WESNET
The Women's Services Network

SUBMISSION RE: THE CHILDREN'S ONLINE PRIVACY CODE

June 2026

WESNET Inc
Freecall: 1800WESNET
Email: wesnet@wesnet.org.au
Web: www.wesnet.org.au
ABN: 16 068 548 631

WESNET
The Women's Services Network

Table of Contents

Acknowledgements

Acknowledgement of Country

Wesnet would like to acknowledge and pay respects to all First Nations people, as the Traditional and only Custodians of this country we call Australia. We recognise First Nations peoples' culture, wisdom, and connection to this land and pay our respects to Elders, past, present and future. We recognise the loss of land and culture, acknowledging the consequences of dispossession and colonisation on First Nations peoples. We acknowledge that sovereignty over this land was never ceded. This land always was and always will be Aboriginal land. First Nations women have multiple roles and identities relating to their culture, community, age, ability, sexual orientation and gender identity. Wesnet works tirelessly for an inclusive future free from violence. We acknowledge the strength and resilience of First Nations women, particularly those who have experienced domestic and family violence, and those who support and advocate for victim survivors of domestic and family violence. We pay our deepest respects to those who have lost loved ones as a result of domestic and family violence. Wesnet will actively work to be informed by the experiences and advocacy of First Nations women, and to support First Nations women in their quest for safety and equality.

Acknowledgement of Victim-Survivors

Wesnet also takes this opportunity to acknowledge all victim-survivors of gender-based violence. We pay respect to those who did not survive and to their family members and friends.

WESNET
The Women's Services Network

About Wesnet

We are the Peak body for Specialist Women's Domestic and Family Violence Services in Australia.

Our vision is a future where all women and children live free of domestic and family violence and its consequences.

With almost 350 eligible members across Australia, Wesnet represents a range of organisations and individuals including women's refuges, shelters, safe houses and information/ referral services.

Harnessing its large national network of members and associate members, Wesnet plays an important role in identifying unmet needs, canvassing new and emerging issues, facilitating policy and sector debate and providing advice to government to provide improved responses to the problem of domestic and family violence. We do this within our communities, and in partnership with non-government stakeholders.

Wesnet works within a feminist framework which promotes understanding domestic and family violence as gendered violence, and that women's and children's experiences are also intrinsically shaped by their ethnicity, culture, ability, age, gender identity and class.

WESNET
The Women's Services Network

Children's Online Privacy Code (the Code)

Introduction

Wesnet welcomes the opportunity to provide a submission to the Office of the Australian Information Commissioner (OAIC) on the exposure draft of the Children's Online Privacy Code (the Code). We welcome the development of the Code, which places responsibility on online services for their collection, use and sharing of children's data to ensure that children's personal information is protected. However, critically the Code currently lacks a domestic and family violence lens. Technology-facilitated abuse (TFA) is a threat to children's privacy, safety and wellbeing, and can be perpetrated in the context of domestic and family violence (DFV).[1] It is incumbent on the OAIC to recognise that children's personal information can be weaponised as a tool of DFV. Failure to explicitly recognise and respond to this risk to children could result in the Code being weaponised by parents who use violence.

This submission introduces findings from forthcoming research led by Wesnet, complemented by other research to highlight the prevalence of TFA, DFV and children, and makes recommendations that strengthen children's online privacy, and their physical and emotional safety and wellbeing.

TFA, DFV and children

In 2025, Wesnet, supported by the University New South Wales and Curtin University conducted a Third National Survey of Technology Abuse and Domestic Violence in Australia (Third National Survey). This survey builds on two earlier surveys in 2015 and 2020.[2]

Almost all practitioners in the Third National Survey reported having witnessed TFA in their work. An overwhelming majority of respondents (99.7%) reported that they had supported clients who had been abused, stalked or threatened via technology. This was a slight increase from 99.3% in 2020 and 98.3% in 2015.

---

[1] A form of controlling behaviour, particularly implicated in DFV. It involves a perpetrator misusing devices (like phones or computers), accounts (like email) and software or platforms (like social media) to abuse, threaten, coerce, stalk, harass or intimidate victim-survivor(s). TFA can include posting or sending harassing, abusive or threatening messages, stalking (tracking someone's activities, movements, communications), and doxxing (publishing identifiable personal information).

