

5th June 2026

Office of the Australian Information Commissioner (OAIC)

Email: copc@oaic.gov.au

Submission:

Privacy (Children's Online Privacy) Code 2026 (the Children's Online Privacy Code)

To whom it may concern,

We thank you for the opportunity to a submission in relation to the *Privacy (Children's Online Privacy) Code 2026 (the Children's Online Privacy Code)*. .

As an agency that works with, and advocates for, survivors of child sexual harm, Bravehearts welcomes the commitment of the Office of the Australian Information Commissioner to strengthening protections for children through the development of a Children's Online Privacy Code. We note that a separate submission is being made on behalf of Bravehearts' Youth Advisory Council.

With extensive experience supporting victims and survivors of child sexual abuse and exploitation, as well as advocating for legislative and policy reform, Bravehearts strongly supports measures that place children's safety, wellbeing, and rights at the centre of digital regulation. In an increasingly connected world, children are engaging with online services from an early age, often without a full understanding of how their personal information is collected, used, and shared. A robust and enforceable Children's Online Privacy Code is therefore essential to safeguarding children's privacy, reducing their vulnerability to exploitation and harm, and ensuring that organisations adopt practices that prioritise the best interests of children by design and default.

Children's Privacy is a Child Protection Issue

Bravehearts submits that children's privacy should not be viewed solely as a matter of data protection or information governance; rather, it is fundamentally a child protection issue. The collection, use, retention, and sharing of children's personal information can have direct implications for their safety and wellbeing, both online and offline.

Children's personal information (including names, locations, images, behavioural data, social connections, interests, routines, and online activities) can be exploited in ways that increase vulnerability to grooming, sexual exploitation, image-based abuse, harassment, stalking, and other forms of online harm (Business for Social Responsibility, 2020; United Nations Committee on the Rights of the Child, 2021). Data-driven profiling and systems may also expose children to inappropriate content, facilitate contact from offenders, or contribute to manipulative practices that undermine children's autonomy and safety (Papadamou et.al., 2020).

Importantly, children often lack the developmental capacity to fully understand the long-term implications of sharing personal information online or to meaningfully consent to complex data

collection practices. This places a heightened responsibility on organisations to ensure that the design and operation of online services prioritise children's safety and best interests by default. Protecting children's personal information is not merely about preventing unauthorised access to data; it is about reducing opportunities for exploitation and harm, safeguarding children's rights, and creating digital environments that are safe for children to participate in.

"Best Interests of the Child" Principle

Bravehearts strongly supports the requirement that organisations handling children's personal information act consistently with the best interests of the child at the forefront. This represents an important shift away from models that place responsibility on children or parents to identify, understand, and manage privacy risks, and instead places obligations on service providers to proactively consider and safeguard children's rights, safety, wellbeing, and developmental needs.

The inclusion of a best interests principle recognises that children engage with digital services in ways that differ from adults and that they may not fully appreciate the nature, extent, or consequences of data collection, profiling, and information sharing practices (Livingstone, Stoilova & Nandagiri, 2019). As a result, children are particularly vulnerable to privacy harms and may be less able to identify or respond to risks arising from the misuse of their personal information. Organisations are therefore best placed to anticipate and mitigate these risks through child-centred design, governance, and decision-making processes.

Bravehearts considers the best interests principle to be a foundational element of the Code and strongly supports its retention as a central and non-negotiable requirement. Importantly, assessments of a child's best interests should extend beyond privacy considerations alone and explicitly encompass children's rights to safety, protection from exploitation and abuse, healthy development, and freedom from commercial manipulation (Livingstone, Carr & Byrne, 2015; United Nations Committee on the Rights of the Child, 2021). In practice, this means organisations and online services should be required to consider not only whether a particular data practice is lawful or commercially beneficial, but also whether it could reasonably expose children to increased risks of harm, exploitation, unwanted contact, or inappropriate influence.

Embedding the best interests of the child throughout the design, development, and operation of online services (Safety by Design) will help ensure that children's rights and wellbeing are prioritised from the outset, rather than addressed only after harms have occurred (eSafety Commissioner, 2026a). This approach is consistent with Australia's obligations under the United Nations Convention on the Rights of the Child and reflects growing international recognition that children's privacy and safety are inextricably linked in digital environments.

