Request for Registration : Phase 2 Online safety codes submitted to Office of eSafety Commissioner on 28 February 2025

Submitted by:

Australian Mobile Telecommunications Association (AMTA)

Communications Alliance Ltd (CA)

Consumer Electronics Suppliers Association (CESA)

Digital Industry Group Inc. (DIGI)

Interactive Games and Entertainment Association (IGEA)

Contents

28 February 2025.

28 February 2025.

1. Drafts of Phase 2 of the Consolidated Industry Codes of Practice for the Online Industry (Class 1C and Class 2 Material) under section 140(1)(c) and 140(2) of the Online Safety Act 2021) submitted on 28 February 2025.

The five industry associations tasked with the development of the Online Safety Codes (the Codes) request that the eSafety Commissioner register the Consolidated Industry Codes of Practice for the Online Industry (Class 1C and Class 2 Material) under section 140(1)(c) and 140(2) of the Online Safety Act 2021.

For this purpose and accordance with the notices provided to the respective industry associations on 1 July 2024 (varied on 13 December 2024):

a. Communications Alliance Ltd (CA) and the Digital Industry Group Inc. (DIGI) submit the *Consolidated Industry Codes of Practice for the Online Industry (Class 1C and Class 2 Material) Head Terms* and *Schedule 1 – Social Media Services Online Safety Code (Class 1C and Class 2 Material)* to the eSafety Commissioner;

b. The Australian Mobile Telecommunications Association (AMTA), CA, DIGI and the Interactive Games and Entertainment Association (IGEA) submit the *Consolidated Industry Codes of Practice for the Online Industry (Class 1C and Class 2 Material) Head Terms* and *Schedule 2 – Relevant Electronic Services Online Safety Code (Class 1C and Class 2 Material* to the eSafety Commissioner for consideration for registration;

c. AMTA, the Consumer Electronics Suppliers' Association (CESA), CA and DIGI submit the *Consolidated Industry Codes of Practice for the Online Industry (Class 1 C and Class 2 Material) Head Terms* and *Schedule 3 – Designated Internet Services Online Safety Code (Class 1C and Class 2 Material)* to the eSafety Commissioner;

d. DIGI and CA submit the *Consolidated Industry Codes of Practice for the Online Industry (Class 1C and Class 2 Material) Head Terms* and *Schedule 5 – Hosting Services Online Safety Code (Class 1C and Class 2 Material)* to the eSafety Commissioner;

e. CA submits a draft of the *Consolidated Industry Codes of Practice for the Online Industry (Class 1C and Class 2 Material) Head Terms* and *Schedule 6 – Internet Carriage Services Online Safety Code (Class 1A and Class 1B Material)* to the eSafety Commissioner;

f. DIGI, AMTA, CA and IGEA submit the *Consolidated Industry Codes of Practice for the Online Industry (Class 1C and Class 2 Material) Head Terms* and *Schedule 7 – Equipment Online Safety Code (Class 1C and Class 2 Material)* to the eSafety Commissioner; and

g. CA and DIGI submit the *Consolidated Industry Codes of Practice for the Online Industry (Class 1C and Class 2 Material) Head Terms* and *Schedule 8 – Internet Search Engine Services Online Safety Code (Class 1C and Class 2 Material)* to the eSafety Commissioner.

In this document we refer to these codes collectively as "draft Phase 2 Codes" or simply as "the Codes".

Additionally CA, DIGI and IGEA will submit a draft of t*he Consolidated Industry Codes of Practice for the Online Industry (Class 1C and Class 2 Material) Head Terms and Schedule 4 – App Distribution Services Online Safety Code (Class 1C and Class 1B Material)* on or before March 28

28 February 2025.

2025 in accordance with the variation of the s141notice received by the associations on 27 February 2025.

2. Purpose of the document

This document forms part of the suite of documents submitted to the Office of the eSafety Commissioner:

1. Request for Registration of Phase 2 Online Safety Codes including Annexures 1- 2 (this document);
2. Summary of industry response to submissions to the public consultation (October 2024);
3. Records of two separate roundtable discussions,one with industry stakeholders and the other with expert stakeholders conducted as part of the public consultation process;
4. Industry Response to eSafety feedback on Head Terms and Phase 2 Codes; and
5. Consolidated Industry Codes of Practice for the Online Industry (Class 1C and Class 2 Material) (consisting of the nine parts, i.e., Head Terms and 8 Schedules, as listed above (in PDF, Word versions together with a mark-up version changes made since 19 December 2024)

The purpose of this document is to assist the Office of the eSafety Commissioner evaluate whether the draft Phase 2 Codes satisfy the criteria for registration under the Online Safety Act 2021 (Cth) (OSA).

3. Background and current regulatory arrangements

Under the OSA, which commenced on 23 January 2022, the eSafety Commissioner can request industry bodies to develop codes for class 1 and class 2 material across eight sections of the online industry. The OSA defines class 1 and class 2 material by referring to the National Classification Scheme (NCS). Section 134 of the Online Safety Act 2021 (OSA) contains a statement of regulatory policy which expresses Parliament's intention that representative industry associations ought to develop codes that are to apply to the respective industry sections in relation to the activities of the participants within those respective sections. If these codes meet the statutory requirements, the Commissioner can register them, making them binding on all industry participants. If a code fails to meet these requirements, eSafety can develop an enforceable industry standard for that section of the online industry instead, to ensure appropriate protections are in place for the community.

The development of codes and standards under the OSA has progressed in two phases. In September 2021, eSafety published an initial position paper (September 2021 Position Paper) to guide the industry in developing the first phase of codes (Phase 1 Codes). These codes apply to 'class 1' material, such as child sexual exploitation and pro-terror content. In April 2022, the eSafety Commissioner issued notices to six industry bodies requesting they develop the Phase 1 Codes. The industry-developed Phase 1 Codes for five industry sections (social media services, app distribution services, equipment, hosting service providers and ISPs) were registered in June 2023 and came into effect in December 2023. A sixth industry code for search engine services was registered in September 2023 and came into effect in March 2024. Following the Commissioner's decision not to register the remaining two codes for relevant electronic services and designated internet services, eSafety developed standards for those industry sections, which were registered in June 2024 and took effect in December 2024. Following the finalisation of the Phase 1 Codes and Standards, on 1 July 2024 the eSafety Commissioner issued section 141 Notices to five of the six industry bodies (Notice Recipients) involved in drafting the Phase 1 Codes, requesting they begin drafting the Phase 2 codes. The notices request the relevant industry associations to develop a code or codes that deal with matters in similar terms to the following:

28 February 2025.

> *1. Protect and prevent children in Australia from accessing or being exposed to class 1C and class 2 material.*
>
> *2. Provide end-users in Australia with effective information, tools and options to limit access and exposure to class 1C and class 2 material.*

The notices required that that relevant industry associations submit draft codes to eSafety for final consideration by 19 December 2024 (Phase 2 Codes). The eSafety Commissioner published a supplementary position paper that outlined eSafety's expectations for developing Phase 2 Codes (**July 2024 Position Paper**) and included suggested measures.

The s141 notices were varied by the Commissioner on 13 December 2024 to require that the Notice Recipients:

1. By 4.00pm AEDT on 19 December 2024, provide to the Commissioner:
    - copies of the submissions received by the Notice Recipients, during the course of the legislatively mandated public consultation period which concluded on 22 November 2024 (noting submissions may be redacted or withheld on the basis of any confidentiality claims),
    - any summary of the submissions prepared by the Notice Recipients, which may be available, and
    - a second preliminary draft of each code.
2. provide the Commissioner with a copy of the code by 4.00pm AEDT Friday 28 February 2025.

4. Outline of Phase 2 Codes development process

Since receipt of s141 notices, a Steering Group of five industry associations formally formed and engaged with eSafety on the development of the Phase 2 Codes. Those associations are:

a. *Australian Mobile Telecommunications Association (AMTA),*
a. *Communications Alliance Ltd (CA),*
b. *Consumer Electronics Suppliers Association (CESA),*
c. *Digital Industry Group Inc. (DIGI), and*
d. *Interactive Games and Entertainment Association (IGEA).*

In addition, under the guidance of the Steering Group, industry has formed several working groups to draft the Codes.

To ensure broad coverage within and across all relevant industry sections, the industry associations reached out to members and non-members of their organisations and invited participation (free of charge, no membership requirement) in the Codes development process. See Annexure 2 for a list of companies that directly contributed to the drafting of the Codes.The Steering Group and eSafety have also engaged in meetings to discuss development of the Codes. eSafety has also provided industry with written feedback on the Codes. Industry's response to that feedback is set out in a separate document.

Part 6, 7 and 8 of this document sets out the criteria for registration and how industry has addressed the criteria in the process of developing the draft Codes, including the measures contained in each Code. Where appropriate, the respective positions of eSafety in the eSafety July 2024 Position Paper, and written feedback are also referenced.

28 February 2025.

5. Other regulatory initiatives that impact Phase 2 Codes development process

Industry notes that since the eSafety Commissioner issued the s141 notices there have been additional policy developments at a Federal level that impact on the development of the Phase 2 Codes, including the amendment of the OSA , passed on 29 November 2024, that requires in-scope 'age-restricted social media platforms', to prevent Australians under the age of 16 from having an account[1]. Part of the rationale for these amendments is to address the risk that young people that hold an account on certain services will be exposed to harmful materials of the kind in scope of the Phase 2 Codes[2]. The Government is currently conducting a targeted consultation on draft Online Safety Rules that enable certain services to be excluded from the social media minimum age obligation in the amended OSA. We note that the Government has proposed that certain services such as messaging services will be excluded from the age restrictions in section 63D of the OSA[3]. This is relevant to the approach industry has adopted for RES services as discussed in section 7.8.3 below.

6. Representation of industry by industry associations.

Part 6 of this document explains how the Phase 2 Codes meet the criteria for registration of codes in the OSA as pertains to representation of the industry by those industry associations.

6.1. Representation of sections of the industry by associations [OSA, section 140(1)(a)]

On 1 July 2024 the eSafety Commissioner gave notice to the five industry associations to develop industry codes pursuant to section 141 of the OSA. The industry associations each received notices to develop industry codes that apply to participants in the online sections as per the table in section 6.2 below.

By giving notice to the five industry associations pursuant to section 141 of the OSA, the eSafety Commissioner expressed satisfaction that these associations represent the respective sections of the industry for which they have received the notices. All sections of the industry that the OSA seeks to cover through industry codes as listed in section 135 of the OSA were represented by at least one of the industry associations that received the notices. In addition, the industry associations consulted with representatives of the porn industry, including via a roundtable also attended by eSafety representatives on 12 September 2024.

[1] section 63D of the *Online Safety Act 202*1(Cth)(OSA).

[2] See references to exposure of young people to drug abuse, suicide or self-harm, and unhealthy eating habits and violent and gory material in the rationale for the restrictions for age restricted social media : *Impact Analysis Equivalent Supplementary Analysis OIA24-08210: Social Media Age Limit,* October 2024 and Michelle Rowalnds MP *We all have a role to play in keeping our kids safe online,* Sunday Telegraph, 8 September 2024

[3] *Exposure Draft Online Safety (AgeRestricted Social Media Platforms) Rules* 2025.

6.2. Industry associations to develop Codes that apply to participants in the respective sections and deal with matters relating to activities of those participants [OSA, section 140(1)(b)]

The five industry associations have developed seven draft industry codes applicable to the participants of the respective industry sections that deal with the online activities (as listed in section 134 of the OSA) of their members and of the industry sections they represent as per the notices given by the eSafety Commissioner.

Those Codes are (contained in the *Consolidated Industry Codes of Practice for the Online Industry (Class 1C and Class 2 Material*) submitted with this Request for Registration:

Title	**section of the online industry to which the code applies**	**Industry association representative as per s141 notice**
Social Media Services Online Safety Code (Class 1C and Class 2 Material)	Providers of social media services, so far as those services are provided to end-users in Australia	● Communications Alliance (CA) ● Digital Industry Group Inc. (DIGI)
Relevant Electronic Services Online Safety Code (Class 1C and Class 2 Material)	Providers of relevant electronic services, so far as those services are provided to end-users in Australia	● Australian Mobile Telecommunications Association (AMTA) ● CA ● DIGI ● Interactive Games and Entertainment Association (IGEA)
Designated Internet Services Online Safety Code (Class 1C and Class 2 Material)	Providers of designated internet services, so far as those services are provided to end-users in Australia, but excluding OS providers (as defined in Schedule 8)	● AMTA ● Consumer Electronics Suppliers' Association (CESA) ● CA ● DIGI [Note IGEA has been now removed from this notice].
Hosting Services Online Safety Code (Class 1C	Providers of hosting services, so far as those services host material in Australia	● DIGI ● CA

28 February 2025.

Title	section of the online industry to which the code applies	Industry association representative as per s141 notice
and Class 2 Material)		
Internet Carriage Services Online Safety Code (Class 1C and Class 2 Material)	Providers of internet carriage services, so far as those services are provided to customers in Australia	• CA
Equipment Online Safety Code (Class 1C and Class 2 Material)	Persons who manufacture, supply, maintain or install equipment that is for use by end-users in Australia of a social media service, relevant electronic service, designated internet service or internet carriage service (in each case in connection with the service) Operating system providers (as defined in the Equipment Online Safety Code (Class 1C and Class 2 Material))	• AMTA • CA • CESA • DIGI • IGEA
Internet Search Engine Services Online Safety Code (Class 1C and Class 2 Material)	Providers of internet search engine services, so far as those services are provided to end-users in Australia	• CA • DIGI

The Codes deal with matters listed as examples that may be dealt with by industry codes and standards under section 138(3)(a) to (zj) of the OSA and in Schedule A of the s141 notices given to industry associations by eSafety on 1 July 2024.

On 28 March 2025 the three associations listed below will submit the remaining code:

App Distribution Services Online Safety Code (Class 1C	Providers of app distribution services, so far as those services are provided to end-users in Australia	• CA • DIGI • IGEA

28 February 2025.

and Class 2 Material)		

7. Criteria for registration concerning substance of Phase 2 Codes

This part 7 sets out how the substantive terms of the documents comprising the Consolidated Industry Codes of Practice for the Online Industry (Class 1C and Class 2 Material) (including the measures contained in each Code), meet the requirements for registration of the Codes in the OSA.

7.1. To the extent the Codes deal with matters of substantial relevance to the community, the Codes are to provide appropriate community safeguards for those matters [OSA, section 140(1)(d)(i)]

The section 141 notices stipulate that the Codes contain community safeguards that :

Matter 1

Protect and prevent children in Australia from accessing or being exposed to class 1C and class 2 material.

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.

Industry submits that the seven Phase 2 Codes (and Head Terms) provided to the Commissioner with this Request for Registration provide appropriate community safeguards for the matters specified in the s141 notices in relation to each industry section that is the subject of a section 141 notice in the manner explained in the remaining sub sections of this section 7. This document will be updated and resubmitted when the App Distribution Services Online Safety Code (Class 1C and Class 2 Material is submitted on 28 March 2025.

7.2. Structure

The Head Terms contain common terms that apply to each industry Code. The seven schedules for each industry section outline the specific measures for those services and equipment in scope of each industry section, together with relevant guidance concerning the application of measures. The seven schedules together with the Head Terms comprise Consolidated Codes of practice for the Online Industry (Class 1C and Class 2 Material).

This structure follows the approach of the Consolidated Codes of practice for the Online Industry (Class 1A and Class 1B Material). This approach is consistent with eSafety's advice in the July 2024 Position paper that foundational issues, including drafting principles and the general structure of the Codes, can be adapted from Phase 1. In addition, we have had regard to the Standard for Relevant Electronic Services and the Standard for Designated Internet Services in devising appropriate measures for the codes relating to social media services, relevant electronic services and designated internet services.

28 February 2025.

7.3. Key Terms

The Phase 2 Codes largely adopt the approach of the Phase 1 Codes with some key changes. Please see the table below which explains these changes.

7.4. Age assurance

7.4.1. Inputs into industry's approach to age assurance

The approach taken to age assurance under these Codes have been informed by the July 2024 Position Paper but also the foundational work carried out by eSafety in developing the *Roadmap for age verification and complementary measures to prevent and mitigate harms to children from online pornography*[4] (the Roadmap), eSafety's research into young people's encounters with pornography online: *Accidental, unsolicited and in your face. Young people's encounters with online pornography: a matter of platform responsibility, education and choice* September 2023 (eSafety research), the Government response to the Roadmap for Age Verification August 2023 (the Government Response) and eSafety's Tech Trends Issues Paper Age assurance, July 2024 .

In the Roadmap, eSafety recommended that the Australian Government develop, implement, and evaluate a cross-government trial of age assurance technologies in Australia before mandating their use. However, the Government Response raised key concerns with implementing age assurance in Australia:

> *It is clear from the Roadmap that at present, each type of age verification or age assurance technology comes with its own privacy, security, effectiveness and implementation issues. For age assurance to be effective, it must:*
>
> *• work reliably without circumvention;*
>
> *• be comprehensively implemented, including where pornography is hosted outside of Australia's jurisdiction; and*
>
> *• balance privacy and security, without introducing risks to the personal information of adults who choose to access legal pornography.*
>
> *Age assurance technologies cannot yet meet all these requirements. While industry is taking steps to further develop these technologies, the Roadmap finds that the age assurance market is, at this time, immature. The Roadmap makes clear that a decision to mandate age assurance is not ready to be taken*[5].

The Government has now decided to implement an age assurance trial encompassing both age verification and age estimation technologies, to explore their efficacy in protecting children from encountering pornography and other high-impact online content.The Trial is being conducted on a voluntary basis. Interested parties are invited to submit Expressions of Interest in submitting age assurance solutions to be considered as part of the trial. As of 20 February, 60 Expressions of Interest have been submitted, the majority of which are for solutions offered by third-party vendors. As far as we are aware some measures of age assurance contemplated by industry in developing these Codes are not being tested by the trial and some age assurance solutions subject to the trial have not been used operationally for many services subject to these Codes[6]. The testing for the trial will occur in a laboratory environment, using a hypothetical online social media platform. As explained in the Evaluation Proposal:

> *The Age Assurance Technology Trial is not designed to develop new technologies or tools for age assurance. Instead, it focuses on assessing existing systems and their practical applications. It is not creating a comparative league table of technologies to rank their performance, nor is it focused on approving or certifying specific technologies for*

[4] eSafety Commissioner, *Roadmap for age verification and complementary measures to prevent and mitigate harms to children from online pornography,* (March 2023).
[5] *Government response to the Roadmap for Age Verification, August 2023*.
[6] https://ageassurance.com.au.

> *compliance or endorsement. The trial does not aim to prescribe specific methods or mandate their use in regulatory frameworks.*
>
> *Furthermore, the trial is not setting industry standards or defining universal benchmarks for age assurance performance. It does not evaluate the commercial viability of these systems, assess their business models or provide a comprehensive policy recommendation for deployment, although the outcome of the trial may assist policy makers, such as the eSafety Commissioner for Australia, to make evidence-based, informed policy decisions.*
>
> *The trial's goal is to gather structured, scientific and impartial evidence on the effectiveness, usability and limitations of current technologies. This is to inform future research, development, policy, guidance and guidelines as to how the technologies could effectively work in practice to help Australia achieve its policy and online safety objectives.*[7].

Industry has been asked to develop commitments in the Phase 2 Codes in advance of the conclusion of the Age Assurance Trial.The July 2024 Position paper says that the Codes will determine when and where age assurance should be implemented, whereas the outcomes of the Age Assurance Trial *may* support industry with' the how of age assurance' (e.g., by informing what reasonable and appropriate steps for compliance may be best within the Australian context). Based on the above statement of the scope of the Trial, it appears that the trial will not directly inform industry as to how to implement age assurance. While we understand that following the conclusion of the Age Assurance Trial, eSafety will be developing guidance around how age restricted social media platforms can comply with section 63D of the OSA. It is unclear when this guidance will be released and if it will be extended to the implementation of age assurance more broadly under the Phase 2 Codes or otherwise, given the range of services caught by the Phase 2 Codes is broader and more complex than those under other legislation.

7.4.2. Regulatory developments related to age assurance

There are also many other developments related to age assurance that are underway domestically (such as progress on digital identity) and internationally[8] including the recent release in Singapore by the Infocomm Media Development Authority of the new Code of Practice for Online Safety for App Distribution Services[9].

While there are a range of online services that are using age assurance for limited jurisdictions or limited services to date there is, as eSafety acknowledges, limited independent or regulatory assessment of their appropriateness[10]. It is hoped that international standards will provide a useful framework for understanding and evaluating the different levels of assurance offered by age assurance providers and facilitating the development of interoperable solutions. The finalisation of this standard is, however, likely to take some years.

7.4.3. User's digital rights

While the primary aim of the Phase 2 Codes is to protect children online from class 2 and class 1C materials online as set out in the section 141 notices, industry has been concerned to minimise the risk that any age assurance measures in the Codes negatively impacts users' digital rights. In particular, the industry has considered how to best address the additional privacy and security risks to end-users that may flow from the collection by service providers of personal data needed to satisfy age assurance requirements in the Codes. In this respect, it should be noted that these risks will vary amongst different services. For example, some service providers currently collect and therefore have the ability to utilise behavioral data of users' on-platform behaviors to estimate users' age. However, not all service providers in scope of the codes currently collect this data and may need to rely on other forms of personal identification. Additionally, the OSA has now been amended to restrict the sole reliance by age restricted social

[7] Dr Asad Ali, Dr Koliya Wedanage, Adrian Ugray, George Billinge, Dr Mark Pedersen, Surya Ramessh, *Age Assurance Technology Trial* , Evaluation Proposal p 12.
[8] See *July 2024 Position Pape*r pp 41-45.
[9] IMDA, *Code of Practice for Online Safety for App Distribution Services*, January 15, 2025
[10] eSafety, *Tech Trends Issues Paper Age assurance*, July 2024 p.7.

28 February 2025.

media platforms of government issued IDs (including digital ID within the meaning of the *Digital ID Act 2024*) in order to comply with section 63 D of the OSA[11].

Industry has also considered the need to ensure that implementation of age assurance by relevant service providers does not negatively impact on the digital rights of the child including rights guaranteed under the United Nations convention on the Rights of the Child[12] as further elaborated upon in General Comment 25 [13].

7.4.4. Need for flexibility in implementing age assurance measures

The Position Paper establishes that eSafety's intent is to offer "the flexibility to implement measures that best suit [each company's] business models and technologies"[14]. Industry has received various suggestions from eSafety, both from the July 2024 Position paper and in meetings and written feedback about how industry might approach the question of age assurance in the Phase 2 Codes on a range of different services types including email services, search engines, and ISP's, in circumstances where many of these have not been tested for the range of materials in scope of the Phase 2 Codes.

The Position paper suggests that age assurance measures could be applied through centralised user accounts in 'ecosystems' of online products and services and that age assurance on an online service should' ideally be interoperable with other online services to the extent possible'.[15] Given the current immature state of age assurance technology and rapid developments in the sector, industry believes that at this time it is better to preserve flexibility in how to require service providers to introduce age assurance in Australia. For example, different companies may differ in their views about whether age assurance should occur upfront, or at the point of a user attempting to access class 2 material. Due to the difference in business models, products and technologies between companies, it is not currently possible for industry to prescribe an effective uniform approach that sets obligations on centralised accounts or to require that age assurance solutions are interoperable, in the short time frame allowed for development of these Codes.

As noted above, the Federal parliament has now considered the extent young people should be restricted from accessing services online and has passed legislation that limits under 16 year olds from holding an account on an 'age restricted social media platforms' under section 63D of the OSA(in part because of concerns of the exposure of young people to harmful content of the types in scope of the Phase 2 Codes)[16].

With these considerations in mind,for the purpose of addressing the matters in the s141 notices we have primarily focused on restricting access to the content in scope of the Codes rather than entire devices or services. Nonetheless, we have endeavoured to draft the Codes in a way that does not preclude the introduction of additional age assurance approaches in future. The Codes seek to apply a layered set of protections at every stage of the tech stack – including obligations for app marketplaces, devices, ISPs and other categories of services – that provide a meaningful uplift in preventing underage access to inappropriate content.

7.4.5. Material in scope of Phase 2 Codes

The material in scope of the Phase 2 Codes is also a complicating factor in devising an appropriate approach to age assurance. The scope of materials within these Codes is much broader than 'pornography' (the subject of the Roadmap and the Government's response to the Roadmap) and is based on the National Classification Scheme. During the development of the

[11] see section 63 DA of OSA.
[12] UN General Assembly, "Convention on the Rights of the Child," 1989, Available: https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child
[13] UN Committee on the Rights of the Child, "General comment No. 25 (2021) on children's rights in relation to the digital environment," CRC/C/GC/25, 2021. Available: https://digitallibrary.un.org/record/3906061/files/CRC_C_GC_25- EN.pdf
[14] *July 2024 Position paper* p.72.
[15] *July 2024 Position paper* p. 83.
[16] n2.

28 February 2025.

Phase 1 Codes industry advised eSafety of the difficulties of managing online content based on the National Classification Scheme which was developed for classifying individual items of professionally produced content before commercial release to the public. The classification process requires nuanced , context based judgments of materials, which is challenging to implement at scale because of the vast range and diversity of online material. These difficulties are magnified in the case of class 2 materials which are lawful for adults, but unsuitable for children.

7.4.6. Approach to age assurance adopted by Phase 2 Codes.

Following the suggestions in the July 2024 Position paper and additional feedback received from eSafety as part of the Phase 2 Code development process, we have attempted to identify 'high priority content types' to make the management of age restrictions and other measures practically feasible (see section 1. Head Terms below).

