Overview of the Phase 2 Industry Codes:

Purpose, scope and key requirements

September 2025

Australian Government | eSafetyCommissioner

eSafety.gov.au

Table of Contents

Background to the Phase 2 Industry Codes

What are the industry codes and why have they been developed?

- The Online Safety Act 2021 (the Act) sets out the Australian Parliament's intent for industry representative bodies to make industry Codes which would apply to content that is illegal and restricted for children (known as class 1 and class 2 material).
- For an industry code to be registered, the eSafety Commissioner must be satisfied that it provides appropriate community safeguards. Otherwise, the eSafety Commissioner may determine industry standards for the relevant online sectors.
- The eSafety Commissioner adopted a 'two phase' approach to the development of industry codes (and standards):
- The Phase 1 Codes and Standards deal with the 'worst of the worst' content, such as child sexual abuse and exploitation and pro-terror material. The Phase 1 Codes and Standards came into effect between December 2023 and December 2024.
- The Phase 2 Codes put in place enforceable requirements on the online industry to protect Australian children from accessing or being exposed to age-restricted content (primarily content that is, or would likely be, rated X18+ or R18+ under the National Classification Scheme).
- The Phase 2 Codes also require the online industry to provide all users with effective information, tools and options to limit their access and exposure to this material, if they so choose.

What types of material do the Phase 2 industry codes cover?

- The Phase 2 Codes focus primarily on material that is or would likely be rated X18+ or R18+ under the National Classification Scheme.
- The National Classification Scheme identifies a broad scope of material as material which could be legally age restricted. With this in mind, eSafety encouraged industry to adopt a harms-based approach in the Phase 2 Codes, focusing the most substantial measures on particular types of material where there is a growing evidence base for harms. These types of material are:

  - online pornography (being sexually explicit images or video)
  - high-impact violence (to the extent it is not covered under the Phase 1 Codes and Standards); and
  - high-impact material which encourage self-harm, suicide and disordered eating.
- Several measures throughout the Codes also specifically apply to simulated gambling material, which was designated R18+ by the Australian Government in September 2023.
- 'Simulated gambling' material is different from online gambling services and loot boxes. The Australian Communications and Media Authority is the regulator of online gambling services. Find out more details on the ACMA's website.
- Other jurisdictions like the United Kingdom, Ireland and Singapore have identified similar types of material as material which should be subject to similar rules like those in the Australian codes.
- The definition of 'material' in the Australian Online Safety Act is broad. Protections as set out in the Codes will apply to different types of material online including images, video, and also services like text-based AI companion chatbots.
- These protections are not a 'one size fits all' solution. Each industry code has specific risk-appropriate measures that apply to different sections of the online industry.

What is required under the Phase 2 Codes?

- The Phase 2 Codes adopt some key good practice measures already being implemented by major platforms. They also uplift safety protections, by introducing new obligations that will require members of the online industry to promote children's online safety.
- Many services captured under the Codes will have to undertake evidence-based assessment of the risk that children will access or be exposed to material harmful to children and implement proportionate protections which:
  - protect and prevent children in Australia from accessing or being exposed to this material; and
  - provide end-users in Australia with effective information, tools and options to limit access and exposure to this material.
- The Codes take a risk-based approach, with most stringent measures applied to three main types of content which is identified as being harmful for children: online pornography, high-impact violence material, and self-harm material.

- The Codes will require services to implement proportionate protections dependent on the risk profile of the service.
- Protections that services may have to implement include:
  - Age assurance and access control measures
  - Removing or de-prioritising material that contravenes their terms of service
  - Default safety tools for child end-users
  - Parental controls
  - Reporting or complaints mechanisms.

The full measures required under the Codes are available within each registered Code.

What are the different industry sections that are covered under the codes?

