ChildFund Australia

# SUBMISSION

## TO THE OAIC'S *CHILDREN'S ONLINE PRIVACY CODE ISSUES PAPER*

AUGUST 2025

## INTRODUCTION

ChildFund Australia welcomes the opportunity to contribute to the Children's Online Privacy Code consultation led by the OAIC.

Our submission draws on programmatic and advocacy experience working with children across Australia and the Indo-Pacific in education, child protection and health, including across digital settings. Our work here includes:

- Digital Literacy programs for children and young people, and their parents and care givers, across the Asia-Pacific, Swipe Safe
- Participating in and facilitating sector, and young peoples consultations, including:
    - As facilitator to the sector consultation organisation by Reset.Tech *Briefing Paper on the APPs & Children's Rights*
    - As a co-author on *Best Interests and Targeting: Implementing the Privacy Act Review to advance children's rights* including facilitating young peoples participation
    - As a co-author on *Capacity of the consent model online*
    - As a co-authors *How outdated approaches to regulation harm children and young people and why Australia urgently needs to pivot*
    - Through consultation with government in reforms to the Privacy Act
    - Supporting consultation with young people about the Children's Online Privacy Code; especially Transparency, Geolocation, Advertising & EdTech
- Workshops, conference presentations and media engagement focussing on program intervention and policy regulation at national, regional and international forums

As a signatory to the UN Convention on the Rights of the Child[1], Australia has clear obligations to children's rights. The Code must reflect these international standards, aligning the Code to children's rights. This includes associated General Comments, in particular General Comment 25[2]. As such we note that:

- Children's rights are indivisible and interconnected — participation, protection, education, information, privacy, play and development cannot be ranked.
- The best interests of the child must be a primary consideration
- This outweighs commercial interests and demands a comprehensive assessment of the needs and rights of each child and children collectively, as an essential part of meeting requirements of the Code.

---

[1] United Nations. (1989). *Convention on the Rights of the Child*. Treaty Series, 1577, 3. https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child

[2] Committee on the Rights of the Child. (2021, March 2). *General comment No. 25 (2021) on children's rights in relation to the digital environment* (CRC/C/GC/25). United Nations. https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation

The UN Special Rapporteur on the Right to Privacy (2021)[3] emphasises the scale of data generated through children's digital immersion, highlighting the urgent need for legislative safeguards and effective implementation.

We further note and commend the OAIC's effort to:

- Engage young people from the outset
- Provide time and space for meaningful civil society input.

Our response against the discussion paper is targeted in scope, and follows.

## QUESTION 1: SCOPE OF SERVICES COVERED BY THE CODE

If a core intent of the Children's Privacy Code is to uplift privacy and focus on the harm to children's privacy, additional entities should be considered to be within scope of the code, including, for example, ed tech, ad tech and gaming.

We also note here findings from the Online Safety Act that identified that the scope of the Act, as defined by a set of 'categories' be restructured to better reflect the digital environment – with a view to 'future-proofing' it. This would serve to reorientate to a 'function' based classification that was centred on harm to the community, rather than a narrow set of labels that held little regard for the size or risks posed by the service. Similar intent could carry over to the scope of the privacy code in that harmful data and privacy practices for children, and those who can mitigate that harm – regardless of what digital platform or category of product or service it occurs on - should be in scope, and the Commissioner given powers and resources to respond, regardless of the size of the service or product.

Specifically, EdTech, AdTech, Artificial Intelligence, and gaming and wearables should be included within the scope of the code. Evidence on the inclusion of additional entities in the Code follows.

**EdTech:** HRW (2022) found 89% of 163 EdTech tools engaged in harmful data practices including:

- Covert surveillance,
- Third-party data sharing with AdTech,
- Profiling and behavioural targeting.

These practices risk distorting children's learning, shaping their behaviour, and compounding stigma and inequality through automated systems. As is noted in the Committee on the Rights of the Child's General Comment 25:

*"...forms of discrimination can arise when automated processes that result in information filtering, profiling or decision-making are based on biased, partial or unfairly obtained data concerning a child."*

**Ad Tech:** The General Comment goes further to compel Government's to explicitly prohibit targeted advertising – as realised through 'ad tech' - in that this could in no way be in the best interest of children. The process of targeted advertising involves the sweeping and arbitrary collection of children's personal data, and the

[3] Office of the United Nations High Commissioner for Human Rights. (2021, September 13). *The right to privacy in the digital age* (A/HRC/48/31). United Nations.

subsequent broadcasting of their data to a non-selective group of advertising buyers.[4]

In this way, Ad Tech should also come within scope of the code.

