Discussion Paper

Review of the Unlawful Material Online Safety Codes

Prepared by DIGI | June 2026

Australia is a World Leader in Online Safety — Here's Why It Matters

The Unlawful Material Online Safety Codes represent some of the most robust, comprehensive, and effective regulations against child sexual abuse material and pro-terror content anywhere in the world. Developed collaboratively by industry, informed by two rounds of public consultation, and enforced by the eSafety Commissioner, these Codes set a high bar against seriously unlawful material that meets or exceeds comparable regimes in the European Union and the United Kingdom.

This review is an opportunity to ensure these protections remain current. We invite the public to have your say.

Unlawful Material Codes review

The Online Safety Codes for Class 1A and Class 1B Material (the Unlawful Material Codes) developed by the Australian digital industry introduced world leading comprehensive safety regulations of digital services to safeguard the community from seriously harmful unlawful materials online. The regulations in these Codes are complemented by the Unlawful Materials Standards developed by eSafety which regulate the harms of Class 1A and IB materials on designated internet services (including websites, apps, file storage and generative AI services) and on relevant electronic services (including messaging and email services, dating services, and online interactive games). Included in the Unlawful Materials Codes and Standards are requirements on the highest-risk platforms to take proactive action against child sexual abuse and pro-terror material, extreme violence, and materials that promote crime and drug use.

A second set of nine industry developed codes - the Online Safety Codes for Class 2 Material (the Age-Restricted Material Codes) introduced a range of additional, enforceable regulations for online content unsuitable for under 18's, including pornography, suicide, self-harm and eating disorder content and violence.

This review of the Unlawful Materials Codes is being conducted by the industry associations who developed the codes, to ensure they remain relevant and effective in preventing and mitigating harm from seriously unlawful Class 1A and Class 1B materials. The approach to the review takes into account the Government's announcement that it will legislate a Digital Duty of Care.

The Codes under review are:

- **The Social Media Services Online Safety Code (Class 1A and Class 1B Materials)**
- **The App Distribution Services Online Safety Code (Class 1A and Class 1B Materials)**
- **The Hosting Services Online Safety Code (Class 1A and Class 1B Materials)**
- **The Internet Carriage Services Online Safety Code (Class 1A and Class 1B Materials)**
- **The Equipment Online Safety Code (Class 1A and Class 1B Materials)**
- **The Search Engine Services Online Safety Code (Class 1A and Class 1B Materials.)**

The registered versions of the Codes can be found in the register of codes and standards on the website of the Office of the eSafety Commissioner at www.esafety.gov.au

This review commenced in March 2026, with the overall process aiming for completion by October 2026.

The industry representatives conducting the review are currently seeking submissions from the public on the Codes, which are accessible at onlinesafety.org.au. This paper has been prepared to guide and assist that public consultation.

Why These Codes Matter: Protecting Australians from the Most Serious Online Harms

Child sexual abuse material and pro-terror content represent some of the most serious unlawful material that can be distributed online. The digital industry recognises that getting the regulatory response right is critical to the online safety of Australians, particularly children.

The Unlawful Material Codes were developed by the Australian digital industry to address these harms in a way that is effective, scalable, and appropriate to the diverse range of online services operating in Australia. Rather than imposing a blunt, one-size-fits-all approach, the Codes recognise that different parts of the digital ecosystem - social media platforms, app stores, hosting services, internet carriage providers, equipment manufacturers, and search engines have important but different roles to play. The result, in combination with the Unlawful Materials Standards, is a framework that is both principled and practical. The Codes hold industry accountable while enabling the kind of innovation and flexibility that effective online safety regulation requires.

✔ Key Strengths of the Unlawful Material Codes at a Glance

- Mandatory proactive detection of child sexual abuse materials and pro-terror material on high-risk platforms
- Obligations that scale across the entire technology stack — not just social media
- Clear, minimum compliance measures backed by the eSafety Commissioner enforcement
- Transparency requirements including annual public reporting by relevant industry participants
- User-facing reporting and complaints mechanisms
- Industry-to-industry cooperation and information sharing obligations
- Risk-based approaches allowing proportionate obligations across different service types

World-Class Protections: How Australia Compares Internationally

A critical question for any regulatory framework is whether it delivers protections that are effective by international standards. The Unlawful Material Codes in combination with the Unlawful Material Standards hold up strongly against comparable regimes in the European Union and the United Kingdom and in several respects go further.

