children and young people and the heightened risks associated with the misuse of personal data,[20] we support efforts to include EdTech within the scope of the Code wherever possible.

AdTech (online data brokers) has collected extensive and excessive amounts of personal information about children and young people, sometimes with completely inadequate disclosure of the use, sale and re-use of the data collected. Again, notice and consent approaches have been ineffective in protecting privacy rights. We support any efforts to include the industry and its extensive integration into products and services within the scope of the Code.

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

We support efforts to consider impacts, provide additional support and where appropriate limit the burden on providers that provide health and other supports to children and young people. We note the critical services to children and young people of providers such as Kids Helpline, Reach Out, Youth Law Australia. The right to privacy and other protections can be balanced in an assessment of the approach that is in the best interests of each child to guide application of the Code.

1.3 Is there criteria that should be used to determine whether a particular APP entity, or class of entities, is appropriately included or excluded from the scope of the Code?
2.1 What threshold should determine when a service is considered 'likely to be accessed by children'?

We maintain that a broad approach to inclusion under the Code and a generously interpreted 'likely to be accessed' test provides a strong commitment to the protection of children and to the development of a rights-respecting online environment.

experiences of children. Many of those processes involve multiple commercial partners, creating a supply chain of commercial activity and the processing of personal data that may result in violations or abuses of children's rights, including through advertising design features that anticipate and guide a child's actions towards more extreme content, automated notifications that can interrupt sleep or the use of a child's personal information or location to target potentially harmful commercially driven content." UN Committee on the Rights of the Child 2021 *General comment No. 25 (2021) on children's rights in relation to the digital environment* para 40

[20] https://www.hrw.org/report/2022/05/25/how-dare-they-peep-my-private-life/childrens-rights-violations-governments

We acknowledge the work of Dr Rob Nichols at the University of Sydney and Reset.Tech in our responses to these questions. They draw on international experience, examination of Australian law and practice and extensive consultations with civil society and children and young people.

International review supports the European principled approach with particular attention to the recent legislative experience in the UK and Ireland.

The threshold phrase "likely to be accessed by children" is the legislative trigger used in Australia's *Online Safety Act 2021*. The services covered by the Code are defined by reference to the Act. The use of the same terminology suggests a clear intent to create a consistent regulatory landscape with a clear focus on the protection of children and young people.

We note that there needs to be a broad approach taken to interpreting the notion of children's 'use'. It must recognise that in some circumstances, children are not active users, but their data are being accessed and used. Where their data are being used, they should be entitled to the full protections of the Code.

We do not support a numerical threshold. Instead, we endorse an approach that has:

1. A **presumption** of application.
2. A clear set of **assessment factors** that draws on all available evidence under broad definitions of use, risk and harm.
3. A **Children's Data Protection Impact Assessment** to build accountability.

A framework will need to be underpinned by established legal principles, committed to effective corporate accountability to create an auditable trail for enforcement. This will ensure that the Code can fulfil its mandate to create a digital environment where the privacy and best interests of Australian children are protected by design with accountability.

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

In the absence of compelling evidence of a more appropriate approach, we support the use of this standard. We support the ongoing gathering of evidence as to its effectiveness.

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

As discussed above, we support a presumption of application for platforms operating in the public domain. We support Reset.Tech's proposal that 'reasonable steps' should require reference to available evidence, internal and external to a platform, including of:

- whether their service is directed to or targeted at children (including market research and advertising data)
- use of the service by children (broadly defined)
- whether their service is a type of service likely to attract children.

2.4 What role, if any, should age gating or other access control mechanisms play in meeting obligations …?
2.5 Are there alternative approaches APP entities could take to meet their obligations under the Code, beyond age gating or age verification methods? If so, is there any evidence on the impact of such approaches on children's access to services or privacy outcomes?

The children and young people we have consulted have been very clear that the protections of the Code should not depend on compliance or otherwise with mechanisms designed to limit, prohibit, measure or restrict access to platforms. Privacy rights should not be compromised by such mechanisms. We support this view.

