

**Submission to the Office of the Australian Information Commissioner
Feedback on the Exposure Draft: Privacy (Children's Online Privacy) Code 2026**

Authored by [REDACTED], submitted on behalf of the Braveheart Youth Advisory Council

Executive summary of recommendations

The Braveheart Youth Advisory Council welcomes the draft Children's Online Privacy Code and strongly supports its child-centered intent. However, based on lived experience, including experience of domestic and family violence and serious online harms, the Council considers that several aspects require strengthening or clarification to protect children who are at heightened risk.

In summary, the Council recommends that the OAIC:

1. Explicitly recognise children affected by domestic and family violence, coercive control, sexual abuse and severe online abuse as a high risk group in the Code and associated guidance, and require entities to address these risks in privacy impact assessments and practice.
2. Clarify and broaden the circumstances in which children under 15 may consent to the handling of their personal information without the involvement of a person with parental responsibility, in particular for services and information related to safety, violence, abuse, neglect and exploitation, beyond narrowly defined "health" or "legal" categories.
3. Provide stronger guidance on age assurance methods that is consistent with data minimisation, discourages the routine use of high risk methods such as government ID uploads and persistent biometric storage, and requires entities to justify that any chosen method is the least privacy intrusive option that is effective.
4. Encourage or require entities whose services are primarily concerned with sensitive activities of children, such as domestic violence support, mental health, sexuality and gender support and similar services, to provide anonymous or pseudonymous modes of use wherever lawful and safe, and to justify any departure from this principle in their privacy impact assessments.
5. Strengthen the provisions on inquiries, complaints and "children's privacy rights" so that entities must design these processes to be safe for children living in unsafe homes, including by offering covert or low risk pathways and by co designing such mechanisms with children and young people, particularly those with lived experience of violence.
6. Clarify how entities should resolve conflicts between parental access, correction and deletion requests and the safety and expressed wishes of the child, including by referencing relevant child protection and family violence principles and court orders, so that privacy law is not used in ways that endanger children or undermine protection mechanisms.

7. Promote meaningful and ongoing youth participation in the implementation and review of the Code, including encouraging entities to involve children and young people in privacy impact assessments and

annual reviews, and establishing or formalising OAIC youth advisory mechanisms on children's privacy.

The following sections expand on these recommendations, assessing key provisions of the draft Code from the perspective of young people, including survivors of domestic and online violence, and proposing concrete refinements that remain consistent with the Privacy Act framework.

1. Introduction and context

The Braveheart Youth Advisory Council (henceforth known as "Council") is a group of young people aged fifteen to twenty four who advise on issues affecting children and young people, with a particular focus on safety, privacy and the impacts of violence. Council members have extensive lived experience across a range of online environments, including social media, gaming platforms, education technology, messaging services and online support services. Some members are survivors of domestic and family violence, coercive control, child sexual abuse and severe online abuse, including stalking, non consensual sharing of images and technology facilitated control.

From this standpoint, online privacy is not just a question of comfort, data protection or consumer choice. For some children it is intimately connected to physical safety, their liberty to seek help and their ability to maintain confidential relationships with trusted adults and peers. A privacy failure can expose a child's location to a violent parent, reveal that a child is seeking help to an abusive caregiver, or enable further harassment and intimidation. The Council therefore welcomes a Code that places the best interests of the child at the centre of privacy protections, but also considers it essential that the Code explicitly addresses the reality of children who live with serious harm risks.

The Council acknowledges that the Exposure Draft contains many strong protections, including strict limitations on collection, use and disclosure of children's personal information, robust consent standards, enhanced transparency obligations, rights to access, correction and destruction of information, and mandatory privacy impact assessments and training. These are important advances. The Council's concern is not that these features are absent, but that they are, in some respects, incomplete for highly vulnerable groups and may in some cases interact in problematic ways with family violence and child protection contexts.

2. Children affected by violence and coercive control marked as a high risk group

The Code recognises, through the best interests of the child standard and through privacy impact assessment obligations, that the handling of children's personal information can cause physical, emotional, developmental and material harm. However, there is no explicit recognition of children affected by domestic and family

violence, coercive control, sexual abuse or severe online abuse as a distinct category whose risks must be specifically considered.

In practice, children in such situations face risks that are qualitatively different from those of their peers. An abusive parent may monitor a child's devices, demand passwords, use parental controls to surveil and restrict activity, access education or health portals to track

communications, or use the child's personal information to locate them or to undermine their attempts to seek help. Similarly, peers or online contacts may engage in stalking, image based abuse or coordinated harassment using personal information that has been collected or inferred.

The Council recommends that the Code, or at minimum binding OAIC guidance, explicitly identify these groups as being at elevated risk and require entities to consider them in their assessment of "best interests" and harms. Privacy impact assessments should specifically include analysis of how features or practices, such as parental dashboards, activity logs, geolocation tracking or cross platform data sharing, could be misused by perpetrators within a child's family or social environment. Entities should be expected to document and implement safeguards to reduce these risks, rather than treating all children as facing homogeneous and relatively low level privacy risks.