*"States parties should prohibit by law the profiling or targeting of children of any age for commercial purposes on the basis of a digital record of their actual or inferred characteristics, including group or collective data, targeting by association or affinity profiling. Practices that rely on neuromarketing, emotional analytics, immersive advertising and advertising in virtual and augmented reality environments to promote products, applications and services should also be prohibited from engagement directly or indirectly with children."*[5]

The *process* required to deliver targetted advertising is data heavy and involves a number of concerning data handling behaviour that would constitute a high risk to children.[6] These include

- arbitrary nature of data processing with little oversight or due diligence
- covert nature of data processing - lack of consent and autonomy offered to children, or right to object
- lack of data minimisation

This also becomes a question of scope and threshold because targeted advertising is broader than APP 7, and crosses a number of APPs.

Aside from the matter of scope, and addressing targeted advertising practices across the APPs, we would strongly recommend the privacy code seeks to outright prohibit targeted practice on privacy grounds.

**Artificial Intelligence Systems[7]:** Frequently, children's data forms part of the data set on which AI systems have been trained. Recent examples in Australia have shown just how detrimental this can be to children. Investigation by the Human Rights Watch found that personal photos of Australian children are being used to create AI tools without the knowledge or consent of children or their parents/caregivers. Images were used to train tools, and then tools used to create deepfakes – essentially child sexual abuse material. The data also contained highly personal information such as full names, ages and pre-school they attended.[8]

---

[4] Irish Council for Civil Liberties 2022 Real Time Bidding, https:// www.iccl.ie/rtb/

[5] United Nations Committed on the Rights of the Child 2021 General comment No. 25 (2021) on children's rights in relation to the digital environment https://docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=fT3nx%2FKEyjPie59GG8iHdDugSg7GO4Dn9 %2BWkWC%2Fa8TLwKtEAuEF1HM7qW2BzwAImZaR0aN5pTFnoVkzMYkxYKQ%3D%3D, Para 42

[6] https://au.reset.tech/news/targeted-advertising-the-children-s-online-privacy-code/#:~:text=Targeted%20advertising%20is%20a%20violation,them%20in%20danger%20of%20harm.

[7] The European Union's (EU) Artificial Intelligence (AI) Act, an 'AI system' means 'a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.' See: European Union (2024) EU Artificial Intelligence Act, Article 3: Definitions.

[8] Human Rights Watch (2024) *Australia: Children's Personal Photos Misused to Power AI Tools Data Privacy Safeguards Needed to Protect Against Exploitation, via* https://www.hrw.org/news/2024/07/03/australia-childrens-personal-photos-misused-power-ai-tools

Another example could be use of recommender systems, while can facilitate or promote children's rights (such as ability to seek and receive information, leisure and play, freedom of association) they frequently violate them. The nature of children's development means that they are predisposed to prioritising immediate need over long term consequences, making them more vulnerable to products and services designed to undermine privacy in order to gather data. Harmful systems can:

- create unfair outcomes, with sometimes lifelong impacts for children, due to decisions that are discriminatory or inaccurate
- create harm: use of data to generate synthetic material that can amount to sexual exploitation and abuse, be used to humiliate or bully, facilitate misinformation or criminal activities, recommend content that is risky like violent or extreme content, disordered eating or promote connections between children and unknown adults
- violate rights to privacy through pervasive data collection, scraping, and processing which is used to profile them (like predicting or provoking thoughts feelings and actions)

Enforcing obligations on such systems through the privacy code to a) assess privacy risks to rights of children and b) mitigate risks would ensure children's rights to the digital environment are progressed, and violations improved upon.

## 2. WHEN AND HOW SHOULD THE CODE APPLY TO APP ENTITIES

The Code must apply to all digital platforms Likely To Be Accessed (LTBA) by children and/or those that process children's data, not just those specifically targeted at children.

We reiterate messages from the Child Rights Taskforce and Rest-Tech Australia that a precautionary approach to scope and threshold is necessary, that in order to uplift privacy, maximum coverage is required, requiring low thresholds.

A definition of children in the code should reiterate the definition provided by the UN Convention on the Rights of the child – up to the age of 18. Noting that the UNCRC General Comment No. 25 affirm the full scope of children's rights extend fully in the digital environment, where "states parties should require the integration of privacy-by-design into digital products and services that affect children".[9]

Size doesn't not always equate to risk. We support threshold criteria that doesn't just apply to 'reach' but also factors in 'risk'. This is built into different codes in various international jurisdictions but is worth explicit mention in Australia's code.

