

CHILDREN'S ONLINE PRIVACY CODE

A Submission by Young People for Young People: Tech Policy Design Institute Youth Ambassadors

Rachael Burns, George Trigenis and Bianca Kendrick

The Youth Ambassadors of the Tech Policy Design Institute acknowledge the lands on which we write this submission, the lands of Aboriginal and Torres Strait Islander peoples, whose cultures span over 65,000 years as the country's first innovators and policymakers.

Executive Summary

This submission welcomes the OAIC's work to strengthen children's online privacy. It posits that Code will be strongest if it is shaped by children and young people directly, applies protections before harm occurs, and does not leave platforms alone to define what children's best interests require. Policymakers should use the Code to make child privacy practical, understandable and enforceable, rather than expecting children to navigate complex data practices after their information has already been collected, shared or used.

Summary of Recommendations

Recommendation 1: Consult children where they are and recognise their lived experience, because a Code designed without the most affected children cannot credibly claim to protect them.

Recommendation 2: Extend baseline protections to young adults and ultimately all users, because turning 18 does not erase the data profile or platform risks built during childhood.

Recommendation 3: Clarify the meaning of "best interests", because leaving the standard to platforms risks turning child protection into a commercial judgement.

Recommendation 4: Close the health, wellbeing and biometric data gap, because children's most sensitive information should not fall outside stronger safeguards due to drafting uncertainty.

Recommendation 5: Strengthen privacy-preserving age assurance, because a child should not lose protection simply because an age prompt was weak or easy to bypass.

Recommendation 6: Co-design standardised child-facing privacy language, because rights are not meaningful if children cannot understand what they are agreeing to.

Recommendation 7: Require visibility over third-party data sharing, because children's privacy cannot stop at the first platform when their data continues moving behind the scenes.

Introduction

In March 2026, the OAIC released a Draft Children's Online Privacy Code (the Code), presenting important opportunities to strengthen children's online privacy, and we welcome each of the 14 rules in the Draft. This submission reflects the diverse lived experience of us as young people, Rachael Burns (23), George Trigenis (20) and Bianca Kendrick (24) and the individuals we engage with who may face barriers to participating in technology policy discussions, including a 19-year-old male participant whom we consulted relating to the Code.

Who gets a seat at the table?

Future consultation on the Code's Rules and application should prioritise broader, targeted engagement with communities facing barriers to participation and higher online risks, recognising that improving accessibility for these groups will benefit all children.

At the outset of our submission, we would like to acknowledge and thank the OAIC for its significant and robust efforts in developing the Code, including the preparation of consultation materials designed to engage children, young people, parents and carers, civil society, academia and industry. However, consistent with the recommendations outlined in the 2020 report commissioned by the OAIC, *Privacy risks and harms for children and other vulnerable groups in the online environment*¹, we would have welcomed broader and more targeted engagement with communities that face barriers to participation and heightened vulnerabilities online. These priority populations include, but are not limited to, people with disability, LGBTQIA+ people, people navigating mental health challenges, Aboriginal and Torres Strait Islander people, neurodivergent people, people from culturally and linguistically diverse backgrounds, people living in rural, regional, and remote communities, and people with intellectual disabilities.

The need for this targeted approach is supported by eSafety research finding that 71% of Australian children aged 10 to 15 had encountered content associated with harm online, with exposure varying by age and gender².

[Consultations] should happen in places we already are, like schools, youth services or community groups. A government website is not really where most young people go to share honest opinions. Also, [when operationalised] I would need simple examples with easy to read terminology, not just legal words. For example, openly stating "we use your location for this reason" and "we share it with these people."

- 19-YEAR-OLD MALE

¹Witzleb, N., Paterson, M., Wilson-Otto, J., Tolkin-Rosen, G., & Marks, M. (2020). Privacy risks and harms for children and other vulnerable groups in the online environment.
https://www.oaic.gov.au/__data/assets/pdf_file/0012/11136/Report-Privacy-risks-and-harms-for-children-and-other-vulnerable-groups-online.pdf

² eSafety Commissioner. (2026). Digital use and risk among children aged 10 to 15.
<https://www.esafety.gov.au/research/the-online-experiences-of-children-in-australia/report-digital-use-and-risk-among-children-aged-10-to-15>



The problem is that formal consultation processes may not reach the children and young people most affected by online harms, meaning the Code risks being shaped mainly by those already able to navigate policy language, institutional processes and online consultation formats.

This is likely to be supported by youth, disability, child rights and community organisations, and can be actioned through schools, youth services and trusted community partners rather than relying only on written submissions or online workshops.