- Under the Act, there are eight sections of the online industry. The Phase 2 Codes provide important safety measures across each of the eight industry sections:
  - **Social media services (SMS)** – services that enable online social interactions between users, discovery of other users and posting of content.
    - The industry associations submitted two Phase 2 SMS Codes, an SMS (Core Features) Code and an SMS (Messaging Features) Code. Social media services with messaging functionality will be required to follow both codes.
  - **App distribution services (APP)** – services that enable users to download third-party apps or software online.
  - **Internet carriage services (ICS)** – services that enable users to access the internet through telecommunications infrastructure (internet service providers).
  - **Hosting services (HOS)** – services that store material provided on websites.
  - **Equipment providers (EQP)** – manufacturers, suppliers, installers and maintainers of electronic equipment which facilitates access to the internet, and providers of operating systems.
  - **Search engine services (SES)** – services that enable users to search an index of websites and receive search results (including results generated by artificial intelligence).

- **Relevant electronic services (RES)** – includes services that enable users to communicate with each other by email, instant messaging, short message services (SMS), multimedia message services (MMS) or chat services. It also includes services that enable users to play online games with each other, and online dating services.
- **Designated internet services (DIS)** – includes services that allow users to access online material, or services that deliver material to persons who have internet-enabled equipment appropriate for receiving that material. Designated internet services include many apps and websites, as well as file and photo storage services, and some services which deploy or distribute generative artificial intelligence (AI) models. Designated internet services do not include social media services, relevant electronic services and other identified services.

Registration of the Phase 2 Industry Codes

How were the Phase 2 Codes created?

Key Milestones

Notices issued to industry to develop Phase 2 Codes

- In July 2024, eSafety issued Notices to five industry associations that represent the eight sections of industry to request they start to develop the Phase 2 Codes:
  - Australian Mobile Telecommunications Association (AMTA), representing providers such as Ericsson Australia, TPG Telecom and Motorola.
  - Australian Telecommunications Alliance (ATA) [formerly Communications Alliance], representing providers such as Optus, Telstra, Aussie Broadband, and Vocus.
  - Consumer Electronics Suppliers Association (CESA), representing providers such as Amazon, Samsung and Sony.
  - Digital Industry Group Inc (DIGI), representing providers such as Apple, Google, Meta, Microsoft and TikTok.
  - Interactive Games & Entertainment Association (IGEA), representing providers such as Sony, Microsoft, Nintendo, Ubisoft and Roblox.
- These Notices are available on eSafety's website. We also published a Position Paper to provide clear guidance to industry on eSafety's expectations for the Phase 2 Codes.
- Under the eSafety issued Notices, the industry associations were required to draft Phase 2 Codes that addressed two 'matters':
  - Matter 1: protect and prevent children in Australia from accessing or being exposed to class 1C and class 2 material; and
  - Matter 2: provide end-users in Australia with effective information, tools and options to limit access and exposure to class 1C and class 2 material.
- Class 1C and class 2 material includes content such as online pornography, high-impact violence and high-impact material which encourage self-harm, suicide and disordered eating.
- As required under the Online Safety Act, the industry associations were also responsible for undertaking consultation on the draft codes with eSafety, industry and the public. Public consultation was conducted between 22 October 2024 – 22 November 2024. This included publishing a draft of the Phase 2 Codes and explanatory materials on their website alongside a discussion paper which explained

how to make a submission and details of the rationale for the measures in each Code.

- Both eSafety and the industry associations promoted the Phase 2 Codes' development and public consultation process through newsletter updates, social media posts and articles in the media. The industry associations proactively contacted over 250 stakeholders to invite them to make submissions to the consultation process.

First drafts submitted by industry

- eSafety received draft industry codes for seven sections of the online industry on 28 February, and the final draft industry code (the APP Code) on 27 March. This was announced in a media release on 3 March 2025.
    - This was after industry sought and was granted an extension of time in December 2024, to have time to account for the Government's introduction of the *Online Safety (Social Media Age Restriction) Act 2024* (Cth).
- Industry associations have published all draft codes submitted on 28 February and 27 March, as well as the submissions received during public consultation on their website.
- On 20 April 2025, the eSafety Commissioner wrote to the industry associations informing them of her preliminary view that the submitted codes would not provide the appropriate community safeguards required for them to be registered.
- Accordingly, the Commissioner provided the associations the opportunity to submit final revised codes for review by 20 May 2025. The receipt of these codes was announced on 21 May 2025.

First three codes registered

- On 24 June 2025, the eSafety Commissioner announced at a televised address at the National Press Club that three codes would be registered: the Search Engine Services Code, the Hosting Services Code and the Internet Carriage Services Code.
- Further detail was published after the codes were registered on 27 June 2025. The majority of the obligations under these codes will come into effect on 27 December 2025. Provisions relating to age assurance in the SES Code will come into force on 27 June 2026.