We support Reset.Tech's views as to a platform's responsibilities where it is not clear whether a user is a child. If a platform is intended for children, assume all relevant data belongs to children. If it is for general use and a user appears to be a child, provide protection.

2.6 Are there classes of APP entities, personal information, or activities of entities, for which different requirements under the Code may be appropriate? If so, what considerations should inform that approach?
2.7 How should the Code accommodate for the varying roles, functions and risk profiles of different kinds of services, activities or personal information?

At this stage of development of the Code, we do not see that there is justification for different requirements. If this is asserted at some point, we would invoke the principles set out in this submission. The protections provided by the Code should be clear and unambiguous. Guidance must address the objectives of respect for the rights of children and seek to provide the most appropriate and comprehensive protection possible.

3.1 Would age-based guidance be appropriate and assist APP entities in tailoring protections and interfaces appropriately and effectively?
3.2 In terms of providing guidance for the processing of children's personal information by APP entities covered by the Code, how appropriate do you consider the above age ranges would be?
3.3 Please provide any views or evidence you have on children's development needs, in an online context in each or any of the above age ranges.

The children and young people we have consulted have expressed the view that guidance should be clear and provide necessary information about their rights, the proposed use of their data and the protections available to all children and young people in appropriate language, format and context.

The Taskforce and its members including children and young people can provide design advice for guidance when appropriate. The proposed age ranges seem sensible at this stage of development.

4.1 What communication methods should APP entities use to ensure privacy policies are meaningfully understood by children of different ages, abilities and backgrounds?
4.2 How should APP entities ensure APP1 obligations are met when their services are used by both adults and children, particularly when children are not the intended primary users?
4.3 What should be considered under the 'reasonable steps' test when implementing internal practices, procedures and systems for managing children's personal information?

At this stage, the principles and key steps outlined below will likely not only provide benefits for adults as well as children and young people. We recommend that platforms could use these principles and key steps to guide improving accessibility for all. The standard required to establish 'reasonable steps' can be adjusted and improved to reflect the measured level of engagement by a platform with children and young people over time.

4.4 What steps should APP entities take to ensure children, and their parents, can easily make privacy-related inquiries or complaints, and how should APP entities respond in a child-appropriate way?
4.5 Do you have any specific views on how APP 1 should be applied or complied with in relation to the privacy of children?

The Taskforce has worked with Reset.Tech Australia, Taskforce members and several groups of children and young people to produce a set of key requirements for platforms to establish effective complaints mechanisms. Additional material is included in appendices to Reset Tech 's submission.

The Key Steps (next page) could be presented with a set of underlying principles that should guide the work. These would likely include respect for the rights of the child including specifically a child's rights to information, to be heard and to be safe; awareness of the stages of child development; cultural awareness and trauma informed; do no harm; and the importance of child-friendly language, information and supports.

A definition of child-friendly language could be provided or set by reference to explanatory materials such as the Guidelines on Child-Friendly Justice (Council of Europe 2010).[21]

[21] https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168045f5a9

The Draft Top Ten Key Steps for Platforms are as follows:

1. Provide clear information to children and young people about their privacy rights – including what privacy rights mean in practice, how to complain, the potential outcomes of a complaint and guidance on the responsibilities and limitations for data sharing on the part of technology platforms.

2. Provide a range of accessible and flexible avenues for complaint that are child friendly, designed to meet children's diverse needs.

3. Provide clear processes that offer reliable and accessible responses to children – including reasonable timeframes, and using appropriate avenues, formats, and language.

4. Make it clear that it is OK to disagree with a platform's approach, provide feedback to the child or young person on the reasons for a decision or practice (in accessible language and formats to that child or young person) and provide opportunity to challenge or review decisions.