[2] The first national survey was led by what was then Domestic Violence Resource Centre Victoria (now Safe and Equal). Safe and Equal is the peak body for specialist family violence services that provide support to victim survivors in Victoria. Wesnet conducted the second survey in 2020. Delanie Woodlock, Karen Bentley, K., Darcee Schulze, Natasha Mahoney, Donna Chung, and Amy Pracilio, *Second National Survey of Technology Abuse and Domestic Violence in Australia* (Wesnet, 2020), https://wesnet.org.au/2ndnatsurvey. The findings from the third national survey are forthcoming.

It is important to note the gendered nature of TFA, whereby people using TFA are mostly men (98.0%) while victim-survivors are mostly women (95.0%). People using TFA often do so against their partners or ex-partners and children. While this submission acknowledges that people using TFA may be doing so outside the context of the family or intimate relationship, it uses 'people or person using TFA' interchangeably with 'parents or parent using violence'. In the context of DFV, intimate knowledge of victim-survivors means that people using violence can employ violent tactics against victim-survivor(s) using information that may seem innocuous to others. This, combined with the omnipresence of technology, can lead victim-survivors to feel 'there is "no escape"', even when they have left the relationship.

Parents who use violence often use technology to exploit their relationship with children and target them as victim-survivors as well as to extend their use of violence towards the whole family unit. This is important to bear in mind for children and young people who are moving between parental homes after separation.[3]

What our evidence says about children experiencing TFA as part of DFV

This section discusses findings specific to children's experience of TFA that challenge the Code's assumption that a person with parental responsibility is a safe person. Taken together, these findings from the Third National Survey highlight the lengths that people using violence will go to monitor, track and intimidate adult and child victim-survivors using technology as a primary tool, particularly in the context of post-separation co-parenting.

The Third National Survey shows that a common violent tactic used by parents using violence is to gift technology to children. This allows for unsupervised communication to remotely access children and potentially locate them, and the opportunity to actively undermine the mother-child relationship. Over half of respondents observed this tactic 'Often' or 'All the time'. A parent using violence may also install hidden GPS monitoring when gifting children devices like smart watches or toys to monitor or contact the non-abusive parent: less than half (41.3%) of respondents reported seeing this 'Often' or 'All the time'.

People using violence can also use children's social media to track or intimidate the non-abusive parent. 45.0% of respondents reported observing this tactic 'Often' or 'All the time'.

[3] "Safety Considerations for Co-Parenting and Visitation Apps," Wesnet, accessed June 3, 2026, https://techsafety.org.au/resources/resources-women/co-parenting-apps/.

Technology is also used to gain access to and groom children by people who have no social or familial connection to them otherwise. Concerningly, over a third of respondents reported seeing the online grooming or coercion of children through digital platforms 'Often' or 'All the time', while 15.6% saw dating apps being used to target women to gain access to their children at the same frequency.

People using violence also use court-ordered child contact via technology to abuse or harass victim-survivors. 66.2% of respondents reported seeing this 'Often' or 'All the time'.

The Third National Survey findings align with research on children and TFA in the context of family violence by the eSafety Commissioner (eSafety) and Griffith University.[4] The study highlights the prevalence of the issue: 27% of domestic violence cases involve TFA of children. Common devices or platforms that are misused to abuse children are phone (79%), text (75%) and social media (59%). The most common forms of TFA that children experienced are:

- monitoring and stalking (45%)
- threats and intimidation (38%)
- blocking communication (33%).

Technology-facilitated abuse directed at children most often occurred alongside abuse directed at mothers. Practitioners reported that 59% of domestic and family violence cases include withholding or threatening to withhold child support, and 46% involve blocking the adult victim's online access to financial accounts. This has direct implications for children's wellbeing.

Children experience a range of negative impacts from TFA.[5] These include mental health issues, feeling fearful, and feeling guilty they had disclosed information. The Code is therefore an opportunity to protect children's personal information in the digital ecosystem, and their physical and emotional safety and wellbeing.

Applying a TFA lens to the Children's Code

The Code must recognise TFA in the context of DFV as a threat to children's privacy. For example, at present, in seeking consent from the person with parental responsibility for children under the age of consent, the draft Code assumes that

[4] Molly Dragiewicz, Patrick O'Leary, Jeffrey Ackerman, Ernest Foo, Christine Bond, Amy Young, and Claire Reid, *Children and technology-facilitated abuse in domestic and family violence situations: Full report* (eSafety, 2020), , https://www.esafety.gov.au/research/children-and-technology-facilitated-abuse-in-domestic-and-family-violence-situations.