Remaining six codes registered

- In June 2025, the eSafety Commissioner wrote to the industry associations asking for clarification around some of the provisions in the submitted codes, and requesting that some provisions in the Codes be strengthened. One of the primary concerns eSafety expressed to industry at this time was that measures for generative AI

companion chatbot functionalities did not extend to how those functions may manifest on relevant electronic services or social media services.

- On 9 September 2025, the eSafety Commissioner registered the remaining six codes submitted by industry associations. These are:
    - the Relevant Electronic Services Code
    - the App Distribution Services Code
    - two codes that cover social media services – the Social Media Services (Core Features) Code and the Social Media Services (Messaging Features) Code
    - the Designated Internet Services Code, and
    - the Equipment Code.
- The majority of obligations under these codes will come into effect on 9 March 2026. Age assurance requirements in the APP Code, will come into effect on 9 September 2026.
- As all submitted Codes were able to be registered by the Commissioner, eSafety will not need to draft Standards, unlike the Phase 1 Industry Codes and Standards process.

Why did the eSafety Commissioner make the decision to register the Phase 2 Codes?

- Section 137 of the *Online Safety Act 2021* (Cth) states:
  "*The Parliament intends that bodies or associations that the Commissioner is satisfied represent sections of the online industry should develop codes (**industry codes**) that are to apply to participants in the respective sections of the industry in relation to their online activities.*"
- Accordingly, eSafety began developing online safety Codes in September 2021. eSafety published an initial Position Paper to commence this process at that time, and then a further Position Paper for the Phase 2 Codes specifically in July 2024.
- Under the Online Safety Act, the Commissioner may register an industry code if she is satisfied that it provides appropriate community safeguards.
- The Commissioner considered that all the submitted Codes provided adequate improvements in safety measures from the online industry to ensure that children would be better protected and prevented from accessing or being

exposed to online pornography, self-harm material, and other age-restricted content. They also made positive changes that empower all users to better control how they choose to encounter this material.

What are the next steps?

- The Phase 2 Industry Codes come into effect six months after registration.
- The ICS, HOS and SES Code come into effect on 27 December 2025, and the remaining Codes come into effect on 9 March 2026. In recognition of the need for product development, select age assurance measures in some Codes (SES and APP) grant extra time for services to comply after the Code comes into effect.
- eSafety is working on regulatory guidance for the Codes, which will help industry and end-users understand what obligations services have under the Phase 2 Codes.
- eSafety has the ability to commence compliance and enforcement actions as the Codes come into effect.

Related online safety developments

How are the Phase 2 Codes different from the Social Media Age Restrictions?

- The Phase 2 Codes primarily focus on preventing children's access or exposure to age-inappropriate **content** (such as pornography, high-impact violence and material relating to self-harm, suicide and disordered eating) across the 8 sections of the online industry.
- The social media age restrictions are focused on preventing children under 16 from **having accounts** on age-restricted social media platforms. The age restrictions aim to protect young people from risks and harms that users can be exposed to while logged in to social media accounts. These come from social media platform design features that encourage users to spend more time on platforms, and risk exposing young people to content that can harm their health and wellbeing. Age-restricted social media platforms can belong to different sections of industry for Phase 2 Codes. For example, a relevant electronic service under Phase 2 Codes may be an age-restricted social media platform.
- Social media platforms that will need to apply the age restrictions will also have obligations under the Phase 2 Codes to protect 16- and 17-year-olds from exposure to age-inappropriate material, and to empower all users with tools to help avoid this material.

- Services that are not required to apply the social media age restrictions will still need to follow the compliance measures under the Phase 2 Codes.
- The Phase 2 Codes and the social media age restrictions will work together to make children's online experiences safer.
- You can find further information about the social media age restrictions on the eSafety website.

How do the Phase 2 Codes interact with the Age Assurance Technology Trial?

- eSafety recommended a pilot of Age Assurance technology in its roadmap submitted to Government in 2023. The Trial and the Codes have been progressing in parallel.