Safety by Design and Default Settings

Bravehearts welcomes the requirement that online services/providers design products and services with children's privacy as a primary consideration and adopt high privacy settings by default. This approach appropriately recognises that responsibility for protecting children online should rest primarily with service providers rather than with children or their parents.

Children should not be expected to navigate complex privacy settings, understand sophisticated data collection practices, or actively manage risks associated with profiling, tracking, and information sharing. Given children's evolving capacities and developmental vulnerabilities, relying on children to make informed privacy decisions places an unrealistic burden on those least equipped to assess and respond to potential harms (Crepax et.al., 2022;

Zhao et.al., 2019). Services likely to be accessed by children should therefore automatically provide the highest level of privacy protection, with any reduction in protections requiring a clear demonstration that it is necessary, proportionate, and consistent with the best interests of the child.

Bravehearts strongly supports the application of both privacy-by-design and safety-by-design principles. These approaches require organisations to proactively identify and mitigate risks to children during the design, development, and operation of digital products and services, rather than responding to harms after they occur (eSafety Commissioner, 2026a; Ta, 2024). In practice, this means considering how platform features, data collection practices, recommendation algorithms, user interactions, and default settings may create opportunities for privacy intrusions, unwanted contact, grooming, exploitation, harassment, or other forms of harm. Children's safety and wellbeing should be embedded into systems, processes, and business practices from the outset rather than treated as secondary considerations.

High privacy default settings are particularly important because default configurations have a significant influence on user behaviour and outcomes. Research consistently demonstrates that most users, including adults, rarely change default settings. For children, the likelihood of reviewing and modifying privacy controls is even lower (Cavoukian, 2011; Stoilova, Livingstone & Nandagiri, 2020). As a result, default settings effectively determine the level of protection that children receive in practice. Settings that minimise data collection, restrict public visibility of profiles and content, limit location sharing, disable behavioural profiling, and prevent unnecessary information sharing should therefore be the standard position for services accessed by children.

Importantly, high privacy settings not only protect children's personal information but also contribute to broader child safety outcomes. Limiting the visibility and accessibility of children's personal information can reduce opportunities for unwanted contact, grooming, exploitation, stalking, and other forms of online abuse (Livingstone, Stoilova & Nandagiri, 2019). Privacy protections should therefore be viewed as an integral component of child safeguarding measures within digital environments.

Bravehearts considers the adoption of privacy-by-design, safety-by-design, and high privacy default settings to be fundamental elements of an effective Children's Online Privacy Code. Together, these measures shift responsibility from children to service providers and create digital environments that are safer, more protective, and more consistent with children's rights and best interests.

Age Assurance Measures

Bravehearts supports the requirement for organisations to take reasonable steps to determine whether users are children where the Code applies. Effective age assurance is a critical component of ensuring that the protections contained within the Code are applied in practice. Without appropriate mechanisms to identify when a user is likely to be a child, organisations may continue to rely on self-declared ages or claim uncertainty regarding the presence of children on their services, thereby avoiding the heightened obligations and protections intended by the Code.

From a child protection perspective, age assurance can help organisations identify when child-specific protections should be applied. Robust age assurance measures can assist organisations to better identify child users and implement protections that reflect children's developmental needs, vulnerabilities, and rights (eSafety Commissioner, 2026b; Livingstone et.al., 2024).

However, Bravehearts acknowledges that age assurance measures present a number of challenges and should not create new privacy or safety risks for children. Age assurance mechanisms must be privacy-preserving, proportionate, and designed to minimise the collection, retention, and sharing of additional personal information (Livingstone et.al., 2024; Organisation for Economic Co-operation and Development, 2025). Requiring children to provide extensive identifying documentation or sensitive personal information to access online services may inadvertently increase privacy risks and create additional opportunities for misuse, unauthorised disclosure, or data breaches.