Industry considers that the best way to navigate these complexities at this time is to take a realistic approach to drafting measures that require age assurance on these Codes, with requirements on age assurance measures being imposed on those content providers who provide access to the highest risk categories of material and able to determine the extent that materials are in scope of the Phase 2 Codes and therefore should be subject to an age-gate. Based on our assessment of the risks, technical feasibility and taking into account the Government's concern about user privacy and security our approach generally is that:

a. certain providers who make *high-priority content* available on their service, or whose sole or primary purpose is in respect of such material, must restrict access to under 18 year old users;

b. certain providers who restrict high priority content and meet certain criteria must implement other measures aimed at preventing under 18 year old users from accessing this content;

c. providers of internet search engine services must implement settings by default to protect under 18 year old account holders from exposure in search results;

d. certain providers such as email, sms and mms, and private communication services should not be subject to age assurance requirements for privacy and security reasons but must implement other measures that for example, limited users exposure to unsolicited high priority materials. This is consistent with the approach taken by the Government The eSafety Youth Advisory Council has advised that it does not consider age assurance appropriate for private messaging[17]. We also note the implications for digital child rights – including access to information and ability to connect and communicate with family and friends – could be significantly impacted by more interventionist requirements on private communication services.

We note that the industry has yet to finalise the approach it will take for app distribution services.

Industry has not prescribed how age assurance must be implemented, considering that at this time it is preferable to preserve flexibility for different services to determine the method that is most suitable for their business models and technologies[18]. However, we have set out a variety of practical and realistic methods, based on our experience to date. This approach allows for future advances in relevant technologies and is largely consistent with the approach emerging in the United Kingdom and outlined in the *Guidance on age assurance and other Part 5 duties for service providers publishing pornographic content on online services* published 5 December 2023 and the d*raft Protection of Children Code of Practice for user-to-user services published* on 17 July 2024 (Ofcom Online Safety Code).

[17] eSafety Youth Advisory Council, *Submission to the Joint Select Committee on Social Media and Australian Society*, 2024.
[18] n11.

28 February 2025.

7.5. Overlapping activities by industry participants

It should be noted that consistent with the Phase 1 Codes, the Phase 2 Codes do not include specific measures for first party hosting services or first party app distribution services. The first party hosting of a service by a provider of a service such as the hosting of a social media service by the provider of a social media service is covered by the Code that governs the underlying service, i.e., in the case of social media, the Code comprising the Head Terms and Schedule 1. Similarly, a first party app such as an app that grants access to a social media service is not the subject of additional measures beyond those that apply to its use or distribution.

7.6. Head Terms

The table below explains the key changes and additions to the Phase 1 Codes that are contained in the Phase 2 Head Terms. We have also provided a mark-up of changes from the Phase 1 Head Terms.

Ongoing commitment to work on age assurance.	Section 1.3 contains a new commitment that acknowledges that different sections of the online industry will have different age assurance capabilities, which may change over time as technology develops. It makes clear that all industry participants will continue to look for ways to collaborate and contribute proactively to prevent and address harms arising from the material covered by this Code, through age assurance. *eSafety has acknowledged that ongoing international dialogue is critical to resolving the challenges associated with global interoperability, privacy, and technical thresholds[19]. Industry is similarly committing in these Codes to continuing a nuanced dialogue with regulators, and other key stakeholders both here and internationally on how age assurance and complementary measures, can be implemented in a safe, secure and privacy preserving way that is both child's-rights respecting and effective.*
Definitions of age assurance and access control measures	**Please note the introduction of the following new definitions in section 2:** **access control measures** means appropriate access controls designed to prevent an Australian end-user who has been identified as a child (via age assurance measures implemented for a relevant service) from proceeding to access the relevant service, the relevant material, or the relevant section of the service as specified in this Code. **age assurance** is an umbrella term for a range of methods for assessing a user's age, including both age verification solutions (being solutions that aim to verify the exact age or age range of a given user) and age estimation solutions (being solutions that aim to estimate the exact age or age range of a given user). *The introduction of these definitions is consistent with the Ofcom approach to implementing age assurance measures, recognition that age assurance needs to be combined with access control measures to effectively prevent users under 18 from accessing age-in-appropriate content online.*
Definitions of material categories	**Section 2 defines various categories of materials dealt with by the Codes in different ways:**

[19] *Age assurance Issues Paper* p. 21.

	class 1C material is a subcategory of class 1 material used for the purpose of this Code that: (a) is class 1 material because it describes or depicts specific fetish practices or fantasies; but (b) excludes class 1A material. **class 2A material** is a subcategory of class 2 material defined for the purposes of this Code as being comprised of material that is a film, the contents of a film, or material that for the purposes of this Code is otherwise to be treated in a corresponding way to the way in which a film would be classified under the Classification Act that: (a) is classified X 18+ under the Classification Act; or (b) has not been classified, but if it were to be classified under the Classification Act, it would likely be classified X 18+, because it depicts actual (not simulated) sexual activity between consenting adults. *Note this definition is essentially intended to capture what is most usually understood to be pornography, excluding class 1C materials.* **class 2B material** is a subcategory of class 2 material defined for the purposes of this Code as being comprised of material that: (a) is class 2 material because it depicts high-impact sexually explicit material (including high impact nudity); but (c) excludes class 2A material. *Note this definition is intended to allow a distinction to be drawn between pornography and other types of high impact nudity such as may form a small excerpt of a film or be described in a written publication. This type of material will not necessarily be pornographic in nature. We are of the view that certain types of measures are not appropriate for this material e.g. detection of this material on communication services as they would likely result in over-blocking, and could for example include news footage, historical footage, research and educational materials.* **high impact online pornography** means class 1C and class 2A material. **high-impact violence material** means class 2 material comprised of material that depicts shocking, gratuitous or exploitative real images, or images that are presented as if they are real, of violence against people or animals and/or gore. **high-priority restricted category** of material means high impact online pornography and self-harm material.

	online pornography means class 1C, class 2A and class 2B material. **self-harm materia**l is a subcategory of class 2 material defined for the purposes of this Code as being comprised of material that is class 2 material because it encourages,promotes or provides instruction for: (a) suicide; (b) an act of deliberate self-injury; and/or (c) an eating disorder or behaviour associated with an eating disorder. **simulated gambling material** is a subcategory of class 2 material defined for the purposes of this Code because it is a computer game that contains simulated gambling and is classified, or would be classified, R 18+ under the Classification Act. *Together this suite of definitions are designed to enable the Codes to deal with different categories of content in a manner that is proportionate to the harm they pose to users under 18. Please note the introduction of definitions of self-harm material, simulated gambling material and class 2A material are intended to capture the range of 'high priority' content that the July 2024 Position paper suggests should be subject to the most stringent measures, in a way that as far as possible is harmonised with the approach taken by Ofcom in the UK in the Ofcom Online Safety Code. This approach is designed to promote harmonisation and interoperability with the UK approach as recommended by the July 2024 Position paper. Please note we have also intended to simplify the drafting of different categories of materials by removing Annexure A of the Phase 1 Codes.*
Online safety objectives	**We have added in a new section 4 which outlines the following safety objectives:** **(a) Objective 1:** Protect and prevent children in Australia from accessing or being exposed to class 1C and class 2 material. **(b) Objective 2:** Provide Australian end-users with effective information, tools and options to limit access and exposure to class 1C and class 2 material. *This section was introduced to align with the matters in the section 141 notices and assist with structuring the measures in the Codes.*
appropriate age assurance	**section 5.1(c) outlines what are 'appropriate age assurance measures" under the Phase 2 Codes:** In determining appropriate age assurance measures for the purpose of this Code: (i) service providers should take into account the technical accuracy, robustness, reliability and fairness of the solution for implementing the measure;

	(ii) appropriate age assurance measures must include reasonable age assurance measures to help the provider to identify whether an Australian end-user is a child; (iii) 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 this Code; *These requirements are intended to reflect that age assurance solutions and approaches are currently at an immature stage of development and to address some of the concerns outlined by the government in its Response.*
Examples of 'appropriate age assurance measures"	**section 5.1(c) (vii) gives examples of 'appropriate age assurance measures' under the Phase 2 Codes:** examples of age assurance measures that will be considered appropriate for the purposes of this Code include: (A) matching of photo identification; (B) facial age estimation; (C) credit card checks; (D) digital identity wallets or systems; (E) attestation by a parent of age or whether an Australian end- user is a child; (F) other measures meeting the requirements of section 8 (Confirmation of age) of the Online Safety (Restricted Access Systems) Declaration 2022; and (G) relying upon appropriate age assurance measures implemented in respect of the relevant end-user by: (1) another party (whether another industry participant, a third party vendor or another third party) and confirmed by an age signal or other mechanism provided to the service provider by that other party; or (2) the service provider in respect of another service (where the relevant end-user has agreed for age assurance signals or settings to be shared between the services, such as by associating both services with a centralised account), *These examples are largely analogous to the Guidance on age assurance and other Part 5 duties for service providers publishing pornographic content on online services published 5 December 2023. These examples also reflect industry's experience with these technologies to-date but are, however, non exclusive to allow for advances in relevant technologies in the future.*
Examples of age assurance measures that are not appropriate	**section 5.1(c) (viii) gives examples of age assurance measures that are not appropriate under the Phase 2 Codes:** Examples of age assurance measures that will not be considered appropriate for the purposes of this Code services include: (A) requiring a user to self-declare their own age or whether the user is a child (without more); and

	(B) contractual restrictions on the use of the relevant service by children (without more). *Note we have had regard to eSafety's views that age declaration is not appropriate as an age assurance method. For example, if users provide false birth dates when accessing a site or setting up an account, and services only rely on this information, these safety measures may not be enabled or effective*[20].
Privacy impact assessments	The July 2024 Position paper suggests that Industry participants should consider conducting a privacy impact assessment of any age assurance measures adopted, to assist with their assessment of both positive and negative privacy impacts of any measures. Guidance to this effect has been included in the Head Terms. This seeks to ensure that helpful guidance regarding relevant privacy considerations (as flagged in the Position Paper) is given to industry participants, whilst maintaining the regulatory distinction between the OSA and the Privacy Act (so that privacy obligations continue to sit under the Privacy Act, avoid regulatory overlap or inconsistency). As noted in the Position Paper, the ongoing rolling reform of Australian privacy law including the new *Privacy and Other Legislation Amendment Act 2024* (which, amongst other things, introduced a statutory tort for serious invasions of privacy, provisions regarding a Children's Online Privacy Code and obligations regarding use of personal information for automated decision making) may also impact the implementation and use of age assurance measures by organisations and how information may be used in connection with that. In particular, there is a likely intersection between the Phase 2 Codes and the forthcoming Children's Online Privacy Code to be developed by the OAIC.
Reports relating to technical feasibility and practicability	**Section 5.2 (c) sets out actions to be taken where mandatory compliance measures are not technically feasible:** **Step 3: Reports relating to technical feasibility and practicability** If requested in writing to do so by eSafety, the industry participant must give to eSafety, within a reasonable period, a report: (i) that describes: (A) the cases in which it was not, or would not, be technically feasible; or (B) the cases in which it was not, or would not, be reasonably practicable, for the industry participant to implement a compliance measure identified in the Schedule involving systems or technologies of a particular kind; and (ii) to the extent that there are alternative actions that are technically feasible and reasonably practicable for the industry participant, that describes the alternative actions taken by the industry participant. The report must provide justification for the actions described, and the conclusions, in the report.

[20] *Age Assurance Issues Paper* p.5.

	Similar to the approach in the Designated Internet Services Standard and the Relevant Electronic Services Standard, there are some measures which are required to be implemented subject to 'technical feasibility'. This recognises that not all services will be technically capable of meeting certain measures. In those cases they must justify its conclusions to the eSafety Commissioner, consistent with the recommendations in the July 2024 Position paper.

7.7. Schedule 1 Social Media Services Online Safety Code (Class 1C and Class 2 Material)

7.7.1. Code structure

This Code comprises the Head Terms and Schedule 1, covering providers of social media services as defined in the OSA.

The following table maps each compliance measure in the *Social Media Services Online Safety Code (Class 1C and Class 2 Material)* against the two online safety objectives issued by eSafety. This table maps each measure against the online safety objective it is primarily aimed at meeting. However, many of the compliance measures in this Code contribute to meeting more than one objective. As such, the table should be read as guidance only.

Objective	Compliance measure
Objective 1 **Protect and prevent children in Australia from accessing or being exposed to class 1C and class 2 material.**	7.1, 9.1, 10.1, 10.2, 10.3, 10.4
Objective 2 **Provide Australian end-users with effective information, tools and options to limit access and exposure to class 1C and class 2 material.**	7.2, 7.3, 8.1, 8.2, 8.3, 9.3, 9.4, 9.5, 9.6, 9.7, 9.8, 10.5, 10.8, 10.9, 10.11
Other supporting compliance measures	7.4, 8.4, 9.2, 9.9, 9.10, 9.11, 9.12, 9.13, 9.14, 10.6, 10.7, 10.10, 10.12, 10.13, 10.14, 10.15, 10.16, 10.17, 10.18

7.7.2. Services that allow online pornography, self-harm material or high-impact violence material

If the posting of online pornography, self-harm material or high-impact violence material is allowed under the applicable terms of use for the social media service, then the service provider will need to comply with compliance measures as set out in clause 6 and the table in clause 7. The service provider will also need to comply with certain general supporting compliance measures, as set out in the table in clause 9.

7.7.3. Services that do not allow online pornography, self-harm material or high-impact violence material

If the posting of online pornography, self-harm material or high-impact violence material is not allowed under the applicable terms of use for the social media service, then the service provider must assess the risk that an Australian child will access or be exposed to such material on the service. Based on the risk assessment, the service provider will need to comply with compliance measures for the relevant category of material as set out in clause 6 and the table in clause 8. A service provider with a Tier 1 or Tier 2 risk profile will also need to comply with certain general supporting compliance measures, as set out in the table in clause 9.

This approach is intended to ensure that the measures for social media services are proportionate to the risk that young people will encounter restricted material on the service and to reflect that the nature of the measures to be implemented by a service provider may differ depending on whether or not material is allowed on a service.

7.7.4. Approach to risk assessment

The approach to risk assessment, departs from the approach of the Phase 1 Codes in that only service providers that prohibit online pornography, self-harm material or high-impact violence material are required to do a risk assessment and provide a risk rating in respect of that prohibited category. Note that the methodology that must be used for a risk assessment has been updated from the Phase 1 Code and includes consideration of any generative AI features on a service (cl 4.3 (a)).

7.7.5. Services automatically accorded a Tier 3 or Tier 1 status

Consistent with the Phase 1 Codes:

- a limited category of social media services are automatically accorded Tier 3 status. This exception is intended to reduce the compliance burden on services that are clearly low risk; and
- providers of social media services who notify eSafety on or before the date that the Code comes into effect that they have a Tier 1 risk profile. This exception is to encourage services to proactively notify eSafety that they have a Tier 1 risk profile, providing clarity to the eSafety of these services' status.

7.7.6. Services that include a messaging feature

A social media service that includes a messaging feature (being an instant messaging feature that enables private communication between two or more end-users of the service) must, irrespective of any compliance measures that may apply to other aspects of the service, comply with compliance measures for the messaging feature as set out in clause 6 and the table in clause 10. This is to ensure consistency across the SMS Code and RES Code as to the compliance measures that apply to messaging.

7.7.7. Approach to measures

This Code codifies industry best practices that provide safeguards for the community in respect of the matters set out in the section 141 notice, based on the extent to which a service allows or prohibits relevant materials, and in the case of a service that prohibits such materials, the service's risk tiering. Some measures apply to specific types of materials, while others apply to the full range of class 1C and class 2 materials to allow a proportionate , graduated approach to the risk of harm presented by different material types on different services.

7.7.8. Compliance measures where online pornography, self-harm material or high-impact violence material is allowed

The compliance measures in this table apply to the extent online pornography, self-harm material or high-impact violence material is allowed to be posted on a social media service under the applicable terms of use, but do not apply to any messaging feature.

Age assurance measures	**Compliance measure 7.1** A provider of a service must, to the extent technically feasible and reasonably practicable, take steps to implement: (a) appropriate age assurance measures; and (b) access control measures, before providing access to online pornography and/or self-harm material.A service provider must also take appropriate steps to test and monitor the effectiveness of its age assurance and access control measures over time. *All service providers that allow online pornography and/or self-harm material are required to restrict access to that material to under age users.*
Safety tools	**Compliance measure 7.2** Except where the primary purpose of the service is to provide access to online pornography, self-harm material and/or high-impact violence material, a service provider must allow all end-users to opt-in at any time to appropriate safety tools which may limit their access or exposure to online pornography, self-harm material and/or high-impact violence material on the service and are appropriate for the service. Appropriate safety tools may include solutions for: (a) implementing age-gates, either on the entire service or on identified areas of services where an end-user is most likely to access or be exposed to online pornography, self-harm material and/or high-impact violence material on the service; (b) filtering online pornography, self-harm material and high-impact violence material, including by downlisting, deprioritising or quarantining; (c) blocking online pornography, self-harm material and high-impact violence material; (d) blurring online pornography, self-harm material and high-impact violence material; (e) halting autoplay of online pornography, self-harm material and high-impact violence material; (f) placing interstitial notices on online pornography, self-harm material and high-impact violence material so that users can click through to view if they wish; (g) ensuring that recommender systems, algorithms, and other choice architecture, do not promote online pornography or self-harm material to child end-users;

	(h) ensuring compatibility with third-party filtering software or tools which may be installed on devices, or provided by internet carriage services. (a) *See suggested measure in 4.1 of the table of suggested measures in the July 2024 Position paper p 88.*
Publishing information about tools and settings	**Compliance measure 7.3** To the extent relevant, a service provider must publish clear and accessible information to Australian end-users about the tools and settings available to limit their access or exposure to online pornography, self-harm material and high-impact violence in their news and discovery feed. *This measure is complementary to measure 7.2.*
Annual reporting to eSafety on Code compliance	**Compliance measure 7.4** A service provider must submit to eSafety a Code report which includes the following information: (a) the steps that the provider has taken to comply with the compliance measures under this Code; and (b) an explanation as to why these steps are appropriate. The first Code report must be submitted by the provider of the social media service to eSafety 12 months after this Code comes into effect. The provider of the social media service must submit subsequent Code reports to eSafety annually. A report under this compliance measure may be combined with any report that the service provider is obliged to provide under any other compliance measure. *This measure extends reporting obligations in the Phase 1 Codes to online pornography, self-harm material and high-impact violence material.*

7.7.9. Compliance measures where online pornography, self-harm material or high-impact violence material is not allowed

The compliance measures in this table apply to the extent online pornography, self-harm material and high-impact violence material is not allowed to be posted on a social media service under the applicable terms of use where the service has a Tier 1 or Tier 2 risk profile for online pornography, self-harm material or high-impact violence material, but do not apply to any messaging feature.

Use of systems, processes and/or technologies to detect and remove online	**Compliance measures 8.1 to 8.3** A service provider must implement systems, processes and/or technologies designed to detect, flag and/or remove online

pornography / self-harm material / high-impact violence material	pornography / self-harm material / high-impact violence material from the service, for example, through the use of keyword searches, hashing, machine learning, artificial intelligence, or other technology designed to identify text, videos and images that may, depending on the context, be online pornography / self-harm material / high-impact violence material and/or other safety technologies or systems or processes that limit users' exposure to such material on the service. A service provider must also take appropriate steps to continuously improve these systems, processes and/or technologies. *This measure requires service providers to proactively seek to detect and remove online pornography, self-harm material and high-impact violence material, and to continuously improve systems, processes and technologies used for this purpose.*
Reporting to eSafety on Code compliance	Where eSafety issues a written request to a service provider to submit a Code report, the provider named in such request must submit to eSafety a Code report which includes the following information: (a) details of any risk assessment it is required to undertake pursuant to this Code in relation to online pornography, self-harm material or high-impact violence material (as applicable); (b) the steps that the provider has taken to comply with the compliance measures under this Code; and (c) an explanation as to why these steps are appropriate. A service provider that has received such a request from eSafety is required to submit a Code report within 2 months of receiving the request, but for the first request no earlier than 12 months after this Code comes into effect. A service provider will not be required to submit a Code report to eSafety more than once in any 12-month period. A report under this compliance measure may be combined with any report that the service provider is obliged to provide under any other compliance measure. *This measure extends reporting obligations in the Phase 1 Codes to online pornography, self-harm material and high-impact violence material.*

7.7.10. Other supporting compliance measures

The compliance measures in this table apply to all social media services that allow online-pornography, self-harm material or high-impact violence material and to other social media services with a Tier 1 or Tier 2 risk profile for online-pornography, self-harm material or high-impact violence material, but do not apply to any messaging feature.

Terms and conditions relating to class 1C and class 2 material	**Compliance measure 9.1** A service provider must have, and enforce, clear actions, policies or terms and conditions relating to online pornography, self-harm material, high-impact violence material and simulated gambling material, which will include, to the extent applicable, terms and conditions dealing with the types of online pornography, self-harm material, high-impact violence material and simulated gambling

	material that are allowed or not allowed on the social media service. In implementing this measure, the service provider must: (a) use simple, plain, and straightforward language; (b) to the extent practicable, be clear about the type of any material that is prohibited; and (c) communicate such terms and conditions, standards and/or policies to all personnel that are directly involved in their enforcement. Relevant policies and actions must be implemented according to a graduated, risk-based approach. This approach may be different for different types of material. *See suggested measure in 1.1 of the table of suggested measures in the July 2024 Position paper p 82.*
Trust and safety function	**Compliance measure 9.2** A service provider must have, or have access to, reasonably adequate personnel to oversee the safety of the service. Such personnel must have the skills, experience and qualifications needed to ensure that the provider complies with the requirements of this Code at all times. *This measure extends the equivalent measure in the Phase 1 Codes to this Code.*
Reporting mechanisms	**Compliance measure 9.3** A service provider must provide tools which enable Australian end-users to report class 1C and class 2 material which they consider may be contrary to the social media service's terms and conditions, and must where appropriate ensure that these reports are evaluated and actioned. Such reporting mechanisms must: (a) be easily accessible and easy to use; (b) be accompanied by clear instructions on how to use them; (c) ensure that the identity of the reporter is not disclosed to the reported end-user or account holder (i.e., the individual who has been reported should not be able to see the person who reported them), without the reporter's express consent, except as required by law. *This measure ensures that end-users can report class 1C and class 2 material that breach terms of use.*
On-platform reporting tools	**Compliance measure 9.4** A service provider must ensure that the reporting tools referred to in compliance measure 9.3 for class 1C and class 2 material are available and accessible to Australian end-users on the interface of the social media service.

	This measure compliments measure 9.3 by ensuring that reporting tools are readily accessible on a service.
Complaints tools	**Compliance measure 9.5** A service provider must provide tools which enable Australian end-users to make a complaint about: (a) the provider's handling of reports about class 1C or class 2 material; or (b) any other aspect of the provider's compliance with this Code. Such complaints tools must: (a) be easily accessible and simple to use; and (b) be accompanied by plain language instructions on how to use them. *This measure ensures that end-users can make complaints about handling of class 1C and class 2 material and broader Code compliance.*
Appropriate steps for informing Australian end-users about actions taken on reports and complaints	**Compliance measure 9.6** A service provider must take appropriate steps to acknowledge a report referred to in compliance measure 9.3 or complaint referred to in compliance measure 9.5 and must ensure that an Australian end-user who makes such a report or complaint is informed in a reasonably timely manner of the outcome of the report or the complaint, and of any review mechanisms that are available, or is otherwise able to access information about the status of the report or the complaint. *This measure ensures that end-users are kept up to date about reports and complaints they may make.*
Training for personnel responding to reports and complaints	**Compliance measure 9.7** A service provider must ensure that personnel responding to reports referred to in compliance measure 9.3 or complaints referred to in compliance measure 9.5 are trained in the social media service's policies and procedures for dealing with such reports and complaints. *This measure ensures that personnel receive appropriate training to enable them to deal effectively with reports and complaints from end-users.*
Reviews of compliance of personnel with systems and processes	**Compliance measure 9.8** A service provider must review the effectiveness of its reporting systems and processes to ensure reports and complaints are assessed and actioned (if necessary) within reasonably expeditious timeframes, based on the level of harm the material poses to Australian children. Such review must occur at least annually. *This measure is complementary to other measures dealing with reports and complaints, as set out above.*

Timely referral of unresolved complaints to eSafety	**Compliance measure 9.9** A service provider must promptly refer to eSafety complaints from Australian end-users concerning a material non-compliance with this Code by the service provider, where the service provider is unable to resolve the complaint within a reasonable timeframe. *This measure ensures that material concerns about non-compliance can be escalated to eSafety for resolution, when needed.*
Updates to eSafety about relevant changes to technology	**Compliance measure 9.10** A service provider must take reasonable steps to ensure eSafety receives updates regarding significant changes to the functionality of their services that are likely to have a material positive or negative effect on the access or exposure to, distribution of, or online storage of online pornography, self-harm material, high-impact violence material or simulated gambling material by an Australian child. A service provider may choose to provide this information in an annual report to eSafety under this Code. In implementing this measure, a service provider is not required to disclose information to eSafety that is confidential. *This measure extends equivalent measures under the Phase 1 Code to cover relevant categories of class 1C and class 2 material.*
Engagement	**Compliance measure 9.11** A service provider must appropriately engage with safety and community organisations (such as civil society groups, public interest groups and representatives of marginalised communities), academics and government to gather information to help inform measures taken for the purposes of protecting or preventing children from accessing or being exposed to class 1C and class 2 material. A service provider must consider information obtained through such engagement. *This measure supports the general commitment made in section 1.3 under the Head Terms.*
Information for Australian end-users about the role and functions of eSafety, including how to make a complaint to eSafety	**Compliance measure 9.12** A service provider must publish clear information that is accessible to Australian end-users which explains the role and functions of eSafety, including how to make a complaint to eSafety. *This measure extends the equivalent measure in the Phase 1 Code.*
Location on service that is dedicated to providing online safety information	**Compliance measure 9.13** A service provider must establish a location on or via the service that is dedicated to providing online safety information, that: (a) contains information required under this Code;

	(b) includes information about how Australian end-users can contact third party services that may provide counselling and support; and (c) is accessible to Australian end-users. *This measure extends the equivalent measure in the Phase 1 Code.*
Information about how services deal with risk of harm	**Compliance measure 9.14** A service provider must publish clear and accessible information that explains the actions they take to reduce the risk of harm to Australian child end-users from online pornography, self-harm material, high-impact violence material and simulated gambling material on its service. *This measure extends the equivalent measure in the Phase 1 Code.*

7.7.11. Compliance measures for messaging features

This Code sets out another table of compliance measures that apply to any messaging feature included as part of a social media service, irrespective of any compliance measures that may apply to other aspects of the social media service. The measures in this table are intended to be identical to those that apply for other communication relevant electronic services under the RES Code, in order to ensure consistency of treatment for messaging features. Please refer to the section on the RES Code below for further information.