[5] Molly Dragiewicz et al, *Children and technology-facilitated abuse in domestic and family violence situations.*

the person with parental responsibility is a safe parent. However, as research shows, a parent using violence often uses and targets children as part of TFA to abuse, threaten and/or stalk them and the non-abusive parent. The following recommendations illustrate how the draft Code can recognise and manage the risk of TFA in the context of DFV. ***Wesnet recommends referring to a person with parental responsibility as a safe person through amending its definition in the Code section 4.***

Current definition	Recommended definition
a) a parent of the child; or ***(b) a guardian of the child; or*** ***(c) a person not covered by paragraph (a) or (b) who is legally responsible for the child's day-to-day care, welfare and development.***	***(a) a safe parent of the child; or*** ***(b) a safe guardian of the child; or*** ***(c) a person not covered by paragraph (a) or (b) who is legally responsible for the child's day-to-day care, safety, welfare and development.***

Another way in which the Code can incorporate a DFV lens is through the principle of the 'best interests of the child'. While the principle recognises child exploitation, this does not explicitly capture DFV. ***Wesnet recommends amending the explanation of the 'best interests of the child' in Explanatory Statement section 10(a).***

Current definition	Recommended definition
(a) the nature and extent of child exploitation risks (child exploitation is any situation where a child is abused, harmed or used by another person for economic, sexual or personal gain	***(a) the nature and extent of child abuse and exploitation risks (child abuse and exploitation is any situation where a child is abused, harmed or used by another person for economic, sexual or personal gain. This includes domestic and family violence.***

In doing so, all requirements of the Code would reflect this strengthened principle.

Transparency by design

Privacy notices and policies

Wesnet welcomes the Code's requirement for services to only collect, use or disclose personal information about a child that is strictly necessary to provide the service. At the same time, safeguarding children's privacy in relation to parents who use violence is critical. ***The requirement for privacy notices and policies to be written in age-appropriate, clear and accessible language can be strengthened to provide information that children's personal information can be misused in the context of DFV through amending the Code, including:***

- ***Notification of the collection of personal information Section 24(2) to include '(e) include information on the risk of domestic and family violence'***
- ***Notification of mechanisms that monitor or control service use or monitor geolocation Section 33(3) to include '(d) include information on the risk of domestic and family violence'***
- ***Information about children's privacy rights Section 35 to include '(d) include information on the risk of domestic and family violence'.***

Inquiry and complaints processes

As stated, children experience negative impacts of TFA. This is exacerbated in DFV as the person using violence is a family member they are expected to trust and love. It can produce conflicting emotions such as guilt, shame and loyalty and have long-term consequences on relationships, health and quality of life.[6] Online services can play a role in understanding and responding to the impacts of TFA trauma to avoid re-traumatising victim-survivors and supporting their safety, choice and control.[7] ***Wesnet recommends strengthening the proposed child-friendly inquiry and complaints processes through amending Section 36(3) to include a clause that the process must be 'trauma-informed for victim-survivors of child abuse and exploitation, including domestic and family violence'.***

[6] The Federal Government, *National Plan to End Violence against Women and Children 2022-2032* (Commonwealth of Australia (Department of Social Services), 2022), https://www.dss.gov.au/national-plan-end-violence-against-women-and-children/resource/national-plan-end-violence-against-women-and-children-2022-2032, p.44 and "Support for children and young people," Safe and Equal, accessed June 3rd, 2026, https://safeandequal.org.au/resources/support-for-children-and-young-people/.

[7] The Federal Government, *National Plan to End Violence against Women and Children 2022-2032*, p.133.