Bravehearts also notes concerns regarding the accuracy and effectiveness of some age assurance technologies. Systems that incorrectly identify children as adults may fail to apply critical protections, while systems that incorrectly classify adults as children may unnecessarily restrict access to services. They also present potential privacy risks if they rely on the collection of sensitive personal information. Furthermore, the capacity for some users to circumvent age assurance systems may limit their effectiveness, reinforcing the need for age assurance to operate alongside broader safety-by-design and privacy-by-design measures rather than as a standalone safeguard (Age Check Certification Scheme, 2025; Lueks et.al., 2026). Importantly, organisations should not be permitted to rely solely on age assurance technologies as a substitute for broader safety-by-design and privacy-by-design obligations. Even where age assurance measures are implemented, online services should continue to be designed with children's safety and best interests in mind, recognising that no age assurance system will be entirely accurate.

Consideration should also be given to the potential impact of age assurance requirements on vulnerable cohorts of children, including those who may have limited access to identity documents, those experiencing family violence, homelessness, or other forms of disadvantage, and children who rely on online services to access information, support, or social connection (Bowler, 2026). Age assurance mechanisms should not create barriers that disproportionately exclude or disadvantage children who may already be vulnerable.

Child-Centred Transparency and Communication

Bravehearts supports the requirement that privacy information be provided in ways that children can understand. However, meaningful transparency should extend beyond the provision of simplified privacy policies. Given children's differing ages, developmental stages, literacy levels, and digital capabilities, privacy information should be developmentally appropriate, accessible, and presented in formats that support genuine understanding (Desimpelaere, Hudders & Van de Sompel, 2020). This may include the use of layered explanations, visual aids, interactive tools, and age-appropriate language tailored to the needs of different groups of children.

Importantly, transparency should be viewed as an outcome to be achieved rather than simply a disclosure obligation to be fulfilled. Privacy information should be provided at key decision points, such as when personal information is collected, privacy settings are changed, or information is shared with third parties, rather than being confined to lengthy privacy policies that children are unlikely to read or understand (Ding & Huang, 2024; Stoilova, Nandagiri & Livingstone, 2021). The effectiveness of transparency measures should be assessed by whether children can meaningfully comprehend how their information is being used and the implications of those practices.

We would also emphasise that transparency alone cannot adequately protect children's privacy rights. Even where information is communicated clearly, children may lack the experience,

capacity, or bargaining power to make fully informed decisions about complex data practices (Livingstone et.al., 2025; Stoilova, Livingstone & Nandagiri, 2020). Child-centred transparency measures should complement, rather than replace, robust privacy-by-design and safety-by-design obligations, ensuring that organisations remain responsible for acting in the best interests of children and safeguarding their privacy and wellbeing.

Support for Strong Enforcement and Regulatory Oversight

The effectiveness of the Code will ultimately depend on robust enforcement and meaningful consequences for non-compliance. Bravehearts supports the proposal that breaches of the Code constitute breaches of the Privacy Act, ensuring that the Code operates as an enforceable regulatory framework rather than an aspirational set of principles. Given the significant power imbalance between children and digital service providers, responsibility for compliance must rest with organisations rather than with children or their families.

Ongoing monitoring, regulatory oversight, and enforcement action will be essential to ensure compliance and maintain public confidence in the Code's ability to protect children (Stoilova, Livingstone & Nandagiri, 2020; United Nations Committee on the Rights of the Child, 2021). This should include proactive regulatory activities, such as audits and compliance reviews, particularly in relation to services that are widely used by children or present elevated privacy and safety risks. A solely complaints-based approach may be insufficient, as children may not recognise privacy infringements or have the capacity to raise concerns.

Strong accountability mechanisms and appropriate penalties for breaches will be critical to ensuring that organisations meaningfully implement the protections contained within the Code. Effective enforcement is critical to ensuring that children's rights are protected in practice rather than existing merely as aspirational principles. Robust oversight and accountability mechanisms help drive organisational compliance and reinforce the expectation that service providers must actively safeguard children's privacy, safety, and best interests in digital environments (Organisation for Economic Co-operation and Development, 2024).