7.8. Schedule 2 Relevant Electronic Services Online Safety Code (Class 1C and Class 2 Material)

7.8.1. Code structure

This Code comprises the Head Terms and Schedule 2, covering relevant electronic services as defined in the OSA. This Code has adopted key features of the Online Safety (Relevant Electronic Services – Class 1A and Class 1B Material) Industry Standard 2024 (Phase 1 RES Standard) where possible, including definitions to promote a consistent approach between Codes and Standards.

The following table maps each compliance measure in the Relevant Electronic Services Online Safety Code (Class 1C and Class 2 Material) (RES Code) against the two online safety objectives issued by eSafety.

This table maps each measure against the online safety objective it is primarily aimed at meeting. However, many of the compliance measures in this Code contribute to meeting more than one objective. As such, the table should be read as guidance only.

Objective	Compliance measure

28 February 2025.

Objective 1 **Protect and prevent children in Australia from accessing or being exposed to class 1C and class 2 material**	7.1, 7.2 8.1, 8.2, 8.7, 8.14, 8.16 9.1, 9.2, 9.7, 9.14, 9.16 10.1, 10.2, 10.3, 10.8, 10.15, 10.17 11.1, 11.2, 11.7, 11.14, 11.16 12.3 14.1, 14.2, 14.7 15.1, 15.2, 15.6, 15.12, 15.14, 15.16
Objective 2 **Provide Australian end-users with effective information, tools and options to limit access and exposure to class 1C and class 2 material**	8.5, 8.8, 8.9, 8.10, 8.11, 8.12 9.5, 9.8, 9.9, 9.10, 9.11, 9.12 10.6, 10.9, 10.10, 10.11, 10.12, 10.13 11.5, 11.8, 11.9, 11.10, 11.11, 11.12 12.1 14.3, 14.4, 14.5 15.5, 15.7, 15.8, 15.9, 15.10, 15.11
Other supporting compliance measures	8.3, 8.4, 8.6, 8.13, 8.15, 8.17, 8.18 9.3, 9.4, 9.6, 9.13, 9.15, 9.17, 9.18 10.4, 10.5, 10.7, 10.14, 10.16, 10.18, 10.19 11.3, 11.4, 11.6, 11.13, 11.15, 11.17, 11.18 12.2 14.6, 14.8 15.3, 15.4, 15.12, 15.13, 15.15, 15.7, 15.18

7.8.2. Approach to risk of relevant electronic services

How this Code applies to a relevant electronic service depends on whether the provider:

a) is required to assess the risk that online pornography, self-harm material or high-impact violence material will be accessed, distributed, or generated on that service and determine a risk profile; or
b) is not required to undertake a risk assessment to determine a risk profile because it falls within a set category of relevant electronic service as set out in clause 4.4 of the Code.

Main categories of relevant electronic services

Consistent with the approach of the Phase 1 RES Standard, a provider of each of the following relevant electronic services is not required to carry out a risk assessment under this Code:

a) an enterprise relevant electronic service;

28 February 2025.

b) a gaming service with limited communications functionality;
c) a pre-assessed relevant electronic service, in this Code meaning:
    - a closed communication relevant electronic service;
    - an other communication relevant electronic service;
    - a dating service; or
    - a gaming service with communications functionality.

Each of these categories is subject to a list of specific compliance measures in this Code.

Treatment of closed communication relevant electronic services and other communication relevant electronic services

The various service sub-categories and their definitions mirror the sub-categories and definitions used in the RES Standard, with the exception of closed communication relevant electronic services and other communication relevant electronic services. In response to feedback from eSafety it was determined by industry that measures needed to be applied in a different way for relevant electronic services that had a more "open" nature by enabling end-users to search for other target end-users on the service, or where services recommended target end-users based on common interests or connections. As such, the definition of "communication relevant electronic service" in the Phase 1 RES Standard was split into two categories utilising the wording contained in section 18(4)(a) of the Phase 1 RES Standard to define the distinction between "other communication relevant electronic services" and "closed communication relevant electronic services" such as email services, where end-users have to have each other's contact details from another source in order to communicate on the service. This distinction has enabled measures to be more tailored for these service categories.

7.8.3. Other categories of relevant electronic services

Whilst it is anticipated that most relevant electronic services will fall into one of the categories that are not required to carry out a risk assessment under this Code (as set out in clause 4.4 of the Code), the definition of relevant electronic services is broad and may include services that may in the future be specified as relevant electronic services in legislative rules[21].

Therefore provisions have been included to ensure that where a relevant electronic service does not fall into one of the categories set out in clause 4.4, it must undertake a risk assessment under this Code, except where a provider chooses to automatically assign a Tier 1 risk profile in accordance with section 5.2(a)(ii) of the Head Terms.

The approach to assessment of risk for other relevant electronic services , and in particular the guidance on risk assessment, draws from Part 3 of the Phase 1 RES Standard. However, it has also been extended further to provide some consistency of approach across the Phase 2 Codes and therefore contains a range of additional considerations where relevant as listed out in clause 5b). Providers have to, at a minimum, consider criteria relating to the functionality, purpose and scale of the service (including the extent to which material posted on, distributed using or generated by the service will be available to end-users in Australia and any generative AI features of the service (clause 4.3a)).

7.8.4. Approach to measures

General

This Code codifies industry best practices that provide safeguards for the community in respect of the matters set out in the section 141 notice.

21 Section 13A, OSA

28 February 2025.

Approach to age-assurance

The Explanatory Memorandum to the Online Safety Amendment (Social Media Minimum Age) Bill 2024 stated that:

a) the Government's intention that messaging apps be excluded by way of legislative rules in order to ensure that "young people have continued access to beneficial online activities, including connection with friends, access to community and support services, and participating in public life"; and
b) feedback from stakeholder engagement helped inform development of that Bill including in particular that "messaging services were widely considered by stakeholders to provide benefits of connection that outweigh the risks of harm on those services to young people. While there are risks of predatory contact through messaging, these are addressed through other existing mechanisms in the Online Safety Act, and powers under the *Criminal Code Act 1995* (such as those that criminalise using a carriage service to 'groom' persons under 16 years of age)."

Similarly, in the second reading speech for the Bill, the Hon Michelle Rowland MP, Minister for Communications, highlighted that "While users can still be exposed to harmful content by other users [on messaging apps and online gaming apps], they do not face the same algorithmic curation of content and psychological manipulation to encourage near endless engagement. Further, the inclusion of messaging apps could have wider consequences, such as making communication within families harder ".

In response to these issues being raised by industry in December 2024, eSafety stated in its letter of 21 January 2025 that its position is that "general communications services" should require end-users to meet age assurance requirements not in order to prohibit access by children but in order to "apply appropriate default safety measures to prevent child users from being exposed to harmful, age-inappropriate material through messages". This statement follows on from previous suggestions from eSafety (for example in its letter of 16 October 2024) that:

> *a. one way that services could "mitigate the likelihood of end-users being exposed to [class 1C and class 2 material] on their service would be to implement active detection and removal measures … for that material where it may be present on such a service;*
>
> *b. "[w]ith effective detection measures implemented, it is practically 'less-likely' that end-users and child end-users will come into contact with class 1C or class 2 material on a service";*
>
> *c. "active detection measures for high-priority restricted categories of material should be implemented"; and*
>
> *d. as "class 2 material which is not high-priority restricted would still not be automatically detected on a service" eSafety "considers that age assurance measures coupled with appropriate default safety settings for younger users that are appropriate for these services to implement".*

It is unclear, short of complete and total age gating, what these appropriate default safety settings would be in circumstances where active detection measures are not appropriate. Regardless, we believe it worth highlighting that all of these suggestions require the implementation of active detection measures / scanning of messaging services for class 1C and class 2 material.

Class 1C and class 2 material contain many broad categories of material that are uncertain in scope, and can be challenging to identify (particularly at scale). To take one example only, certain crime and violence and drug and alcohol dependency related material falls into class 2, but the distinction between this and extreme crime and violence material (falling within class 1A), crime

and violence material (falling within class 1B) and drug-related material (falling within class 1B), will not always be clear cut.

Further, to implement active detection measures (on by default in many instances) on private messaging services would carry significant privacy and surveillance consequences for users. Industry believes there is a significant risk that such intrusion would be disproportionate to the level of risk, noting for instance the part of the second reading speech for the Online Safety Amendment (Social Media Minimum Age) Bill 2024 highlighted above where the Minister for Communications highlighted that "[w]hile users can still be exposed to harmful content by other users [on messaging apps and online gaming apps], they do not face the same algorithmic curation of content and psychological manipulation to encourage near endless engagement".

Similar concerns about the consequences of measures such as these were raised with respect to the Online Safety (Relevant Electronic Services – Class 1A and 1B Material) Industry Standards 2024 (Phase 1 RES Standard) in the Parliamentary Joint Committee on Human Rights Human Rights Scrutiny Report 9 of 2024. This report stated with respect to CSEM, material depicting sexual violence, and pro-terror material reaching relevant thresholds of severity, that "the committee considers that to the extent that regulating these types of material limits the rights to freedom of expression and privacy, such limitations are likely permissible under international human rights law. However, n*oting that the scope of materials captured by the measures is much broader, it is necessary to assess where the regulation of these other types of material, such as crime and violence or drug-related material that offends against the standards of morality, decency and propriety, is reasonable, necessary and proportionate*" (emphasis added). Industry notes that the scope of material covered by the Phase 2 Codes is much broader still than these class 1B categories.

The committee went on to make a number of findings, including that "[t]he committee considers that there is also a risk that the measures may significantly interfere with rights, noting that while not required to do so, providers have the discretion to proactively scan communications in order to comply with their obligations under these standards…The committee therefore considers that there is a risk that the measures may not constitute a proportionate limitation on the rights to freedom of expression and privacy. Further, if an individual's rights to freedom of expression and privacy were violated, it is not clear that there would be an effective remedy available."

In response, in the Supplementary Statement for the RES Standard eSafety took the position that proactive detection obligations should *not* extend beyond class 1A as there could potentially be "more risks of infringement to privacy and free expression if providers were subject to broad detection measures [beyond class 1A], and were to implement these in a manner that did not recognise context".

Industry submits that those risks are even more heightened for class 1C and class 2 material, which are much broader and less certain categories of content.

Industry's position above does *not* mean that industry disagrees that appropriate steps should be taken to empower families and protect children when using general communications services such as messaging and email services (covered by the Relevant Electronic Services Online Safety Code (Class 1C and Class 2 Material)). To the contrary, industry firmly supports such an approach. However, industry is of the view that given the positions of the Government, the Minister, the Joint Committee on Human Rights and eSafety itself in the past, it is inappropriate for an industry code of practice to mandate age assurance and/or age gating or proactive detection requirements (or requirements that, in practice, rely on proactive detection) for such services with respect to class 1C and class 2 material. Given the history surrounding this issue, industry believes that such a decision should be one for Parliament.

Industry believes, instead, that the industry code of practice should clearly articulate ways in which families can be empowered to make safe choices with respect to their children's use of such services, and has proposed a range of measures that industry believes achieves the two online safety objectives prescribed by eSafety.

28 February 2025.

Consistent with that approach, age assurance and age gating obligations have been included for certain high risk relevant electronic services only, namely:

a) any relevant electronic service (regardless of which sub-category of service) with the sole or predominant purpose of permitting end-users to share online pornography or self-harm material; and
b) gaming services that enable end-users to play computer games that have been classified as R18+ (or regardless of its classification status, where a game would likely be classified as R18+ because it constitutes simulated gambling material).

In addition, whilst age assurance and age gating requirements are not mandated for dating services, some of the measures for dating services turn on whether or not a provider has applied age assurance and age gating measures to its service and in addition industry has mirrored certain provisions from the voluntary Online Safety Code for Dating Services as suggested by eSafety to provide additional protections specific to such services (including detection obligations).

Capability of relevant electronic services to remove/review and/or assess materials.

This Code explains in clause 6 b) that:

> *Certain measures in this Code require a provider to take appropriate and proportionate action if it becomes aware of a breach of the terms and conditions it has in place with Australian end-users, including where contacted with information about such a breach by an end-user. For the avoidance of any doubt, some providers of relevant electronic services may not be capable of reviewing, assessing and/or removing material from their services in all circumstances (because such activity is not technically feasible or reasonably practicable) and a provider's awareness of a breach, and the appropriateness of any action taken in response, will be assessed in that context.*

In light of this context, the measures in this Code take into account the different capacity of services to assess, review, and remove materials. We note that this approach is consistent with the regulatory context of these Codes: the OSA does not penalise services that are not capable of removing material pursuant to a removal notice given by eSafety.[22] Furthermore the classification of material under the Codes requires providers to be capable of assessing the context of the materials. This is made clear in the National Classification Guidelines for publications, films and computer games. For example, the introduction to the Guidelines for the Classification of Films 2012 (Cth) states that context is the foremost principle underlying classification decisions:

> Importance of context
>
> *Context is crucial in determining whether a classifiable element is justified by the story-line or themes. In particular, the way in which important social issues are dealt with may require a mature or adult perspective. This means that material that falls into a particular classification category in one context may fall outside it in another.*

See also Head Terms section 5.3 (c) that requires providers to explain to eSafety where a measure is not technically feasible.

Approach to prohibitions on end-user activity

Industry has framed measures regarding terms of use for relevant electronic services in a way that effectively targets high risk material, whilst doing so in a way that is achievable and appropriate for communications services and does not cut across existing Australian laws.

22 See for example, section 90, section 91, section 111 and section 121, OSA

28 February 2025.

There are a broad range of circumstances in which sharing of class 1C and class 2 material by an end-user via communications and messaging services covered by this Code will be legal in Australia.

Industry believes that providers of relevant electronic services should generally not be in a position where they are required (by law) to prohibit (and enforce a prohibition on) material or activity that is entirely legal under Australian law.

Further, whilst many RES providers already contractually prohibit illegal activity on their services, enforcement of such prohibitions can be extremely complex. Many of the offences involved in the limited circumstances where sharing of class 1C and class 2 material *is* illegal differ across jurisdictions within Australia, and involve a range of defences and fault elements that are extremely difficult for a RES provider to adjudicate on. Circumstances involving capability constraints of the type outlined above where a provider has no or only limited access to relevant communications (e.g. due to encryption or other security controls) or where the communication is between a user on its service and a user of a third party service (of whom the RES provider has no visibility at all) can make this even more complex.

For this reason, industry has generally included measures in this Code requiring providers to have contractual prohibitions on three main categories of illegal activity which industry believes will commonly involve sharing of class 1C and class 2 material, and that are clear enough to reasonably be operationalised by providers given the complexities noted above.

A slightly different approach has been taken for "other communication relevant electronic services" and "dating services" given the different nature of those services, and what is possible on those services.

7.8.5. Compliance measures that apply to all RES

Table 7 of the Code contains age assurance and age gating requirements for a number of relevant electronic services. Please see detail above regarding the approach taken to age-assurance of relevant electronic services.

Age assurance measures for online pornography and self-harm material	**Compliance measure 7.1** A provider who provides a relevant electronic service with the sole or predominant purpose of permitting end-users to share online pornography or self-harm material must, where technically feasible and reasonably practicable, implement: a) appropriate age assurance measures; and b) access control measures, before providing access to that service. A provider must also take appropriate steps to test and monitor the effectiveness of its age assurance and access control measures over time. *This measure requires age assurance and access control measures for services that actively solicit pornographic materials on their services e.g. Chaturbate.*

28 February 2025.

Age assurance measures for gaming services	**Compliance measure 7.2** A provider who provides a gaming service that enables end-users to play a computer game that: a) is, or would likely be, classified as R18+, because it constitutes simulated gambling material; or b) has otherwise been classified as R18+ in accordance with the Classification Act, must, where technically feasible and reasonably practicable, implement: c) appropriate age assurance measures; and d) access control measures, before providing access to that computer game. A provider must also take appropriate steps to test and monitor the effectiveness of its age assurance and access control measures over time. *This measure requires age assurance and access control measures for simulated gambling games, as well as any other games that have been classified as R18+.*

7.8.5. Compliance measures for closed communication relevant electronic services

Table 8 of this Code contains measures for closed communication relevant electronic services such as email services. These apply in addition to table 7 (where relevant).

Terms and conditions prohibiting illegal activity (closed communication relevant electronic services)	**Compliance measure 8.1** A provider of a service must: a) have terms and conditions in place with Australian end-users prohibiting the end-user from sharing material via the service in the course of engaging in any of the following categories of criminal activity: i. non-consensual sharing of intimate images; ii. grooming of children; or iii. sexual extortion (or sextortion); b) publish the terms and conditions by making them accessible on a website and/or application for the service (as relevant); c) ensure the prohibition described in a) is set out in plain language in the terms and conditions; and d) if the provider becomes aware of a breach of the prohibition described in a), take appropriate and proportionate action in a reasonably timely manner. It is not necessary that a particular form of words be used in the terms and conditions so long as the contractual effect of the terms and conditions is as required by sub-measure a). A provider must have systems and/or processes in place to support compliance with the obligation in d). *Please see comments above regarding the approach taken to prohibitions on end-user activity.* *Most closed communications relevant electronic services such as email services do not restrict material on their services unless it is unlawful. Consequently, they do not intervene in communications between users that share lawful materials. eSafety has suggested that these services could implement age verification and then take steps to minimise the exposure of young people on these services to pornography, for example by filtering out 'nude content' using AI classifiers. There are a number of issues with this approach. Based on eSafety's research to date , it is unclear to us to what extent the intentional sharing of pornographic or other class 2 material on these services between users presents a risk of harm to young people under 18. Further, using AI classifiers to strip content from children's feeds without the ability to assess context is likely to result in the over-removal of a large amount of material that is not pornographic in nature. We note the views of the eSafety Youth Council that:* Messaging platforms, such as WhatsApp, Messenger, iMessage and Discord, should not be included in age verification reforms. Social media platforms and messaging apps are distinctive from each other. While social media platforms have an undefined set of users accessing and interacting with content from all other users, messaging apps have a definite pre-defined list and destination of who the messages will go to. Their differing risk profiles should be considered[1] [1]eSafety Youth Council, Submission to the Joint Select Committee on Social Media and Australian Society, 2024]

	Following feedback from eSafety about the types of pornographic material that would be most harmful to children we have therefore taken an approach that: *(i) obliges closed communication RES falling in certain high risk categories to implement age assurance measures and access controls (see table at 7.8.4 above);* *(ii) included a measure that is intended to address the harm identified in eSafety's feedback by requiring providers to have tools to assist Australians to limit receipt of unsolicited material (including online pornography) (see measure 8.5 below); and* *(iii) included measures 8.1 to 8.4 (and supporting measures) which require providers to have (and appropriately action) terms prohibiting certain categories of illegal activity.* *Industry believes this approach provides an appropriate and proportionate suite of protections, while respecting the rights of under 18 year old users to access critical communications tools.* *With respect to this measure 8.1 specifically, the types of illegal activity listed in measure 8.1a)i. to iii. will often involve the sharing of material that would fall within the scope of class 1C and class 2 material, such as high impact nude images.*

Reporting mechanisms (closed communication relevant electronic services)	**Compliance measure 8.2** A provider of a service must provide a tool or mechanism which enables Australian end-users to report breaches of the prohibitions described in measure 8.1 a) by end-users of the service. If an Australian end-user reports a breach via the tool or mechanism, the provider must: a) respond promptly to the end-user acknowledging receipt of the report; and b) consider any relevant information provided by the end-user pursuant to this tool or mechanism in a reasonably timely manner, and if appropriate take action pursuant to measure 8.1d). The reporting tool or mechanism must: c) be easily accessible and easy to use; d) where the tool or mechanism does not involve use of a widely used communication mechanism – have clear instructions on how to use it; and e) ensure that the identity of the reporter is not disclosed to the reported end-user (i.e. the individual who has been reported should not be able to see the person who reported them), without the reporter's express consent, except as required by applicable law. The provider must develop and comply with internal policies and procedures for dealing with reports made through this mechanism. *This measure supports measure 8.1 and ensures that robust reports handling approaches will be applied. The measure is slightly different to the reporting measures included in the other Codes given that RES reporting is specifically tied to measure 8.1(d) for the reasons noted under measure 8.1 above.*
Training for personnel responding to reports (closed communication relevant electronic services)	**Compliance measure 8.3** A provider of a service must ensure that personnel responding to reports made by Australian end-users under measure 8.2 are trained in the closed communications relevant electronic service's policies and procedures for dealing with such reports. *This measure supports measure 8.2 and ensures that robust reports handling approaches will be applied by requiring training for personnel.*

Review of compliance of personnel with systems and processes (closed communication relevant electronic services)	**Compliance measure 8.4** A provider of a service must review the effectiveness of its reporting mechanism (as required by measure 8.2) and processes to ensure information received via the reporting mechanism is considered and actioned (if necessary) as appropriate pursuant to measure 8.1 d). Such review must occur at least annually. *This measure supports measures 8.2 and 8.3.*
Tools, features and/or settings (closed communication relevant electronic services)	**Compliance measure 8.5** A provider of a service must ensure that it has appropriate tools, features and/or settings available and accessible to assist Australian end-users to limit receipt of unsolicited material (including class 1C and class 2 material). Examples of such tools, or features and/or settings includes: a) tools, features and/or settings that allow Australian end-users to block messages from other end-users; and/or b) with respect to online pornography, tools, features and/or settings that automatically blur images detected as containing nudity on receipt. *This measure works in tandem with measure 8.1. See comments on measure 8.1 regarding the combined approach that has been taken. Given the challenges with broader prohibitions on user activity as outlined above, this measure ensures that users are always empowered to take steps to limit receipt of unsolicited material (including class 1C and class 2 material).* *The focus on unsolicited material ensures that there are a number of ways that a provider could effectively reduce risk. With respect to children, providers may, for example, use tools that detect nudity, or other forms of content, likely to suggest the presence of forms of class 1C or class 2 material and may implement such tools via parental settings. However, a provider may also effectively limit the risk of unsolicited receipt of class 1C and class 2 material by a child (for example) by permitting their parent or guardian to limit contact with their child on the service to an approved list of trusted family and friends to avoid unwanted contact. In all cases, the tools, features and/or settings must be "appropriate" as defined in section 5.1(b) of the Head Terms and be available and accessible to Australian end-users. In this way, industry believes that users have methods available to them to limit receipt of pornography, and other types of class 1C and class 2 material.*

Updates to eSafety about relevant changes to technology (closed communication relevant electronic services)	**Compliance measure 8.6** A provider of a service must share information with eSafety in writing about significant changes to the functionality of its service that are likely to have a material positive or negative effect on the access or exposure to, distribution to, or online storage of online pornography, self-harm material or high-impact violence material by Australian children. A provider may choose to provide this information in a Code report to eSafety under this Code. In implementing this measure, a provider is not required to disclose information to eSafety that is confidential. *This extends obligations in the Phase 1 RES Standard to update eSafety on changes to the functionality of services where those changes fall in categories relevant to Phase 2.* *This mirrors the update obligations included across relevant Phase 2 Codes.*
Significant changes to the service (closed communication relevant electronic services)	**Compliance measure 8.7** Before the provider of a service makes a material change to the service (including any significant new feature of the service enabled by generative artificial intelligence) that will significantly increase the risk of sharing of online pornography, self-harm material or high-impact violence material to Australian children, it must: a) carry out an assessment of the kinds of measures that could reasonably be incorporated into the service to minimise that risk; and b) where appropriate, apply measures so identified to help to mitigate that risk. *This measure requires providers to make appropriate adjustments to mitigate risk where required as a result of material changes that significantly increase risks of sharing of online pornography, self-harm material or high-impact violence material to Australian children.*