Application of the Code

Smaller services

Wesnet notes that the draft Code will cover organisations and companies that make over $3 million a year. There is potential here for children to find smaller alternative services to continue digital engagement with their online networks and communities, as they did prior to the social media age restrictions coming into effect.[8] To address this, eSafety monitored for signs of user movement from age-restricted platforms to other services. eSafety also included a self-assessment process when a platform had to report a significant increase in users under the age of 16 or a change in the way it's being used.[9] While the scope of the Code is broader than social media services, ***OAIC could consider similar monitoring activities and self-assessment processes to those eSafety uses for social media age restrictions. This would support smaller services to align with the Code.***

Supporting the ecosystem of users

As online services are part of everyday life, the ecosystem of users should be supported to protect child safety. Child care centres, schools and recreational clubs use apps with many staff who can collect and share information about children. ***Services can implement role-based access controls to improve the security of children's personal information. This can be supported through strengthening the Explanatory Statement section on Review of privacy practices Section 25 to include 'establishing procedures such as role-based access controls to improve the security of children's personal information'.*** However, if a child or non-abusive parent chooses to keep personal information such as location or images private on a service used by a sports centre private, for example, it should not inhibit their participation in sporting activities. While this is already captured by the 'best interests of the child', resources for users would be valuable. ***Mechanisms and guidance should be in place to support specific roles to ensure they do not inadvertently share children's or non-abusive parent's personal information if they have not consented for that information to be collected and shared.***

---

[8] Matilda Boseley, "Teens hoping to get around Australia's social media ban are rushing to smaller apps. Where are they going?," *The Guardian Australia,* December 5, 2025, https://www.theguardian.com/australia-news/2025/dec/04/under-16s-are-already-fleeing-to-apps-not-covered-by-australias-social-media-ban-heres-where-theyre-going.

[9] "Social media age restrictions and your family," eSafety, accessed June 3, 2026, https://www.esafety.gov.au/parents/social-media-age-restrictions.

Marketing

Direct marketing

The Draft Code enables online services to market directly to children with parental consent. ***Wesnet recommends a ban on direct marketing as it does not support the best interests of the child. This can be achieved through amending the Code section 29 on Opting out of direct marketing to 'Opting into direct marketing'.***

Personalised content

Fix Our Feeds

Wesnet is a signatory to *Fix Our Feeds*, a campaign by Teach Us Consent to regulate social media algorithms.[10] Currently, algorithms are flooding boys' and young men's feeds with radical misogynistic content associated with the 'manosphere', which has been linked to real-world harm to girls and young women,[11] and negative mental health outcomes for young men.[12] A recent study reveals how this content is embedded and promoted in online content that young men care about such as gaming, sports and music and intensified through algorithmic recommendation.[13] The *Fix Our Feeds* campaign calls on the Australian Government to introduce an opt-in feature for social media algorithms to bring affirmative consent to their services, and turn feeds on and off at will. While the proposed Code introduces high privacy by default settings, whereby additional elements like personalised content can be turned off and on, it may not go far enough to prevent misogynistic content. ***Wesnet recommends that the Code requires social media services to introduce an opt-in feature for social media algorithms to bring affirmative consent to their services, as it aligns with the 'best interests of the child'. While this can be captured by the Code's sections 10 and 11 on the collection, use or disclosure of personal information about a child in consistency with best interests of the child, Wesnet recommends strengthening these sections by including a requirement to***

---

[10] "Fix Our Feeds," Teach Us Consent, accessed June 3, 2026, https://www.teachusconsent.com/fix-our-feeds.

[11] Dr. Naomi Pfitzner, Dr Sarah McCook, Dr Alexandra Phelan, Dr Stephanie Westcott, Professor Steven Roberts and Ben Scott, *An Introductory Guide to the Manosphere and the Impacts for Young People, Teachers and Schools* (ANROWS, 2026), https://www.anrows.org.au/resources/guide-to-the-manosphere/.

[12] Krista Fisher, Simon Rice and Zac Seidler, *Young men's health in a digital world* (Movember Institute of Men's Health, 2025), https://au.movember.com/movember-institute/masculinities-report.

[13] Krista Fisher, Ruben Benakovic, Kieran O'Gorman, Simon Rice, Kaitlyn Tierney, Cynthia Miller-Idriss, Pasha Dashtgard, and Zac Seidler, *The Manosphere Content Classification Framework* (Movember Institute of Men's Health, 2026), https://movember.com/uploads/files/2026/Movember%20Institute%20-%20Manosphere%20Content%20Classification%20Framework.pdf.

introduce an opt-in feature for social media algorithms to bring affirmative consent to their services.