Recognition of Child Sexual Abuse and Exploitation Risks

While the Code appropriately focuses on privacy harms, Bravehearts recommends that greater recognition be given to the relationship between privacy breaches and risks of child sexual abuse, exploitation, and grooming. Children's privacy and safety are inextricably linked, and the misuse of personal information can have consequences that extend beyond traditional privacy concerns to create or exacerbate risks of serious harm (Livingstone, Stoilova & Nandagiri, 2019; Organisation for Economic Co-operation and Development, 2024; United Nations Committee on the Rights of the Child, 2021)

The collection, aggregation, sharing, and profiling of children's personal information can create opportunities for offenders to identify, target, manipulate, or exploit children (Livingstone, Stoilova & Nandagiri, 2019; United Nations Committee on the Rights of the Child, 2021). Information such as a child's age, location, interests, online behaviours, social connections, routines, photographs, and other personal characteristics may be used to facilitate grooming, establish trust, identify vulnerabilities, or enable unwanted contact. While individual data points may appear innocuous in isolation, the aggregation of information across multiple platforms and services can create detailed profiles that increase children's visibility and accessibility to those seeking to cause harm.

Bravehearts is particularly concerned about data practices that increase the discoverability of children, facilitate contact between children and unknown adults, or enable extensive profiling of children's behaviours and interests. Behavioural profiling, location-sharing features, public-by-default settings, and the unnecessary collection or retention of personal information may all contribute to environments in which children are more vulnerable to exploitation or abuse (Livingstone, Stoilova & Nandagiri, 2019; Minihan et.al., 2024). Although these practices may not be intended to cause harm, organisations should be required to consider whether they create foreseeable risks that could be exploited by offenders.

Bravehearts recommends that the Code explicitly recognise child sexual abuse, exploitation, and grooming as relevant risks when assessing the impact of data handling practices on children. Organisations should be required to consider not only the privacy implications of collecting and processing children's personal information, but also how those practices may affect children's safety and vulnerability to exploitation. This would align with a safety-by-design approach and reinforce the principle that children's personal information should be handled in a manner that supports both their privacy rights and their protection from harm.

Recognising the connection between privacy and child protection would strengthen the Code's ability to address the real-world risks that children face in digital environments. Privacy protections should not be viewed solely as safeguards against inappropriate data use, but also as important measures for reducing opportunities for grooming, exploitation, and other forms of child sexual abuse.

General Comment

Bravehearts welcomes the development of the Children's Online Privacy Code as an important step towards strengthening protections for children in the digital environment. While privacy is often viewed through the lens of data protection, as we have stated in this submission, children's privacy is fundamentally a child protection issue. The collection, use, and sharing of children's personal information can have significant implications for their safety, wellbeing, and vulnerability to online harms, including grooming, exploitation, and image-based abuse. As children's engagement with digital services continues to grow, it is essential that organisations are required to proactively safeguard children's personal information and place their best interests at the centre of service design and operation. A strong and enforceable Code will not only enhance children's privacy rights but will also contribute to creating safer online environments and reducing opportunities for harm. Bravehearts therefore strongly supports the introduction of a robust Children's Online Privacy Code and encourages the OAIC to ensure that child safety and wellbeing remain central considerations throughout its implementation and enforcement.

Please contact us on research@bravehearts.org.au should you have any questions relating to our submission.