Improvement (closed communication relevant electronic services)	**Compliance measure 8.8** Where technically feasible and reasonably practicable, a provider of a service must either take appropriate steps to further develop and improve the tools, features, and/or settings it has in place under measure 8.5 over time. Examples of activities that a provider may engage in to meet this measure include the following (to the extent directed towards, or relevant to, the matters covered by this Code): a) any activities designed to further develop the effectiveness of the tools, features and/or settings; b) tracking new and emerging risks or issues that may be causing harm to Australian children; c) investment in research and development and/or testing of novel technological solutions; d) investment in trust and safety teams dedicated to implementing regulatory requirements and policies which enhance online safety for users of online services; e) investment in review teams who conduct human review of reported material, and can consider material including factors like context; f) providing financial or technical support to non-governmental organisations with recognised online safety expertise to improve their infrastructure and/or technical capabilities; g) contributing to programs operated by non-governmental organisations; h) joining relevant industry organisations or other third party organisations intended to address online harm to children and sharing information on best practice approaches; i) contributing to industry initiatives (including initiatives led by industry associations or other third party organisations); j) conducting or supporting research into and development of online safety tools, features and/or settings and approaches; k) providing support, either financial or in kind, to organisations the functions of which are or include protection of children online; l) extending the application of a feature or tool applied under another industry code or standard to operate in connection with its service; and

	m) activities that aim to refine algorithms or inputs into tools to improve their effectiveness. The provider must, at a minimum, engage in at least some of the example activities above in each calendar year. *This measure recognises that technological solutions that work to protect children from high impact restricted materials need improvement and that this will require commitments by industry of the kind outlined in this measure. This measure has been informed by requirements in the Phase 1 RES Standard. It also incorporates suggestions for improvement of protective tools on page 88 of the Position Paper with examples of relevant activity that may contribute to this. A requirement for a trust and safety function has also been included at measure 8.14 in this regard.* *A specific timing requirement has been included to ensure that providers engage in relevant activities in each calendar year.*
Information about tools and contact mechanisms (closed communication relevant electronic services)	**Compliance measure 8.9** A provider of a service must provide clear and accessible information to Australian end-users regarding: a) the tools, features and/or settings required by measure 8.5; and b) the contact tools and/or mechanisms required by measure 8.2 and 8.16. Information must be provided in a manner that is reasonably capable of being easily understood by most users of all ages permitted on the service. *This supports measures 8.2, 8.5 and 8.16. It incorporates suggestions from the Position Paper that the Code contains measures requiring providers to make information available. Note that this provision builds on existing information requirements already included in the Phase 1 Codes.*
Information for Australian end-users about the role and functions of eSafety, including how to make a complaint to eSafety (closed communication relevant electronic services)	**Compliance measure 8.10** A provider must publish clear information that is accessible to Australian end-users which explains the role and functions of eSafety, including how to make a complaint to eSafety. *See equivalent measures in the other Codes. This incorporates suggestions from the Position Paper that the Code contains measures requiring providers to make information available.*

Information to assist end-users with managing risks relating to class 1C and class 2 material (closed communication relevant electronic services)	**Compliance measure 8.11** A provider of a service must provide clear information that is accessible to Australian end-users about steps that end-users can take to manage and mitigate risks relating to class 1C and class 2 material. *This measure supports the other measures in this Code by requiring providers to publish information that more generally helps to empower users to manage and mitigate risks relating to class 1C and class 2 material. This may not necessarily be limited to information about the tools, features and/or settings available on services (although such information is clearly important and required by measure 8.9) but could extend to support or help articles on topics such as safe behaviour on services.*
Location on or via service that is dedicated to providing online safety information (closed communication relevant electronic services)	**Compliance measure 8.12** A provider of a service must establish a location on or via the service that is dedicated to providing online safety information, that: a) contains information required under this Code; b) includes information about how Australian end-users can contact third party services that may provide counselling and support; and c) is accessible to Australian end-users. *This measure ensures that information will be accessible in a dedicated location.*
Reporting to eSafety on Code compliance (closed communication relevant electronic services)	**Compliance measure 8.13** Where eSafety issues a written request to a provider of a service to submit a Code report, the provider named in such request must submit to eSafety a Code report which includes the following information: a) the steps that the provider has taken to comply with the compliance measures under this Code; and b) an explanation as to why those measures are appropriate. A provider that has received such a request from eSafety is required to submit a Code report within 2 months of receiving the request, but for the first request no earlier than 12 months after this Code comes into effect. A provider will not be required to submit a Code report to eSafety more than once in any 12-month period. *This mirrors the Code reporting obligations included across relevant Phase 2 Codes and also extends the reporting requirements of section 36 of the Phase 1 RES Standard, as amended as appropriate for Phase 2.*

Trust and safety function (closed communication relevant electronic services)	**Compliance measure 8.14** A provider of a service must have, or have access to, sufficient personnel to oversee the safety of the service. Such personnel must have the skills, experience and qualifications needed to ensure that the provider complies with the requirements of this Code at all times. *This measure extends requirements in section 17 of the Phase 1 RES Standard to this Code, as appropriate for Phase 2. See also the comment on measure 8.8 above.*
Engagement (closed communication relevant electronic services)	**Compliance measure 8.15** A provider of a service must either: a) appropriately engage with safety and community organisations (such as civil society groups, public interest groups and representatives of marginalised communities), academics and government to gather information to help inform the measures taken for the purposes of protecting or preventing children from accessing or being exposed to class 1C and class 2 material; or b) enter into arrangements for cooperating and collaborating with other organisations (such as industry associations) in activities of the kind referred to in paragraph a) to enhance online safety for Australians. *This provision is also supplementary to section 22 of the Phase 1 RES Standard.* *This mirrors the engagement obligations included across a number of other relevant Phase 2 Codes. The option set out in b) has been included in this Code as there are a number of active industry associations operating in the relevant electronic services space, and there are benefits to leveraging those existing relationships and structures to conduct engagement activities. The outcome will be the same as engagement carried out under a) and the information gathered via the engagement needs to be considered by the provider, regardless of how it is obtained (i.e. regardless of which option is taken for engagement).*

Complaints tools (closed communication relevant electronic services)	**Compliance measure 8.16** A provider of a service must provide a tool or mechanism which enables Australian end-users to make a complaint about a breach of this Code by the provider. If an Australian end-user makes a complaint of the kind referred to in this measure, the provider must consider any relevant information provided by the Australian end-user pursuant to their complaint in a reasonably timely manner. The complaints tool or mechanism must: a) be easily accessible and simple to use; and b) where the tool or mechanism does not involve use of a widely used communication mechanism – have clear instructions on how to use it. The provider must develop and comply with internal policies and procedures for dealing with complaints made through this tool or mechanism. *This extends section 28 of the Phase 1 RES Standard to this Code, with appropriate amendments for Phase 2.*
Timely referral of unresolved complaints to eSafety (closed communication relevant electronic services)	**Compliance measure 8.17** A provider of a service must promptly refer to eSafety complaints from Australian end-users concerning a material non-compliance with this Code by the provider, where the provider is unable to resolve the complaint within a reasonable timeframe. *This measure extends section 26 of the Phase 1 RES Standard to this Code, with amendments as appropriate for Phase 2.*
Timely response to communications from eSafety (closed communication relevant electronic services)	**Compliance measure 8.18** A provider of a service must implement policies and procedures that ensure that it responds in a timely and appropriate manner to communications from eSafety about compliance with this Code.

7.8.6. Compliance measures for other communications relevant electronic services

Table 9 of this Code contains measures for other communication relevant electronic services. These apply in addition to table 7 (where relevant).

In general, other communications relevant electronic services have the same obligations in this Code as closed communication relevant electronic services subject to minor differences only.

However different measures of significance to note are as follows:

Terms and conditions prohibiting illegal activity (other communication relevant electronic services)	**Compliance measure 9.1** A provider of a service must: a) have terms and conditions in place with Australian end-users prohibiting the sharing of online pornography by an end-user to an end-user who is an Australian child; b) publish the terms and conditions by making them accessible on a website and/or application for the service (as relevant); c) ensure the prohibition described in a) is set out in plain language in the terms and conditions; and d) if the provider becomes aware of a breach of the prohibition described in a), take appropriate and proportionate action in a reasonably timely manner. It is not necessary that a particular form of words be used in the terms and conditions so long as the contractual effect of the terms and conditions is as required by sub-measure a). A provider must have systems and/or processes in place to support compliance with the obligation in d). *This measure differs from measure 8.1 above. Given the nature of other communications relevant electronic services, and differences in what is possible for these services, providers have been required to contractually prohibit the sharing of online pornography by an end-user to another end-user who is an Australian child.*

Reporting mechanisms (other communication relevant electronic services)	**Compliance measure 9.2** A provider of a service must provide a tool or mechanism which enables Australian end-users to report breaches of the prohibition described in measure 9.1 a). If an Australian end-user reports a breach via the tool or mechanism, the provider must: a) respond promptly to the end-user acknowledging receipt of the report; and b) if appropriate, take action pursuant to measure 9.1 d). The reporting tool or mechanism must: c) be available in-service, that is, not solely on a website separate to the website for the service, unless it is not technically feasible or reasonably practicable for the provider to do this; d) be easily accessible and easy to use; and e) ensure that the identity of the reporter is not disclosed to the reported end-user (i.e. the individual who has been reported should not be able to see the person who reported them) without the reporter's express consent, except as required by applicable law. The provider must develop and comply with internal policies and procedures for dealing with reports made through this tool or mechanism. *This measure differs from measure 8.2 above. Reporting tools or mechanisms for other communication relevant electronic services must be in-service.*

Safety features and settings (other communication relevant electronic services)	**Compliance measure 9.5** A provider of a service must ensure that it has appropriate tools, features and/or settings available and accessible to assist Australian end-users to limit receipt of unsolicited material (including class 1C and class 2 material). At a minimum, such tools, features and/or settings must include: a) if the service allows the sending of messages between end-users: i. tools that allow Australian end-users to block direct messages from other end-users; and ii. settings for Australian end-users that allow them to prevent the receipt of unwanted messages from other end-users; and b) if the service allows the sending of messages in a group chat between three or more end-users – tools that allow Australian end-users to leave that group chat. If the provider allows Australian children to become end-users of the service, the provider must ensure that the settings referred to in paragraph a)ii. above are defaulted to the most restrictive settings for an Australian child at the time of account registration. Other examples of such tools, features and/or settings include: c) with respect to online pornography, tools, features and/or settings that automatically blur images detected as containing nudity on receipt; d) if the service uses recommender systems to present material to end-users – tools, features and/or settings that prevent or reduce the occurrence of online pornography, self-harm material and high-impact violence material from being promoted to Australian children; and e) if the provider allows Australian children to become end-users of services – have default settings for Australian children that prevent an end-user who is over the age of 18 years and is not connected to an Australian child from being able to use the service to send a direct message to that Australian child. *This measure differs from measure 8.5 above. This measure has been designed to address common features of other communications relevant electronic services.*

28 February 2025.

7.8.7. Compliance measures for dating services

Table 10 of this Code contains measures for dating services. These apply in addition to table 7 (where relevant).

In general, dating services have the same obligations in this Code as closed communications relevant electronic services subject to minor differences only.

However, measures 10.7 and 10.8 only apply if a provider has not implemented appropriate age assurance measures and access control measures before providing access to its service.

In addition the following measures contain differences that have been included for consistency with the Online Safety Code for Dating Services. This includes content detection obligations for dating services given the nature of these services.

Terms and conditions prohibiting illegal activity (dating services)	**Compliance measure 10.1** A provider of a service must: a) have terms and conditions in place with Australian end-users that include any restrictions that they impose in relation to the sharing of class 1C and class 2 material on their service including at a minimum prohibiting the end-user from sharing material via the service in the course of engaging in any of the following categories of criminal activity i. non-consensual sharing of intimate images; ii. grooming of children; or iii. sexual extortion (or sextortion); b) publish the terms and conditions by making them accessible on a website and/or application for the service (as relevant); c) ensure the prohibition described in a) is set out in plain language in the terms and conditions; and d) if the provider becomes aware of a breach of the prohibition described in a), take appropriate and proportionate action in a reasonably timely manner including the moderation of content to comply with the terms and conditions. It is not necessary that a particular form of words be used in the terms and conditions so long as the contractual effect of the terms and conditions is as required by sub-measure a).

	A provider must have systems and/or processes in place to support compliance with the obligation in d). *This measure differs from measure 8.1 above. Changes have been made to sub-measure a) and d) for consistency with the Online Safety Code for Dating Services.*
Detection (dating services)	**Compliance measure 10.2** A provider of a dating service must implement appropriate systems, processes, and policies: a) which allow, where technically feasible and reasonably practicable, for the detection of class 1C or class 2 material sent in a communication involving an Australian end-user where that incident violates the provider's terms and conditions; and b) to review any such detected incidents that violate the provider's terms and conditions and take action as required by measure 10.1 d). *This measure has only been included for dating services. This measure has been added due to the nature of dating services, and for consistency with the Online Safety Code for Dating Services.*

7.8.8. Compliance measures for gaming services with communications functionality

As in the Phase 1 RES Standard, this Code distinguishes between gaming services with limited communications functionality and gaming services with communications functionality.

Table 11 of this Code contains measures for gaming services with communications functionality. These apply in addition to table 7 (where relevant).

In general, gaming services with communications functionality have the same obligations in this Code as closed communication relevant electronic services subject to minor differences only.

However different measures of significance to note are as follows:

Safety features and settings (gaming services with communications functionality)	**Compliance measure 11.5** A provider of a service must ensure that it has appropriate tools, features and/or settings available and accessible to assist Australian end-users to limit receipt of unsolicited material (including class 1C and class 2 material). At a minimum, such tools, features and/or settings must include: a) if the service allows the sending of messages between end-users – tools, features and/or settings that allow Australian end-users to block, mute or otherwise prevent receipt of messages (including messages containing class 1C and class 2 material) from other end-users: and b) if the service allows the sending of messages in a group chat between three or more end-users – tools, features and/or settings that allow Australian end-users to leave that group chat. An example of other such tools, features and/or settings includes: c) if the service uses recommender systems to present material to end-users – it has tools, features and/or settings that prevent or reduce the occurrence of class 1C and class 2 material from being promoted to Australian children. *This measure differs from measure 8.5 above. This measure has adopted some of the additional requirements applied to other communications relevant electronic services in measure 9.5 given some of these additional requirements are also relevant to gaming services with communications functionality.*

7.8.9. Compliance measures for gaming services with limited communications functionality

Table 12 of this Code contains measures for gaming services with *limited* communications functionality. These apply in addition to table 7 (where relevant).

The measures in table 12 only apply to gaming services with limited communications functionality that are simulated gambling games, as well as any other gaming services with limited communications functionality that have been classified as R18+.

28 February 2025.

Gaming services with limited communications functionality are subject to a more limited set of measures (given that the limits on their functionality significantly reduces potential risk levels).

The measures for gaming services with *limited* communications functionality are limited to measures equivalent to measures 8.13 and 8.16 as well as information requirements as set out below.

Information for Australian end-users (gaming services with limited communications functionality)	**Compliance measure 12.1** A provider of a service must publish clear online safety information that is accessible to Australian end-users which: a) explains the role and functions of eSafety, including how to make a complaint to eSafety; b) includes information about the complaints tool or mechanism required by measure 12.3; and c) includes information about how Australian end-users can contact third party services that may provide counselling and support. *This measure has been drafted specifically to reflect the measures included in this Code for gaming services with limited communications functionality.*

7.8.10. Compliance measures for telephony RES

Table 14 of this Code contains measures for telephony relevant electronic services. These apply in addition to table 7 (where relevant).

The compliance measures for telephony relevant electronic services are more limited owing to the characteristics of these services. A screening of SMS and MMS services, as potentially envisaged by eSafety, is not feasible either because of technical and legal limitations and/or because the implementation of measures would be vastly disproportionate to the likely harm caused and exceedingly costly to implement.

It is worth noting that account holders for telephony relevant electronic services typically are adults or have the permission of a parent or guardian to be account holders.

The measures for telephony relevant electronic services mirror measures 8.1 8.2, 8.9 (as relevant to reporting and complaints mechanisms), 8.10, 8.11, 8.13, 8.16 and 8.18 with minor changes only.

7.8.11. Compliance measures for Tier 1 – Tier 3

Table 15 of this Code contains measures for Tier 1 to Tier 2 relevant electronic services. These apply in addition to table 7 (where relevant).

The compliance measures are for categories of services that are presently unknown.

In general, Tier 1 relevant electronic services have the same obligations in this Code as closed communication relevant electronic services subject to minor differences only.

28 February 2025.

However, measure 15.5 is aligned with measure 9.5 (the other communications relevant electronic services measure) not measure 8.5 (the closed communications relevant electronic services measure). Minor changes have been made (when compared to measure 9.5) to take account of the current lack of visibility surrounding what types of services could fall into this category in the future.

Tier 2 services have the same measures as Tier 1 other than measures 15.5, 15.6, 15.7, 15.11, 15.12, 15.15 and 15.18 (which apply to Tier 1 only).

7.8.12. Compliance measures for enterprise relevant electronic services

There are no additional compliance measures for these services in this Code.

7.9. Schedule 3 Designated Internet Services Online Safety Code (Class 1C and Class 2 material)

7.9.1. Code structure

This Code comprises the Head Terms and Schedule 3, covering designated internet services as defined in the OSA. As per the Designated Internet Standard, the Code also includes safeguards for end-user-managed hosting services.

The following table maps each compliance measure in the *Designated Internet Services Online Safety Code (Class 1C and Class 2 Material)* against the two online safety objectives issued by eSafety. This table maps each measure against the online safety objective it is primarily aimed at meeting. However, many of the compliance measures in this Code contribute to meeting more than one objective. As such, the table should be read as guidance only.

Objective	Compliance measure
Objective 1 *Protect and prevent children in Australia from accessing or being exposed to class 1C and class 2 material.*	7.1; 7.2; 7.3; 7.4; 7.6; ,7.7; 7.8; 7.18; 7.19; 7.22; 7.24; 8.1; 8.2; 8.3; 8.4; 8.9; 9.1; 9.2; 9.4; 9.5; 10.1; 10.3; 10.4; 10.5; 10.6; 10.7; 10.10; 10.19; 10.20; 10.23; 11.1; 11.2; 11.3.
Objective 2 *Provide Australian end-users with effective information, tools and options to limit access and exposure to class 1C and class 2 material*	7.5; 7.9; 7.10; 7.15; 7.16; 7.17; 8.7; 8.8; 9.6; 10.2; 10.8; 10.9; 10.16; 10.17; 10.18
Other Supporting compliance measures	7.11; 7.12; 7.13; 7.14; 7.20; 7.21; 7.23; 7.25; 8.5; 8.6; 8.10; 8.11; 8.12; 9.3;10.11; 10.12; 10.13; 10.14; 10.15; 10.21; 10.22; 10.24; 11.4; 11.5.

eSafety will be aware that a broad range of services are captured by the definition of designated internet services (also referred to as "**DIS**") in the OSA, i.e., the majority of apps and websites that can be accessed by end-users in Australia, including grocery and retail websites, websites

containing contact and service information for small businesses such as cafes, hairdressers and plumbers, apps offered by medical providers to allow patients to access x-ray imagery, information apps such as train or bus timetable apps, newspaper websites, personal blogs, artistic websites, as well as websites aimed at providing educational, information and entertainment content to Australian end-users and adult websites. Furthermore, the definition of designated internet service in the OSA is not fixed but broad and open-ended, covering: (a) a service that allows end-users to access material using an internet carriage service; and (b) a service that delivers material to persons having equipment appropriate for receiving that material, where the delivery of the service is by means of an internet carriage service. Like the definitions of 'relevant electronic service' (also referred to as "**RES**") and 'social media service' (also referred to as "**SMS**"), the Minister can in future specify services as designed internet services by legislative instrument.

7.9.2. DIS categories

Given the breadth of services captured as designated internet services, this Code adopts the approach taken in the Designated Internet Services Standard.

Specifically, the Code includes equivalent definitions for the following service categories:

- **classified DIS**
- **end-user managed hosting service**
- **enterprise DIS**
- **general purpose DIS**
- **model distribution platform; and**
- **pre-assessed DIS**

This Code also includes new DIS categories being:

- **high impact class 2 DIS** means a DIS that:

(i) has the sole or predominant purpose of enabling end-users to access any or all of the following types of material:

(A) online pornography;

(B) self-harm material; and/or

(C) high impact violence material

(ii) includes a service that is taken to be a high impact class 2 DIS because of clause 6(d)(i).

- **high impact class 2 generative AI DIS** means a DIS that:

(i) uses machine learning models to enable an end-user to produce material; and

(ii) has the sole or predominant purpose of being used to generate any of the following types of material:

(A) online pornography;

(B) self-harm material; and/or

(C) high impact violence material

and includes a service that is taken to be a high impact class 2 generative AI DIS because of clauses 6(d)(i) and 6(d)(ii).

These new categories ensure that the Code targets measures at those services that present the greatest risk of harm to Australian children.

28 February 2025.

7.9.3. Approach to risk assessment

As a general principle, designated internet services must assess their risk under this Code except for:

- designated internet services who notify eSafety on or before commencement date of the Code that they have a Tier 1 risk profile. This exception intends to encourage services to proactively notify eSafety that they have a Tier 1 risk profile, providing clarity to eSafety of the status of these services;
- operating systems, which are dealt with under the Equipment Code (please refer to the Equipment Code for further detail);
- a pre-assessed DIS and an enterprise DIS both of which are deemed to have a Tier 3 risk profile in respect of the restricted categories of material. This limits the compliance burden on a vast range of low-risk services that primarily provide information for business, commerce, charitable and health purposes such as counselling and support services and services that are primarily provided to enterprise customers. A website or app that does not meet this criteria, such as a wiki or news service that allows end users to chat with other end users would be required to do a risk assessment and determine its risk profile as either Tier 1, 2 or 3 in respect of each restricted category of material;
- classified DIS that has the sole or predominant purpose of providing general entertainment content that is, or would be classified a certain way under the *Classification (Publications, Films and Computer Games) Act 1995* (Cth);
- high impact class 2 DIS, in respect of the category of material it has the sole or predominant purpose for. These services are automatically deemed to have a Tier 1 risk profile in respect of that material. This will capture, for example pornography sites and websites dedicated to pro-suicide material. We note that eSafety's research found that 70% of young people surveyed who accessed pornography did so on mainstream pornography websites;
- high impact class 2 generative AI DIS, in respect of the category of material it has the sole or predominant purpose for. These services are automatically deemed to have a Tier 1 risk profile in respect of that material;
- end-user managed hosting services; and
- model distribution platforms.

A provider of a DIS not referred to above, must undertake a risk assessment in respect of each restricted category of material to determine its risk profile for each category. The requirements in relation to the risk assessment methodology and documentation have been aligned with the Designated Internet Services Standard.

7.9.4. Approach to measures

This Code codifies industry best practices that provide safeguards for the community in respect of the matters set out in the section 141 notice. The Code applies these safeguards and makes them enforceable for a much broader range of designated internet service providers (including future and developing designated internet service providers) than the existing range of designated internet service providers that currently adopt best industry practices in respect of those matters. As with the RES Code, there are different measures for each category of designated internet service and each measure is proportionate to the relevant service. For example, there are less measures for end-users managed hosting services as these services do not themselves entail a risk of harm to children (and none were identified by eSafety's research). In contrast, pornography services pose the highest risk of harm to children and are subject to the

most stringent measures. In the case of a classified DIS, many services will not offer pornography, but may offer content that would be classified as only suitable for adults because it contains other sexually explicit content, and measures have been included that are proportional to the risk of harm presented by that material. Where a classified DIS makes available pornography, the age assurance measures that apply to a high impact class 2 DIS (e.g. a pornography site) apply in the same way to the classified DIS.

7.9.5. Compliance measures for DIS with a Tier 1 – Tier 3 risk profile (excluding high impact generative AI DIS)

Age assurance measures	**Compliance measure 7.1** The provider of the service must, where technically feasible and reasonably practicable, implement: (a) appropriate age assurance measures; and (b) access control measures, before providing access to the designated internet service or the relevant high impact materials. A service provider must also take appropriate steps to test and monitor the effectiveness of its age assurance and access control measures over time. *As this measure applies to Tier 1 services (including those with the sole or predominant purpose of providing access to a relevant high risk materials), compliance can be achieved through either a service level restriction (i.e. age assurance and access control occurs prior to the service being accessed by any Australian end-users) or as a category level restriction (i.e. age assurance occurs prior to accessing the relevant high risk material).*
Continuous improvement for systems regarding online pornography and/or self-harm material	**Compliance measure 7.2** A provider of a service that: (a) is not a deemed tier 1 high impact service; and (b) does not allow online pornography and/or self-harm material on its service; must invest in and take appropriate steps to continuously improve systems which can detect online pornography and/or self-harm material and automatically action that material before it is encountered by end-users. *Similar to the approach taken in the SMS Code, DIS services that do not allow a restricted category of material must detect and automatically action that material before it is encountered by end-users.*

28 February 2025.

Reporting mechanisms	**Compliance measure 7.3** The provider of the service must provide tools which enable Australian end-users to report, flag and/or make a complaint about class 1C and/or class 2 materials which they consider may be contrary to a service's terms and conditions, and must, where appropriate ensure that these reports are evaluated and actioned. Such reporting mechanisms must: (a) be easily accessible and easy to use; and (b) be accompanied by clear instructions on how to use them. The provider must ensure that the identity of a complainant is not accessible, directly or indirectly, by any other end-user or account holder of the service without the express consent of the complainant, except as required by law. *See suggested measure in 1.1 of the table of suggested measures in the eSafety Position Paper July 2024, page 82.*
On interface reporting tools	**Compliance measure 7.4** The provider of the service must ensure that the reporting tools referred to in measure 7.3 above are available and accessible to Australian end-users on-the interface of the designated internet service. *This measure compliments Compliance measure 7.3 by ensuring that reporting tools are readily accessible on a service. See equivalent measure in SMS Code.*

Safety Tools	**Compliance measure 7.5** The provider of a service that: (a) is not a deemed tier 1 high impact service; and (b) allows online pornography and/or self-harm material on the service must allow all end-users to opt-in at any time to appropriate safety tools which may limit their access or exposure to online pornography and/or self-harm material on the service. Appropriate safety tools may include solutions for: (a) filtering material; (b) removing material from marketing and/or recommender systems; (c) blocking material; (d) blurring material; (e) halting autoplay of material; and/or (f) placing interstitial notices on material so that users can click through to view if they wish. Information about the appropriate safety tools implemented by the provider must be readily accessible to Australian end-users. *eSafety's Position Paper July 2024 recommends that DIS services should set default privacy and safety levels to the highest settings available for child end-users to protect and prevent children from being exposed to class 1C and class 2 material. While child end-users should not be able to access high-risk materials where age assurance (Compliance measure 7.1) or proactive detection (Compliance measure 7.2) is required, this measure is intended to enable all end-users (not specifically children) to manage their exposure to restricted categories of material.*
Terms and conditions	**Compliance measure 7.6 & 7.7** The provider of the service must have, and enforce, clear actions, policies or terms and conditions relating to the relevant high-risk material, which will include, to the extent applicable, terms and conditions dealing with the types of relevant high-risk material that are allowed or not allowed on the designated internet service. In implementing this measure, a provider of a DIS must: (a) use simple, plain, and straightforward language; (b) to the extent practicable, be clear about the type of any material that is prohibited; and (c) communicate such terms and conditions, standards and/or policies to all personnel that are directly involved in their enforcement. Relevant policies and actions must be implemented according to a graduated, risk-based approach. This approach may be different for different types of material.

