

Our Ref: MN/SPB:JM

22 September 2026

The Hon Anika Wells MP
Minister for Communications
Minister for Sports

Via email: digitaldutyofcare@communications.gov.au

Dear Minister,

Online Safety Amendment (Digital Duty of Care) Bill 2026 – exposure draft

Knowmore broadly supports the exposure draft of the *Online Safety Amendment (Digital Duty of Care) Bill 2026* (the draft bill). As a nation-wide community legal centre assisting victims and survivors of child abuse, we have a strong interest in laws to improve the safety of children in all places, including online environments. We have attached more information about our service.

This submission addresses the following matters:

- our support for a digital duty of care
- recommendations for improving the draft bill.

We intend to publish our submission.

Our support for a digital duty of care

Knowmore strongly supports the implementation of a digital duty of care in Australia. In our view, a digital duty of care is an essential part of broader efforts to address the unacceptable rates of online child abuse. We

consider that this reform is long overdue, as internet use by children in Australia has now been widespread for decades. In addition, internet use by children in Australia generally begins at a very young age. In 2018, 81% of parents said that their 2- to 5-year old children use the internet, with 94% of these children starting their internet use before the age of 4 years.¹

The Royal Commission into Institutional Responses to Child Sexual Abuse (Royal Commission) recognised the importance of online environments for children, observing that:

... access to the internet, including social media platforms and mobile devices, serves as a positive and beneficial aspect in children's lives in many ways. They build and maintain social relationships and networks; and have access to self-directed learning, information and professional advice and support, recreational spaces and initiatives that promote health and wellbeing, financial literacy and empowerment.

*Access to online environments can also have some benefits in relation to child sexual abuse. It can help young people to find information and advice on this issue, and provide channels for disclosure of child sexual abuse.*²

Knowmore shares this perspective. We note the guidance provided by the United Nations Committee on the Rights of the Child that 'national policies should be aimed at providing children with the opportunity to benefit from engaging with the digital environment and ensuring their safe access'.³

¹ Australian eSafety Commissioner, *Supervising preschoolers online*, last updated 11 November 2021, <<https://www.esafety.gov.au/research/digital-parenting/supervising-preschoolers-online>>.

² Royal Commission into Institutional Responses to Child Sexual Abuse (Royal Commission), *Final report: volume 6, making institutions child safe*, December 2017, p 344, <www.childabuseroyalcommission.gov.au/making-institutions-child-safe>.

³ United Nations Committee on the Rights of the Child, *General comment no. 25 (2021) on children's rights in relation to the digital environment*, p 5, paragraph 24, <tbinetnet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CRC/C/GC/25&Lang=en>.

At the same time, it is clear that the existing regulatory framework in Australia is failing to keep children safe online. Online child abuse is widespread and increasing,⁴ with almost 15% of children experiencing online sexual abuse.⁵ Knowmore has particularly assisted younger victims and survivors in seeking safety, justice and healing in relation to online child sexual abuse.

In relation to child sexual exploitation material specifically, recent data released by the Australian Federal Police shows that more than 100,000 reports of online child sexual exploitation were received during the 2025–26 financial year. We are further concerned by the significant increase in reports of online child sexual exploitation in Australia, which have more than doubled since the 2022–23 financial year.⁶

Knowmore is deeply concerned by the growing role of generative artificial intelligence (AI) in child abuse.⁷ eSafety provides the following outline of this issue:

⁴ Kerryann Walsh et al., *Prevalence and characteristics of online child sexual victimisation: findings from the Australian Child Maltreatment Study*, Child Abuse and Neglect, February 2025, volume 160, <www.sciencedirect.com/science/article/pii/S0145213424005799>; Parliament of Australia, *Quality and safety of Australia's early childhood education and care system*, March 2026, p 25, paragraph 2.4, <https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Education_and_Employment/ECECqualitysafety>.

⁵ Timothy Cubitt et al., *AI- and non-AI online child sexual victimisation, disclosures and help seeking A national study of Australian adolescents*, 6 July 2026, p 31, <https://icmec.org.au/wp-content/uploads/2026/07/Cubitt_et_al_AI_and_non_AI_online_child-sexual_victimisation_disclosures_and_help_seeking.pdf>.

