Factsheet

Age-Restricted Material Codes

- The **Age-Restricted Material Codes**, were drafted by members of the technology industry under the Online Safety Act. They seek to protect children from access to age-restricted material such as online pornography, as well as violent content and themes such as suicide and self-harm.
- The Codes promote children's right to be protected from accidental and unsolicited exposure to this age-inappropriate material while protecting adults' right to access to this content. These measures have come at a time when **eSafety research shows** that **one in three young people who had seen online pornography first encountered content unintentionally before the age of 13**.
- There are nine new codes which apply across a wide range of services like social media services, messaging services, gaming services, pornography websites, AI companions and chatbots, search engines and app stores. eSafety regulates the Codes, which are legally enforceable and breach of a direction to comply may result in **civil penalties of up to $49.5 million**.
- No piece of regulation will mitigate all risks and harms – a holistic approach is required to address these challenges. However, eSafety believes the ARM Codes, alongside the Online Safety Act's existing codes and standards focussed on unlawful material (such as child sexual exploitation), as well as the social media age restrictions, **create meaningful protections for children across the tech ecosystem**. They put responsibility where it belongs – with the providers designing and delivering these services.

What are the Age-Restricted Material Codes?

- The Codes create legally enforceable rules that online services must follow to protect children from a range of this potentially harmful age-restricted content. The Codes focus on online pornography, high-impact violence material, and content which instructs disordered eating and self-harm material, including suicide. The Australian Government's **National Classification Scheme** designates this material as **legally age-restricted** (rated R18+ or X18+).
- The Codes' requirements focus on images and videos, but also deal with other types of content – for example, material generated by artificial intelligence (AI) and companion chatbots.
- In addition to providing stronger protections for children, the Codes also require services to give all Australians better information, tools and options to limit their exposure to age-restricted material content, if they wish.
- **The Codes were drafted by industry, for industry**. The code drafting process also included a **public consultation**. As the Codes were deemed to provide 'appropriate community safeguards', eSafety registered them, and will be monitoring the implementation to identify whether industry can uphold the level of protections they have created for themselves in these Codes. We will take enforcement action where there is systemic non-compliance.

What do the Age-Restricted Material Codes aim to achieve?

- The Codes seek to address the ease with which potentially harmful age-inappropriate material, such as pornography or violent material, can be accessed online, without safeguards preventing unintentional exposure. **eSafety research** has shown high rates of **accidental or unsolicited exposure of children** to materials like online pornography on online services.
- Across the Codes, requirements are more robust for some types of services compared to others, with a focus on the strongest obligations applying to the highest-risk services.
- No piece of regulation will mitigate all risks and harms – a holistic approach is required to address these challenges. However, the Codes were designed to limit accidental or unintended exposure to age-inappropriate material, especially for young children, while adults maintain the right to access lawful content they wish to see.
- The Age-Restricted Material Codes will operate alongside the pre-existing **Unlawful Material Codes and Standards**, and other requirements like the **Social Media Minimum Age obligation**.

What's required under these new Codes?

- The Codes require services to implement various protections depending on the risk of children accessing online pornography, high-impact violence material, and self-harm material on the service.
- Some services will have to do age checks to prevent children's access, particularly services where there is a high risk of being exposed to age-inappropriate content. This includes:
  - adult websites like online pornography sites
  - social media services that allow online pornography or self-harm material to be shared
  - AI chatbots or generative AI services that are capable of generating age-restricted material without appropriate safeguards
  - online games rated R18+ according to the National Classification Scheme
  - some app stores when the user wants to download apps rated 18+ (please note, some of the requirements around age checks for app distribution services only need to be in place from 9 September 2026)
  - search engine services, when search results feature age-restricted material, which will be blurred by default until the user logs in to an account (like Google) and confirms they are 18 or older (please note, some of the requirements around age checks only need to be in place from 27 June 2026).
- The nine Codes all work in tandem to create a layered safety approach across the technology service stack. For example, if a child conducts an image search on a search engine for pornography, they will not be immediately exposed to adult images through search engine results; and if they click through to results for websites which provide this content, those individual sites will also have to conduct age checks. Other protections also apply through services like app stores and social media services.

What's not required under these Codes

- The Codes do not stop adults from accessing legal but age-restricted material.
- Services must continue to comply with applicable privacy laws.
- Where age assurance is required, online services have flexibility to implement the most appropriate and proportionate method of age assurance for their service.
- In particular, the Codes don't require any specific type of age assurance, and do not require services to verify age using government ID. Instead, a range of age assurance tools designated as appropriate by the service provider will be used. There are no requirements to share user information or service use information with any third parties such as government.

How will eSafety monitor and enforce the Codes?

- eSafety's Online Safety Codes and Standards target systemic safety failures, rather than focusing on individual incidents where children may access age-restricted materials. The obligations are on industry, and there are no penalties for children accessing age-restricted materials.
- In 2026 eSafety's first regulatory priorities under the new Codes will be:
  - focusing on AI chatbots that can generate sexually explicit and other harmful materials, ensuring they have appropriate safeguards for children
  - ensuring the largest and highest-reach and risk service providers that host or provide access to pornography are complying with their obligations to prevent children from accessing their services
  - making sure large gatekeeper services like search engines and app stores are enforcing their own terms of service to provide safe experiences to users.

For more information, see...

- **eSafety's Online Safety Codes and Standards page**
  - Includes background information about Code development
- **Register of Industry Codes and Standards**
  - See Codes Head Terms for definition of 'appropriate age assurance'
- **Regulatory Guidance on Online Safety Codes and Standards**
  - See Appendix F for Regulatory Guidance on age assurance
- **Online Safety Codes and Standards Complaints Form**
- FAQs for **general public** and **Regulated Entities**