	Note: Compliance measure 7.6 and Compliance measure 7.7 differ slightly depending on the risk profile of the DIS. The language from Compliance measure 7.6 has been extracted here. *This approach replicates the approach taken in the SMS Code.*
Trust and safety function	**Compliance measure 7.8** The provider of the service must have, or have access to sufficient personnel to oversee the safety of the service. Such personnel must have the skills, experience and qualifications needed to ensure that the provider complies with the requirements of this Code at all times. *This measure extends appropriate requirements in section 19 of the DIS Standard to this Code for relevant services.*
Information about how services deal relevant high-risk materials	**Compliance measures 7.9 & 7.10** The provider of the service must publish clear and accessible information that explains the actions they take to reduce the risk of harm to Australian children caused by the distribution of relevant high-risk material on its service. *Note: Compliance measures 7.9 and Compliance measures 7.10 differ slightly depending on the risk profile of the DIS. The language from Compliance measure 7.9 has been extracted here.* *These measures complement Compliance measure 7.1 and Compliance measure 7.2.*
Timely referral of unresolved complaints to eSafety	**Compliance measure 7.11** The provider of the service must promptly refer to eSafety complaints from Australian end-users concerning a material non-compliance with this Code by the service provider, where the service provider is unable to resolve the complaint within a reasonable time frame. *This measure extends appropriate requirements in section 30 of the DIS Standard to this Code for relevant services.*
Timely response to communications for eSafety	**Compliance measure 7.12** The provider of a service must implement policies and procedures that ensure that it responds in a timely and appropriate manner to communications from the Commissioner about compliance with this Code.

28 February 2025.

Updates to eSafety about relevant changes to technology	**Compliance measures 7.13 & 7.14** A service provider must share information with eSafety in writing about significant changes to the functionality of their services that are likely to have a material positive or negative effect on the access or exposure to, distribution of, or online storage of relevant high-risk materials by Australian children. A service provider may choose to provide this information in an annual report to eSafety under this Code. In implementing this measure, a provider is not required to disclose information to eSafety that is confidential. *Note: Compliance measure 7.13 and Compliance measure 7.14 differ slightly depending on the risk profile of the DIS. The language from Compliance measure 7.13 has been extracted here.* *This measure extends appropriate measures requiring notification of changes to a service in section 34 of the DIS Standard to this Code, for relevant services*.
Information for Australian end-users about the role and functions of eSafety, including how to make a complaint to eSafety	**Compliance measures 7.15 & 7.16** The provider of the service must publish clear information that is accessible to Australian end-users which explains the role and functions of eSafety, including how to make a complaint to eSafety. *This measure extends appropriate requirements in section 26 of the DIS Standard to this Code for relevant services.*
Location on or via service that is dedicated to providing online safety information	**Compliance measure 7.17** The provider of the service must establish a location accessible on or via the service that is dedicated to providing online safety information that: a. contains information required under this Code; b. includes information about how Australian end-users can contact third party services that may provide counselling and support; and c. is accessible to Australian end-users. *This measure extends appropriate requirements in section 26 of the DIS Standard to this Code for relevant services.*

28 February 2025.

Complaints tools	**Compliance measure 7.18 & 7.19** The provider of the service, other than a deemed tier 1 high impact service, must provide tools which enable Australian end-users to make a complaint about: (a) the provider's handling of reports about online pornography and/or self- harm material that is accessible on the service; or (b) any other aspect of the provider's compliance with this Code. Such complaints tools must: (a) be easily accessible on or through the service and easy to use; (b) be accompanied by plain language instructions on how to use them; and (c) enable the complainant to specify the non-compliance to which the report or complaint relates. The provider must ensure that the identity of a complainant is not accessible, directly or indirectly, by any other end-user or account holder of the service without the express consent of the complainant, except as required by law. *Note: Compliance measure 7.18 and Compliance measure 7.19 differ slightly depending on the risk profile of the DIS. The language from Compliance measure 7.18 has been extracted here.* *This measure extends appropriate requirements in section 27 of the DIS Standard to this Code for relevant services.*
Training for personnel responding to reports and complaints	**Compliance measure 7.20** The provider of the service must ensure that personnel responding to reports referred to in compliance measures 7.3, 7.18 and 7.19 are trained in the designated internet service's policies and procedures for dealing with reports and complaints. *This measure replicates the equivalent requirement in the SMS Code for higher risk services.*
Review of compliance personnel with systems and processes	**Compliance measure 7.21** The provider of the service must review the effectiveness of its reporting systems and processes to ensure reports are assessed and actioned (if necessary) within reasonably expeditious timeframes, based on the level of harm the material poses to Australian children. Such review must occur at least annually. *This measure replicates the equivalent requirement in the SMS Code for higher risk services.*

28 February 2025.

Significant changes to services	**Compliance measure 7.22** The provider of the service must ensure that before it makes a material change to the service that will significantly increase the risk of sharing of relevant high-risk material to an Australian child it must: a) carry out an assessment of the kinds of features and settings that could reasonably be incorporated into the service to minimise that risk; and b) where appropriate, apply features and settings so identified to help to mitigate that risk. *This measure extends appropriate requirements in section 24 of the DIS Standard to this Code for relevant services.*
Engagement	**Compliance measure 7.23** The provider of the service must appropriately engage with safety and community organisations (such as civil society groups, public interest groups and representatives of marginalised communities), academics and governments to gather information to help inform measures taken for the purposes of protecting or preventing children from accessing or being exposed to class 1C and class 2 material. The provider of the service must consider information obtained through such engagement. *This measure compliments the Head Terms.*
Notifying changes to features and functions – generating high impact material	**Compliance measure 7.24** A service provider must share information with eSafety in writing about significant changes to the functionality of their services that are likely to significantly increase or decrease the risk of generation of online pornography and/or self-harm material by Australian children using generative artificial intelligence. Where applicable, a service provider may choose to provide this information in an annual report to eSafety under this Code. In implementing this measure, a provider is not required to disclose information to eSafety that is confidential. *This measure extends appropriate requirements in section 33 of the DIS Standard to this Code for relevant services.*

28 February 2025.

Reporting to eSafety on Code compliance	**Compliance measure 7.25** Where eSafety issues a written request to a provider of a service to submit a Code report, the provider named in such request must submit to eSafety a Code report which includes the following information: (a) the steps that the provider has taken to comply with the compliance measures under this Code; (b) details of any risk assessment it is required to undertake pursuant to this Code; and (c) an explanation as to why these steps are appropriate. A provider of a service that has received such a request from eSafety is required to submit a Code report within 2 months of receiving the request, but for the first request no earlier than 12 months after this Code comes into effect. A provider of a service will not be required to submit a Code report to eSafety more than once in any 12-month period. *This measure extends appropriate requirements in section 36 of the DIS Standard to this Code for relevant services.*

7.9.6. Compliance measures for class 1C and class 2 material - end-user managed hosting services

The measures for end-user managed hosting services are largely consistent with the approach taken for communication relevant electronic services in relation to the sharing of certain categories of illegal materials.

7.9.7. Compliance measures for classified DIS

The measures for classified DIS, distinguish between a classified DIS that makes available high impact materials and those which do not.

28 February 2025.

Reporting mechanisms	**Compliance measure 9.1** A provider of a classified DIS that only makes available content that has been classified in accordance with the Classification Act must ensure end-users are provided a mechanism to report content which they consider may have been incorrectly classified. All other providers of classified DIS, must provide tools which enable Australian end-users to report, flag and/or make a complaint about content which they consider may be contrary to a service's terms and conditions, and ensure that these reports are considered and actioned appropriately. Such reporting mechanisms must: a. be easily accessible and easy to use; and b. be accompanied by clear instructions on how to use them. The provider must ensure that the identity of a complainant is not accessible, directly or indirectly, by any other end-user or account holder of the service without the express consent of the complainant. *This measure distinguishes between DIS that only provide materials that are classified under the National Classification Scheme e.g. films and video, and DIS which may have unclassified and classified materials.* *See suggested measure in 1.1 of the table of suggested measures in the eSafety Position Paper July 2024, page 82.*
Trust and safety function	**Compliance measure 9.2** The provider of the service must have, or have access to sufficient personnel to oversee the safety of the service. Such personnel must have the skills, experience and qualifications needed to ensure that the provider complies with the requirements of this Code at all times. *This measure extends appropriate requirements in section 19 of the DIS Standard to this Code for relevant services.*
Reporting to eSafety on Code compliance	**Compliance measure 9.3** Where eSafety issues a written request to the provider of the service to submit a Code report, the provider named in such request must submit to eSafety a Code report which includes the following information: (a) the steps that the provider has taken to comply with the compliance measures under this Code; and (b) an explanation as to why these steps are appropriate. A provider of a service that has received such a request from eSafety is required to submit a Code report within 2 months of receiving the request, but for the first request no earlier than 12 months after this Code comes into effect. A provider of a service will not be required to submit a Code report to eSafety more than once in any 12-month period. *This measure extends appropriate requirements in section 36 of the DIS Standard to this Code for relevant services.*

Compliance measures for high impact classified material	Please note the introduction of this concept for this Code: **high impact classified material** means any of the following: (i) films or the contents of a film that has: (A) been classified X18+ by the Classification Board under the Classification Act; (B) not been classified, but if classified, would likely be classified X18+ (collectively, **X18+ material**); (ii) Films or the contents of a film that has been classified R18+ in accordance with the Classification Act (R18+ Material); and (iii) publications and other material that is not a film or the contents of a film that is otherwise Class 2A material under the Code (other 2A material); Note: This may include, for example, books, newspapers and magazines, whether in digital or audio form, podcasts or digital music that if required to be classified, would likely be classified X18+ in a corresponding way in which a film would be classified under the Classification Act. (iv) self-harm material; and (v) simulated gambling material.
Appropriate measures to limit the risk of child end-users accessing or being exposed to other 2A and/or self-harm material	**Compliance measure 9.4** A provider of a classified DIS must, to the extent technically feasible and reasonably practicable implement appropriate measures that limit the risk of Australian children accessing or being exposed to other 2A material, R18+ and/or self- harm material. Examples of how a classified DIS could comply with this measure include: (a) enabling the creation of child profiles on the service to limit children's access to other 2A material, R18+ and/or self-harm material; or (b) implementing notices or functions e.g. warning labels, blurring, halting autoplay, and notice screens on other class 2A material, R18+ and self-harm material; or (c) filtering other 2A material, R18+ and self- harm material out of discovery feeds by downlisting, deprioritising or quarantining such material to Australian children; or (d) ensuring that recommender systems, algorithms, and other choice architecture, do not promote other 2A material, R18+ or self- harm material to Australian children; or (e) enabling users to opt in at any time to appropriate safety tools which may limit their access or exposure to other 2A material, R18+ or self- harm materials. *These measures deal with 2A materials that are not films (e.g. publications) as well as R18+ and self-harm material, and are designed to restrict and limit the exposure of users to these materials.*

28 February 2025.

Age assurance measures	**Compliance measure 9.5** A provider of a classified DIS must, where technically feasible and reasonably practicable, implement: (a) appropriate age assurance measures; and (b) access control measures, before providing access to X18+ material and/or simulated gambling material. A service provider must also take appropriate steps to test and monitor the effectiveness of its age assurance and access control measures over time. *This measure extends age assurance requirements that apply to providers of Tier 1 DIS services to classified DIS in respect of appropriate categories of material given the nature of those services.*
Information about tools and settings	**Compliance measure 9.6** To the extent a provider of a classified DIS implements features, functionalities or settings to comply with Compliance measure 9.4 and Compliance measure 9.5, the provider must provide clear and accessible information to explain those features, functionalities or settings in a manner that is easily understood by users of all ages permitted on the service. *This measure complements Compliance measure 9.4 and Compliance measure 9.5.*

7.9.8. Compliance measures for high impact generative AI DIS

Compliance measures for high impact generative AI DIS largely replicate measures for high impact class 2 DIS. The key differences are that the measures have been tailored to ensure they are appropriate for generative AI services (e.g. safety by design defaults include measures that are only appropriate for models), and that for services that are not Tier 1, some of the measures apply to the creation of online pornography only (so less contextual assessment is required for lower risk services). Even so, requirements that are not content specific (e.g. the requirement to have trust and safety personnel, display safety information and implement appropriate processes and review mechanisms) will apply to a broader range of generative AI services.

7.9.9. Compliance measures for model distribution platforms

The eSafety Position Paper July 2024 did not recommend any compliance measures for model distribution platforms. Nevertheless, we have proposed appropriate compliance measures for these services. The compliance measures proposed are substantively identical to those for hosting service providers given the similar roles these services play in the tech stack.

Policies and contractual terms relating to applicable Australian content laws	**Compliance measure 11.1** A provider of a model distribution platform must have in place policies and/or contractual terms that make clear to customers of the service that customers must, when using the service, comply with applicable Australian content laws and regulations, including industry codes or standards made pursuant to the OSA, that create legal obligations for customers relating to class 1C and class 2 material.

	This measure implements the suggested measures for hosting service providers at 3.4 of the table of suggested measures in the eSafety Position Paper July 2024, page 86.
Enforcement action relating to customer breaches of policies and contractual terms	**Compliance measure 11.2** A provider of a model distribution platform service must: (a) take appropriate and proportionate enforcement action with respect to customers of the service that breach its policies and/or contractual terms relating to complying with applicable Australian content laws and regulations, including industry codes or standards made pursuant to the OSA that create legal obligations for customers relating to class 1C and class 2 material; (b) Have systems and processes, including standard operating procedures to: i. enforce their policies when they become aware of non-compliance with the policies and/or contractual terms outlined in measure 11.1; and ii. escalate reports of non-compliance with measure 11.1 above. *This measure supports Compliance measure 11.1.*
Contact mechanisms	**Compliance measure 11.3** A provider of a model distribution platform must: (a) ensure that end-users can contact the provider in relation to breaches of applicable Australian content laws and regulations by customers of the model distribution platform service; (b) provide information or links to information about: i. applicable Australian content laws and regulations; and ii. the role and function of eSafety and how to make a complaint to eSafety under the Online Safety Act. *This measure extends the requirement for reporting mechanisms in section 27 of the DIS Standard that apply to model distribution platforms to this Code.*
Timely response to communications from eSafety	**Compliance measure 11.4** The provider of a service must implement policies and procedures that ensure that it responds in a timely and appropriate manner to communications from the Commissioner about compliance with this Code. *This is similar to the approach taken in the Hosting Code.*

28 February 2025.

Reporting to eSafety on Code compliance	**Compliance measure 11.5** Where eSafety issues a written request to a provider of a model distribution platform, the provider named in such request must submit to eSafety a Code report which includes the following information: (a) the steps that the provider has taken to comply with their applicable compliance measures; and (b) an explanation as to why these steps are appropriate. A provider of a model distribution platform who has received such a request from eSafety is required to submit a Code report within 2 months of receiving the request, but for the first request no earlier than 12 months after this Code comes into effect. A provider of a model distribution platform will not be required to submit a Code report to eSafety more than once in any 12-month period. *This measure extends appropriate requirements for reporting to eSafety that apply to model distribution platforms in section 36 of the DIS Standard to this Code.*

7.10. Schedule 4 App Distribution Services Online Safety Code (Class 1C and Class 2 Material)

This Code Schedule will be submitted to eSafety with an updated Request for Registration on or before March 28 2025.

7.11. Schedule 5 Hosting Services Online Safety Code (Class 1C and Class 2 Material)

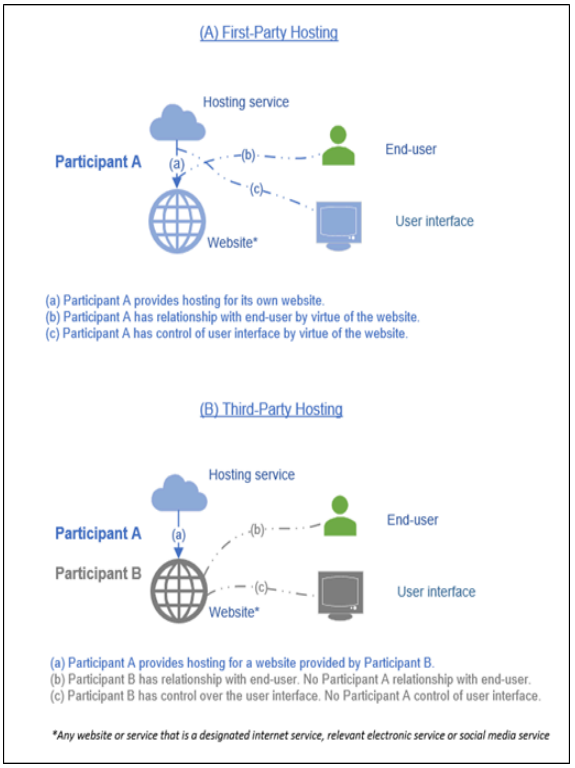
7.11.1. Code structure

This Code comprises the Head Terms and Schedule 5, covering Third-Party Hosting Services. A Third-Party Hosting Service is defined in this Code as a service provided by a person that hosts stored material that has been provided on another person's social media service, relevant electronic service, or designated internet service. The following table maps each compliance measure in the *Hosting Services Online Safety Code (Class 1C and Class 2 Material)* against the two online safety objectives issued by eSafety. This table maps each measure against the online safety objective it is primarily aimed at meeting. However, many of the compliance measures in this Code contribute to meeting more than one objective. As such, the table should be read as guidance only.

Compliance measures for the first party hosting of materials by a social media service, relevant electronic service, or designated internet service (including an end-user-managed hosting service) are dealt with within the applicable Code for that service (see Preamble to Head Terms). A First-Party Hosting Service is defined in this Code as a service provided by a person that hosts stored material that has been provided on that person's own social media service, relevant electronic service, or designated internet service. This is consistent with the approach adopted for the Phase 1 Hosting Services code.

Objective	Compliance measure
Objective 1 *Protect and prevent children in Australia from accessing or being exposed to class 1C and class 2 material.*	1 & 2
Objective 2 *Provide Australian end-users with effective information, tools and options to limit access and exposure to class 1C and class 2 material*	3, 4
Other Supporting compliance measures	5

The following diagram illustrates the distinction between a First-Party Hosting Service and a Third-Party Hosting Service:



Distinguishing between Third-Party Hosting Services and First-Party Hosting Services is important given the significant differences between the two, not only in terms of end-user engagement, but also in the different purposes they have in relation to hosting material online and their technical, legal, and practical ability to exercise control over an individual piece of material.

While the distinction between Third-Party Hosting Services and First-Party Hosting Services is not set out in the OSA, it is contemplated by the two-pronged nature of the 'hosting service'

definition in section 17 of the OSA, with subsection (b) acknowledging the possibility of either the 'first person or another person' providing the social media service, relevant electronic service, or designated internet service on which hosted material is provided. As required by the definition of 'hosting service' in the OSA, the definitions of "Third-Party Hosting Service" and "First-Party Hosting Service" also necessarily include reference to social media service, relevant electronic service, and designated internet service.

This distinction between Third-Party Hosting Services and First-Party Hosting Services also aligns with feedback provided by eSafety during the Code development process that services like 'end-user-managed hosting services' were better dealt with in other Codes.

7.11.2. Approach to risk assessment

While there are different kinds of Third-Party Hosting Services, they have the generally equivalent purpose and functionality of supporting the delivery of another service online, performing a 'back-end' or technical function. As such, for the purpose of this Code and the compliance measures in this Code, all Third-Party Hosting Services are deemed to have a generally equivalent risk profile.

7.11.3. Approach to measures

This Code codifies industry best practices that provide safeguards for the community in respect of the matters set out in the section 141 notice. As Third-Party Hosting Services are deemed to have a generally equivalent risk profile, this Code applies these safeguards and makes them enforceable for all providers of Third-Party Hosting Services.

The measures in this Code recognise that the nature of a Third-Party Hosting service inherently limits the control that can be exercised over individual pieces of material on the service. Providers of Third-Party Hosting Services do not have an effective ability to engage with end-users, and instead have their relationship with other service providers, who themselves have relationships with their end-users.

Policies and contractual terms relating to applicable Australian content laws	**Compliance measure 1** A provider of a third-party hosting service must have in place policies and/or contractual terms that make clear to customers of the service that customers must, when using the service, comply with applicable Australian content laws and regulations, including industry codes or standards made pursuant to the OSA, that create legal obligations for customers relating to class 1C and class 2 material. *This measure implements the suggested measure in 3.4 of the table of suggested measures in the eSafety Position Paper July 2024, page 86.*

Enforcement action relating to customer breaches of policies and contractual terms	**Compliance measure 2** A provider of a third-party hosting service must: (a) take appropriate and proportionate enforcement action with respect to customers of the service that breach its policies and/or contractual terms relating to complying with applicable Australian content laws and regulations, including industry codes or standards made pursuant to the OSA, that create legal obligations for customers relating to class 1C and class 2 material; (b) have systems and processes, including standard operating procedures to: i. enforce their policies when they become aware of non-compliance with the policies and/or contractual terms outlined in measure 1; and ii. escalate reports of non-compliance with measure 1 above. *This measure supports Compliance measure 1.*
Contact Mechanisms	**Compliance measure 3** A provider of a third-party hosting service must: (a) ensure that end-users can contact the provider in relation to breaches of applicable Australian content laws and regulations of the third-party hosting service; (b) provide information or links to information about: i. applicable Australian content laws and regulations; and ii. the role and function of eSafety and how to make a complaint to eSafety under the OSA. *This extends equivalent provisions in the Hosting Services Online Safety Code (Class 1A and Class 1B Material) to this Code.*
Timely response to communications from eSafety	**Compliance measure 4** A provider of a third-party hosting service must implement policies and procedures that ensure it responds in a timely and appropriate manner to communications from eSafety about compliance with this Code. *This extends equivalent provisions in the Hosting Services Online Safety Code (Class 1A and Class 1B Material) to this Code.*

28 February 2025.

Reporting to eSafety on Code compliance	**Compliance measure 5** Where eSafety issues a written request to a provider of a third-party hosting service to submit a Code report, the provider named in such request must submit to eSafety a Code report which includes the following information: a) the steps that the provider has taken to comply with their applicable compliance measures; and b) an explanation as to why these steps are appropriate. A provider of a third-party hosting service who has received such a request from eSafety is required to submit a Code report within 2 months of receiving the request, but for the first request no earlier than 12 months after this Code comes into effect. A provider of a third-party hosting service will not be required to submit a Code report to eSafety more than once in any 12-month period. *This extends equivalent provisions in the Hosting Services Online Safety Code (Class 1A and Class 1B Material) to this Code.*

7.12. Schedule 6 Internet Carriage Services Online Safety Code (Class 1C and Class 2 Material)

7.12.1. Approach

This Code comprises the Head Terms and Schedule 6, and applies to providers of internet carriage services (internet service providers or ISPs). It only applies to retail ISPs, that means entities that supply internet carriage services to Australian end-users.

Objective	Compliance measure
Objective 1 Protect and prevent children in Australia from accessing or being exposed to class 1C and class 2 material.	While some compliance measures may have a greater bearing on a specific objective, all compliance measures seek to address both Objectives.

Objective 2 Provide Australian end-users with effective information, tools and options to limit access and exposure to class 1C and class 2 material.	

This Code provides safeguards for the community in respect of the matters set out in the section 141 notice for ISPs.

Given that the role and capabilities of ISPs remain the same irrespective of the material that may be transmitted or accessed using their services, this Code heavily builds on the *Internet Carriage Services Online Safety Code (class 1A and class 1B Material*) but further strengthens protections in line with proposed measures from eSafety's Position Paper.

In line with the Position Paper, when determining what compliance measures are appropriate for ISPs, consideration has been given to the role of ISPs in the supply chain[1]:

Online safety is a shared responsibility, and ISPs can and should enhance online safety by implementing safeguards appropriate to their role in communications and the online environment.

ISPs, due to the nature of the services they provide and extensive existing regulations, pose a lower risk compared to content providers or providers of services that provide access to content 'over-the-top', which are more directly involved in the creation and distribution of online content.

ISPs are already regulated under separate telecommunications-specific legislation with extensive consumer protections, which also help to mitigate risks associated with their services. ISPs are also subject to a highly prescriptive and extensive Complaint Handling Standard which is enforced by the regulator, ACMA.

ISPs act as a mere conduit for content/services/applications to be provided, i.e. they only provide connectivity. Their role in the 'technology stack' (i.e. of technologies/providers that enable end-users to interact/communicate online) means that they neither create nor control or have visibility of content transmitted through their infrastructure (networks) or of the applications/platforms on which content it is disseminated.

In addition, ISPs are required to adhere to the requirements of *the Telecommunications Act 1997* and the *Telecommunications (Access and Interception) Act 1979* (amongst other regulations) which prohibit the access, disclosure and/or use of content transmitted (unless under a warrant). The very limited exemptions in relation to scams that regulations provide do not apply to the screening of content for class 1 or class 2 content.

Consequently, the options within the control of ISPs in relation to content and applications are limited to the blocking of user access to domains which host/transmit harmful or unlawful content on request. Importantly, this can only occur on a whole-of-domain basis, i.e. no blocking of individual posts etc.

ISPs can also seek to influence application vendors in relation to particular safety features or content outcomes. However, given Australia's role in global markets, this influence is limited.

Nevertheless, ISPs contribute to the safety of end-users through the provision of information and the promotion of filters, at the time of sale and in regular (annual) intervals. Moreover, they will assist filter providers, where technically possible, with compatibility issues. They also assist end-users with any complaints and reports made in relation to class 1 and class 2 material.