Protection	Australia (Unlawful Material Codes and Standards)	EU: Digital Services Act (DSA) / Terrorist Content Regulation)	UK (Online Safety Act 2023)
Proactive detection of known CSAM	Mandatory proactive detection and takedown for relevant services (minimum compliance measure)	No current hard legal requirement to proactively detect child sexual abuse materials General requirements under DSA for designated very large online platforms and very large online search engines to assess systemic risks relating to the dissemination of illegal content (including child sexual abuse material) and adopt effective mitigation measures Ongoing negotiations on a regulation of child sexual abuse material, where a requirement to proactively detect this content by certain service providers is being debated	Required under illegal content duties for services in scope
Pro-terror content obligations	Mandatory proactive detection and takedown for relevant services	No current hard legal requirement to proactively detect terrorist content Under Terrorist Content	Required under illegal content duties for services in scope

		Online Regulation, online platforms that have been deemed exposed to terrorist content, may be required to put in place specific measures aimed at tackling risk of terrorist content on the platform although this is subject to prohibition on requirement to carry out proactive monitoring per DSA General requirements under DSA for designated very large online platforms and very large online search engines to assess systemic risks relating the dissemination of illegal content (including terrorist content) and adopt effective mitigation measures	
Risk-based approach	Yes — risk assessments required for certain service categories	Very large platforms face obligations under DSA	Yes — categorisation by size and risk determines obligations
Covers full technology stack	Yes — social media, hosting, ISPs, search engines, app stores, equipment. Additional coverage under the Standards for apps, websites, gaming services, dating services, messaging, email services, AI generative services and more	Partial — DSA systemic risk and mitigation duties apply to services designated as very large online platforms and very large online search engines only Terrorist Content Online Regulation requirements apply to online platforms which host and publicly disseminate content	Partial — primary focus on user-to-user services and search. ISP's, email and equipment are out of scope

		The scope of the child sexual abuse regulation is currently being debated, with different requirements potentially applying to different online intermediary services	
Mandatory reporting to regulator	Yes — annual reports and/or co-operation obligations	Yes — transparency reports required under the DSA	Yes — transparency reporting for certain services
User reporting mechanisms	Mandatory	Required under DSA	Required under OSA 2023
Enforceable by regulator	Yes — eSafety Commissioner	Yes — Digital Services Coordinators / European Commission	Yes — Ofcom
Industry co-operation obligations	Explicit — Matter 5 requires cross-industry collaboration	Encouraged but not required	Encouraged but not required
Developed with public consultation	Yes — two rounds, over 120 submissions	Yes — European legislative process	Yes — UK parliamentary process with extensive public consultation

The table above demonstrates that the Unlawful Material Codes and Standards impose robust, enforceable obligations across a broader range of online services. In particular, the inclusion of internet carriage services, hosting services, equipment providers, and private communications services such as messaging and email in Australia's framework goes beyond what is required in the EU and the UK, providing a more comprehensive set of protections across the technology stack.

The Unlawful Material Codes also reflect a uniquely Australian approach: rather than waiting for lengthy legislative cycles, industry worked proactively with the eSafety Commissioner and civil society to develop detailed, technical obligations that are already in force and being enforced. This means Australians currently benefit from strong protections under clear and enforceable regulations.

The role of the industry in developing the Unlawful Material Codes

A steering group of industry associations were tasked with the development of the Codes from 2021 to

2023. The Codes were the subject of two rounds of public consultation, resulting in over 120 submissions from a wide range of industry, civil society, government, and community stakeholders.

The Codes were developed by industry in consultation with the eSafety Commissioner. Industry associations representing the diverse digital businesses covered by the Online Safety Act were given the opportunity and responsibility to design robust technical and operational measures that would achieve the objectives proposed by the eSafety Commissioner and provide enforceable community safeguards against seriously unlawful materials. This approach enabled industry to:

- Leverage its combined technical expertise across the full spectrum of online services across the technology stack, to develop measures that are technically feasible and effective at scale.
- Develop regulations to address seriously illegal materials faster that could be achieved via legislation.
- Work collaboratively with the eSafety Commissioner, drawing on the regulators expertise and experience.
- Conduct a very transparent and open consultation with over 120 public submissions received during the development of the Codes, each of which was reviewed in detail and the response published. This extensive consultation process ensured the Codes reflect a broad range of perspectives, not just the interests of industry.

The eSafety Commissioner registered these Codes in 2023 and 2024. The first tranche of Codes commenced on 16 December 2023, and the Search Engine Services Code commenced on 12 March 2024.

The Codes extend to all industry participants in the relevant industry sections and are enforceable by the eSafety Commissioner under the Online Safety Act 2021 (OSA).

Material Covered by the Codes

The Unlawful Materials Codes outline steps that online industry participants must take to enhance online protections for Australian end-users by reducing access and exposure to Class 1A and Class 1B material. Class 1 and Class 2 material is defined by reference to the National Classification Scheme.

Class 1A Material includes:

- Child sexual abuse material
- Pro-terror material; and
- Extreme crime and violence

Class 1B Material includes content that:

- Crime and violence; and
- Drug-related content.

The scale of material available online is immense. While the classification scheme allows for consideration of context such as literary, artistic, or educational merit, this type of assessment is challenging when looking to comprehensively prevent and restrict such material at scale. The Codes recognise these limitations and are designed to be practically implementable by industry participants of all sizes.

It is worth noting that the National Classification Scheme is currently under review, and adjustments may be required to the Codes in light of any changes made to that scheme because of that review.