⁶ Australian Federal Police, *AFP launches community education resource as annual online child sexual exploitation reports pass 100,000*, 10 September 2026, accessed 16 September 2026, <www.afp.gov.au/news-centre/media-release/afp-launches-community-education-resource-annual-online-child-sexual>.

⁷ Australian eSafety Commissioner, *Designing for safety: preventing child sexual exploitation and abuse online*, March 2026, pp 10–13, <www.esafety.gov.au/sites/default/files/2026-02/Designing-for-Safety_Preventing-child-sexual-exploitation-and-abuse-online_CSEA-toolkit.pdf>.

Perpetrators are using AI to create and distribute true-to-life images of child abuse, sometimes based on images of victim-survivors, and sometimes using completely synthetic models of children ...

Generative AI tools that can be used to produce explicit content – such as ‘nudify’ apps that digitally remove clothing – are proliferating online. They are widely available, and quick and easy to use. Many are also free. The accessibility of such platforms has also made it easier for children to create inappropriate or harmful material of their peers.

Synthetic images of children are being used for extortion and exploitation, creating complex challenges ... This is incredibly important, because if it is authentic, it may depict a child in need of rescuing.⁸

eSafety observed ‘a 218% increase in reports of AI-generated CSEA [that is, child sexual exploitation and abuse material] from 2023 to 2024 alone’. A recent study by the Australian Cybercrime Observatory found that one in 25 children have experienced or have a friend who has experienced online sexual abuse involving the use of AI.⁹ In addition, children who have experienced online sexual abuse are more likely to disclose the abuse to AI than to the police, teachers, reporting lines or reporting websites.¹⁰

The severe and often lifelong impacts of child abuse have been well documented. For example, the Royal Commission made detailed comments about the impacts of child sexual abuse in volume 3 of its *Final*

⁸ Australian eSafety Commissioner, *Generative AI and child safety: A convergence of innovation and exploitation*, accessed 21 September 2026, <www.esafety.gov.au/industry/tech-trends-and-challenges/convergence-series/generative-ai-and-child-safety-a-convergence-of-innovation-and-exploitation>.

⁹ Timothy Cubitt et al., *AI- and non-AI online child sexual victimisation, disclosures and help seeking A national study of Australian adolescents*, p 40.

¹⁰ Timothy Cubitt et al., *AI- and non-AI online child sexual victimisation, disclosures and help seeking A national study of Australian adolescents*, p 43.

report.¹¹ eSafety has detailed the social, emotional, psychological and physical impacts of online child abuse, while also highlighting how harm can spread in online environments:

*... if a nude or sexual image or video of a child or young person has been shared online and not removed, they can be retraumatised every time it's seen again – for the rest of their lives.*¹²

Victims and survivors of online child abuse often experience additional barriers to accessing redress, justice-making and support options. For example, each state and territory has its own victims' support scheme for victims and survivors of crime, including child abuse. These victims' support schemes do not consistently recognise online child abuse as meeting their eligibility criteria. Victims' support schemes may also require victims and survivors to prove that they have been injured or suffered a loss as the result of a crime. For some forms of online child abuse, it can be particularly challenging to provide evidence of an injury or loss to the satisfaction of the relevant victims' support scheme or decision-maker, despite the traumatic impacts of the abuse.¹³

Australia's existing approach to online safety has failed to hold big technology companies accountable for the online abuse facilitated by their services. We note the eSafety Commissioner's assessment that technology companies, including Apple, Google, Meta and Microsoft, have failed to address critical safety gaps in detecting and preventing child

¹¹ See, for example, Royal Commission, *Final report: volume 3, impacts*, December 2017, p 9 and pp 73-156,

<www.childabuseroyalcommission.gov.au/sites/default/files/final_report_-_volume_3_impacts.pdf>.

¹² Australian eSafety Commissioner, *Online risks for children in your community*, accessed 21 September 2026, <www.esafety.gov.au/communities/child-safe-communities/risks#what-are-the-impacts>.

¹³ See Knowmore, *Submission on the National Strategy to Prevent and Respond to Child Sexual Abuse – Second Action Plan*, 31 July 2026, p 76, <knowmore.org.au/wp-content/uploads/2026/08/submission-national-strategy-to-prevent-and-respond-to-child-sexual-abuse-second-action-plan-cth.pdf>.

sexual abuse on their services.¹⁴ These companies can have annual revenues in the billions of dollars,¹⁵ and their online services play a role in everyday life that is significant and difficult to escape. As the Royal Commission highlighted, everyone has a role to play in improving child safety –¹⁶ it is time that big technology companies pulled their weight.