28 February 2025.

The market for internet filters is mature and competitive. A large number of suppliers serve this market. There are currently eleven filters certified under the Family Friendly Filter program, in addition to filters which are not accredited but may provide equal or better protection. The decision to develop filters is a commercial decision that cannot be mandated through regulation. ISPs may decide to develop their own filters or 'partner' with filter providers.

ISPs are distinct from hosting service providers and relevant electronic services providers. Where an ISP provides a hosting or relevant electronic service (for example, a telephony (voice) or SMS service), these services are being dealt with under the respective codes for such services. Internet carriage services are purely limited to the provision of connectivity to the internet.

7.12.2. Risk

Under this Code, owing to the role of ISPs in the ecosystem, all retail ISPs are deemed to have the same risk and are subject to the same minimum compliance measures. All compliance measures are mandatory.

It is noted that, at eSafety's request in relation to the class 1A and 1B Material, this Code does not impose (contrary to industry's intention, as discussed during the development of the Code for class 1A/B material) a minimum compliance measure requiring ISPs to have processes in place to check that new Australian account holders seeking an internet carriage service are adults, or if they are a child, that they have the consent of a parent/guardian or responsible adult.

Easily Accessible User Information Providers should ensure that Australian end-users are advised of how to help prevent access to class 2 material by child end-users on an ICS, including by regularly notifying them about filter products, including the Family Friendly Filter program.	**Compliance measure 1:** An internet service provider must make information available to Australian end-users on filtering products, how they can be obtained and how end-users can provide feedback about compatibility issues between the filtering product and the internet service provided by the internet service provider. This information must be easily accessible on an internet service provider's website (if the internet service provider has a website), in plain language and be provided at or close to the time of the sale, as well as at least annually thereafter. *This measure addresses the Position Paper's request for ISPs to promote internet filters.* *This measure has been strengthened beyond the already existing measure of the class 1 ICS Code to also include the provision of information as to how end-users can provide feedback about compatibility issues (where they exist/are perceived to exist) between the filtering product and the internet service provided by the internet service provider.* *The Compliance measure has also been strengthened by requiring the provision of such information in plain language (a newly defined term) and that the information be provided on a provider's website. The definition of 'plain language' aligns with the definition in the revised Telecommunications Consumer Protections (TCP) Code (under revision, 'plain language' definition not controversial).* *Under the revised TCP Code, an ISP is to make available, the contact details of an interpreter service in at least five 'community languages', on its website with its own contact information, on bills and Critical Information Summaries (prominently available for all offers on the website/in store etc.). In addition, ISPs must make available information about translation tools or services that a consumer may use to translate key information.* *A translation of information into multiple languages would be disproportionate and is unnecessary with the increasing availability of AI tools.* *This approach (translation into other languages) is in line with the approach taken in the energy sector which also does not require translation of similar information into multiple languages. (In fact, the requirements in the TCP Code go beyond the requirements in most other sectors.)* *Importantly, the information is not only provided as a 'one-off' but must now also be provided on an annual basis to ensure end-users remain aware of the options that filters provide.* *ISPs have tens of millions of customers/services in operation and receive complaints on a multitude of issues in significant numbers. Complaints on class 1 or 2 materials are, to our knowledge, non-existent. It would, therefore, be disproportionate to train each ISP's entire complaint handling frontline staff/design processes to provide filtering-specific information at the time of a complaint or as part of the complaints handling process for the eventuality that a complaint in that respect may be made/an exceedingly small number of complaints.* *Also refer to our comments on Safety Tools further below.* *In addition, Compliance measure 2 requires the promotion of the FFF:*

	Compliance measure 2: When providing the information as required in measure 1, an internet service provider must also promote the Communications Alliance FFF program, either by incorporating information on its own website or by linking to a Communications Alliance page that contains this information. If an internet service provider already provides non-FFF program filters, the provision of those filters will not be impacted, but internet service providers must also promote the FFF program so that Australian end-users have the option of taking up an FFF. *By linking this measure to Compliance measure 1, this measure has also been strengthened as the information on FFF will now also need to be provided in annual intervals.* *Communications Alliance would consult with eSafety regarding any proposed changes to the FFF program and eSafety would be provided with associated information about how the Codes are proposed to be amended following any change.*
Right to complaint, links to complaint processes, responding to complaints Providing end-users with links to complaint systems (both those administered by industry and by eSafety)	**Compliance measure 3:** An internet service provider must make available information to Australian end-users on their right to complain to a content provider and eSafety (including where a complaint to a content provider remains unresolved) about class 1C and class 2 material, or unsolicited electronic messages that promote such material. **Compliance measure 4:** An internet service provider must make available, via its website, a link to eSafety's online content complaints reporting process. *Compliance measures 3 and 4 ensure that end-users are aware of their right to complain. These Compliance measures remain unchanged from the class 1 codes. No feedback to alter these Compliance measures was received.* **Compliance measure 5:** An internet service provider must either establish processes, procedures and/or systems to respond to any complaint or report it receives from an Australian end-user about class 1C and class 2 material or refer the complainant/reporter to eSafety. An internet service provider's process to respond to a complaint or report about class 1C and class 2 material must be easily accessible, easy to use and include or be accompanied by clear instructions on how to use the process.

	An internet service provider must respond to the complaint or report in a timely manner, including where the provider refers the complainant/reporter to eSafety. *Compliance measure 5 was strengthened to require ISPs to establish processes, procedures and/or systems to respond to complaints and reports of class 1C and class 2 material, in line with the feedback received from eSafety. The Compliance measure continues to include an option for referral to eSafety, as per the class 1 code.* *In line with the language from the class 1 RES standard, this process must be easily accessible, easy to use and include or be accompanied by clear instructions on how to use the process.* *Corresponding to the language of the class 1 RES standard, a response to the complaint or report, including a referral to eSafety, must occur in a timely manner.* *It is important to highlight that ISPs are subject to the Telecommunications (Consumer Complaints Handling) Industry Standard 2018 (CHS), and, irrespective of interpretation of the standard, deal with complaints made to them following the processes and timelines set out in the CHS.* *The CHS sets out detailed rules for the handling of complaints, including timeframes for responding to complaints The CHS contains detailed requirements on processes, procedures and systems, for monitoring and analysing their respective complaints records to identify systemic issues and problems, and prevent those systemic issues, problems and related complaints from recurring.* *The replication of current requirements in the CHS is impractical (given likely future change) and contrary to regulatory best practice. Given eSafety is of the opinion that the CHS would not find legal application to complaints made to ISPs in relation to material, language that is consistent with the CHS and aligned to the RES Standard has been chosen. The establishment of a separate, and potentially deviating (deviating from the class 1 ICS Code as well as from the Complaint Handling Standard), complaint handling requirement in the class 2 Code would be impractical and disproportionate.*
Safety Tools Ensure compatibility between internet carriage services provided to end-users and third party filtering or blocking tools which may be activated by customers of that service to prevent and protect children from being exposed to class 1C and class 2 material.	**Compliance measure 1:** An internet service provider must make information available to Australian end-users on filtering products, how they can be obtained and how end-users can provide feedback about compatibility issues between the filtering product and the internet service provided by the internet service provider. This information must be easily accessible on an internet service provider's website (if the internet service provider has a website), in plain language and be provided at or close to the time of the sale, as well as at least annually thereafter. *This measure ensures that end-users not only receive information about the availability of filters but also about how to provide feedback about potential compatibility issues. This information must be easily accessible, in plain language, on a provider's website and be provided at/close to time of sale as well as annually, to remind end-users of their options.* *ISPs are not aware of any compatibility issues between filter products and ISP services, and consequently do not suggest greater specificity.*

	Drops in speed can have many reasons and would most likely <u>not</u> be associated with filtering products. It would be helpful, or indeed counter-productive, to suggest that filtering products are a likely cause of speed issues. *Third-party filtering or blocking tools – as well as filters provided or sold as an 'add-on' by ISPs – are typically installed by an end-user on their respective device. Compatibility relates to the operating system and/or software installed (e.g. malware software) on that device, i.e. it is not related to the service provided by the ISP. Sometimes, very tech-savvy end-users may want to re-configure routers to block access to specific URLs or domains. Provided this functionality is generally possible for the specific router, it could typically also not be influenced by the ISP. Filters not performing as intended or malfunctioning routers would typically be the result of user-error, i.e. the user having tempered with the router settings to render the router ineffective and/or not having the desired blocking effect. This equally holds for filters that are proprietary to ISPs, i.e. most compatibility issues are not within the control of the ISP. (In fact, it is hard to think of any that fall within the ISPs control.)* *Due to the number of different types of routers available through third parties (even if supplied by the ISP), ISPs would not be in a position to guarantee compatibility of re-configured devices with their network. The same would also hold for filters on devices.* *Filtering products, even if proprietary to an ISP, are applied at a device level. Compatibility is a function of the device and its settings, it is not a function of the internet service provided by the ISP. Therefore, ISPs also do not retain control over the compatibility of the filtering products with devices, be they proprietary or third-party.* *This measure is further complemented by additional measures to improve any compatibility issues with ISP proprietary and third-party filter products if/where they arise for end-users. Please refer to Compliance measures 7 and 8 (see further below).* **Compliance measure 6:** An internet service provider must make easily accessible to Australian end-users plain-language information on online safety in respect of class 1C and class 2 material, including information for parents/carers about how to supervise and control children's access and exposure to class 1C and class 2 material, and provide Australian-end-users information about the role and functions of the eSafety Commissioner. *This Compliance measure complements the other Compliance measures by providing additional information, in plain language, on online safety and how parents/carers can supervise and control access and exposure to harmful material.* *In addition, ISPs will provide information about the role of eSafety, thereby further strengthening the avenues for end-users to seek assistance (if needed) and information.*
Improvement of protective tools Providers should measurably invest in and improve the efficacy and end-user experience with filters and parental controls, to	**Compliance measure 7:** If an internet service provider makes available a proprietary filtering product, the internet service provider must, except where not technically feasible and reasonably practicable, ensure compatibility of that filtering product and the internet service it provides.

encourage users to adopt these tools and reduce user drop-off from filters as the result of poor service or user experience.	**Compliance measure 8:** Where an internet service provider becomes aware, or should reasonably be aware, of compatibility issues between the internet service provided by the internet service provider and a filtering product that is either a) directly endorsed by the internet service provider, or b) a filtering product that is part of the FFF program, the internet service provider must provide feedback on the compatibility issue to c) the provider of the filtering product where the filtering product has been directly endorsed, or d) Communications Alliance where the product is part of the FFF program. Except where not technically feasible and reasonably practicable, an internet service provider must attempt to assist a filtering provider in relation to the filtering products it promotes or endorses by taking appropriate actions to resolve any identified compatibility issues between that filtering product and its internet service. *The market for filters is mature and competitive. A large number of suppliers serve this market. There are currently eleven filters certified under the Family Friendly Filter program, in addition to filters which are not accredited but may provide equal or better protection. The decision to develop filters is a commercial decision that cannot be mandated through regulation. ISPs may decide to develop their own (proprietary) filters or 'partner' with filter providers.* *Noting our feedback above, these measures have been added to ensure that, to the extent possible, ISPs will ensure compatibility with proprietary filters and provide feedback on compatibility issues that they become aware of to third party filter providers and/or CA.* *A requirement for ongoing investment into proprietary filters is likely to be counter-productive as it could act to disincentivise ISPs to invest into proprietary filters in the first place. Where ISPs wish to invest into proprietary filters, commercial imperatives will drive improvement of such filters, including in areas of product adoption, user attrition, performance and user experience etc.* *ISPs will also attempt to assist the third-party filtering providers to resolve compatibility issues. A reasonableness standard for awareness has been included to strengthen this measure. The measure seeks to further improve the user experience with filtering tools.* *As highlighted above, ISPs do not have control over any parental controls – these are to be set at a device/ecosystem level and/or through the filtering software.* *ISPs can also not provide any metrics around efficacy of filters. This data would, if at all, only be available from the filter providers. We assume that commercial filters now may use AI to incorporate user behaviour in relation to potentially unwanted material.*

28 February 2025.

Reporting	**Compliance measure 9:** Where eSafety issues a written request to a provider of an internet service to submit a Code report, the provider named in such request must submit to eSafety a Code report which includes the following information: a) the steps that the provider has taken to comply with their applicable minimum compliance measures; b) an explanation as to why these measures are appropriate; c) the number of complaints in relation to class 1C and class 2 material an internet service provider has responded to under minimum compliance measure 8 above; and d) the number of complaints received about compliance with this Code. A provider of an internet service who has received such a request from eSafety is required to submit a Code report within 2 months of receiving the request, but for the first request no earlier than 12 months after this Code comes into effect. A provider of an internet service will not be required to submit a Code report to eSafety more than once in any 12-month period. *Compliance measure 9 is the same as for the class 1 codes. Given the risk profile of ISPs is the same as for class 1 material and given the Compliance measure references applicable minimum compliance measures (which have been adjusted to strengthen requirements), the Compliance measure remains appropriate and adequate.*

[1] eSafety Commissioner, *Development of industry codes under the Online Safety Act, Position Paper*, September 2021 p.51.

7.13. Schedule 7 Equipment Online Safety Code (Class 1C and Class 2 Material)

7.13.1. Scope

Following the approach in the Phase 1 Codes, this Code covers manufacturers, suppliers and maintenance and installation providers as defined in the OSA, and also covers operating system providers (defined in this Code as OS providers) for certain devices with higher risk profiles.

This Code codifies and further develops industry best practices that provide safeguards for the community in respect of the matters set out in the section 141 notice for such providers.

28 February 2025.

In particular, this Code includes a very significant uplift in the measures applied to both higher risk devices *and* devices with lower risk profiles when compared to the Phase 1 Codes as set out further in 7.12.2 below. Industry has achieved this by building on the measures in the Phase 1 Codes, resulting in a set of measures that goes significantly beyond what was put in place in 2023 at a device level.

The following table maps each compliance measure in the Equipment Online Safety Code (Class 1C and Class 2 Material) (Equipment Code) against the two online safety objectives issued by eSafety.

This table maps each measure against the online safety objective it is primarily aimed at meeting. However, many of the compliance measures in this Code contribute to meeting more than one objective. As such, the table should be read as guidance only.

Objective	Compliance measure
Objective 1 **Protect and prevent children in Australia from accessing or being exposed to class 1C and class 2 material**	1, 2, 3, 4, 15, 17, 23 14 (as it relates to measures 2 and 3)
Objective 2 **Provide Australian end-users with effective information, tools and options to limit access and exposure to class 1C and class 2 material**	5, 6, 8, 9, 10, 11, 12, 13, 16 14 (as it relates to measure 8)
Other supporting compliance measures	7, 18, 19, 20, 21, 22, 24 and 25

7.13.2. Approach to risk of devices

Definitions for different categories of device

The Equipment Code defines devices into three mutually exclusive categories: interactive (Tier 1) devices, secondary (Tier 2) devices and non-interactive (Tier 3) devices. The definitions for these categories exactly mirror the three categories that were used in the Phase 1 Codes.

Rather than requiring a risk assessment to be undertaken (as some of the other Phase 1 Codes do), the Equipment Online Safety Code (Class 1A and Class 1B Material) (Phase 1 Equipment Code) contained set definitions for each category of device. For instance, to be an interactive (Tier 1) device, a piece of equipment must satisfy all four of the limbs set out in that definition – which go to factors such as the interactivity of the device, whether it is personal and portable (in the sense that it may be carried with the end-user), whether it is a standalone device and whether general internet browsing via a screen or display is an intended significant function. These factors were seen as uniform risk factors that should contribute to an interactive (Tier 1) device categorisation.

28 February 2025.

Devices covered by the Code that do *not* satisfy these four limbs will fall into one of the other two categories reflecting the lower risk levels associated with such devices. To take an example, unlike interactive (Tier 1) devices like mobile phones and tablets, a smart screen generally has the intended significant function of enabling end-users to watch or stream content for general entertainment purposes via pre-loaded apps, as opposed to enabling users to interact with the device or services on the device, or to browse the internet. Such screens will also frequently be communal and not designed to be portable/carried with the end-user. Such factors reduce the risk with such a device and result in such devices falling outside the interactive (Tier 1) device categorisation.

All of the key definitions from the Phase 1 Equipment Code have been retained without amendment in this Code to ensure that the approach that the Commissioner found to meet appropriate community safeguards with respect to class 1A and class 1B material has been retained, and to enable a consistent approach to categorisation for providers.

For absolute certainty given the uplift in measures described above, an additional standalone category of "other interactive device" has been added in this Code. This ensures that *any* device covered by the Code that falls outside the interactive (Tier 1) device definition but has general internet browsing as a significant intended function and certain communications functionality will be subject to relevant measures.

A table with criteria designed to guide industry participants subject to this Code with determining their devices has been provided in section 6, which reflects the same approach taken in the Phase 1 Codes.

Approach to different device categories

The compliance measures in this Code once again place the most significant obligations on providers of interactive (Tier 1) devices (and associated operating systems of these devices). OS providers for such devices are obliged to enable Australian end-users to set up child accounts or profiles (for children under 13 at a minimum) and restricted accounts or profiles (for children under 18) and the Code obliges providers to apply certain mandatory defaults and settings to such accounts or profiles as described further below.

Unlike the Phase 1 Equipment Code where the vast majority of mandatory minimum compliance measures were applied to interactive (Tier 1) devices, this Code also applies very significant measures to a number of devices that fall outside of that category – with a particular focus on "other interactive devices". In the Phase 1 Equipment Code, unless a secondary (Tier 2) device was a gaming device, it primarily had a set of optional measures to consider as required by the Head Terms. Whilst devices that fall outside of the interactive (Tier 1) device category remain lower risk and have therefore been dealt with in a risk proportionate manner, there are now significant mandatory measures applied to other interactive devices in Phase 2 in response to eSafety's suggestions. This includes measures such as requiring the development and implementation of tools, features and/or settings to assist Australian end-users to safely manage the experience of children using such devices, as well as associated information and reporting requirements.

Also unlike the Phase 1 Equipment Code, this Code does not include measures specifically aimed at 'children's interactive devices' (devices targeted at children) or 'gaming devices' (devices specifically designed for online gaming). Instead, the compliance measures apply to all relevant devices regardless of whether the equipment is targeted at children or specifically designed for gaming. This approach is consistent with the July 2024 Position Paper where eSafety indicated that focusing on child-targeted devices is not useful for the purposes of the Phase 2 measures as it does not adequately address the practical reality of device use among children in relation to class 2 material such as pornography.[23] Further, this ensures that gaming devices with general internet browsing capability, and therefore the highest risk of enabling access to class 2 material

[23] *July 2024 Position Paper p76*

by a child, are subject to the measures in this Code in the same way as other devices not specifically designed for gaming.

7.13.2. Approach to supply chain/equipment providers

Compliance measures have been applied to participants in the supply chain/group of equipment providers where they are most effective with respect to the aim of targeting class 1C/2 material and/or where they can most efficiently be handled given global distribution networks of devices. Consideration has been given to the impact of measures on small businesses, such as maintenance providers and installation providers.

7.13.4. Approach to device level measures

Devices and operating systems are the furthest point in the tech stack away from the provision of actual class 1C and class 2 content, making it more challenging to devise compliance measures that are proportionate and tailored *only* to class 1A and class 2 materials.

Approach to age-related signals

Industry has not adopted the model of upfront full age assurance for all device users, regardless of what services/ content they wish to access. However, industry has worked constructively and in good faith to develop a series of tailored approaches that it believes address eSafety's online safety objectives, whilst ensuring that the Equipment Code will operate in tandem with the other Phase 2 Codes to provide a set of interrelated protections at all levels of the tech stack.

In terms of the approach taken in this Code, industry has built up the requirements regarding age-related signals at a device level in order to ensure that appropriate protections are in place across the entire technology stack.

In particular, for interactive (Tier 1) devices such as mobile phones and tablets it has:

a) introduced default safety requirements for child accounts or profiles set up for younger Australian child end-users under the age of thirteen, and restricted accounts or profiles set up for Australian end-users under the age of eighteen;
b) ensured that only linked adult accounts can adjust relevant default settings for younger Australian child end-users with child accounts or profiles; and
c) added a provision regarding sharing information about such accounts or profiles, or otherwise restricting them, within an OS provider's organisation where necessary to facilitate compliance with child-protection obligations under the other Phase 2 Codes.

This is in addition to requirements to make tools, features and/or settings more broadly available to Australian end-users.

This approach offers flexibility (bearing in mind the extremely broad range of devices covered by the Equipment Code) whilst ensuring that default protections for child end-users are always in place at a device level as an additional safeguard to the other measures in place under the other Phase 2 Codes.

Industry wishes to highlight that it is not possible to view the equipment provider's role with respect to the services offered on devices in isolation. Whilst equipment providers have an important role to play, and take their role as an additional line of protection very seriously, in considering whether appropriate community safeguards have been applied, the Equipment Code operates in combination with the other Phase 2 Codes which apply to the services accessed via these devices (as well as the existing measures in the Phase 1 Codes) and should be considered in combination with those Codes as a combined set of community safeguards.

28 February 2025.

Approach to device level measures

As noted above, devices and operating systems are the furthest point in the tech stack away from the provision of actual class 1C and class 2 content, making it more challenging to devise compliance measures that are proportionate and tailored only to class 1A and class 2 material.

For example, unlike content services, device providers generally do not have terms and conditions in place with end-users regulating content (because they are not providing content to end-users). As such, alternative and complementary measures have been developed in the Equipment Code that take advantage of the unique nature of this Code (by comparison to the Codes applicable to content services) – such as ensuring that providers take advantage of the various "touch points" that occur in the course of equipment manufacturer, supply and support to provide information and education to end-users.

In addition, the approach taken on the Equipment Code recognises the facts that:

a) many device-level settings involve intervention at the service/app level (e.g. switching particular apps on or off, or blocking particular services, on devices being shared to children), or at the "contactability" level (e.g. blocking/approving contacts) rather than at the content level;
b) there are an extremely broad range of device types covered by the Equipment Code and what may be possible on one device, or one provider's device, may not be possible, practicable, workable or the most optimal solution on others;
c) even where some providers have content-level interventions in place at a device level, these are often more suited to some particular service-types or some forms of material (e.g. nudity that could suggest the presence of online pornography) than others; and
d) some provider settings only work on some services, or groups of services, available on the provider's device.

Because they are the furthest point in the tech stack away from the provision of content, the steps that are available at a device level will always supplement those available at a service level and as noted above should be considered in combination. These principles have underpinned the approach taken to various measures across the Code.