The UK Age Appropriate Design Code (AADC)[10], for example, makes clear that a service does not need to be designed for children, or have children make up a

---

[9] United Nations Committee on the Rights of the Child. (2021). *General comment No. 25 (2021) on children's rights in relation to the digital environment* (CRC/C/GC/25), para. 70. United Nations. https://digitallibrary.un.org/record/3906061

[10] Information Commissioner's Office. (2020). ***Age-Appropriate Design Code: A code of practice for online services***. UK Information Commissioner's Office. Available via https://ico.org.uk/for-

substantial proportion of users, for the Code to apply. Instead, the standard is whether child use is meaningful.

Importantly, the AADC stresses that determining whether use is significant requires consideration of both:

- the number of child users, and
- the risks those users face in relation to their data.

This approach recognises that even if only a small percentage of users are children, the potential for harm may still be high, particularly where high-risk data processing applies, such as where data is used to profile, target, or influence children in ways that interfere with their rights or development.

This principle is especially relevant given how children often use general-purpose or mixed-audience services (e.g. gaming platforms, social media, search engines) that are not strictly "child-directed," but still collect or process children's data at scale.

We do not support dispensing of responsibilities through disclaimers in products or services Terms of Use that state intentions around users above or below a certain age.

The Children's Privacy Code should adopt a risk-and-reach-based threshold for application — not a "child-directed" threshold.

Specifically:

- The Code should apply to any service that is likely to be accessed by children or that processes children's data, regardless of whether children are the primary audience.
- The threshold for inclusion should be more than a de minimis level of child use, consistent with the UK's AADC.
- Regulatory guidance should clarify that a service's obligations under the Code are triggered by:
    - Significant or meaningful use by children (even if they are not the majority of users), and/or
    - Nature and severity of risks to the rights of children, including their right to privacy, wellbeing and development – not just size or type of entity. This should be based on real-life understanding of how children use digital environments
- When compliance with the code is triggered, a child rights impact assessment based on prevailing principle of the best interests of the child, should be the backbone of a child specific privacy impact assessments. These should be made publicly accessible to promote trust, transparency and research to the benefit of children.

**Consideration for cultural rights of Aboriginal and Torres Strait Islander Children**

---

organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/

The Code must give due consideration to what additional protections for Aboriginal and Torres Strait Islander children are owed, recognising:

- Cultural knowledge and community-held data as sensitive and distinct from individual personal data.
- Data sovereignty as a foundational principle — including rights to self-determination over data collection, use, sharing and reuse.
- Culturally safe consent mechanisms, designed in partnership with First Nations-led organisations

### 3. AGE RANGE SPECIFIC GUIDANCE

We support the use of age-based guidance, but would note that these be used in conjunction with child rights impact assessments which supports risk identification and mitigation not just across age, but capacities and developmental needs.

Guidance should recognise that while all children require protection, vulnerabilities shift across developmental stages and contexts of use. Younger children face specific risks due to limited digital literacy and reliance on adult support; however, they are not always the most vulnerable users across all digital services. Adolescents, for example, are undergoing a second major period of neurological development, second only to early childhood, which coincides with increased independence, reduced adult supervision, and a marked shift toward peer influence and adults outside the family home – a broader social network. This stage is often marked by greater exposure to complex digital environment, with less oversight from parents, and more frequent online risks, highlighting the need for age-responsive, developmentally informed protections that go beyond static age assumptions.

This necessitates an approach that includes direct participation of children and young people, and informed by real-world use.

This should be back up by auditing and enforcement action on how services are recognising and responding to different needs and capacities at different ages and stages.

### QUESTION 4: APP 1 – OPEN AND TRANSPARENT MANAGEMENT OF PERSONAL INFORMATION

The Code should include obligations on products and services to provide child-friendly information about privacy. There has been a good level of research in the Australia context with young people who have identified communication methods that would support their understanding of privacy information.

Information about their rights is the precursor to being able to claim the – and encourages help-seeking behaviour. Therefore, entities must provide clear, plain-language information to children about their privacy rights, including what data the platform is allowed to collect, use, and especially share or disclose. This should also include the consequences of sharing such data with the entity.

Information provided should also explain what children have the right to question or complain about, and what might happen as a result of making a complaint.

We would support explicit guidance given to entities that prohibits the use of child friendly information to encourage children to engage in data sharing practices, through for example,  gamification, illustrations and colourful graphics.