In the absence of a digital duty of care, children and parents must be ever-vigilant in the face of pervasive technology over which they have limited control. We recognise that the digital duty of care will not completely eliminate the risk of harm to children in online environments. However, we consider that the digital duty of care has significant potential to improve child safety online by requiring technology companies to proactively take steps to prevent harm before it occurs.

Alongside other requirements of the digital duty of care, we welcome the requirement for online services to ‘manage design features of the service appropriately, including by providing user empowerment tools as required’ by ministerial regulations.¹⁷ We note that the Australian Government has committed to requiring social media platforms to provide users with the choice to opt-in or opt-out of algorithm driven content.¹⁸ We commend the Australian Government for committing to meaningful action in response to the advocacy undertaken by Chanel Contos and the *Fix Our Feeds*

¹⁴ Australian eSafety Commissioner, *eSafety report shows while tech giants have made some progress they still have a long way to go in stamping out online child sexual abuse*, 5 February 2026, <www.esafety.gov.au/newsroom/media-releases/esafety-report-shows-while-tech-giants-have-made-some-progress-they-still-have-a-long-way-to-go-in-stamping-out-online-child-sexual-abuse>.

¹⁵ Jennifer Rankin, *Meta found in breach of EU law for failing to keep children off platforms*, The Guardian, 29 April 2026, <www.theguardian.com/technology/2026/apr/29/meta-found-in-breach-of-eu-law-for-failing-to-keep-children-off-platforms>.

¹⁶ Royal Commission, *Final report: volume 6, making institutions child safe*, p 14.

¹⁷ Exposure draft of the *Online Safety Amendment (Digital Duty of Care) Bill 2026* (Cth) (draft bill), schedule 2, clause 7, proposed sections 26(3)–(6) of the *Online Safety Act 2021* (Cth) (*Online Safety Act*).

¹⁸ The Hon Anthony Albanese MP and The Hon Anika Wells MP, *My Feed, My Way*, 8 September 2026, accessed 16 September 2026, <www.pm.gov.au/media/my-feed-my-way>.

campaign.¹⁹ We share the campaign's perspective that there is a need 'to ensure the legislation is air-tight and matches the ambition'.²⁰

Improving the draft bill

Although Knowmore broadly supports the draft bill, we have identified 2 key areas where we consider the draft bill may be improved:

- the Minister's powers to make regulations specifying additional categories of harmful material or conduct, beyond those specified in the draft bill itself
- the maximum penalty for breaching with the digital duty of care.

We discuss each of these issues in more detail below.

The Minister's powers to make regulations

The draft bill would empower the Minister for Communications (the Minister) to make regulations specifying additional categories of harmful material or conduct, beyond those specified in the draft bill itself (regulation-making powers).²¹ This would effectively require online services to protect people in Australia from the additional categories of harmful material or conduct specified by the regulations, including by conducting risk assessments in relation to the additional categories of harm and taking effective measures to address those assessments.²² There would be no objective element that must be met in order for the Minister to exercise

¹⁹ See Teach Us Consent, *Fix our feeds*, accessed 18 September 2026, <www.teachusconsent.com/fix-our-feeds>; Clare Armstrong, *Algorithm opt-in best way to stop big tech serving manosphere content to young men, says advocate*, ABC News, 2 September 2026, <www.abc.net.au/news/2026-09-02/algorithm-social-media-sexism-manosphere/107104586>; Brittany Busch, *Chalmers backs assault on big tech as Contos sounds alarm on manosphere*, 2 September 2026, Sydney Morning Herald, <www.smh.com.au/politics/federal/chalmers-backs-assault-on-big-tech-as-contos-sounds-alarm-on-sexual-violence-20260902-p60tnl.html>.

²⁰ Teach Us Consent, *Fix our feeds*.

²¹ See draft bill, schedule 2, clause 7, proposed sections 25C(2) and 25D(2) of the *Online Safety Act*.

