BCA
Business Council of Australia

22 September 2026

Digital Duty of Care Team
Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts
digitaldutyofcare@communications.gov.au

Dear Digital Duty of Care Team

The Business Council of Australia (BCA) supports the introduction of a digital duty of care and the Bill's objective of reducing online harm, especially harm to children. People should be able to use online services with confidence that they are safe and their privacy is protected, particularly where children may be exposed to serious harm. Providers should take reasonable and proportionate steps to identify foreseeable risks arising from their services and address them through service design and operation.

However, the BCA has significant concerns about how the Bill would operate as drafted. The duty could apply well beyond large digital platforms to a wide range of ordinary business services such as online banking and workplace software, while important questions about scope, the standard of compliance and regulatory safeguards remain unresolved. If these issues are not addressed, the framework may create uncertainty, duplicate existing regulation and impose material implementation costs without a corresponding improvement in safety. The recommendations below are intended to make the duty workable and keep it focused on protecting people, particularly children, from serious online harm.

1. Confine the duty to the services and persons that can control the risk

The Bill should set the principal scope boundaries, including for enterprise, business-to-business and infrastructure services, before commencement. Ministerial exemptions and published screening questions and thresholds should supplement, not replace, those statutory boundaries.

Subsection 25A(3) allows the Government to formally exempt low-risk services from requirements in Part 2. We also understand that the proposed risk-assessment process will include screening questions about matters such as a service's features and number of users, allowing some low-risk services to be filtered out. The Government should clarify whether being filtered out will legally exempt a provider from further requirements or simply reduce the assessment it must complete. It should also explain whether either mechanism will apply to the separate transparency, research-access and Australian point-of-contact obligations. Scope decisions should be based on the function and risk of the service, not simply whether it falls within a broad service category. Search and discovery services, news websites, transactional websites and social platforms serve different purposes and should not face identical requirements where the risks and their ability to address them differ.

Consistent with the policy objectives of the Bill, regulated financial services should be excluded from the duty and related obligations. The Bill is principally directed at online safety risks arising from

services that disseminate content, facilitate interaction between users or use systems that recommend or amplify content. Regulated financial services generally do not perform these functions. Bank websites and digital banking platforms are primarily used to provide product information, account access and transactional services, but may nevertheless be captured by the broad definition of an online service.

Financial service providers are already subject to extensive prudential, conduct, complaints-handling, scams and fraud obligations. Applying overlapping requirements to services that present little or no risk of the online harms targeted by the Bill would duplicate regulation and impose material compliance costs without a commensurate customer benefit.

If the recommended exclusion is not adopted, regulated financial services should, at a minimum, be prescribed as exempt from Part 2 under subsection 25A(3). The exemption instrument should be made and published well before commencement so that businesses do not incur unnecessary costs preparing risk assessments, governance arrangements and documentation for services that are ultimately exempt.

Paragraph 25A(1)(h) should be limited to risks arising from functions that an equipment supplier can control or influence. An equipment supplier generally cannot inspect or change the online service that uses its equipment, so it cannot assess or reduce risks created by how that service operates. If equipment services remain in scope, the duty should apply only to risks arising from functions the supplier can control or materially influence.

An online service is often delivered by several businesses. A customer-facing service may rely on third-party hosting, messaging software and an AI model. Depending on how they operate, these may be separate online services under the Bill. While subsection 25A(2) identifies who may be responsible for a service, it does not clearly allocate responsibility where one business creates a risk and another business controls the means of addressing it. Guidance should allocate responsibility according to what each business can control or influence. It should also distinguish between a business using an AI assistant and the provider of the underlying model or infrastructure. Whether an AI service is covered, and what it must do, should depend on its functions and level of risk rather than simply on the fact that it uses AI.

2. Make the compliance standard explicit and scale risk assessments to the service

The Bill should clarify how the reasonably practicable test in section 25H applies to each mandatory requirement in subsection 26(3). It should also confirm that compliance is assessed using the information available at the time and that harmful content or conduct does not, by itself, establish a breach.

The Commissioner's guidelines have no stated evidentiary status, so a provider that follows them can still be found in breach. Courts and the Commissioner should have regard to relevant guidance and rules, the controls implemented, and testing and remediation, while allowing providers to demonstrate compliance through an equally effective approach.