In this instance, we acknowledge the OAIC's constrained budget environment. We recommend the Government consider increasing OAIC resourcing to support community consultations.

Protections to online privacy should not expire at 18

We would welcome the extension of key protections in the Draft Children's Online Privacy Code to young people aged 18–25, with a view to applying them to all users of digital platforms. In particular, standards such as data handling that is “strictly necessary” and applied “by default” (s9), consent that is “voluntary, informed, current, specific and unambiguous” (ss14–19), and prohibitions on “manipulative, deceptive or misleading practices” (s21) should be baseline protections for all users.

As young people aged over 18, we are concerned that the scope of the Code is limited to individuals under 18 years of age. We request that the application of key provisions be extended to provide protections for young people aged 18–25, and believe there is broader benefit in extending these protections to all Australian users of digital platforms. In particular, best-practice standards such as data handling that is “strictly necessary” and applied “by default” (s9), consent that is “voluntary, informed, current, specific and unambiguous” (ss14–19), prohibitions on “manipulative, deceptive or misleading practices” (s21), requirements for information to be “clear, concise, transparent” and “easily accessible” (ss23–24), rights to access information about the “handling of personal information” and request its destruction (ss27–28, 32), and a “simple and easy means” to opt out of direct marketing (s29) should be recognised as baseline protections for all users, not only children.

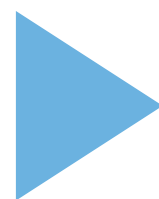
The practical gap is that a young person may remain on the same platforms and carry the same online profile after turning 18, while key protections no longer apply. Platform providers may argue that this extends beyond the intended remit of a children's code; however, the protections identified above are baseline privacy protections rather than a claim that young adults should be treated as children.

The OAIC-commissioned report also notes that privacy is a human right enjoyed regardless of age, ability or status, supporting the view that these protections should be understood as baseline safeguards rather than exceptional protections (OAIC, 2020).

We believe that timely implementation of the outstanding elements of the Privacy Act Review is an essential part of protecting Australians of all ages.

Who defines ‘best interests’?

We recommend that the “best interests” requirement be supported by clearer, more specific guidance and enforceable benchmarks to ensure consistent interpretation and application by platforms. Without



this, there is insufficient assurance that platforms will operationalise the standard in a way that genuinely prioritises children’s wellbeing.

Different children experience risk differently, and this cannot be adequately captured by a broad standard alone. This highlights the limitations of relying on platforms to interpret and operationalise “best interests”. Without greater specificity and regulatory guidance, the concept risks inconsistent interpretation, places a high degree of trust in industry actors, and presents challenges for effective oversight and enforcement.

[Best interests are not the same for each person], because people have different families, cultures, disabilities, mental health and experiences online. That is why the rules should not assume there is only one kind of young person.

I would worry they would say something is “for our safety” when it could covertly be helping them collect more information about us. I don’t think companies should get to decide [what best interests are] by themselves.

- 19-YEAR-OLD MALE

The impact is that “best interests” may be applied differently across platforms, or used to justify practices such as additional data collection where a platform frames the practice as safety, personalisation or convenience.

This concern is consistent with the United Nations Committee on the Rights of the Child’s guidance that privacy is vital to children’s agency, dignity and safety, and that risks can arise from data collection and profiling by businesses and other organisations³. Clearer benchmarks would also assist platforms by reducing uncertainty about what the standard requires.

Not all ‘health’ platforms deserve an exemption

We recommend that the scope of the Code be clarified and expanded to ensure that digital platforms collecting children’s biometric and health-related data, such as wearables and health tracking applications are brought within scope where appropriate. This could include narrowing the definition of “health service” or introducing additional criteria to ensure that services handling sensitive health data are subject to the Code’s heightened privacy protections, particularly where there is a risk of harm arising from profiling, advertising, or other secondary uses of that data.

As users of digital health and wellbeing services, we are concerned that the Code’s exclusion of entities “providing a health service” (Section 5) may unintentionally create a gap in protections for children’s most sensitive personal information. While recognising that some health service providers may be appropriately exempt (such as KidsHelpline), the current drafting appears to extend beyond traditional healthcare contexts to encompass a range of digital platforms, including wearable technologies and health-related applications that collect significant volumes of biometric and health data.

³ 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. <https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation>



This is particularly concerning given that these platforms may not be subject to the Code's strengthened safeguards, such as requirements that data handling be "strictly necessary" and consistent with the best interests of the child. This creates heightened risks where sensitive health and biometric data could be used for purposes such as targeted advertising, profiling, or behavioural influence. These risks may be especially acute for children experiencing mental ill health or disordered eating, where exposure to targeted content based on health data could exacerbate existing vulnerabilities. In practice, this means platforms should be expected to document why a particular data practice is necessary, what less intrusive alternatives were considered, and how the practice advances the child's wellbeing, privacy, autonomy and development.