²² See draft bill, schedule 2, clause 7, proposed section 26A of the *Online Safety Act*.

the regulation-making powers. However, the Australian Senate's usual ability to disallow regulations within a limited time period would apply.²³

We note that the Minister's regulation-making powers proposed by the draft bill have raised significant concerns, including concerns that the regulation-making powers pose a threat to free speech.²⁴ These are closely related to concerns that the draft bill would give the Minister 'unfettered powers to make regulations' that might not really be about online safety.²⁵

Before discussing these issues further, we wish to emphasise that our comments are addressed to the design of the regulation-making powers in the draft bill, not to the integrity of the present Minister or any person who may be the Minister in future. We consider that appropriate design of the regulation-making powers would have strong checks and balances, while also allowing the Minister to act quickly to respond to emerging threats to child safety in online environments.

We note the balanced perspective provided by the President of the Australian Human Rights Commission (AHRC), Hugh de Kretser. While noting that the AHRC supports a digital duty of care, the President has also observed that:

... there are risks that laws like this result in the over-removal of lawful content or limiting legitimate public debate and there are ways to mitigate these risks ... an alternative way to protect free speech is to require any changes to the harm categories to be

²³ See *Legislation Act 2003* (Cth), section 42.

²⁴ Clare Armstrong, *Labor proposes social media algorithm choice under new digital duty of care*, ABC News, 8 September 2026, accessed 11 September 2026, <www.abc.net.au/news/2026-09-08/labour-s-social-media-algorithm-choice-duty-of-care-bill/107130100>; Liberal Party of Australia, *Greens bell the cat on Labor's political censorship bill*, 18 September 2026, accessed 21 September 2026, <sarahhenderson.com.au/greens-bell-the-cat-on-labors-political-censorship-bill/>.

²⁵ Clare Armstrong, *Labor proposes social media algorithm choice under new digital duty of care*.

*made to the primary legislation which would require full parliamentary scrutiny and approval.*²⁶

Requiring ‘full parliamentary scrutiny and approval’ would strengthen the relevant checks and balances, but is also likely to slow down responses to emerging threats to child safety. We would like to suggest a further alternative that, in our view, would strike a more appropriate balance: amending the draft bill to include an objective element that must be met in order for the Minister to exercise the regulation-making powers.

We suggest that this might be achieved by adding the words ‘on reasonable grounds’ after the word ‘satisfied’ in proposed sections 25C(2) and 25D(2) of the *Online Safety Act 2021* (Cth) (Online Safety Act). This would maintain the Minister’s ability to respond quickly to emerging threats to child safety in online environments, while also allowing the courts to strike down exercises of the regulation-making powers that do not have reasonable grounds.

In Knowmore’s view, this issue also highlights the importance of implementing comprehensive Human Rights Acts in all Australian jurisdictions, including the federal jurisdiction. A federal Human Rights Act would provide a coherent framework for reconciling the tensions that might sometimes appear between rights, such as a tension between the right to freedom of speech and the right of children to protection. In the absence of a federal Human Rights Act, both of these rights are inadequately protected.²⁷

²⁶ Australian Human Rights Commission, *President's message: September 2026*, accessed 21 September 2026, <humanrights.gov.au/about-us/media-centre/articles/president-hugh-de-kretser/presidents-message-september-2026>.

²⁷ See, Knowmore, *Submission to the inquiry into Australia’s Human Rights Framework*, 17 July 2023, pp 5–6, <knowmore.org.au/wp-content/uploads/2023/08/submission-inquiry-into-australias-human-rights-framework-cth.pdf>.

Maximum penalty for breaching the digital duty of care

Under the draft bill, a breach of the digital duty of care would attract a maximum penalty of \$109.2 million.²⁸ In our view, the maximum penalty for breaching the digital duty of care should be strengthened to better encourage compliance with the duty and deter technology companies from putting profits before child safety.

We consider that fines for online service providers, particularly large technology companies, should reflect the scale and seriousness of the harm facilitated by their platforms and the annual revenues of such companies. As noted on page 6, these companies can have annual revenues in the billions of dollars.²⁹

When considering what effective compliance with a digital duty of care in Australia would look like, the 2024 Statutory Review of the Online Safety Act (statutory review) recommended that:

*The maximum civil penalty that a court can impose should be increased to the greater of 5 per cent of global annual turnover or \$50 million.*³⁰

We note that, in the United Kingdom and Europe, the maximum penalties for breaches of online safety laws are ‘primarily framed as a percentage of that service’s global annual turnover’.³¹

²⁸ Draft bill, schedule 2, clause 7, proposed section 26B of the *Online Safety Act; Regulatory Powers (Standard Provisions) Act 2014* (Act), section 82(5)(a); *Crimes (Amount of a Penalty Unit) Instrument 2026* (Cth), section 5; Australian Financial Security Authority, *Penalty units*, accessed 21 September 2026, <www.afsa.gov.au/professionals/resource-hub/penalty-units>.