Subparagraph 26A(2)(a)(i) requires providers to identify "all reasonably foreseeable risks, including those relevant to the provider's digital duty of care". This wording could require providers to assess risks beyond the online harms covered by Part 2. Risk assessments should focus on risks relevant to the objectives of the Act and be proportionate to the service's functions, reach and level of risk. Equivalent assessments completed under internal or comparable overseas frameworks should be recognised, without requiring businesses to repeat or reformat assurance work where it already meets Australian requirements. If the assessment is also intended to screen out low-risk services, providers

should be told when they may stop the assessment and be able to rely on that outcome when demonstrating compliance.

Consistency with international standards and comparable regulatory frameworks is particularly important for services that operate common systems across several markets. The United Kingdom has already implemented a statutory duty-of-care regime under the Online Safety Act 2023, supported by Ofcom risk-assessment guidance, risk profiles and codes of practice. Where the intended outcomes are comparable, Australian requirements should use compatible concepts and evidence requirements and recognise assessments, controls and assurance completed for the United Kingdom or another trusted jurisdiction. This would allow providers to direct resources to reducing risk rather than duplicating process, while preserving Australia's ability to address distinct local risks.

Section 26A requires an assessment before a service change that could introduce new or additional risks. However, the Bill does not explain how significant a risk must be before this requirement applies. Large services may release hundreds of changes each week, including routine maintenance and urgent security fixes. A pre-change assessment should be required only where a change is likely to materially alter the service's risk profile. Providers should be able to update an existing assessment, group related changes and screen out routine changes. Where urgent security or safety fixes cannot be assessed in advance, providers should be able to complete the assessment within a reasonable period after implementation.

3. Define harms with regard to context, and protect access to lawful services

The harm definitions should explain how context will be considered and provide thresholds supporting objective, evidence-based and consistent assessment. In particular, section 25C uses broad language for material relating to child sexual exploitation, child sexual abuse and grooming, which could capture prevention and education material designed to protect children, while section 25D includes open-ended categories and allows further categories to be added by legislative instrument. The Bill should make clear that legitimate health information, clinical communications, education, journalism and prevention material will not be considered harmful simply because it discusses a covered subject. Without this safeguard, health providers, search services and platforms may restrict lawful and beneficial material because they are uncertain about their legal exposure.

Section 25H recognises privacy but does not expressly address freedom of expression, access to information, accessibility or security. These considerations should also be expressly recognised. This would keep safety central while ensuring that measures are proportionate to their effects on other rights and public interests. Compliance should not require general monitoring of private communications, weaker encryption or unnecessary collection of identity or age information. Age assurance should match the level of risk and preserve access to essential services. Where appropriate, providers should be able to use trusted digital identity or attribute-verification services so they can confirm a user's age without collecting more personal information than necessary.

4. Narrow the design feature definitions (section 25F and 25G) and target user empowerment rules at demonstrated risk

Sections 25F and 25G should focus on features that present a genuine behavioural risk and account for how a feature operates in the particular service. For example, selecting information using account data could include ordinary transactional displays, while the definitions of endless feeds and time-limited features could include routine ways of presenting information such as search results or product listings. Section 25G then treats these features as having negative behavioural effects without considering how they operate in a particular service. The definitions should exclude functions needed for security, accessibility and personalisation requested by the user. Providers should also be

able to demonstrate that a feature does not cause the relevant negative effects in the context of their service.

The Department should clarify how paragraph 25B(1)(c) applies to services without accounts, services exempt from the minimum-age regime and age-assurance errors. User-empowerment rules should address demonstrated risks and specify outcomes rather than a single design. Any alternative-feed requirement should accommodate differences among social feeds, search, video, news and other recommendation services. Equivalent approaches should be permitted where they provide meaningful user control and preserve fraud prevention, security, accessibility, essential functions and useful content. Proposed rules should be supported by consultation, evidence, implementation costs and commencement arrangements.

5. Set the core obligations in the Bill and publish a single implementation timetable

The Government should publish one commencement timetable. Although the Bill provides for Schedules 2 and 3 to commence 12 months after Royal Assent, Appendix 1 of the consultation paper indicates that section 25A and the rule-making powers commence immediately. Providers need at least 12 months after relevant rules and essential guidance are finalised to implement requirements involving material systems changes.

The BCA welcomes the Department's indication that the first instruments will be released for consultation when the Bill is introduced into Parliament. This approach should apply to all significant instruments and later amendments. Consultation should include the proposed scope, supporting evidence, likely implementation costs and commencement arrangements. Because these powers can shape how services are designed, the Bill should set clear limits and a transparent process for their use. Before making or materially changing a significant rule, the Minister should be required to identify the safety risk, explain why the measure is necessary and proportionate, assess its effects on privacy, access to information, competition, innovation and security, consult affected parties, and allow enough time for implementation. Section 27B should also require the Minister to seek and consider the eSafety Commissioner's advice before using the service-classification power in subsection 25B(2) or the user-empowerment power in subsection 26(4). Significant rules should be reviewed after implementation.