- eSafety has been following the results of the Trial as an official observer, and it has helped to inform our understanding of what is technically feasible and reasonably practical when it comes to age assurance measures in the Codes.

eSafety will continue to consider the Trial Report further in the development of regulatory guidance to help industry understand how to comply with the Phase 2 Codes.

Requirements under each Code

Why are certain measures in the Codes limited to online pornography, self-harm material, high-impact violence material and simulated gambling material?

- The Phase 2 Codes deal with material which is legally age-restricted and designated as harmful for children by the Australian Government under the National Classification Scheme.
- In drafting the Codes, the industry associations have attempted to deal with categories of content in a manner that is proportionate to the harm that they pose to end-users aged under 18. Online pornography, self-harm material, high-impact violence material and simulated gambling material have been identified as content that can cause harm to children and also be addressed by services at-scale, and so have applied the most stringent measures to these categories of content.
- This also aligns with international norms that are emerging identifying this material as high-risk for children, including the UK's Online Safety Act 2023, which also focuses on this high-risk content.

Why are there two SMS Codes?

- Often there are online services which meet the definition of multiple online sectors under the Online Safety Act. In particular, there are many social media services that have messaging and/or chat functionality that as a result also meet the definition of a relevant electronic service. By registering a second SMS Code containing the same messaging requirements as those that apply in the RES Code, social media services can still have and comply with obligations tailored to their messaging features, while also complying with the 'core features' SMS Code.
- Note: Services that meet the definition of a relevant electronic service and social media service are still required to comply the Phase 1 RES Standard which prevails over the Phase 1 SMS Code. For Phase 1, the industry associations did not provide eSafety with equivalent SMS 'core features' and 'messaging' codes, instead providing eSafety with a single SMS code.

What are the key requirements under the Search Engine Services Code?

- By 27 June 2026, search engine services must implement appropriate age assurance measures for logged-in account holders. This means logged out users, or users without an account will not have to undergo age assurance when using a search engine.
- If you are under 18 years of age, safety tools and settings will be enabled by default to the highest setting on that account. This includes the filtering out of high-risk material detected in search results.
- For users without an account, services must apply safety measures to reduce unintentional exposure to age-inappropriate material including the default blurring of this material.
- Crisis prevention information must be provided for a user seeking self-harm material such as suicide, self-injury, or eating disorder content.

What are the key requirements under the Designated Internet Services Code?

- Websites that have the highest risk of enabling children to access or be exposed to pornography and self-harm material must implement appropriate age assurance measures. This includes online pornography sites.
- Generative AI services that have the highest risk of enabling children to generate online pornography, self-harm material and high-impact violence material must implement appropriate age assurance and access control measures to stop them accessing these features.
- These sites must undertake a risk assessment to understand how likely it is that Australian children will access or be exposed to online pornography and self-harm material.

What are the key requirements under the Relevant Electronic Services Code?

- Relevant electronic services with the sole or predominant purpose of permitting end-users to share online pornography or self-harm material must implement appropriate age assurance measures before providing access to the service.
- If services have AI companion chatbot features, they must follow measures based on the risk of children generating online pornography, self-harm material and high-impact violence material. This includes appropriate age assurance measures for the services with the highest risk.
- Providers of video games rated R18+ by the National Classification Board must also implement appropriate age assurance measures before providing access to the game.
- Other than this, services must ensure they have appropriate safety tools to assist Australian end-users to limit receipt of unsolicited materials and exposure to harmful material.

What are the key requirements under the Social Media Services (Core Features) Code?

- Social media services that allow online pornography or self-harm material on their service must implement appropriate age assurance measures before allowing access to this material.
- If services have AI companion chatbot features, they must follow measures based on the risk of children generating online pornography, self-harm material and high-impact violence material. This includes appropriate age assurance measures for the services with the highest risk.
- Services that do not allow online pornography or self-harm material must utilise systems and technologies to detect and remove this material, and continuously improve these systems over time.

What are the key requirements under the Social Media Services (Messaging Features) Code?

- Social media services must have terms and conditions which prohibit illegal activity, specifically that users can't use the service to share pornography with an Australian child.
- Services must ensure they have appropriate safety tools to assist Australian end-users to limit receipt of unsolicited materials and exposure to harmful material, including the ability to block other users and to leave group chats.