5. Provide clear pathways to appropriate support services, including advocacy support.

6. Ensure compliance with all relevant Child Safe Standards including confidentiality and consultation with children and young people, in addition to complaint mechanisms.

7. Do not take technical objections to complaints and provide confidentiality for children who may not have 'permission' to be on a platform (subject to regulatory or legal requirements).

8. Allow for indirect complaints (made on behalf of a child) and mechanisms for super-complaints (made on behalf of a group including children) and allow for advocacy support for these complaints.

9. Provide regular transparency reports on complaints, mechanisms, and outcomes and collaborate with the regulator to build knowledge on systemic trends.

10. Offer remedies that are meaningful to the child, that acknowledge and respond to a child's views and expectations and thereby build children's confidence in the complaints process.

Commentary from Young People on Draft Top Ten Key Steps

Our review sessions with young people tested the draft key steps and here are their additional observations:

Provide clear information to children and young people about their privacy rights – including what privacy rights mean in practice, how to complain, the potential outcomes of a complaint and guidance on the responsibilities and limitations for data sharing on the part of technology platforms.

Many children don't know that they can complain, let alone how to complain. They want clear information about what privacy is. Terms and conditions must be much clearer and easier to understand. It should be clear what data is being collected and why. They fear not being believed, taken seriously, or facing consequences (especially if they've broken "rules" or terms of service themselves).

Provide a range of accessible and flexible avenues for complaint that are child friendly, designed to meet children's diverse needs.

A complaints process can be intimidating and appear complicated and unfamiliar. This will be especially important for children who lack strong and informed support structures as children's worlds are not always consistent and documented. Children lose phones, passwords, contacts, and consistent support including homes! But also consider the risk of parents as facilitators of abuse (such as in DFV settings): not all children have a protective parent. Confidentiality remains important.

Provide clear processes that offer reliable and accessible responses to children – including reasonable timeframes, and using appropriate avenues, formats, and language.

Guidance is often written in adult language and requires literacy and digital skills that not all children have. There are resources available that have been designed specifically for adolescents. Peer-created or peer-reviewed explainer content can be hugely powerful as young people often trust other young people.

Make it clear that it is OK to disagree with a platform's approach, provide feedback to the child or young person on the reasons for a decision or practice (in accessible language and formats to that child or young person) and provide opportunity to challenge or review decisions.

Children and young people generally believe that they are talking to 'scary' government organisations or big companies, which may be seen as unapproachable. Sometimes children and young people may think that their concerns won't be acted on. Embed a "right to complain" as part of onboarding processes so it's something that is learnt and familiar before they run into trouble.

This is still a huge cultural challenge especially for children and young people who have experienced exploitation and abuse. There will be fear of consequences or of no response at all if you complain. Young people (often males) will turn to their peers rather than adults especially in dealing with online experiences such as sexploitation.

Platforms can normalise help-seeking behaviours (for example by offering pop-ups "Is something bothering you?" with a simple tap-through complaint button).

Provide clear pathways to appropriate support services, including advocacy support.

Some children lack consistent support structures. There will need to allowance for the involvement of a trusted adult, peer or sibling. Peer support mechanisms and training will be important especially as options for a child or young person who may not have confidence in a support service.

Ensure compliance with all relevant Child Safe Standards including confidentiality and consultation with children and young people, in addition to complaint mechanisms.

There should be a dedicated children's privacy and safety team, with lived experience and / or specialist training; and a "test your complaint" sandbox tool that lets children walk through the complaint process safely.

Do not take technical objections to complaints and provide confidentiality for children who may not have 'permission' to be on a platform (subject to regulatory or legal requirements).

This was reinforced as important in the context of the layers that may surround a child's experience, especially if it includes exploitation or abuse. Disability, lower literacy, non-English speaking backgrounds may be part of that experience and create additional barriers to access. Being aware of and addressing these factors should be part of the responsibility of the platform.