**Child Friendly Complaints Mechanisms**

Child Friendly complaints mechanisms for violation of rights is essential to children's ability to access justice, right to remedy and redress. Ensuring effective complaints mechanisms is a key recommendation coming from the Royal Commission into Institutional Responses to Child Sexual Abuse (Royal Commission) and a key action in the National Principles for Child Safe Organisations. This would ensure the Code aligns with international treaties as well as aligned to national policies deliberately established to increase safety and survival of children.

We support the work of the Australian Child Rights Taskforce in their submission to the Commission, particular in relation to complaints mechanisms.

There are a number of key findings from the royal commissioner that could inform the steps entities could take to ensure children and their parents can make privacy related inquires or complaints.[11]

| **Royal Commission Finding** | **Implications for Children's Privacy Code Complaint Mechanisms** |
|---|---|
| A complaint is more than a formal report | Recognise and accept informal, non-verbal, and third-party reports as valid complaints, especially where children cannot articulate harm in conventional ways.<br><br>Complaints should also include not just a violation of the code, but claims for imminent or foreseeable harms. |
| Common failures undermine safety | Mandate clear, child-focused complaint procedures to avoid ignoring, minimising, or poorly investigating complaints related to digital privacy and data harms. |
| Complaint mechanisms must be child-focused | Ensure mechanisms are accessible, understandable, and developmentally appropriate. Children should be able to lodge complaints independently. |
| Support must be proactive and inclusive | Provide communication aids, culturally appropriate support, and proactively assist children from diverse backgrounds to raise complaints. |

[11] Royal Commission into Institutional Responses to Child Sexual Abuse. (2017, December). Final Report: Volume 7, Improving Institutional Responding and Reporting. Sydney: Royal Commission into Institutional Responses to Child Sexual Abuse, via https://www.childabuseroyalcommission.gov.au/improving-institutional-responding-and-reporting

| | |
|---|---|
| Transparency and accountability are crucial | Designate responsible officers, respond promptly, and keep children informed throughout the process in accessible formats. |
| Investigations require procedural fairness | Ensure complaints are handled impartially, proportionally, and transparently, with clear documentation and fair processes. |
| Outcomes must lead to change | Use complaints to drive systemic improvements, regulatory oversight, and continuous accountability for children's data protection. |

UNICEF has also provided further guidance for key operational considerations when operating child-sensitive complaint mechanisms.

| Principle | Key Requirements |
|---|---|
| Accessibility | - Children are aware of the mechanism and how to use it (child-friendly outreach).<br>- Minimal formalities; accept all forms of complaints, verbal or written.<br>- Direct access for children without requiring parental consent.<br>- Proactively remove barriers: attitudinal, physical, communication, geographic, economic. |
| Responsiveness | - All complaints must be acknowledged and acted upon.<br>- Clear explanation of the process and outcomes in age-appropriate formats.<br>- Investigate where possible; refer cases outside mandate with active follow-up.<br>- Maintain communication with the child throughout. |
| Timeliness | - Recognise the urgency of complaints due to children's development and time sensitivity.<br>- Set and follow internal timeframes (e.g. 30–60 days).<br>- Fast-track urgent cases (e.g. violence, neglect).<br>- Inform children of delays and reasons. |
| Fairness | - Handle complaints impartially, thoroughly, and transparently.<br>- Engage multiple staff for complex cases to reduce bias.<br>- Ensure children's views are meaningfully considered.<br>- Provide appeal options and access to alternative remedies. |
| Information for the Child | - Clearly explain the process, rights, and support available.<br>- Provide regular updates on complaint status and decisions.<br>- Explain how the child's input was used in decision-making.<br>- Use accessible formats (e.g. visuals, plain language). |

| | |
|---|---|
| Privacy & Confidentiality | - Enable confidential submission (e.g. untraceable hotlines, online forms, sealed boxes).<br>- Inform child if confidentiality must be breached, and explain why.<br>- Enforce strict data privacy policies, including limited disclosure and staff confidentiality.<br>- Protect identity in all documentation and public communications. |

(Source: UNICEF: https://www.unicef.org/eca/sites/unicef.org.eca/files/2019-02/NHRI_ComplaintMechanisms.pdf )

## QUESTION 6: APP 3 – COLLECTION OF SOLICITED PERSONAL INFORMATION // QUESTION 9: APP 6 – USE OR DISCLOSURE OF PERSONAL INFORMATION