6. Differentiate penalties and give providers an opportunity to remediate

The Bill should distinguish between substantive safety failures and minor administrative or documentation failures, with lower maximum penalties for the latter. The explanatory material should also clarify when separate failures, or a failure that continues over time, may be treated as multiple contraventions.

A failure to prepare, keep or provide a risk assessment that meets section 26A can attract the same maximum penalty of 60,000 penalty units as a substantive failure to protect users from seriously harmful material. A court can impose a lower penalty, but businesses must still manage their governance, insurance and financial exposure against the statutory maximum.

Except where urgent action is justified, enforcement should begin with notice of the alleged deficiency and the reasons for it, followed by an opportunity to respond and reasonable time to remedy the issue before stronger action is taken. Clear criteria should govern the use of infringement notices where compliance with the duty is reasonably contestable. The Bill already provides review rights for some remedial directions and transparency-report notices. Similar review rights should apply to other decisions that can have significant legal or commercial consequences for a provider,

including point-of-contact notices and decisions about confidential information or access to research data.

7. Protect confidential and security-sensitive information in transparency and information gathering

Transparency-report, publication and researcher-access mechanisms should be coordinated to avoid duplication. Providers should have a clear process to identify protected material and resolve disputes before publication.

Detailed risk assessments identify weaknesses in a service and the measures being taken to address them. Publishing that information may help bad actors target those weaknesses or avoid safeguards. The Bill allows the Commissioner to protect this information under subsection 192M(6), but only through a discretionary determination. The default should instead be publication of a public summary, with the detailed assessment provided confidentially to the Commissioner. The mandatory protections that apply under subsection 192G(2) should also apply to section 192M. Both should protect security-sensitive information, trade secrets, legally privileged advice and material that could help a person circumvent safeguards.

The Bill should set a reasonable minimum response period, provide a clear process for extensions and restore an appropriate reasonable-excuse defence. Section 199 gives the Commissioner broad powers to require information and documents but does not set a minimum response period or an express process for requesting more time. Failure to comply can result in criminal and civil penalties, and the consultation paper confirms that the previous reasonable-excuse defence has been removed. The Bill should also provide a process for raising legal professional privilege or conflicting legal obligations before penalties apply.

The Department and the Office of the Australian Information Commissioner should issue joint guidance explaining how expanded information-sharing powers will operate and how customer and employee information will be protected. The consultation paper states that Schedule 1 item 44 will allow the Commissioner to share information with a broader range of Commonwealth bodies. However, it does not explain the limits or safeguards applying to the use, retention or further sharing of that information. It also does not explain the effect of Schedule 2 item 63, which would make the eSafety Commissioner an "enforcement body" under the Privacy Act.

8. Set minimum safeguards for research access and fictitious identity testing in the legislation

The Bill itself should require necessity and proportionality, data minimisation, secure access, retention limits, controls on further disclosure and a process to vary or challenge a request before information is released. The research access rules may include safeguards for confidentiality, security, conflicts of interest, costs and review, but the Bill does not require any of them. Aggregated or de-identified data and secure research environments should be used where they meet the research purpose.

The Bill should preserve legitimate fraud prevention, customer identification and cybersecurity controls, distinguish authorised research from prohibited interference, and clarify when a provider may act on suspected misuse. The Bill allows authorised researchers to use fictitious identities despite other laws and contractual restrictions. Providers need clear rules for handling an account that their fraud or cybersecurity systems correctly identify as fictitious.

9. Confine complaints and contact obligations to matters within the provider's responsibility

Requirements should apply only to online safety matters within the provider's responsibility, and an existing sector process should be able to satisfy an equivalent requirement. The proposed complaints

power in section 26F does not expressly limit the required complaint processes to online safety matters and may overlap with established complaint schemes in banking, telecommunications and health. The rules should also address accessibility, proportionate response periods, review of moderation decisions and abusive or repetitive complaints, without preventing legitimate ones.

The Bill should clarify that the point of contact is responsible for receiving communications and notices only and does not personally assume the provider's duties or penalty liability. Subsection 229A(4) allows certain things that would normally be done in relation to a provider to be done through its nominated Australian point of contact.

The BCA welcomes further engagement on these amendments and on the development of the supporting rules and guidance.

Yours sincerely

Wendy Black
Executive Director Policy
Business Council of Australia