Kind Regards,



Director of Research



CEO

References

- Age Check Certification Scheme (2025). *Age Assurance Technology Trial: Final report*. Australian Government.
- Bowler, L. (2026). The digital rights of children and youth: An annual review of information science and technology (ARIST) paper. *Journal of the Association for Information Science and Technology*. doi.org/10.1002/asi.70048
- Business for Social Responsibility (2020). *Child rights impact assessments in relation to the digital environment*. Accessed online: <https://www.unicef.org/documents/child-rights-impact-assessments-digital-environment>
- Cavoukian, A. (2011). *Privacy by design: The 7 foundational principles*. Information and Privacy Commissioner of Ontario
- Crepax, T., Muntés-Mulero, V., Martinez, J. & Ruiz, A. (2022). Information technologies exposing children to privacy risks: Domains and children-specific technical controls. *Computer Standards & Interfaces*, 82. doi.org/10.1016/j.csi.2022.103624.
- Desimpelaere, L., Hudders, L. & Van de Sompel, D. (2020). Knowledge as a strategy for privacy protection: How a privacy literacy training affects children's online disclosure behavior. *Computers in Human Behavior*, 110. doi.org/10.1016/j.chb.2020.106382.
- Ding, X. & Huang, H. (2024). For whom is privacy policy written? A new understanding of transparency in data privacy law. *Computer Law & Security Review*, 55. doi.org/10.1016/j.clsr.2024.106072
- eSafety Commissioner (2026a). *Safety by Design*. Accessed online: <https://www.esafety.gov.au/industry/safety-by-design>
- eSafety Commissioner (2026b). *Social media age restrictions*. Accessed online: <https://www.esafety.gov.au/about-us/industry-regulation/social-media-age-restrictions>
- Lueks, W., Dreyer, S., Federrath, H., & Simon, J. (2026). *Assessing age assurance technologies: Effectiveness, side-effects, and acceptance*. Accessed online: <https://arxiv.org/abs/2603.25695>
- Livingstone, S., Carr, J., & Byrne, J. (2015). *One in three: Internet governance and children's rights*. Centre for International Governance Innovation & Chatham House
- Livingstone, S., Lievens, E., Graham, R., Pothong, K., Steinberg, S., Stoilova, M. (2025). Children's Privacy in the Digital Age: US and UK Experiences and Policy Responses. In: Christakis, D.A., Hale, L. (eds) *Handbook of Children and Screens*. Springer. doi.org/10.1007/978-3-031-69362-5_67
- Livingstone, S., Nair, A., Stoilova, M., van der Hof, S., & Caglar, C. (2024). Children's Rights and Online Age Assurance Systems: The Way Forward. *The International Journal of Children's Rights*, 32(3), 721-747. doi.org/10.1163/15718182-32030001
- Livingstone, S., Stoilova, M. & Nandagiri, R. (2019). *Children's data and privacy online: Growing up in a digital age. An evidence review*. London School of Economics and Political Science.
- Minihan, S., Burton, M., Nicholas, M., Trengove, K., Napier, S. & Brown, R. (2024). Prevalence and predictors of requests for facilitated child sexual exploitation on online platforms. *Trends & issues in crime and criminal justice* no. 692. Canberra: Australian Institute of Criminology. doi.org/10.52922/ti77406
- Organisation for Economic Co-operation and Development (2024). *Towards digital safety by design for children*, *OECD Digital Economy Papers*, No. 363. doi.org/10.1787/c167b650-en.

- Organisation for Economic Co-operation and Development (2025). *The legal and policy landscape of age assurance online for child safety and well-being*. OECD Publishing.
- Papadamou, K., Papasavva, A., Zannettou, S., Blackburn, J., Kourtellis, N., Leontiadis, I., Stringhini, G., & Sirivianos, M. (2020). *Disturbed YouTube for Kids: Characterizing and Detecting Inappropriate Videos Targeting Young Children*. Proceedings of the International AAAI Conference on Web and Social Media. Accessed online: <https://arxiv.org/abs/1901.07046>
- Stoilova, M., Livingstone, S., & Nandagiri, R. (2020). Digital by Default: Children's Capacity to Understand and Manage Online Data and Privacy. *Media and Communication*, 8(4), 197-207. doi.org/10.17645/mac.v8i4.3407
- Stoilova, M., Nandagiri, R., & Livingstone, S. (2021). Children's understanding of personal data and privacy online – a systematic evidence mapping. *Information, Communication & Society*, 24(4), 557–575. doi.org/10.1080/1369118X.2019.1657164
- Ta, V.-T. (2024). *A safety risk assessment framework for children's online safety based on a novel safety weakness assessment approach*. Accessed online: <https://arxiv.org/abs/2401.14713>
- 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)*. Access online: <https://digitallibrary.un.org/record/3906061>
- Zhao, J., Wang, G., Dally, C., Slovak, P., Childs, J., Van Kleek, M., & Shadbolt, N. (2019). "I make up a silly name": Understanding children's perception of privacy risks online. *Proceedings of the ACM on Human-Computer Interaction*. doi.org/10.1145/3290605.3300336