²⁹ Jennifer Rankin, *Meta found in breach of EU law for failing to keep children off platforms*.

³⁰ Delia Rickard PSM, *Report of the Statutory Review of the Online Safety Act 2021*, October 2024, p 137, recommendation 34, <www.infrastructure.gov.au/sites/default/files/documents/report-of-the-statutory-review-of-the-online-safety-act-2021-february-2025.pdf>.

³¹ Delia Rickard PSM, *Report of the Statutory Review of the Online Safety Act 2021*, p 137.

Recognising the importance of child safety in online environments and the rapid development of online threats, Knowmore supports a maximum penalty that reflects the strongest elements of both the draft bill and the statutory review. We therefore recommend that proposed section 26B of the Online Safety Act under the draft bill should be amended to provide that the maximum penalty for breaching the digital duty of care is the greater of 5% of global annual turnover for the online service or \$109.2 million.

Thank you again for the opportunity to provide feedback on the draft bill. Should we be able to provide any further information, please do not hesitate to contact Jackie Mead on 03 8663 7400 or at jackie.mead@knowmore.org.au.

Yours sincerely,

A handwritten signature in blue ink, appearing to read 'Jackie Mead', with a stylized, flowing script.

JACKIE MEAD

Chief Executive Officer

ENCL.

- Attachment: about Knowmore

Attachment: about Knowmore

Our service

Knowmore legal service (Knowmore) is a nation-wide, free and independent community legal centre providing legal information, advice, representation and referrals, education and systemic advocacy for victims and survivors of child abuse. Our vision is a community that is accountable to survivors and free of child abuse. Our aim is to facilitate access to justice for victims and survivors of child abuse and to work with survivors and their supporters to stop child abuse.

From 2013 to 2018, our service assisted people who were engaging with or considering engaging with the Royal Commission into Institutional Responses to Child Sexual Abuse (the Royal Commission). From 1 July 2018, Knowmore has delivered legal support services to assist survivors of institutional child sexual abuse to access their redress options, including under the National Redress Scheme. Since 2022, Knowmore has assisted survivors who experienced child sexual abuse in non-institutional settings, and provided legal and financial counselling support to people engaging with the Territories Stolen Generations Redress Scheme. Knowmore has also been providing legal and financial counselling support to people who have received a redress offer from the Western Australian Stolen Generations Redress Scheme, which commenced in 2025.

Knowmore uses a multidisciplinary model to provide trauma-informed, client-centred and culturally safe legal assistance to clients. Knowmore has offices in Sydney, Melbourne, Brisbane, Perth, Adelaide and Darwin. Our service model brings together lawyers, social workers and counsellors, Aboriginal and Torres Strait Islander engagement advisors and financial counsellors to provide coordinated support to clients.

Knowmore is funded by the Commonwealth Government, represented by the Departments of Attorney-General and Social Services and the National Indigenous Australians Agency, and the Western Australian Government.

Our clients

In our Royal Commission-related work, from July 2013 to the end of March 2018, Knowmore assisted 8,954 individual clients. The majority of those clients were survivors of institutional child sexual abuse. Almost a quarter (24%) of the clients assisted during our Royal Commission work identified as Aboriginal and/or Torres Strait Islander peoples.

Since the commencement of the National Redress Scheme for survivors of institutional child sexual abuse on 1 July 2018 to 31 July 2026, Knowmore has received 260,070 calls to its 1800 telephone line and has completed intake processes for, and has assisted or is currently assisting, 27,538 clients.

About 2 in 5 clients (39%) identify as Aboriginal and/or Torres Strait Islander peoples. About 1 in 10 clients (9%) are classified as priority clients due to advanced age and/or immediate and serious health concerns including terminal cancer or other life-limiting illness.

100% of clients we assist with the Territories Redress Scheme identify as Aboriginal and/or Torres Strait Islander peoples.