What are the key requirements under the App Distribution Services Code?

- By 9 September 2026 (six months after the Code comes into effect), app distribution services must implement appropriate age assurance measures before permitting end-users to download or purchase apps rated as 18+.
- App distribution services must also ensure that apps are appropriately rated and that age rating information is provided in a clear and accessible manner for end-users.

What are the key requirements under the Internet Carriage Services Code?

- Services must provide easily accessible and clear information about how to prevent children's access to harmful material, including through filtering products.
- Services must address compatibility issues with third-party filtering products.

What are the key requirements under the Hosting Services Code?

- Services must have clear policies in place relating to relevant material, and take appropriate and proportionate enforcement action where customers are in breach of these policies.

What are the key requirements under the Equipment Providers Code?

- Users of portable interactive devices which enable general internet browsing (such as smart phones, tablets, etc) will have to be given the option to create child accounts with relevant safety tools to prevent access to relevant material. This responsibility sits with the operating system (OS) provider (such as Microsoft's Windows, Apple's iOS and macOS, and Google's Android and ChromeOS). OS providers must also take appropriate steps to further develop and improve these safety tools.
- Other devices that provide access to the internet must make available similar safety tools that end-users can choose to opt-in to.

What about Generative AI?

- Most requirements for stand-alone generative AI services fall under the DIS Code. These requirements include implementing appropriate age assurance features for services with a high risk of child end-users generating or accessing age-restricted material. Services with a lower risk profile will be required to implement appropriate age assurance or have systems, processes and/or technologies that prevent age-restricted material from being generated on the service.

What are the requirements for chatbots?

- Industry representatives have recognised the emerging safety concerns with generative AI chatbots, which are capable of simulating personal relationships.
- The DIS Code, RES Code and SMS (Core Features) Code will require services to undertake a risk assessment if chatbot functionality is added to the service.
- Chatbot features with a high risk of child end-users generating age-restricted material, which includes potentially sexually explicit conversations between a chatbot and a child user, will need to implement appropriate age assurance measures. A service with a lower risk profile for its chatbot features will be required to have systems, processes and/or technologies that prevent age-restricted material from being generated.

Age assurance

Find out more about age assurance

Why are the Phase 2 Codes introducing age assurance?

- To implement appropriate tools and safeguards to prevent children from accessing or being exposed to material that can harm them, services first need to understand whether the user trying to access this material is a child.
- We know that many online services currently don't enforce their own terms and conditions about age of use.
    - eSafety's research and industry information provided in response to transparency notices issued under the Basic Online Safety Expectations showed that 80% of 8- to 12-year-old children in Australia are accessing social media, despite most social media services having an age minimum of 13 (with exceptions, like YouTube accounts that are linked to adult accounts).
- We also know self-declaration doesn't work.
    - eSafety's research also shows that social media services rely on self-declared ages to prevent underage users from access, but this is easily circumvented. Many social media services have additional tools that are meant to determine if a user is likely a child, but the accuracy of these tools is usually not assessed. 80% of surveyed children aged 8 to 12 with a social media account had not experienced their account being shut down due to age.
- As required under the Online Safety Act, these codes are drafted by industry. Industry representatives wrote to eSafety that the Codes included industry-agreed age assurance measures which they consider to be proportionate and proximate to the risks that minors using a service will be exposed to relevant types of material. eSafety will be able to take compliance and enforcement action if measures are not adhered to by industry. Further information about the reasoning behind certain measures of each code is available in the industry associations' Request for Registration.
- In the Phase 2 Codes Position Paper, eSafety suggested that codes should require providers to implement risk-proportionate age assurance measures, given the different role each sector plays, for example, as gatekeepers to the internet. The recommendations built on the findings of eSafety's Age Verification Roadmap.