3. Overall consent, parental responsibility and safe exceptions

3.1 Strengths in the draft consent framework

The Council acknowledges several positive aspects of the consent framework. The rule that children aged 15 years and over may give consent for themselves recognises evolving capacities and aligns with existing OAIC guidance. The detailed requirements that consent be voluntary, informed, current, specific and unambiguous are also welcome. Prohibitions on manipulative, deceptive or coercive practices in obtaining consent are particularly important in commercial contexts, where design patterns can pressure children into oversharing and thus, posing themselves vulnerable.

The Council also notes and strongly supports the exception that permits children under 15 to consent for themselves when they are seeking legal or health related information or support in connection with a person with parental responsibility. This acknowledges that there are circumstances in which involving a parent would be inappropriate or harmful.

3.2 Limitations for children in unsafe family situations

Despite these strengths, the Council considers that the consent provisions do not yet adequately accommodate the position of children in unsafe family environments. The requirement that entities obtain consent from a person with parental responsibility for children under 15, and the requirement to take reasonable steps to confirm that the person has parental responsibility, assume that such persons are generally protective and safe. In

many cases that is correct. In other cases, however, the person exercising parental responsibility is a perpetrator or is aligned with a perpetrator.

The current drafting leaves substantial uncertainty about how entities should proceed where a child indicates that involving a parent would place them at risk, or where there is a history of violence or a relevant court order. Whilst there is an exception for legal or health support related to a parent, many services that children use in these situations may not clearly identify themselves as "health" or "legal" services. For example, youth helplines, online peer support communities, domestic violence information sites, sexual assault services and child advocacy organisations may straddle multiple categories. Entities may feel unsure whether they are legally permitted to rely on a child's consent alone, and may default to requiring parental involvement even when it is dangerous or when the child explicitly objects in fear of legal liability and retaliation.

The Council therefore recommends that the OAIC clarify and broaden the exception in section 13(4) so that children under 15 can consent on their own, without parental involvement, whenever they seek information or support relating to violence, abuse, neglect, exploitation, bullying or coercive control involving a person with parental responsibility or another adult in a position of power. This should explicitly extend to services that provide counselling, advocacy, information and peer support in relation to these issues, even if they are not formally classified as health services.

Furthermore, OAIC guidance should make clear that, where there is a reasonable basis to believe that involving a parent would create a risk of harm, entities may treat the child as capable of consenting alone, or may work through recognised third parties such as counsellors, social workers, helpline staff or independent advocates. Reasonable steps to confirm parental responsibility should not be interpreted in ways that override court orders, protection orders or other legal restrictions, and should not lead to disclosure of a child's help seeking behavior to an unsafe parent.

4. Age assurance and privacy by default

The Code's requirement that entities take reasonable steps to ascertain the age of end users before collecting personal information, unless they choose to treat all users as if they were children, is a central mechanism for targeting protections. The accompanying rule that entities may collect, use or disclose only personal information that is strictly necessary to provide the service establishes a strong privacy by default standard.

From a survivor perspective, however, the manner in which age assurance is implemented can significantly affect risk. Methods that involve uploading scans of government identification, capturing and storing facial images or using other biometric identifiers can themselves create highly sensitive datasets. If such datasets are compromised, misused internally or accessed by abusive family members or partners, children may face new harms.

The Code provides that sensitive information collected solely to comply with the age assurance requirement must be destroyed when no longer needed and when there is no legal requirement to retain it. This is an important safeguard. Nevertheless, the Council considers that further guidance is needed to ensure that entities choose age assurance methods that are as privacy protective as reasonably possible and that genuinely comply with the principle of strict necessity.

The Council recommends that OAIC develop and publish detailed guidance on privacy preserving age assurance consistent with the Code. This guidance should set out a hierarchy of preferred methods, strongly discouraging routine reliance on high risk options such as storage of copies of government identification or long term retention of biometric templates, except where clearly justified, proportionate and subject to rigorous safeguards. Entities should be expected, through their privacy impact assessments, to explain why their chosen method is effective yet the least privacy intrusive available in the circumstances, and to describe in detail how data collected solely for age verification is handled and destroyed in practice.

5. Anonymous and pseudonymous access for high risk services

The Code requires that entities explain when and how users may deal with them anonymously or by using a pseudonym, and that they provide anonymous options for general inquiries and complaints where lawful and practicable. These provisions are positive, but they are limited to certain interactions and do not directly address the design of the service itself.

For children who are seeking information or support about violence, abuse, mental health, sexuality or gender, anonymous or pseudonymous use of services can be critical. In many cases, full identification is not strictly necessary to provide information or to facilitate certain types of support. Requiring real names or detailed personal information in these contexts may expose children to serious harm if their activity is discovered by abusive parents or others.

The Council recommends that OAIC encourage or, where consistent with other legal obligations, require entities whose services are primarily concerned with sensitive aspects of children's lives, such as domestic violence support, sexual assault services, mental health support and LGBTQIA plus support, to provide anonymous or pseudonymous modes of use for key functions. The principle should be that, where full identification is not strictly necessary for safety, legal compliance or service delivery, the best interests of the child will ordinarily favour allowing children to engage without revealing their full identity.