This also requires an awareness of the limitations of older technologies as well as developing newer technologies. Children often have older mobile phones or lack access to easy-to-use computers. Again, note the previous point on lack of consistent support structures.

Taking a child back to the platform that facilitated their abuse, or exploitation can create a risk of re-traumatisation. Children and young people should be supported to complain in a way that is safe and meaningful for them, that might not require returning to the platform itself.

Allow for indirect complaints (made on behalf of a child) and mechanisms for super-complaints (made on behalf of a group including children) and allow for advocacy support for these.

This should include clear information and resources that can be shared amongst young people to allow for peer supports. Third party complaints should be supported. If a complaint is made on behalf of a child or young person (or a group of them), there should be appropriate opportunities for the children or young people involved to be involved to the extent that they wish.

Provide regular transparency reports on complaints, mechanisms, and outcomes and collaborate with the regulator to build knowledge on systemic trends.

Build in the requirement to support independent research as well, including participatory action research with children and young people.

Offer remedies that are meaningful to the child, that acknowledge and respond to a child's views and expectations and thereby build children's confidence in the complaints process.

Follow up interactions and responses must continue to be appropriate for the child or young person involved. This will be more challenging because of the social media ban. Follow-up mechanisms should not drop into an email black hole. Platform messaging or check-in bots should speak in age-appropriate language. Feedback tools such as "dislike' buttons could lead to a complaint mechanism. Algorithms should treat responses appropriately and not just as 'engagement'.

5.1 How can APP entities provide children with meaningful options to use services anonymously or under pseudonyms, considering their developmental stages at different ages?
5.2 In what scenarios would it be justifiable to require children to identify themselves to access an APP entity's service? How can these instances be minimised to protect their privacy?
5.3 Are there instances where age assurance technologies conflict with an individual's right to remain anonymous or pseudonymous, and what evidence supports this, or suggests otherwise?
5.4 Do you have any specific views on how APP 2 should be applied or complied with in relation to the privacy of children?

The Taskforce has no detailed specific views on these questions. The right to anonymity and pseudonymity afforded by APP 2 should be available to children and young people. It provides avenues for privacy and protection for children and young people in a range of circumstances that have been under-explored in policy and practical terms. Age assurance technologies should not operate in a manner that will undermine a young person's ability to manage their online activity safely and to protect their own privacy rights. We support greater engagement with these questions in the future. They offer the opportunity for activating a young person's awareness of their privacy rights and guiding responsible and rights-respecting regulatory development.

6.1 What criteria should define what is 'reasonably necessary' for an APP entity's functions or activities when collecting children's personal information, and how can APP entities ensure they adhere to this?
6.2 What does 'lawful 'and 'fair' mean in the context of children's personal information? How should these terms be applied specifically for children, given their evolving developmental and digital engagement stages?
6.3 Are there cases in which the collection of children's personal information would not be considered fair in any circumstances?
6.4 How can APP entities obtain genuine consent from children, or their parents or guardians, for the collection of sensitive information?
6.5 Do you have any specific views on how APP 3 should be applied, or complied with, in relation to the privacy of children?

The Taskforce supports Reset Tech's advocacy for a child rights approach to the collection of personal information of children and young people. There is appropriate international use of child rights and the "best interests" principle in assessments on children's rights in the digital world.[22] The *UN Convention on the Rights of the Child* proposes the principle as a primary consideration in policy decision-making[23] and the UN Committee on the Rights of the Child have endorsed the use of the principle in the digital environment.[24]

Generally, we support much greater attention to the collection of children's personal information by platforms and to closer examination of whether the collection of such information is necessary and justified as in the child's best interests. We believe that there may be many practices of the collection of children's personal information that are not in their best interests. Targeted advertising is one such practice.

We support the use of a requirement of a Children's Data Protection Impact Assessment by platforms that includes an examination of whether a practice is in the best interests of children.

