Australian Telecommunications Alliance

Setting The Standard.
Driving Progress.

4 June 2026

Andrew Hyles

Assistant Secretary – Digital Platforms, International and Policy,
Online Safety and Classification

Department of Infrastructure, Transport, Regional Development,
Communications, Sports and the Arts

Via email only: Andrew.Hyles@communications.gov.au, OSAReform@communications.gov.au

Dear Andrew,

Feedback on the Issues Paper *A Digital Duty of Care for Australia*

The Australian Telecommunications Associations (ATA) and our CSP members welcome the opportunity to provide feedback on the Issues Paper on a digital duty of care (DDOC). We also appreciated the opportunity to meet with you and your team to discuss the proposals.

Following on from our submission in response to survey on the DDOC in December 2025, the Issues Paper, and our recent discussions with your team, we provide the following high-level feedback:

1. Clarity of Scope and Proportionality:

- We maintain that exemptions from the DDOC for the services that our CSP/ISP members provide would provide the most practical and appropriate approach to a DDOC for such services, given the very limited control over and risk profile of such services.
- Failing such exemptions, we acknowledge that CSPs (including ISPs) would be included under the proposed, board DDOC framework. We emphasise that obligations must be calibrated by both risk and reach (together), and actual control – meaning that lower-risk services (e.g., basic connectivity/infrastructure with minimal content involvement) should face only proportionate, technically feasible duties, consistent with the 'so far as is reasonably practicable' standard. Given ISPs' primary role as connectivity providers (with broad reach but limited content control), we consider these ISP services have comparatively low online content risks.
- For services with minimal content exposure – such as products for enterprise customers, services delivered via reseller/wholesale arrangements, or one-to-one communications (like SMS, MMS, and email) – regulatory expectations should remain limited, reflecting CSPs' limited ability to monitor or influence user content. Notably, utility communications services such as SMS/MMS and email already have dedicated anti-abuse frameworks (e.g. *Spam Act 2003* requirements and telco anti-scam/cybercrime measures) and do not facilitate the kind of open content sharing seen on social media platforms. The DDOC should explicitly account for these differences and ensure any obligations on such services are minimal and technically feasible, to avoid imposing unrealistic or duplicative requirements on channels where broad content moderation is impractical.

2. Interaction with Existing Online Safety Frameworks:

- We support ensuring the new DDOC complements (and does not duplicate) existing *Online Safety Act 2021* (OSA) complaint schemes, codes, and standards. We note that the Department has verbally indicated that the DDOC is intended to incorporate and/or replace elements of the existing framework over time. Notwithstanding this, greater clarity is required on which components will be incorporated, which will be replaced, and how this transition will operate in practice.
- In this context, we seek clarity on whether the DDOC will incorporate, supersede, or operate alongside the current suite of 17 industry codes and standards (which cover numerous service categories and types of materials), and how a CSP's compliance with existing obligations (e.g. responding to eSafety removal notices, meeting *Basic Online Safety Expectations* (BOSE), and abiding by the industry codes/standards) will be recognised under the DDOC. It is essential to maintain coherence and minimise regulatory complexity, particularly during any transition where elements of the existing regime may be progressively replaced.
- We understand the Department is seeking views on whether the codes and standards should cease or coexist with the DDOC (with deemed compliance). Some ATA members have expressed a clear preference for the continued coexistence of the two frameworks/instruments, whereby compliance with the applicable codes and standards would be deemed sufficient to demonstrate compliance with the DDOC. Other members consider it too early to take a position without greater clarity on the DDOC's scope and how it will operate in practice.

3. Need for Clear and Practical Guidance:

- We emphasise that a broad, principles-based DDOC must be underpinned by clear, authoritative guidance to ensure practical and consistent implementation. We strongly support the Department's plan to develop detailed guidance (and if needed, service-specific rules) during the transition, and we urge the early release of these materials.
- Such guidance should clearly spell out what 'effective systems and processes' entail for different types of services, reflect safety-by-design best practices, and provide concrete examples of risk assessment and mitigation measures. This will enable CSPs – especially those with limited content visibility or control – to confidently align their internal processes and governance with the DDOC's expectations.

4. Transition Timing and Implementation:

- We welcome the proposed 12-month transition period, which is essential for orderly implementation. We recommend that the key compliance guidance and any binding rules be released well before the DDOC's commencement, allowing sufficient time for CSPs' implementation planning, system updates, staff training, and risk assessments.
- If there are delays in finalising guidance or subordinate instruments, we suggest considering flexible timing or phased obligations to ensure CSPs are not forced into non-compliance due to late-breaking requirements.

5. Support for Simplifying the Online Safety Framework:

- We are broadly supportive of a proportionate, flexible DDOC that helps uplift and simplify the online safety framework. We appreciate the collaborative consultation process and the Government's emphasis on minimising regulatory burden and complexity.
- By focusing on clear scope, non-duplication with existing schemes, and robust guidance (including clarity on how the current framework will be incorporated or replaced), the DDOC can be well-calibrated to protect users while providing certainty for industry.

If you have any questions or wish to discuss, please contact Deputy CEO, Christiane Gillespie-Jones (c.gillespiejones@austelco.org.au).

Kind regards,

Christiane Gillespie-Jones
Deputy CEO