Privacy impact assessments should be used to justify any decision to require identified use for particular features of high risk services. Entities should be expected to explain why anonymous or pseudonymous use is not feasible in those cases and what alternative safeguards are in place to protect children who may be endangered if their participation becomes known.

6. Access, correction, destruction and parental controls

The Council strongly supports the enhanced rights of access, correction and destruction of personal information about children, including the obligation to respond within defined timeframes, and the requirement to destroy information upon request, subject to clearly stated exceptions. For survivors, the ability to have certain records or data deleted, where this does not conflict with legal obligations or safety considerations, can be an important part of healing and of regaining control.

However, when these rights are exercised by persons with parental responsibility on behalf of younger children, complex issues arise. A parent who is also a perpetrator may seek access to a child's records in order to monitor communications with support services or professionals. They may attempt to have records removed that document their own abusive behavior. While the Code requires entities to act consistently with the best interests of the child, it does not spell out how conflicts between parental requests and child safety should be resolved in practice.

The Council recommends that OAIC issue guidance clarifying that entities should not automatically accede to parental requests for access, correction or destruction of information where doing so would likely put the child at risk or would conflict with child protection or family violence orders. Entities should be directed to consider the child's expressed wishes, the existence of any legal restrictions or protection orders, and the views of relevant professionals, such as social workers or counsellors, when making these decisions.

The provisions regarding notifications of parental control and geolocation monitoring are a welcome step in transparency. Children should know when their location can be seen by others or when their use of a service is being controlled or observed. Nevertheless, the Council considers that the Code could further encourage safe design of such features. For example, entities might be advised not to offer "stealth" monitoring modes that provide no indication to the child, and to design notifications in ways that are clear yet do not provoke retaliation from abusers. This will require careful, trauma informed design, which should involve consultation with affected children.

7. Inquiries, complaints and child friendly rights in unsafe homes

The Council commends the requirement that entities provide children with clear, age appropriate information about their privacy rights and embed simple and accessible inquiry and complaint processes. The obligations to respond in an age appropriate manner and within reasonable timeframes are also positive.

However, from the perspective of children living with violence or severe control, inquiry and complaint mechanisms must also be safe to use when a perpetrator may be monitoring devices, accounts or communications. A visible "complaints" button, obvious confirmation emails or records that appear in account

histories may all alert an abuser that the child is questioning or challenging something about the service, including perhaps a parental control feature.

The Council recommends that entities be encouraged, through OAIC guidance and best practice examples, to design inquiry and complaint pathways that include covert or low risk options. These might include neutral labels that do not attract attention, quick exit features, and the option to receive responses via alternate channels that an abuser is less likely to monitor. Entities should be prompted to test these mechanisms with children and young people who have lived experience of unsafe homes, so that the practical risks are properly understood and addressed.

8. Youth participation in implementation and review

The Code already requires entities to review and update their privacy practices at least annually, to conduct privacy impact assessments for new services or major changes, and to publish registers of those assessments. These are important accountability tools.

To fully honour the principle of placing children and young people at the centre, the Council recommends that OAIC encourage entities, particularly large platforms and widely used services, to incorporate meaningful youth participation into these processes. This might include consulting youth advisory groups, conducting focus groups with diverse cohorts of children, and specifically including the voices of those who have experienced violence, disability, discrimination or other forms of disadvantage.

Moreover, the Council recommends that OAIC itself establish or formalise ongoing youth advisory structures focused on children's privacy and the operation of the Code. This would enable regular feedback on how the Code is working in practice, how entities are implementing it, and where emerging risks or gaps may be appearing as technology and patterns of abuse evolve.

9. Conclusion

The Braveheart Youth Advisory Council considers the draft Children's Online Privacy Code to be a major and commendable step toward a rights respecting framework for children's privacy in Australia. The core features of the Code, including the best interests requirement, strict limits on collection and use, robust consent standards, child oriented transparency and strengthened rights of access and deletion, are strongly supported.

At the same time, the Council's lived experience as survivors of domestic and online violence highlights specific ways in which the Code can be refined to better protect those children who face the greatest risks. Explicit recognition of children affected by violence and coercive control, clearer and broader exceptions to parental consent where parents may be unsafe, stronger guidance on privacy preserving age assurance, promotion of anonymous and pseudonymous access for high risk services, safe and trauma informed inquiry and complaint

pathways, careful handling of conflicts between parental requests and child safety, and meaningful youth participation in implementation and review, will all help ensure that the Code functions as intended in the most difficult and dangerous situations.

The Council would welcome further engagement with the OAIC on these issues and stands ready to contribute additional insights from young people's perspectives as the Code is finalised and put into practice. Children and young people are experts in their own online lives. Many of us have survived systems that did not listen when we said we were not safe. A Code that truly serves the best interests of the child must be built and maintained in partnership with us, not only for us.