[22] Detailed in the Reset.Tech Australia submission
[23] Article 3 of the Convention
[24] Committee on the Rights of the Child 2021 G*eneral comment No. 25 (2021) on children's rights in relation to the digital environment*., https://www.ohchr.org/en/documents/general-commentsand-recommendations/generalcomment-no-25-2021-childrensrights-relation, Paragraph 12 & 13

7.1 What processes should APP entities implement to identify and appropriately handle unsolicited personal information related to children?
7.2 Do you have any specific views on how APP 4 should be applied, or complied with, in relation to the privacy of children?

We believe that direct marketing to children and young people is not appropriate. We note that it was described as 'creepy' in our consultations with young people.

8.1 What methods can be employed by APP entities to effectively notify or ensure children are aware of data collection practices in a manner that is age-appropriate and can be easily understood by children?
8.2 How can APP entities ensure that notifications are accessible to children with diverse needs, including those from culturally and linguistically diverse backgrounds, or living with disability?
8.3 Are there circumstances in which an APP entity would be justified in taking no steps to notify or ensure children are aware about data collection practices? How can we minimise these instances to ensure that APP entities are adopting a best practice approach when it comes to notification and awareness?
8.4 Do you have any specific views on how APP 5 should be applied or complied with in relation to the privacy of children?

As discussed above, the children and young people we have consulted have indicated that guidance from platforms should be clear and provide necessary information about their rights, the proposed use of their data and the protections available to all children and young people in appropriate language, format and context.

We refer to the insights provide by young people in our review consultations (on pages 9 and 10) as to the layers of a child's experience, and the expectation that platforms would act proactively to address these matters. These matters should be addressed in an ongoing manner through assessment and review, both internally and through appropriate accountability measures.

The Taskforce and Taskforce members including children and young people can provide design advice for guidance when appropriate. The proposed age ranges seem sensible at this stage of development.

9.1 How can APP entities obtain genuine consent from children, or their parents or guardians, for the use or disclosure of their personal information, while ensuring that they comprehend the implications of such use or disclosure?
9.2 What safeguards should APP entities put in place to prevent the misuse of children's personal information for secondary purposes without appropriate consent or where other exceptions apply?
9.3 What secondary uses or disclosures of personal information could be reasonably expected by children, and how should these expectations vary by age and stage of development?
9.4 Do you have any specific views on how APP 6 should be applied or complied with in relation to the privacy of children?

Our consultations disclosed a deep disquiet with current practices around obtaining consent. Children and young people were clear that the starting point for any process should be the transparent provision of clear and accessible information about their rights to privacy.

Several of the key steps to be required of platforms offer guidance (see answers to Question 4)

- Provide clear information about your privacy rights
- Provide clear processes for that offer reliable and accessible responses to children
- Provide feedback to the child or young person on the reasons for a decision or practice (in accessible language and formats)

Evidence of attention to these key steps as part of a Children's Data Protection Impact Assessment would be welcome.

10.1 Can an APP entity ensure that it creates a 'reasonable expectation' that it may use or disclose children's personal information for the purposes of direct marketing? And if so, how?
10.2 How can APP entities ensure mechanisms are in place for children to opt-out of receiving direct marketing communications, in a simple and accessible way?
10.3 Do you have any specific views on how APP 7 should be applied or complied with in relation to the privacy of children?

We believe that direct marketing to children and young people is not appropriate.

11.1 How can APP entities ensure that cross-border transfers of children's personal information are conducted in a way that protects children's privacy rights, especially when laws in other countries may not offer equivalent protections?
11.2 What steps should APP entities take to communicate with children (or their parents or guardians) about the risks of cross-border data transfers?
11.3 Do you have any specific views on how APP 8 should be applied or complied with in relation to the privacy of children?

The Taskforce has no detailed specific views on these questions.

We support Reset. Tech's views that this is an area that will require further examination. We have concerns about the secure storage of children's data offshore and even greater concerns about the processing and potentially unregulated use of that data. It would appear to be a significant challenge in terms of compliance and enforcement.