Right to delete

In our experience, the option to delete personal information to prevent it being accessed and weaponised by a person using violence can be an important safety measure for survivors of violence. Equally, deleting personal information can also be used as a tactic of abuse by parents who use violence. These alternative scenarios present a critical tension in practice for the principle of right to delete. In one instance, it can be life-saving and in the other, detrimental.

Wesnet strongly welcomes the right for children (or the person with parental responsibility if they are under the age of consent) to delete children's personal information. We note that a request to do so must be responded to within 30 days. Due to the potential harm a parent using violence can perpetrate when information reveals, for example, location through images, ***Wesnet recommends the Code section 32 (a and b) Request to destroy personal information about a child should include that the organisation or entity must respond to a request with a faster response time if it was made on the grounds of domestic and family violence or if there is serious threat to the life, health or safety of any individual.***

At the same time, there should be safeguards as parents who use violence may use the right to delete as a family violence tactic. Wesnet recommends including information on safeguarding in Explanatory Statement section 32. For example, international parental child abduction is a risk factor for migrant and refugee women and their children.[14] In this instance, deleting an account can prevent victim-survivors from accessing and locating their child.

The right to delete should also apply to adults. Adults have a right for their personal information as a child to be deleted as information and images when they were children can be weaponised against them in the context of DFV, for example, in the creation and distribution of synthetic child sexual abuse material. ***Strengthening the right to delete can be achieved through amending the Code section 32(1) Request to include that 'the child who is now an adult' can request to destroy personal information about themselves as a child.***

[14] "I'm Worried the Other Parent Will Take My Child Overseas," inTouch Multicultural Centre against Family Violence, accessed June 3, 2026, https://intouch.org.au/im-worried-the-other-parent-will-take-my-child-overseas/ and "International Parental Child Abduction," International Social Service Australia, accessed June 3, 2026, https://www.iss.org.au/our-services/international-parental-child-abduction.

Privacy impact assessments and education and training

Given the threat of DFV to children's privacy, privacy impact assessments, training and education must include a foundational understanding of DFV and skills for identifying and responding safely. ***Wesnet recommends that Explanatory Statement sections 38 and 40 include that privacy impact assessments and education and training require a DFV lens.***

Procedures to manage conflict of interest

Given the prevalence of TFA, ***entity staff who regularly access and handle children's personal information should declare a conflict of interest and be excluded if their children's personal information is included. This would in part help to prevent parents who use violence from accessing their children's personal information. This can be achieved through strengthening of the Explanatory Statement under Section 25, Review of privacy practices by including 'establishing procedures to manage conflict of interests in the handling of children's personal information'.***

Implementation of the Code

Lead in time and contextualised guidance

Wesnet understands that the Code will be in place by 10 December 2026. However, it is unclear when entities are expected to comply with the Code. The United Kingdom *Age Appropriate Design Code* allowed for a 12 month lead time, and provided guidance and resources for services of various sizes and from all sectors.[15] ***Lead in time for implementation should be 12 months and include contextualised guidance, detailing potential misuse of children's personal information and the impact of DFV in different settings.***

Media and communications plan

There should be a media and communications plan to support the Code's implementation. The plan should also include raising awareness about protecting children's personal information in the context of DFV. Although not specific to DFV, Ireland's Data Protection Commission 'Pause before you post' campaign is an example of an accessible campaign, aimed to raise awareness about the risks of sharenting,' 'a combination of the words 'parenting' and 'sharing' … used to describe the practice of parents regularly sharing information, photos and videos about their children on social media and other online

[15] "Children's code guidance and resources," Information Commissioner's Office, accessed June 3, 2026, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/#.

platforms'. [16] The media and communications plan should take into account how schools, childcare centres and recreational clubs can collect children's personal information such as images on personal devices to then upload onto online services, which should be prohibited.

Final remarks

Wesnet thanks you for the opportunity to contribute to the Code to ensure it is safe for all children, including victim-survivors of DFV.

[16] "Children: "Pause Before You Post" Awareness Campaign," Data Protection Commission Ireland, accessed June 3, 2026, https://dataprotection.ie/en/children and Data Protection Commission Ireland, "Pause Before You Post," posted November 25, 2025 by Data Protection Commission Ireland, YouTube, 40 seconds, https://www.youtube.com/watch?v=4QL1FmBaof8.