- The Phase 2 Codes also reflect emerging international regulatory norms for how numerous different governments are also requiring age assurance, such as:
    - The UK's Online Safety Act 2023 and associated Online Safety Codes, which has required all user-to-user services that allow online pornography to implement 'highly effective age assurance' from 25 July 2025.
    - Ireland's Online Safety Code for Video Sharing Platforms (VSPs), which require the use of effective age assurance measures to ensure that 'adult-only' content cannot be seen by children.
    - The European Union's Digital Services Act, which requires platforms to undertake risk management frameworks, assessments, and mitigations, include taking targeted measures to protect the rights of the child, including age verification and parental control tools, tools aimed at helping minors signal abuse or obtain support, as appropriate.
    - Singapore's Online Safety Code of Practice for App Distribution Services, which requires designated app stores to implement age assurance to prevent children downloading age-restricted apps.
    - Twenty different states in the United States have age assurance laws, including different approaches which relate to adult content, social media services, and app distribution platforms.

What kind of age assurance methods are allowed under the Codes?

- In the Head Terms to the Phase 2 Codes, the industry representative groups have listed several examples of age assurance measures that would be considered appropriate for the purposes of the Codes. These include, but are not limited to:
    - matching of photo identification
    - facial age estimation
    - credit card checks
- digital identity wallets or systems
    - attestation by a parent of age or whether an Australian end-user is a child
    - use of artificial intelligence technology to estimate age based on relevant data inputs.
- In determining appropriate age assurance measures, services must also:

  - Take into account the technical accuracy, robustness, reliability and fairness of the solution for implementing the measure.
  - Consider whether age assurance measures have been designed to comply with privacy laws.
  - Consider whether the impact on user privacy of any such measures for a service is proportionate to the online safety objectives.
- Members of industry submitted to eSafety that this formulation of industry-agreed age assurance measures was the right approach to take in the Codes because:
  - Services that have the sole or predominant purpose of providing access to age-restricted material like online pornography must implement effective age assurance.
  - Key access points to age-restricted material such as search engines, social media services and app distribution services must implement effective age assurance if they find themselves to have a high risk-profile.
- Less intrusive measures are included for providers when they are an effective alternative to age assurance.
  - The Head Terms require providers to take into account the interaction between the Codes and other Australian laws to minimise the collection of personal data.
  - By implementing best practice approaches from comparable international jurisdictions, there can be greater regulatory parity which will enable stronger compliance by industry.

How do these Codes balance the need to protect children from online harm and their right to participate in the digital environment?

- eSafety believes that children's right to digital participation and their right to safety are mutually reinforced through sensible and age-appropriate protections, such as filtering out harmful content for child users.
- The measures set out in the Codes do not seek to restrict young people's access to online platforms and services. Instead, the Codes establish guardrails that support age-appropriate experiences to protect children from harmful material when they *are* online. For example:
  - Social media services and websites that do not allow pornography according to their own terms of service must implement systems designed to detect and

remove online pornography from the service, and they must improve these systems over time.

- Search engine services must have measures that prevent autocomplete predictions for searches from being sexually explicit or violent.
- Messaging services must give users the ability to block unwanted measures and leave unwanted group chats.
- App distribution services must have procedures to consider, and change if necessary, the age ratings of apps on the service.
- Services must give users the ability to report potential breaches of their terms and conditions.

How can we be sure that personal data held by services for the purpose of age assurance will be protected?

- Many services covered under the Phase 2 Codes are also required to abide by the Privacy Act, which was amended in December 2024 following the Privacy Act Review.
- The Code Head Terms expressly state that, in determining appropriate age assurance measures to adopt under the Codes, 'service providers must consider whether age assurance measures have been designed to comply with Privacy Laws and whether the impact on user privacy of any such measures for a service is proportionate to the online safety objectives specified in section 4 of [the Head Terms].'
- A guidance note in the Head Terms also notes that service providers 'should consider conducting a privacy impact assessment of any age assurance measures they implement, to assist with the service provider's assessment of both positive and negative privacy impacts of those measures and ensure any relevant privacy notices are given, and other steps are taken, as required by Privacy Laws.'
- The Office of the Australian Information Commissioner (OAIC) is the Australian privacy regulator and it is open to them to take action where applicable if they are satisfied that a company's personal data handling is non-compliant with Australian law. The OAIC is also in the process of developing the Children's Online Privacy Code which may establish further protections for children's data online. eSafety coordinates with the OAIC both bilaterally and via DP-REG. The OAIC was also consulted on the relevant aspects of the Phase 2 Position Paper, which eSafety published to inform industry's drafting of the Codes.

eSafety.gov.au