7.13.5. Compliance measures:

Account set-up (OS providers of Tier 1 devices)	**Compliance measure 1** An OS provider must enable Australian end-users to set up child accounts or profiles and restricted accounts or profiles for use on interactive (Tier 1) devices. *The default settings applied to child accounts or profiles and restricted accounts or profiles by this Code build on the requirements already applied to children's interactive devices in the Phase 1 Codes. A drafting note has been included to draw providers' attention to that existing requirement.*

Defaults and settings for child accounts or profiles (OS providers of Tier 1 devices)	**Compliance measure 2** An OS provider must: a) have: (i) appropriate default safety settings for child accounts or profiles set up under measure 1 that reduce the risk of such accounts or profiles being used to view online pornography; and (ii) for interactive (Tier 1) devices that are mobile phones or tablets, have tools, features and/or settings available to Australian end-users that can be used to reduce the risk of unsolicited contact (including unsolicited contact containing class 1C or class 2 material) via such child accounts or profiles; and b) only permit the default safety settings, and tools, features and/or settings, referred to in sub-measure a) to be adjusted via an adult account or profile that is linked to the child account or profile. A number of examples of such default safety settings, and tools, features and/or settings, are provided. *This reflects the July 2024 Position Paper p 76-77 regarding the creation of parent and child accounts, and associated parental safety controls. This measure also reflects the 2024 Position Paper p 86 that on-device measures to protect children from access or exposure to class 2 material should be turned on by default and the ability to opt-out is restricted to parents. This measure applies to child accounts or profiles, which is defined in this Code as accounts or profiles for end-users under the age of thirteen. This ensures the most vulnerable, young Australian child end-users are protected via default safety settings. This measure is complemented by measure 3 of this Code which provides protections for restricted accounts or profiles (which provides coverage for children aged thirteen to seventeen) as well as measure 8 which requires safety tools, features and/or settings to be made available to Australian end-users more broadly.* *Compliance measure 2 takes a risk proportionate approach which recognises that mobile phones and tablets are the interactive (Tier 1) devices most frequently and widely carried with children outside of the home without adult supervision, and accordingly applies additional measures to such devices.* *Given the variety of interactive (Tier 1) devices, and the broad and varying range of services offered on them, significant guidance is included on this measure to provide clarity to OS providers as to how to comply with this measure. For example, the guidance makes it clear that default safety settings at a device level may not operate across all services that an end-user may utilise on the device noting that device users may access a broad range of third party apps, websites and services on their device and the OS provider will often be limited in what it can do at a device level with respect to such third-party services. This does not alter the substantive measure to (to take one requirement), have appropriate default safety settings for child accounts or profiles.*

	The requirements regarding tools, features and/or settings to reduce unsolicited contact have not been described as defaults given they will always require parental input to set-up (e.g. in order for the responsible adult to specify which individuals should or should be able to contact their child using relevant messaging functionality that is enabled). However, such tools, features and/or settings must be a key part of a child account or profile and the child must not be able to adjust the settings (this must only be done via the linked adult account.
Defaults and settings for restricted accounts or profiles (OS providers of Tier 1 devices that are mobile phones or tablets)	**Compliance measure 3** For interactive (Tier 1) devices that are mobile phones or tablets, an OS provider must have: a) default safety settings for restricted accounts or profiles set up under measure 1 that reduce the risk of such accounts or profiles being used to view online pornography; and b) have tools, features and/or settings available to Australian end-users that can be used to reduce the risk of unsolicited contact (including unsolicited contact containing class 1C or class 2 material) via such restricted accounts or profiles. A number of examples of such default safety settings, and tools, features and/or settings, are provided. *Similar guidance to measure 2 has been included.* *As with some parts of measure 2, measure 3 recognises that mobile phones and tablets are the interactive (Tier 1) devices most frequently and widely carried with children outside of the home without adult supervision, and has therefore subjected such devices to a more significant set of obligations.* *Compliance measure 3 recognises that older children will frequently be granted more autonomy and responsibility within family units, whilst ensuring that protections are still on by default for such accounts.*

Facilitating tools, features and/or settings on other OS provider services (OS providers of Tier 1 devices)	**Compliance measure 4** Where: a) an OS provider provides the operating system for an interactive (Tier 1) device; b) the OS provider also offers any of the OS provider's own services on the interactive (Tier 1) device; and c) the OS provider has obligations under other Phase 2 Codes to have tools, features and/or settings to mitigate risks to Australian children on such services, that OS provider must share information about whether an account or profile is a child account or profile, or a restricted account or profile, with those services, or otherwise restrict a child account or profile, or a restricted account or profile, for those services, as necessary to facilitate such tools, features and/or settings. *This ensures that OS providers leverage account or profile settings as necessary within their organisations to facilitate child protection obligations under the Codes.*
On-device measures for adult accounts or profiles (OS providers of Tier 1 devices)	**Compliance measure 5** An OS provider for an interactive (Tier 1) device must permit an Australian end-user with an adult account or profile to adjust safety settings to a more restrictive level for a device which they intend to give to, or share with, a child. *This measure reflects the guidance at p 86 of the July 2024 Position Paper to give adult users options to restrict content on a device which they intend to give to, or share with a child.*
Information regarding default measures (manufacturers and OS providers of Tier 1 devices)	**Compliance measure 6** A person who is a manufacturer of an interactive (Tier 1) device or an OS provider must ensure that easily accessible information in plain language is made available to Australian end-users about: a) how to set up child accounts or profiles; b) how to set up restricted accounts or profiles; c) the default safety settings it has applied pursuant to measure 2a)i) and 3a) above; d) how to adjust those default safety settings; e) the tools, features and/or settings it has available pursuant to measure 2a)ii. and 3b) above; and f) how to adjust those tools, features and/or settings. *This measure builds on measure 5 and optional measure 8 in the Phase 1 Equipment Code and adopts the feedback from eSafety in the July 2024 Position Paper at p 77.*

Cost and application (manufacturers and OS providers of Tier 1 devices)	**Compliance measure 7** A person who is a manufacturer of an interactive (Tier 1) device or an OS provider must ensure that the person does not impose any additional charge to the end-user for the features and settings described in measures 2, 3 or 5. *This measure reflects the guidance in the July 2024 Position Paper at p 86 to ensure safety features are free for end-users.*
Tools, features and/or settings (OS providers of Tier 1 devices)	**Compliance measure 8** In addition to the default safety settings and tools, features and/or settings required by measure 2 and 3, an OS provider must develop and implement appropriate tools, features and/or settings that assist Australian end-users to safely manage their experience when using the device including at a minimum managing the risk of exposure to online pornography. A number of examples of such tools, features and/or settings, are provided. *This measure reflects the guidance in the July 2024 Position Paper at p 88 to enable users to opt-in at any time to safety tools which may limit their access or exposure to class 2 material.* *This builds on the existing requirement in the Phase 1 Codes for OS providers to develop and implement relevant tools where appropriate within operating systems to allow Australian end-users to help reduce the risk of harm to children when using interactive (Tier 1) devices. A drafting note has been included to draw providers' attention to that existing requirement.* *Similar guidance to measure 2 has been included.*
Tools, features and/or settings (manufacturer of other interactive devices)	**Compliance measure 9** A manufacturer of an other interactive device must develop and implement appropriate tools, features and/or settings that assist Australian end-users to safely manage the experience of children when using the device including at a minimum managing the risk of exposure to online pornography. A number of examples of such tools, features and/or settings, are provided. *This measure builds on the existing requirement in the Phase 1 Codes for manufacturers of gaming devices to develop and implement appropriate tools that allow Australian end-users to help reduce the risk of harm to children when using gaming devices. The new measure applies much more broadly to all other interactive devices. A drafting note has been included to draw providers' attention to that existing requirement.*

Provision of information about safe use of equipment online (manufacturers of Tier 1 Devices)	**Compliance measure 10** A manufacturer of interactive (Tier 1) devices must ensure that easily accessible information in plain language with respect to: a) the tools, features and/or settings described in measure 8; and b) the role of eSafety, including a link to eSafety's complaints form, is available in the form of online safety resources. This information must include information about how Australian end-users can limit access to online pornography through use of those tools when using that equipment. *This measure builds on measure 5 of the Phase 1 Equipment Code which requires manufacturers of interactive (Tier 1) devices to ensure that certain information is available in the form of online safety resources. A drafting note has been included to draw providers' attention to that existing requirement. The new measure extends this information requirement to include information about the tools, features and/or settings required by this Code.*
Provision of information about safe use of equipment online (manufacturers of other interactive devices)	**Compliance measure 11** A manufacturer of an other interactive device must ensure that easily accessible information in plain language is made available to Australian end-users with respect to: a) the role of eSafety, including a link to eSafety's complaints form; and b) the tools, features and/or settings described in measure 9. *This measure builds on the Phase 1 Codes requirement for manufacturers of gaming devices to provide certain information to Australian end-users. This new measure supplements that requirement by adding requirements for all other interactive devices (including gaming devices that are other interactive devices). A drafting note has been included to draw providers' attention to that existing requirement.*

Provision of information about safe use of equipment online (suppliers of Tier 1 devices)	**Compliance measure 12** A supplier of interactive (Tier 1) devices must provide easily accessible information in plain language about: a) the fact that such devices have some default safety settings that will be applied if a child account or profile or restricted account or profile is set up; and b) the fact that other tools, features and/or settings are available that will help Australian end-users manage access to forms of inappropriate material and to otherwise safely manage their experience when using the device, at or around the time of a sale. It is not necessary that a particular form of words be used so long as the effect of the information is as required by sub-measure a) and b). *This measure builds on measure 5 of the Phase 1 Equipment Code which required suppliers of interactive (Tier 1) devices to provide certain information at or around the time of a sale. This measure extends that requirement to include information about default safety settings and tools, features and/or settings required by this Code. A drafting note has been included to draw providers' attention to that existing requirement.* *This measure also adopts the feedback from eSafety in the July 2024 Position Paper at p 77.*
Provision of information about safe use of equipment online (maintenance and installation providers of Tier 1 devices)	**Compliance measure 13** If a person is a maintenance provider or an installation provider of interactive (Tier 1) devices, that person must provide information with respect to: a) the availability of default safety settings for interactive (Tier 1) devices; and b) that these will be applied to child profiles or accounts, and restricted accounts or profiles, upon request. *This measure builds on measure 5 of the Phase 1 Equipment Code which required maintenance and installation providers to provide information to end-users upon request. The new measure extends this requirement to ensure the information covered includes information about the default safety settings, for child accounts or profiles and restricted accounts or profiles as required by this Code. A drafting note has been included to draw providers' attention to that existing requirement.* *This measure also adopts the feedback from eSafety in the July 2024 Position Paper at p 77.*

28 February 2025.

Improvement (OS providers of Tier 1 devices)	**Compliance measure 14** Where technically feasible and reasonably practicable, an OS provider must take appropriate steps to further develop and improve the safety tools, features and/or settings it has in place under measures 2, 3 and 8 over time. Examples of activities that a provider may engage in to meet this measure include the following (to the extent directed towards, or relevant to, the matters covered by this Code): a) any activities designed to further develop the effectiveness of the tools, features and/or settings; b) tracking new and emerging risks or issues that may be causing harm to Australian children; c) investment in research and development and/or testing of novel technological solutions; d) investment in trust and safety teams dedicated to implementing regulatory requirements and policies which enhance online safety for users of online services; e) providing financial or technical support to non-governmental organisations with recognised online safety expertise to improve their infrastructure and/or technical capabilities; f) contributing to programs operated by non-governmental organisations; g) joining relevant industry organisations or other third party organisations intended to address online harm to children and sharing information on best practice approaches; h) conducting or supporting research into and development of online safety tools, features and/or settings and approaches; i) providing support, either financial or in kind, to organisations the functions of which are or include protection of children online; j) extending the application of a tool, feature and/or setting applied to a service that is subject to a different industry code or standard under the OSA to operate in connection with its interactive (Tier 1) device; and k) activities that aim to refine algorithms or inputs into tools to improve their effectiveness. The OS provider must, at a minimum, engage in at least some of the example activities above in each calendar year. *This measure recognises that technological solutions that work to protect children from high impact restricted materials need improvement and that this will require commitments by industry of the kind outlined in this measure. This measure has been informed by the improvement requirements in the RES Standard.* *A timing requirement has been included requiring OS providers to engage in relevant activities in each calendar year.*

Trust and safety function (manufacturers and OS Providers of Tier 1 devices, as well as manufacturers of secondary (Tier 2) devices and other interactive devices)	**Compliance measure 15** A person who is a manufacturer of an interactive (Tier 1) device, a secondary (Tier 2) device or an other interactive device, or an OS provider for an interactive (Tier 1) device, must have, or have access to, sufficient personnel to oversee the safety of the device. Such personnel must have the skills, experience and qualifications needed to ensure that the provider complies with the requirements of this Code at all times. *This measure replicates the approach taken in other Codes and Standards (e.g. section 19 of the Standard for Designated Internet Services)*
Right to complain (manufacturers and suppliers of Tier 1 devices)	**Compliance measure 16** If a person is a manufacturer or supplier of interactive (Tier 1) devices, that person must make available information to Australian end-users on their right to complain to a content provider under the Phase 2 Codes and/or eSafety (including where a complaint to a content provider remains unresolved). *This measure extends the requirement in measure 10 of the Phase 1 Equipment Code to this Code.*
Complaints mechanism (manufacturers and OS providers of Tier 1 devices)	**Compliance measure 17** If a person is a manufacturer of interactive (Tier 1) devices, or an OS provider, that person must have a complaints mechanism which enables Australian end-users to make a complaint about a breach of this Code by the provider. Such complaints mechanism must: a) be easily accessible and simple to use; and b) be accompanied by plain language instructions on how to use it. If an Australian end-user makes a complaint of the kind referred to in this measure, the provider must consider any relevant information provided by the Australian end-user pursuant to their complaint in a reasonably timely manner. *This measure extends the requirement in measure 12 of the Phase 1 Equipment Code to this Code.*

Timely referral of unresolved complaints to eSafety (manufacturers and OS providers of Tier 1 devices)	**Compliance measure 18** A person who is a manufacturer of interactive (Tier 1) devices, or an OS provider, must promptly refer to eSafety complaints from Australian end-users concerning a material non-compliance with this Code by the provider, where the provider is unable to resolve the complaint within a reasonable timeframe.
Communication with eSafety concerning complaints (manufacturers and supplies of Tier 1 devices)	**Compliance measure 19** If a person is a manufacturer or supplier of interactive (Tier 1) devices, that person must implement policies and processes that ensure it responds in a timely and appropriate manner to communications from eSafety about complaints of breach of this Code. *This measure extends the requirement in measure 3 of the Phase 1 Equipment Code to this Code.*
Engagement (manufacturers and OS providers of Tier 1 devices)	**Compliance measure 20** A person who is a manufacturer of interactive (Tier 1) devices or an OS provider must appropriately engage with safety and community organisations (such as civil society groups, public interest groups and representatives of marginalised communities), academics and government to gather information to help inform the measures it takes to protect or prevent Australian children from accessing or being exposed to class 1C and class 2 material. A provider must consider information obtained through such engagement. *This measure supports the general commitment made in section 1.6 under the Head Terms.*

Staff (suppliers of Tier 1 devices)	**Compliance measure 21** A supplier of interactive (Tier 1) devices must provide tools or training to staff to: a) enable staff to appropriately comply with measure 12 (to the extent those staff are involved in meeting measure 12); and b) enable staff to appropriately respond to questions from Australian end-users regarding available complaints mechanisms in place under measure 17 (to the extent those staff are involved in responding to such questions. *This complements measure 7 of this Code.* *This builds on the existing requirement in the Phase 1 Codes for suppliers of interactive (Tier 1) devices to provide tools or training to staff to enable staff to appropriately respond to questions from Australian end-users regarding online safety, including available complaints mechanisms. This measure builds on that existing requirement to ensure this includes key training points for Phase 2. A drafting note has been included to draw providers' attention to that existing requirement.*
Updates to eSafety about relevant changes in technology (manufacturers and OS providers of Tier 1 devices, and manufacturers of Tier 2 devices and other interactive devices)	**Compliance measure 22** If a person is a manufacturer of an interactive (Tier 1) device, a secondary (Tier 2) device or an other interactive device, or an OS provider, that person must share information with eSafety in writing about significant changes to the functionality of such devices (or operating systems) released by the manufacturer or OS provider (as applicable) that are likely to have a material positive or negative effect on the access or exposure to, distribution of, and online storage of online pornography by Australian children. The person may choose to provide this information in a Code report to eSafety under this Code. In implementing this measure, a provider is not required to disclose information to eSafety that is confidential. *This extends obligations requiring notification of significant changes to eSafety that are analogous to measure 4 of the Phase 1 Equipment Code.*

Significant changes to an operating system (OS providers)	**Compliance measure 23** Before an OS provider makes a material change to the operating system for an interactive (Tier 1) device (including any new feature of the operating system enabled by generative artificial intelligence) that will significantly increase the risk of sharing of online pornography to an Australian child, it must: a) carry out an assessment of the kinds of measures that could reasonably be incorporated into the operating system to minimise that risk; and b) where appropriate, apply measures so identified to help to mitigate that risk. *This mirrors the approach taken in other Codes to material changes to key services that carry significant increases in risk.*
Reporting to eSafety on Code compliance (manufacturers and OS providers of Tier 1 devices)	**Compliance measure 24** If a person is a manufacturer of an interactive (Tier 1) device or an OS provider, then where eSafety issues a written request to that person to submit a Code report, the person named in such request must submit to eSafety a Code report which includes the following information: a) the steps that the provider has taken to comply with the compliance measures under this Code; and b) an explanation as to why these measures are appropriate. A person that has received such a request from eSafety is required to submit a Code report within 2 months of receiving the request, but for the first request no earlier than 12 months after this Code comes into effect. A person will not be required to submit a Code report to eSafety more than once in any 12 month period. *This measure extends the requirement in measure 13 of the Phase 1 Equipment Code to this Code.*

Reporting to eSafety on Code compliance (manufacturers of secondary (Tier 2) devices and other interactive devices)	**Compliance measure 25** If a person is a manufacturer of a secondary (Tier 2) device or an other interactive device, then where eSafety issues a written request to that person to submit a Code report, the person named in such request must submit to eSafety a Code report which includes the following information: a) an explanation as to why the manufacturer considers the device to be a secondary (Tier 2) device or an other interactive device (as relevant); b) if the manufacturer considers a secondary (Tier 2) device not to be an other interactive device, an explanation as to why this is the case; c) the steps that the provider has taken to comply with the compliance measures under this Code; and d) an explanation as to why these measures are appropriate. A person that has received such a request from eSafety is required to submit a Code report within 2 months of receiving the request, but for the first request no earlier than 12 months after this Code comes into effect. A person will not be required to submit a Code report to eSafety more than once in any 12 month period. *This measure extends the requirement in measure 14 of the Phase 1 Equipment Code to this Code, and also extends to all other interactive devices for the sake of certainty.*

7.14. Schedule 8 Internet Search Engine Services Online Safety Code (Class 1C and Class 2 Material)

7.14.1. Structure of Code

This Code covers providers of internet search engine services. The OSA does not define internet search engine services. To make clear how search engines are differentiated from other services defined under the OSA, the Code defines internet search engines as:

> **Internet search engine services** are software-based services designed to collect and rank information on the WWW in response to user queries. An internet search engine returns relevant results to search queries and has the functionality explained in clause 4(b). As such, search engine services acknowledge that they play an important role in the digital ecosystem concerning the safety of end-users.

28 February 2025.

> This Code **does not apply** to search functionality within platforms where content or information can only be surfaced from that which has been generated / uploaded / created within the platform itself or on devices and not from the WWW more broadly.

Furthermore, the Code defines the provider of an internet search engine service so as to ensure that only providers that can implement community safeguards on the service are subject to the Code:

> **A provider of an internet search engine service:**
>
> (i) includes the licensor of search functionality that enables a licensee to operate a third-party search engine service where the licensor retains legal or operational control of the search algorithm, the index from which results are generated and the ranking order in which they are provided; and
>
> (ii) does not include the licensee of search functionality for the purpose of enabling the licensee to operate a third-party search engine service in circumstances where the licensee has no legal or operational control of the search algorithm, the index from which results are generated nor the ranking order in which they are provided.

7.14.2. Approach to Outcomes

The following table maps each compliance measure in the Code against the two online safety objectives identified in the s141 notice for internet search engine services.

Objective	Compliance measure
Objective 1: Protect and prevent children in Australia from accessing or being exposed to class 1C and class 2 material.	1 to 8 (inclusive), 11 to 26 (inclusive)
Objective 2: Online industry must provide Australian end-users with effective information, tools and options to limit access and exposure to class 1C and class 2 material	1, 6, 8 to 26 (inclusive)

7.14.3. Approach to risk

Internet search engine services are designed for general public use and have a generally equivalent purpose and functionality and, therefore, have an equivalent risk profile under this Code.

The Code requires providers to conduct a review of the risk that Australian children will access or be exposed to online pornography, high-impact violence material and self-harm material in search results. This includes consideration of the likelihood that an internet search engine service may be used to directly expose children to online pornography, high-impact violence material and self-harm material, and the likelihood that a child will use an internet search engine service to access online pornography, high-impact violence material and self-harm material.

7.14.4. Approach to measures

The Code codifies best practices concerning online pornography, high-impact violence and self-harm material that provide safeguards for the community in respect of the matters set out in the section 141 notice for search engine services. The Code applies these safeguards and makes them enforceable for all search engine services.

Compliance measures have not been included in respect of simulated gambling material because search results include links to webpages. Search results do not include games, which are the only content which may constitute simulated gambling material.

Compliance measure 5 of the Internet Search Engine Services Online Safety Code (Class 1A and Class 1B material) (“**Phase 1 Search Code**”) addresses a range of drug and crime material.

28 February 2025.

Policies, processes, systems and technologies	**Compliance measure 1** A provider of an internet search engine service must have and enforce clear actions, policies, processes or terms and conditions relating to how the service deals with: a) online pornography; b) high-impact violence material; and c) self-harm material. At a minimum, such actions, policies, processes or terms and conditions must deal with: d) how such material is to be dealt with on the service; and e) how the provider reduces the risk that Australian children will access or be exposed to such material in search results. Providers must have and implement systems and technologies to apply and enforce such actions, policies, processes or terms and conditions. This measure reflects item 1.1 (Terms and conditions) of the suggested minimum compliance measures for search engine services in the July 2024 Position Paper.
Age assurance or defaults	**Compliance measure 2** A provider of an internet search engine service must, to the extent technically feasible and reasonably practicable, either: a) implement appropriate age assurance measures for account holders and comply with compliance measure 3; or b) implement defaults in accordance with compliance measure 4. *Providers of internet search engine services are not required to implement age assurance measures for users who are not logged into an account.* *This compliance measure reflects the suggestion that defaults be applied to all users for whom age assurance is not completed in item 3.2 (Default settings for safety tools) of the suggested minimum compliance measures for search engine services in the July 2024 Position Paper.* *This compliance measure makes it clear that providers are not required to perform age assurance in respect of logged out users. A requirement for age assurance for logged out users would be an unreasonable infringement on user privacy. It is imperative to balance preserving adults' ability to privately access legal adult content with restricting children's exposure to this material.* *The approach taken in this Code strikes the right balance between those factors by:* ● *Requiring default 'blur' settings to be applied where users are logged out (compliance measure 4);* ● *Requiring those default settings to be set to the strictest setting to filter out material for users identified as a child, either via age assurance mechanisms (compliance measure 3) or otherwise via the provider's systems (compliance measure 4); and* ● *preserving users' ability to privately access pornography and other legal content, including where a user has specifically chosen to*

	log out of their account. The Code puts protections in place to reduce the risk of these users being exposed to this material in search results, by requiring that material be blurred by default for all end-users (compliance measure 4) and imposing measures to reduce unintentional exposure to material (compliance measure 8 and compliance measure 11). T*he recently enacted Online Safety Amendment (Social Media Minimum Age) Act 2024 recognises the distinction between signed in and signed out users by placing restrictions only on users below the age of 16 holding an account. In her second reading speech for that Act, Minister Rowland noted "By regulating the act of 'having an account', as opposed to 'accessing' social media more generally, we are seeking to strike a balance between protecting young people from harm, while limiting the regulatory burden on the broader population." This Code's approach is consistent with the Government's approach in Online Safety Amendment (Social Media Minimum Age) Act 2024*.
Default tools and/or settings for Australian children where age assurance is adopted	**Compliance measure 3** A provider of an internet search engine service must apply tools and/or settings, like 'safe search' functionality, at the highest safety setting by default for an account holder its age assurance systems indicate is likely to be an Australian child, designed to protect and prevent Australian children from accessing or being exposed to online pornography and high-impact violence material in search results. At a minimum, such tools and settings must filter out online pornography and high-impact violence material detected in search results. Providers of search engine services must either comply with this measure or compliance measure 4. *This measure ensures that children that are logged into an account receive, by default, a safe search experience that restricts access and exposure to online pornography and high-impact violence material.* *This measure applies to online pornography and high-impact violence material because those are the categories of class 1C and class 2 material which search engine services' classifiers are unable to reliably identify. Classifiers are unable to distinguish reliably between material that encourages, promotes or provides instruction in suicide, self-harm and eating disorders, and content that discusses suicide, self-harm and eating disorders for the purposes of prevention, crisis support or education, which would not constitute class 2 material.* *By requiring tools and/or settings to be set to the highest safety setting by default, this measure reflects item 4.1 (Parental controls and options) of the suggested minimum compliance measures for search engine services in the July 2024 Position Paper.*
Default tools and/or settings where age assurance is not adopted	**Compliance measure 4** Where a provider does not comply with compliance measure 3, the provider must apply tools and/or settings, by default, to reduce the risk of Australian children accessing or being exposed to online pornography and high-impact violence material in search results.

	At a minimum, such tools and/or settings measures must include: a) the highest safety settings applied by default to filter out images of online pornography and high-impact violence material detected in search results for an account holder the provider knows with reasonable certainty is an Australian child; and b) for all other end-users, default blurring of images of online pornography and high-impact violence material detected in search results. Providers of search engine services must either comply with this measure or compliance measure 3. *This compliance measure also ensures that the search experience for users who have not completed an age assurance process includes default measures to reduce the risk of exposure to online pornography and high-impact violence material.* *The measure requires the highest safety settings to be applied to users the provider knows are children. The highest safety settings filter online pornography and high-impact violence material from appearing in search results. Default blurring of material is the appropriate minimum requirement for other users as it ensures that users are protected from unintentional exposure to this material. Applying filtering settings to users who may, for example, be adults exercising their ability to access content more privately as a logged out user, intrudes upon their ability to access lawful content. For this reason, compliance measure 4(b) requires that defaults for these users be applied to blur material by default.* *By requiring that defaults be applied to all users for whom age assurance is not completed, this compliance measure reflects item 3.2 (Default settings for safety tools) of the suggested minimum compliance measures for search engine services in the July 2024 Position Paper.*
Parental controls	**Compliance measure 5** A provider of an internet search engine service must make available parental controls to limit or alter an Australian child's access to online pornography and high-impact violence material in search results. At a minimum, parental controls must include the ability to control settings to blur or filter detected online pornography and high-impact violence material from the Australian child's search results. *Compliance measures in respect of self-harm material apply to all users regardless of age, so are not subject to parental controls.* *This measure reflects item 2.1 (Interaction with parental controls) of the suggested minimum compliance measures for search engine services in the July 2024 Position Paper.*
Active detection of online pornography and high-impact violence material	**Compliance measure 6** A provider of an internet search engine service must actively detect online pornography and high-impact violence material in order to apply tools and/or settings to that material in accordance with compliance measure 3 or compliance measure 4 (Default tools/and/or settings), compliance measure 5 (Parental controls)

	and compliance measure 9 (Tools and/or settings for all end-users). *This measure applies only to online pornography and high-impact violence material because that material is the subject of compliance measure 3 and compliance measure 4 (Default tools/and/or settings), compliance measure 5 (Parental controls) and compliance measure 9 (Tools and/or settings for all end-users). Please refer to entries above and below for those compliance measures.*
Search advertising	**Compliance measure 7** A provider of an internet search engine service must take appropriate steps to ensure that advertising for online pornography, high-impact violence material and self-harm material is not served on search results pages for an account holder the provider knows with reasonable certainty is an Australian child. *This measure reflects item 3.2 (Search advertising) of the suggested minimum compliance measures for search engine services in the July 2024 Position Paper.*
Compliance measures to reduce unintentional exposure to online pornography and high-impact violence material for end-users	**Compliance measure 8** A provider of an internet search engine service must apply measures to protect and prevent end-users from being unintentionally exposed to online pornography and high-impact violence material in search results. At a minimum, such measures must include: a) ranking systems and algorithms designed to reduce the risk of online pornography and high-impact violence material appearing in search results for search queries not intended to solicit the material; and b) measures designed to prevent autocomplete predictions that are sexually explicit or violent. This measure affords protection to users of all ages against unintentional exposure to online pornography and high-impact violence material, including through ranking systems and autocomplete predictions. *Compliance measure 11 provides similar protections in respect of self-harm material.*
Tools and/or settings for end-users	**Compliance measure 9** A provider of an internet search engine service must allow end-users who are not Australian children to opt-in at any time to tools and/or settings, such as 'safe search' functionality, which restrict their access and exposure to online pornography and high-impact violence material in search results. At a minimum, such tools and/or settings must allow an end-user to choose between blurring and filtering online pornography and high-impact violence material detected in search results.