Structure of the Codes

Each of the Unlawful Materials Industry Codes comprise a Head Terms containing a set of common requirements that cover all industry sections, including definitions, and a schedule containing specific requirements that apply to the relevant section of the online industry. As per the Position Paper, the Unlawful Material Codes include a mix of mandatory 'minimum compliance measures' and discretionary 'optional compliance measures'. Minimum compliance measures aim to hold industry to account and lift the standard of minimum protections in place for Class 1A and Class 1B materials. Under some Codes, companies are required to undertake a risk assessment of their service or product, as different compliance measures are appropriate for different risk profiles in those service categories.

Areas of Focus for the Review

The current review is based on Terms of Reference informed by feedback from the eSafety Commissioner and a range of industry and civil society stakeholders. These include the following key areas of focus:

- **Changes in the Threat and Technological Landscape**: including the evolution of the online safety landscape since 2022.
- **The Changing Regulatory Settings in Australia:** considering changes since the Codes commenced, such as the Unlawful Material Standards, Age-Restricted Material Codes, and the Government's plans for a digital duty of care and for reforms to the National Classification Scheme.
- **Addressing Confusion and Challenges:** including inconsistencies in terminology or similar measures and ensuring proposed amendments consider the risks and benefits of current safeguards.

Exclusions from the review

It is important for stakeholders to note the following exclusions from the review:

- **Unlawful Material Standards:** The review does not extend to the Unlawful Material Standards developed by the eSafety Commissioner for Relevant Electronic Services (RES) and Designated Internet Services (DIS), which were registered on 21 June 2024.
- **Interaction between RES Standard and Social Media Services Code:** The effect of section 5 in the RES Standard and its interaction with the Social Media Services Code should remain out of scope for this review.
- The **Age Restricted Materials Codes** of which the initial codes covering internet search engine services, hosting services and ISPs came into force in December 2025 and the remaining codes for apps stores, social media, equipment providers, and other digital services (including communications based services, websites and generative AI services) came into force in March 2026.

How to Make a Submission

The industry associations invite submissions from industry and the public on the Unlawful Materials Codes. This is your opportunity to provide feedback on Australia's online safety framework. All perspectives are welcome, whether you are a concerned parent, a civil society organisation, a technology company, or an individual with views on how these Codes should operate.

How to Submit

Email: hello@onlinesafety.org.au

Website: www.onlinesafety.org.au

Each submission should include:

- **Your name (or a pseudonym, or 'anonymous' if you prefer)**
- **Contact details (telephone, postal address, or email)**
- **The name of any organisation you represent**

Closing date: 7 July 2026

If you require an extension or need an alternative method of making a submission, please contact us at hello@onlinesafety.org.au.

We prefer to receive submissions that are not claimed to be confidential. However, we accept that people may sometimes wish to provide information in confidence. In these circumstances, we ask you to identify the material over which confidentiality is claimed and provide a written explanation so that we can consider whether we can accept the submission on that basis. We will not publish confidential information without the agreement of the submitter.

In the interests of transparency, the industry associations intend to publish submissions received on our website, including any personal information in the submissions. Please ensure you do not include any personal information you do not want published

Privacy Information

We collect personal information for the purpose of considering the issues raised in this discussion paper and to contribute to the transparency of the consultation process by clarifying, where appropriate, whose views are represented by a submission. We may also use your details to contact you regarding your submission. For more information about how we may use your personal information, please see our privacy policy at www.onlinesafety.org.au/privacy/.

Discussion Questions

We have provided discussion questions to assist in focusing submissions. They are a guide only and not intended to limit the scope of submissions. Responses can be provided to all, any, or none of the questions.

Relevance of Measures

Are the measures in the Codes reasonable and proportionate to the harm posed by different types of Class 1A and Class 1B material?

Human Rights Considerations

Do you think the Codes strike an appropriate balance between user privacy, freedom of expression, and online safety?

Relevance of Risk Assessment Methodology

Are the risk assessment methodologies and compliance measures set out in the Codes still relevant?

Threat Landscape and Technological Developments

- Are there any technological developments that have created gaps in the Codes or rendered existing compliance measures unnecessary?
- Are there any potential changes in risk vectors for specific industry sections or subsections?
- Have any technological developments impacted the effective detection of material covered under the Codes?

Regulatory Alignment and Clarity

- What areas have caused confusion for consumers, and are there inconsistencies in terminology or similar measures that should be addressed?
- How should industry assess the risks and benefits of current safeguards?
- How should this review take into account the forthcoming Digital Duty of Care?

Drafting Inconsistencies

Are there any inconsistencies or drafting issues across the Codes that should be addressed?

International Comparisons

Are there aspects of comparable international regulatory frameworks that Australia's Codes should draw upon or learn from? Equally, are there areas where Australia's approach is leading internationally and should be preserved?

Stakeholder Engagement and External Input

What other matters need to be considered in the review?

Help Us Keep Australia Safe Online

The Unlawful Material Online Safety Codes protect Australians from some of the most serious harms that exist online. They represent an important achievement for online safety : robust, enforceable, world-class protections developed through collaboration between industry, government, and civil society.

This review is an opportunity for you to have your say.

Submit by email: hello@onlinesafety.org.au

Visit: www.onlinesafety.org.au