Platform providers may argue that health service exclusions are needed to protect genuine support services from over-regulation. Our concern is narrower: that commercial health-adjacent products collecting sensitive biometric or wellbeing data should not fall outside the Code where that data may be used for profiling, advertising or other secondary purposes.

Reliance on self-declared age is insufficient

We recommend strengthening requirements around age assurance to ensure that protections apply consistently, regardless of self-declared age. This could include clearer minimum standards for "reasonable steps" to verify age, or encouraging the application of the Code's protections to all users by default where age cannot be reliably determined, to mitigate risks of exclusion and improve compliance certainty. This recognises the administrative burden for platform providers while still prioritising child-protective defaults where age cannot be reliably established.

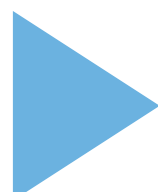
We note that the Code relies on entities taking "reasonable steps... to establish the age of the end-user," which may include methods such as self-declaration (Section 8). This raises concerns that where a child misrepresents their age, they may fall outside the intended protections of the Code in practice. If age entry is the primary safeguard, there is limited assurance that children are consistently identified and protected, and it becomes difficult to determine whether platforms are effectively adhering to the Code's obligations.

At the same time, stronger age assurance should not become a reason to collect excessive identity information from children and young people. The UK Children's Code provides a useful comparator by taking a risk-based approach to recognising age, and by applying children's standards to all users where age cannot be established with certainty appropriate to the risk⁴.

The key implementation issue is therefore not simply whether age assurance is used, but whether it is proportionate, privacy-preserving and matched to the level of risk created by the service.

Ensure consistency of platform communication and consent processes

⁴ Information Commissioner's Office. (2020). Age appropriate design: A code of practice for online services. <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/>



We recommend the co-design of a cross-platform, standardised language and communication guide for digital platforms, aligned with the Code's requirements that information be "clear, concise, [and] transparent," to support consistent, accessible, and user-centred privacy and consent practices across the digital ecosystem. This would reduce confusion for children navigating multiple services and improve the usability of privacy tools.

This recommendation is practical because it does not require every platform to invent a separate communication framework. It instead creates a shared baseline that can be co-designed with children and adapted for different ages, literacy levels and support needs.

We welcome the Code's emphasis on ensuring that privacy policies and consent processes are clearly communicated to children and young people. It is critical that these processes are not only "age appropriate" and "easily accessible" (Sections 23–24), but also sufficiently clear, simple and inclusive to meet the needs of vulnerable communities, including those with diverse literacy levels or additional support needs. We also note that children and young people often engage across multiple platforms and report difficulty keeping up with varying approaches and frequent changes, reinforcing the importance of consistency in how information is presented.

Ensure that data protections travel with the data

The Code should require entities to maintain meaningful visibility over children's data flows, including where data is shared with or processed by third parties.

Platforms should be required to retain clear responsibility for children's personal information across the full data lifecycle, including where it is shared with third parties for service delivery.

While the Code appropriately seeks to minimise the sharing of children's data, we acknowledge that some disclosure to external providers will remain necessary in modern digital systems. In these circumstances, platforms should ensure that such sharing is limited to what is strictly necessary and in the best interests of the child, and that children, parents and carers are able to understand, track and challenge how data is used beyond the initial service.

This includes maintaining transparency about downstream data-sharing arrangements and ensuring that accountability does not become fragmented once data leaves the platform. The intention is not to make platforms responsible for every unrelated third-party practice, but to ensure that protections travel with the data and that clear responsibility is maintained throughout the data ecosystem.

We hope our recommendations contribute to expanding the scope of the Code and improving its application and accessibility. We would be delighted at the opportunity to discuss any of these further.

Written By Rachael Burns, George Trigenis and Bianca Kendrick



About the Tech Policy Design Institute

TPDi is an independent, non-partisan think tank dedicated to tech policy. We work with all actors across the tech ecosystem to shape technology for the benefit of humanity. After 3 years of incubation, we spun-out of the Australian National University in January 2025. We are a registered not-for-profit with the Australian Charities and Not-for-Profit Commission.

TPDi's Tech Policy Youth Ambassadors program creates a mentored, professional pathway for young people to contribute directly to national and global tech policy conversations.

This submission was independently developed and authored by the Tech Policy Youth Ambassadors. While the Ambassadors are supported and mentored through TPDi's program, the views, analysis and recommendations presented here are their own.

More information about the program can be found here: <https://techpolicy.au/nextgen>