The collection, processing, and use of children's personal data must be governed by clear baseline principles that prioritise the best interests of the child. These include, but not be limited to:

- Privacy by default: All settings should default to the highest level of privacy, with children required to actively opt in to lower privacy options.
- Data minimisation: Only the minimum amount of personal data necessary to deliver a service should be collected, used, or stored.
- No manipulative design: Platforms must not use persuasive design or dark patterns to encourage children to reduce their privacy, provide more data, or make choices that are not in their best interests.
- Sensitive features off by default: Geolocation, microphone, and camera functions must be switched off by default. If geolocation is activated during a session, it must automatically turn off at session end. While active, location tracking must be clearly visible and easily understood by children.
- Necessity vs. optionality: Platforms must clearly distinguish between data that is strictly necessary for the service and data that is optional, and ensure children are not penalised or excluded for refusing to provide optional data.
-

If collecting, using, or disclosing a child's data does not serve their best interests, it cannot be regarded as fair or justified.

**Consent**

The UN CRC General comment notes:

*"Where consent is sought to process a child's data, States parties should ensure that consent is informed and freely given by the child or, depending on the child's age and evolving capacity, by the parent or caregiver, and obtained prior to processing those data. Where a child's own consent is considered insufficient and parental consent is required to process a child's personal data, States parties*

*should require that organizations processing such data verify that consent is informed, meaningful and given by the child's parent or caregiver."* [12]

Consent should be informed, free (voluntarily), specific, prior and ongoing (current) and age appropriate. However, we note that consent is fraught in the digital environment, and we note consultations with children and young people provided in depth information the coercive nature of consent when it comes to handing over their data – essentially, where exchange of data is necessary to access services, and marked by a huge imbalance of power, particularly where data collection goes beyond what is required for provision of the services, and on sold to the detriment of children, terms are imposed and not freely negotiated.

Consent implies the ability to decline, yet in Australia, children often have no real option to opt out without losing access to essential services. As services like EdTech in classrooms, Centrelink payments, or emergency apps become digitised, refusing data collection can effectively mean being excluded from education, social support, or safety systems. In such cases, consent is not freely given, but functionally coerced. Drawing from a joint paper with Reset Tech, we surmised that when it comes to consent:

1. A greater emphasis is placed on the fair and reasonable test, and ensuring a child's best interests is a key principle in establishing fairness.
2. Engaging children and young people in the process.
3. Exploring how the application of the National Principles for Child Safe Organisations could reframe obligations around privacy and consent
4. Commissioning a targeted review into mechanisms that could improve informed consent, including dynamic consent and automated consent processes.

We recommend that consent should not be used to justify practices that are not in the best interests of children, such as secondary data use for commercial purposes or targeted advertising. These practices undermine children's rights and consent should not be a tool to legitimise such types of data collection, processing and use.

## QUESTION 10: APP 7 – DIRECT MARKETING

The Children's Privacy Code should provide clear guidance on the distinction between direct marketing and targeted advertising.

We strongly support an outright prohibition on targeted advertising, given its reliance on behavioural profiling, data surveillance, and its incompatibility with children's rights to privacy and protection from exploitation.

Direct marketing, however, could warrant a different approach. While it is rarely in a child's best interests, there may be limited and clearly defined circumstances where it can support the realisation of their rights, such as promoting access to free health services, education programs, or protective resources. In these cases, direct marketing must be strictly non-commercial, transparent, and delivered in a child-

[12] Para 72

safe, developmentally appropriate, and rights-based manner. It should be subject to strong safeguards, including clear purpose limitations and oversight to ensure it serves the best interests of the child.

There could be an argument that, for example, a child signing up to receive news of the latest release of a game, or the latest Nike shoe, or through following their favourite AFL team, be subject to marketing to purchase team collateral - might promote their rights to leisure or play, or economic participation. However question of children's ability to understand and differentiate in commercial advertising should come into play, determining whether it is fair or in their best interest.

Research has shown that children are particularly vulnerable to commercial influence, due to their cognitive development stage, at some stages being unable to distinguish between ads or content, fiction or reality, and up until at least 12 – unable to fully comprehend the persuasive intent of ads. [13]

## CONTACT

[redacted]

[13] Report by Professor Yves de la Taille on PL 5921/2001 developed by request of the Federal Psychology Council, 'Advertising Aimed at Children: Psychological Considerations'. Available at: https://site.cfp.org.br/wp-content/uploads/2008/10/cartilha_publicidade_infantil.pdf.