12.1 What does 'accurate', 'up-to-date', 'complete' and 'relevant' mean in the context of children's personal information? How should these terms be applied specifically for children, given their evolving developmental and digital engagement stages?
12.2 How can APP entities effectively ensure that the personal information they collect from children remains accurate and up to date, considering the dynamic nature of a child's life and the potential challenges in maintaining this data?

This raises important considerations about evolving development[25] and children's changing circumstances and views. It may be helpful to consider, alongside the process of supporting complaints, a parallel and more pro-active process of data review. This could provide a child with the opportunity at various stages to re-examine their decisions and correct, amend or delete their data. It may offer a staged process for parents, carers and guardians to manage the transition of decision making to support a child's developing independence. This may be built into the requirements on a platform based on their level of interaction with children at various stages of development.

13.1 Are there any additional or specific technical measures that APP entities should adopt to safeguard children's personal information from security risks, considering their heightened vulnerability?
13.2 Are there any additional or specific organisational measures that APP entities should adopt to safeguard children's personal information from security risks, considering their heightened vulnerability?
13.3 How can APP entities ensure their data retention policies are appropriate for children's data, including timely deletion or de-identification when the information is no longer needed?
13.4 Do you have any specific views on how APP 11 should be applied, or complied with, in relation to the privacy of children?

The Taskforce has no detailed specific views on these questions beyond the views expressed elsewhere in this submission.

[25] Article 5 of the UN Convention on the Rights of the Child

14.1 What mechanisms are needed to ensure children can easily access their own personal information?
14.2 In what circumstances might providing a child access not be in their best interests? What would help entities navigate these situations responsibly?
14.3 In what circumstances should a parent or guardian be able to make an access request on their child's behalf and receive a copy of their child's personal information? How should the balance be struck between a parent's right to protect the best interests of their child and the child's right to privacy, when APP entities are dealing with access requests for a child's personal information?
14.4 What timeframe should be considered a 'reasonable period' for responding to a child's access request?
14.5 In what manner or format should personal information be provided to a child when an access request is made, so that it is both practicable for APP entities and developmentally appropriate for children of different ages and capacities?
14.6 Do you have any specific views on how APP 12 should be applied or complied with in relation to the privacy of children?

15.1 What does 'accurate, 'up to date', 'complete', 'relevant' and 'not misleading' mean, in the context of children's personal information, given their evolving developmental and digital engagement stages?
15.2 What processes or mechanisms should be established to allow children to request corrections of their personal information easily?
15.3 In what circumstances should a parent or guardian be able to make a correction request on their child's behalf?
15.4 What timeframe should be considered a 'reasonable period' for responding to a child's correction request?
15.5 Do you have any specific views on how APP 13 should be applied or complied with in relation to the privacy of children?

We refer to our comments in answer to Questions 4 and 12 and our guidance in relation to a child's right to complain. This could help to design a more comprehensive and active process of data review. We note with support Reset Tech's reference to detail in existing Codes internationally in answer to Question 14 and 15 and to previous advice on a child's sense of time in relation to timeframes. We also support Reset Tech's recommendation for the inclusion of a right to erasure which would be a key component of an effective right to review of previous privacy decisions (including by a parent or guardian or in the absence of a decision).

Prepared by the Australian Child Rights Taskforce Policy Working Group
on behalf of the Australian Child Rights Taskforce

With assistance from Reset. Tech Australia, Bravehearts, Project Rockit,
Reach Out, your town / Kids Helpline UNICEF Australia, Child Fund Australia.

James McDougall
Dr Rys Farthing
Associate Professor Georgina Dimopoulos, Southern Cross University

For contact and further information
James McDougall
M +61 (0) 419 243 179
E james@policyconsultants.com.au

We acknowledge the Traditional Owners of the lands on which I live and work, and their continuing connection to land, sea and community. I pay my respects to Elders past, present and emerging.