	Where an internet search engine service is made available as part of a technological ecosystem of interrelated products and services offered by that internet search engine provider, a provider of an internet search engine service must allow such tools and/or settings to attach to a centralised end-user account with the provider. *This compliance measure provides tools to adult users to restrict access and exposure to online pornography and high-impact violence material, including through ranking systems and autocomplete predictions.* *This measure does not apply to Australian children, as it may not be appropriate for younger children to override default settings and parental controls.* *This measure reflects item 4.1 (Safety Tools) of the suggested minimum compliance measures for search engine services in the July 2024 Position Paper.*
User choice about algorithms	**Compliance measure 10** A provider of an internet search engine service must take appropriate steps to empower end-users who are not Australian children to make choices about filtering and/or other algorithms to reduce the occurrence of online pornography and high-impact violence material appearing in or being accessible in search results. At a minimum, end-users must be able to enable settings to filter web pages containing online pornography and high-impact violence material from search results. *This measure allows adult users to restrict their access and exposure to online pornography and high-impact violence material, including through ranking systems and autocomplete predictions.* *This measure does not apply to Australian children, as it may not be appropriate for younger children to override default settings (see compliance measure 3) and parental controls (see compliance measure 5).* *This measure reflects item 5.1 (Algorithm and recommender system options) of the suggested minimum compliance measures for search engine services in the July 2024 Position Paper.*
Compliance measures to reduce unintentional exposure to self-harm material	**Compliance measure 11** A provider of an internet search engine service must apply measures to protect and prevent end-users from being unintentionally exposed to self-harm material in search results. At a minimum, such measures must include: a) ranking or other algorithmic protections that promote trustworthy and authoritative content over self-harm material; and b) measures to prevent autocomplete predictions that will result in search queries seeking self-harm material. *This measure affords protection to users of all ages against exposure to self-harm violence material, including through ranking systems and autocomplete predictions.*

Crisis prevention information – suicide and self-injury	**Compliance measure 12** A provider of an internet search engine service must employ means to detect and provide crisis prevention information in response to search requests that contain: a) general queries regarding suicide or an act of deliberate self-injury; and b) queries seeking specific, practical or instructive information regarding suicide methods, about suicide or relating to an act of deliberate self-injury. The crisis prevention information must: c) be prominently displayed to users in search results; d) be comprehensible and suitable in tone and content for as many users as possible, including children; and e) provide the following: i) a helpline associated with a reputable mental health organisation, suicide prevention organisation, or organisation with expertise in acts of deliberate self-injury that is able to provide support relevant to children; and ii) link(s) to information and support that is freely available and relevant to children through a reputable mental health organisation, suicide prevention organisation, or organisation with expertise in acts of deliberate self-injury. *This measure is consistent with OfCom's draft Protection of Children Code of Practice for search services PCS E3UK as it applies to suicide and self-injury.*
Crisis prevention information – expansion to eating disorders	**Compliance measure 13** A provider of an internet search engine service must take reasonable steps to identify a reputable organisation with expertise in eating disorders that is able to provide support relevant to children and which operates a helpline, provides information and support that is freely available and relevant to children and is a suitable and willing partner for the provider of an internet search engine service to provide crisis prevention information in respect of eating disorders ("**eating disorder crisis information partner**"). Within a reasonable period of timing following the provider of a search engine service identifying an eating disorder crisis information partner, the provider of an internet search engine service must detect and provide crisis prevention information in response to search queries regarding an eating disorder or behaviours associated with an eating disorder. The crisis prevention information must: a) be prominently displayed to users in search results; b) be comprehensible and suitable in tone and content for as many users as possible, including children; c) provide the following:

	i) a helpline associated with the eating disorder crisis information partner; and **ii)** link(s) to information and support made available by the eating disorder crisis information partner. *This measure is designed to afford the same protections to Australian users as would be available to those in the UK under OfCom's draft Protection of Children Code of Practice for search services PCS E3UK in respect of eating disorders, but reflects the stage of development of these programs in Australia.*
User feedback	**Compliance measure 14** A provider of an internet search engine service must provide tools which enable end-users to provide feedback about the accessibility of class 1C and class 2 material in search results. Feedback tools must be easily accessible and simple to use. Feedback tools must be easily accessible and simple to use. Guidance on this compliance measure encourages providers to consider the diverse accessibility needs of Australian users. *This measure extends equivalent measures in the Phase 1 Search Code to class 1C and class 2 materials.* *Given the enormous volume of feedback that may be received by search engines, providers are unable to ensure it is considered in all cases as a practical matter. However, the guidance note for this compliance measure notes that feedback should be considered when making decisions about safety tools, systems, processes and policies.*
End-user legal delist request process for illegal content	**Compliance measure 15** A provider of an internet search engine service must have a process for end-users to make legal delist requests for webpages that contain class 1C or class 2 material that is illegal. Such a process for making legal delist requests must: a) be easily accessible and simple to use; and b) be accompanied by plain language instructions on how to use it. A provider of an internet search engine service must: c) implement policies, processes, systems and/or technologies to enable the automated, human or hybrid triaging, and review and action (as appropriate) of legal delist requests; d) implement policies, processes, systems and technologies to enable the handling of complaints by Australian end-users about the response by the provider of the internet search engine to legal delist requests made under this compliance measure; and e) communicate the status or outcome of legal delist requests to the end-users who made them. *Guidance on this compliance measure encourages providers to consider the diverse accessibility needs of Australian users.*

	Guidance also requires that policies, processes, systems and/or technologies that are implemented to satisfy this measure should enable the internet search engine provider to take appropriate action in response to such legal delist requests taking into account factors such as urgency and scope of potential harm that is related to the reported material, the efficacy of different types of intervention that are available on the service, and the source of legal delist request. *A provider may communicate the status or outcome of a legal delist request to an end-user either by directly responding to the user or by displaying the status of the report to the user via a dashboard or similar interface.* *This measure extends measures relevant to legal delist requests in the Phase 1 Search Code to illegal class 1C and class 2 materials.* *This compliance measure is specific to illegal class 1C or class 2 material. For example, sexually explicit deep fakes. It is part of a suite of feedback, reporting and complaint options offered to end-users through this and the following compliance measures.*
eSafety delist notices	**Compliance measure 16** Where: a) the provider of a webpage has failed to comply with a Code in respect of the webpage; b) eSafety has notified the provider of the webpage of the failure and the failure has not been remedied within 30 days after the date of the notice; and c) eSafety notifies the provider of an internet search engine service that the webpage has failed to comply with Australian law and must be removed from search results ('**eSafety delist notice**'), the provider of an internet search engine service must cease providing a link to that webpage. The provider of an internet search engine service may provide a link to a webpage the subject of an eSafety delist notice if eSafety notifies the provider that it revokes the eSafety delist notice. An application may be made to the Administrative Review Tribunal for a review of a decision of eSafety to give an eSafety delist notice. *This compliance measure supports eSafety's enforcement of other codes by requiring search engines to cease linking to web pages eSafety has notified the provider are noncompliant.*
Process to report material	**Compliance measure 17** A provider of an internet search engine service must provide a tool to enable end-users to report web pages that contain online pornography and high-impact violence material that are not filtered from or blurred in search results when tools and/or settings, such as 'safe search' functionality, are on. Such reporting tools must: a) be easily accessible and simple to use; and

	b) be accompanied by plain language instructions on how to use them. A provider of an internet search engine service must: c) implement policies, processes, systems and/or technologies to enable the automated, human or hybrid triaging, and review and action (as appropriate) of such reports; and d) communicate the status or outcome of such reports to the end-users who made them. *Guidance on this compliance measure encourages providers to consider the diverse accessibility needs of Australian users.* *Guidance also requires that policies, processes, systems and/or technologies that are implemented to satisfy this measure should enable the internet search engine provider to take appropriate action in response to such reports taking into account factors such as urgency and scope of potential harm that is related to the reported material, the efficacy of different types of intervention that are available on the service, and the source of the report.* *A provider may communicate the status or outcome of a report to an end-user either by directly responding to the user or by displaying the status of the report to the user via a dashboard or similar interface.* *This measure extends measures relevant to user reports in the Phase 1 Search Code to online pornography and high-impact violence material.*
End-user complaints	**Compliance measure 18** A provider of an internet search engine service must provide tools which enable end-users to make complaints about the provider's non-compliance with this Code. Such complaints tools must: a) be easily accessible and simple to use; and b) be accompanied by plain language instructions on how to use them. A provider of an internet search engine service must implement policies, processes, systems and/or technologies to: c) consider and take appropriate action in response to such complaints; and d) enable the handling of complaints by end-users about the response by the provider of the internet search engine to complaints made in accordance with this measure. *Guidance on this compliance measure encourages providers to consider the diverse accessibility needs of Australian users.* *Guidance also requires that policies, processes, systems and/or technologies that are implemented to satisfy this measure should enable the internet search engine provider to take appropriate action in response to such complaints taking into account factors such as urgency and scope of potential harm that is related to the reported material, the efficacy of different types of intervention that are available on the service, and the source of the report.*

	The Head Terms imposes an obligation across all Codes for providers to complete an investigation and notify the complainant of the outcome of a complaint within a reasonable time.
Timely referral of unresolved complaints to eSafety	**Compliance measure 19** A provider of an internet search engine service must promptly refer to eSafety complaints from end-users concerning a material non-compliance with this Code by the provider, where the provider is unable to resolve the complaint within a reasonable timeframe. *This measure extends the equivalent measure in the Phase 1 Code to material complaints of non-compliance with this code.* *We have added a materiality threshold to reflect that age assurance mechanisms are imperfect and the greater difficulties in classifying class 1C and class 2 material compared to some types of material subject to the Phase 1 Search Code. A material non-compliance with this Code will relate to a substantial issue with age assurance measures, tools, settings, policies, processes or terms and conditions as required by this Code.*
Information for end users	**Compliance measure 20** Providers of internet search engine services must publish clear and easily accessible information that explains the actions they take to limit access or exposure to online pornography, high-impact violence material and self-harm material in search results. A provider of an internet search engine service must at a minimum: a) make available to end-users information about tools and/or settings made available by the provider to reduce access and exposure to online pornography and high-impact violence material in search results; b) make available to end-users information about default measures applied by the provider to reduce the risk of harm to end-users from accessing or being exposed to self-harm material in search results; c) make available to end-users clear and accessible information about parental controls to limit or alter an Australian child's access to online pornography and high-impact violence material in search results. This information must be provided to parents at the time a parent creates a child account and be easily accessible thereafter; d) where relevant, provide information to end-users about how any search engine features using generative artificial intelligence to generate longer form answers, summaries or materials, protects Australian children from exposure to online pornography and high-impact violence material; e) establish or maintain a hub, portal or other online location that houses online safety information that can be accessed by end-users or refers end-users to where they can find appropriate online safety information;

	f) provide information to end-users about the actions they may take to: a. provide feedback about the service under compliance measure 14; b. submit a legal delist request under compliance measure 15; and c. submit a report under compliance measure 17; g) provide information on how an end-user can make a complaint under compliance measure 18 and contact eSafety where a complaint made under compliance measure 18 is not resolved to that end-user's satisfaction; and h) provide information to end-users about the role and functions of eSafety, including how to make a complaint to eSafety under the OSA. *Guidance on this compliance measure encourages providers to consider the diverse accessibility needs of Australian users.* *This measure reflects eSafety's suggested supportive measures set out at page 80 of the July 2024 Position Paper.*
New features or functionality posing increased risk	**Compliance measure 21** Where a provider of an internet search engine service implements a new feature or functionality of the service that is likely to significantly increase the risk that Australian children will access or be exposed to class 1C and class 2 material in search results, the provider must: a) conduct additional reviews of the risk that Australian children will access or be exposed to class 1C and class 2 material in search results prior to implementing the new feature or functionality; and b) take reasonable steps to mitigate any additional risks that Australian children will access or be exposed to class 1C and class 2 material that result from the new feature or functionality, subject to the limitations in section 6.1 of the Head Terms. *Guidance on this measure notes that when conducting an assessment under this measure, the provider of an internet search engine service should consider whether any of the age assurance measures, tools, settings, policies, processes or terms and conditions covered by this Code need to be updated in light of such new feature or functionality. In implementing this measure, the provider of the internet search engine service may, for example:* *a) use the safety by design tools published by eSafety to assess the safety risks associated with a new feature or functionality; and* ***b)** consult additional guidance related to safety risks published by eSafety.* *This measure extends equivalent obligations in the Phase 1 Search Code to class 1C and class 2 material, and helps ensure* that providers of internet search engine services are committed to assessing and mitigating risks associated with new features and functionality.

Update eSafety on changes	**Compliance measure 22** A provider of an internet search engine service must update eSafety on any significant changes to the functionality of the service that are likely to have a material positive or negative effect on the access or exposure to class 1C and class 2 material by Australian children, such as significant changes to its machine learning algorithms and/or models (including large language models and multimodal foundation models) that reduce the risk that Australian children will access or be exposed to class 1C and class 2 material in search results. Updates under this measure must be provided: a) in the case of new features or functionality that has a material negative effect on risk, within 42 days of a written request by eSafety; and b) in the provider's report under compliance measure 26. *In implementing this measure, a provider of an internet search engine service is not required to disclose information to eSafety that is confidential.* *Guidance provides that changes that have a material negative effect should ideally be communicated before a public announcement of the relevant changes.* *This extends equivalent measures in the Phase 1 Search Code to class 1C and class 2 material.*
Engagement	**Compliance measure 23** A provider of an internet search engine service must appropriately engage annually with safety and community organisations (such as civil society groups, public interest groups and representatives of marginalised communities), academics and government to gather information to help inform the measures taken for the purposes of protecting or preventing children from accessing or being exposed to class 1C and class 2 material. A provider of an internet search engine service must consider information obtained through such engagement. *Guidance provides that engagement may occur within and/or outside Australia as relevant to the issue under consideration.* *Engagement may occur regularly in the course of ongoing relationships with organisations, academics or government, during development of new service features or in other appropriate circumstances.* *This measure complements the commitment in section 1.3 (Ongoing work on age assurance and other measures) of the Head Terms.*
Ongoing improvements	**Compliance measure 24** A provider of an internet search engine service must take appropriate steps to improve the effectiveness of its machine learning algorithms and/or model(s) operating within an internet search engine service in reducing the risk of Australian children accessing or being exposed to class 1C and class 2 material in search results.

	At a minimum, a provider of an internet search engine service must take appropriate steps to: a) if the provider implements age assurance measures for account holders, test and monitor the effectiveness of its age assurance measures over time; b) invest in ongoing improvements to its systems to automatically detect online pornography and high-impact violence material and automatically apply protections in accordance with the provider's policies and processes; c) regularly review and/or test the performance of algorithms in reducing the accessibility or discoverability by Australian children of online pornography and high-impact violence material in search results; d) following review and/or testing in sub-measure b), where appropriate, adjust algorithms to reduce the risk that online pornography and high-impact violence material is accessible or discoverable in search results by Australian children; e) deploy appropriate mitigations, such as tuning, classifiers, adversarial testing or meta prompts, to mitigate the risk online pornography and high-impact violence material are returned in search results for Australian children; f) make ongoing improvements to its systems and technologies including machine learning algorithms and/or models or technologies with the aim of reducing the accessibility of online pornography and high-impact violence material in search results for Australian children; g) make ongoing improvements to ranking or other algorithmic protections to promote trustworthy and authoritative content over self-harm material; h) invest in ongoing improvements to its systems to automatically detect queries seeking self-harm material and automatically apply protections in accordance with the provider's policies and processes; i) improve systems, processes and/or technologies that aim to reduce the safety risks to end-users concerning synthetic materials generated by artificial intelligence that may be accessible via the internet search engine service, and j) research detection technologies that assist end-users in identifying deep fake images that are accessible from the service. *This measure complements the commitment in section 1.3 (Ongoing work on age assurance and other measures) of the Head Terms.*

	This measure extends equivalent measures in the Phase 1 Codes to class 1C and class 2 material. It also reflects item 6.1 (Improvement of protective tools) of the suggested minimum compliance measures for search engine services in the July 2024 Position Paper.
Invest in and adequately resource teams	**Compliance measure 25** A provider of an internet search engine service must measurably invest in and sufficiently resource: a) trust and safety teams dedicated to implementing regulatory requirements and implementing policies which enhance safety for users on internet search engine services; and b) moderation teams who conduct human review of reported material and can consider material including factors like context where automated consideration of such factors is not technically feasible or reasonably practicable. A provider of an internet search engine service must ensure such teams complete annual training in the provider's relevant policies and processes addressing how the service deals with online pornography, high-impact violence material and self-harm material. This measure reflects item 6.1 (Improvement of protective tools) of the suggested minimum compliance measures for search engine services in the July 2024 Position Paper.
Reporting on Code compliance	**Compliance measure 26** Where eSafety issues a written request to a provider of an internet search engine service to provide a Code report, the provider named in the request must submit a Code report which includes the following information: a) the steps that the provider has taken to comply with the compliance measures; and b) an explanation as to why such measures are appropriate. A provider of an internet search engine service who has received such a request from eSafety is required to submit a Code report within 2 months of receiving the request, but for the first request no earlier than 12 months after this Code comes into effect. A provider of an internet search engine service will not be required to submit a Code report to eSafety more than once in any 12-month period.

8. Criteria concerning consultation processes for Phase 2 Codes

This section 8 explains how industry consulted with different stakeholders in the development of the Phase 2 Codes and met the relevant requirements in the OSA.

8.1. The Codes have been published and members of the public have been invited to make submissions to the associations within no less than 30 days [OSA, section 140(1)(e)(i) & Position 8, Position Paper]

8.1.1. Outline of process

In accordance with the requirement of section 140(1)(e)((i) and (3)of the OSA, the industry association facilitated a first public consultation on drafts of the Phase 2 Codes for a period of 30 days from 22 October to 22 November 22, 2024.

The draft Phase 2 Codes and explanatory materials were published on onlinesafety.org.au, a public website maintained by the industry associations. This included a discussion paper which explained how to make a submission and details of the rationale for the measures in each Code.

Industry associations also extensively promoted the Phase 2 Codes' public consultation process. Associations publicised the consultation through newsletter updates reaching industry, government, and civil society organisations. We also made updates on social media channels and to association websites to publicise the consultation.

In addition to owned communications channels, associations prepared and released a media alert, promoting public awareness of the draft Phase 2 Codes' consultation process. Additionally, we secured 123 print stories and 80 radio stories (including syndications) that raised awareness of the consultation process and explained how associations approached the development of the codes, to assist public awareness and understanding of the process and the draft code commitments.

Industry associations proactively contacted over 250 stakeholders from the relevant consultation categories outlined in eSafety's discussion paper, inviting them to make submissions to the consultation process.

8.1.2. Stakeholders contacted by industry associations

Consumer Action
ACCAN
Choice
Consumer Policy Research Centre
Consumer Action Law Centre
Consumers Federation of Australia

Consumers Association - General
Queensland Consumers Association
Civil society groups (note digital rights orgs covered separately below)
Alannah & Madeleine Foundation
The Carly Ryan Foundation
Australian Community Managers
GIFCT
Tech Against Terrorism
Digital Trust & Safety Partnership
NECMEC
ICMEC
Australian Seniors Computer Clubs Association
Australia's Internet Governance Forum
Law Council of Australia
Australian Council for Civil Liberties
Reset Australia
Centre for Digital Wellbeing
Centre for Responsible Technology
Inhope
WeProtect Global Alliance
ACCCE
Australian Institute of Criminology
Australian Privacy Foundation
IIS Partners
The Daniel Morcombe Foundation
Bravehearts
Community legal and advocacy groups
Law Council of Asia & the Pacific
Law Council of Asia & the Pacific
Law Council of Australia
Community Legal Centres Australia
Darwin Community Legal Service
Justice and Equity Centre
Law Society of Tasmania
Law Society of Victoria
Law Society of Western Australia
Law Society of Australian Capital Territory

Law Society of New South Wales
Law Society of the Northern Territory
Queensland Law Society
Representatives from academia
UWS Young & Resilient Centre
UTS Centre for Media Transition
ANU College of Law
ANU Tech Policy Design Centre
Charles Sturt University, Centre for Law and Justice
QUT DIGITAL MEDIA CENTRE
Canberra Uni
Latrobe
Swinburne University
Swinburne University
ASPI
UNSW School of Law, Society & Criminology
UNSW, School of Social Sciences
UNSW and The Allens Hub for Technology, Law and Innovation
UNSW Allens Hub
UNSW School of Global & Public Law
UCI (GNI academic)
University of Ottawa
University of Melbourne Law School, Co-Director of the Centre for AI and Digital Ethics
University of Western Australia and the Minderoo Tech & Policy Lab
Berkeley School of Information
Institute for Cyber Investigations and Forensics at USC Australia
Institute for Cyber Investigations and Forensics at USC Australia
Stanford
The ARC Centre of Excellence on Automated Decision-Making and Society
• children and young people
UNICEF
AYAC
MYAN NSW

Youth Affairs Council of Western Australia
Australian Youth Affairs Coalition
Australian Youth Affairs Coalition
Youth Affairs Council of Victoria
Commissioner for Children and Young People SA
Australian Research Alliance for Children and Youth
National Children's Commissioner, Australian Human Rights Commission
The Children and Young People Commissioner Australian Capital Territory
The Children's Commissioner Northern Territory
The Office of the Public Guardian Queensland
The Office of the Guardian for Children and Young People South Australia
Commissioner for Children and Young people Tasmania
Commission for Children and Young People Victoria
Commissioner for Children and Young People Western Australia
Office of the Advocate for Children and Young People (NSW)
Office of the Advocate for Children and Young People (NSW)
Yourtown
QORIA
• parents, carers, teachers and educators (including their representative groups)
NSW Teachers Federation
AEU ACT Branch
Australian Education Union Victoria
Queensland Teachers Union
State School Teachers Union of Western Australia
AEU TAS Branch
AEU SA Branch
AEU NT Branch
Daniel Morecombe Foundation
Family Zone
• users of the services and devices (including content creators impacted by the codes)
ACT | The App Association
ACT | The App Association
AUDA

AUDA
AUDA
AUDA
COSBOA
Business Council of Australia
Asia Internet Coalition
Australian Banking Association
The Australian Chamber of Commerce
Australian Industry Group
Australian Information Industry Association
The Tech Council of Australia
Internet Association of Australia
ITI
ITI
CCIA
Tech UK
Standards Australia
Australian Copyright Council
Screen Australia
Australian Society of Authors
The Australian Digital Alliance
Universities Australia
• digital rights groups
Digital Rights Watch
Electronic Frontiers Australia
Irish Bentley Lawyers
AccessNow
Internet Australia
Global Network Initiative (GNI)
Center for Democracy & Technology (CDT)
ACLU
Internet Society
Electronic Frontier Foundation
LGBT Tech
Future of Privacy Forum
Knight First Amendment Institute
OTI/ Ranking Digital Rights

Human Rights Watch
Brookings
Center for Information Policy Leadership
Index on Censorship
• women's advocacy groups
White Ribbon Australia
Womens Legal Service NSW
National Council of Women Australia
UN Women
• domestic and family violence groups
WESNET
EARG - Economic Abuse Reference Group
Relationships Australia
DV Service Management
Communicare
Safe Steps
DV Connect
Katherine Women's Legal Service
• groups representing sex workers
Scarlett Alliance
Assembly Four
Eros Association
Australian Queer Archives
LGBTIQ+ Health Australia
• safety tech sector
Online Safety Tech Industry Association (OSTIA)
Safety Tech Innovation Network; British Consul
Department for International Trade (London), requested being added as the contact for UK safety tech companies.
Government
Australian Human Rights Commission
Office of the Australian Information Commissioner
Department of Home Affairs
Australian Communications & Media Authority
Department of Infrastructure, Transport, Regional Development and Communications
Additional parental groups

P&C QLD
Western Australian Council of State School Organisations
Council of Catholic School Parents NSW/ACT
ARACY
Dept. of Child Safety, Seniors & Disability Services
Office of the Childrens Guardian
Headspace
The Kids Research Institute Australia
Isolated Children's Parents Association of Australia
Australian Parents Council
NSW P&C
Harmony Alliance
Raising Children Network
Triple P
Family and Relationships Services Australia
The CEntre for Excellence in Child & Family Welfare
The Smith Family
NAPCAN
Australian Institute of Family Studies
Australian Childhood Foundation
Early Childhood Australia
ACECQA
OzChild
Mental Health Organisations
Reach Out
Blackdog
Beyond Blue
Prevention United
Project Rockit
Suicide Prevention Australia
Gayaa Dhuwi (Proud Spirit) Australia
First nations mental health and tech
inDigiMOB
Queensland Remote Aboriginal Media
13YARN

28 February 2025.

8.1.3. Roundtables

On 12 September 2024 industry associations conducted a virtual roundtable to give representatives of the pornography and other key industry sections engaged in the development of Phase 2 Codes an opportunity to raise and discuss the process and some of the issues that had arisen around the drafting of the phase 2 Codes. A summary of this discussion under Chatham House Rules is provided with this Request for Registration.

On 13 November 2024 industry associations conducted an additional virtual Expert Stakeholder Roundtable, as part of the public consultation process for the Phase 2 Codes. Discussion focused on the questions published in the Discussion Paper accompanying the Phase 2 Codes[24]. There was also an opportunity to raise general questions about the draft codes and the consultation process. A summary of this discussion under Chatham House Rule is provided with this Request for Registration and is available publicly on onlinesafety.org.au.

8.2. The associations gave consideration to any submissions that were received from members of the public [OSA, section 140(1)(e)(ii) & Position 8, Position Paper]

The associations have given consideration to all the submissions received as part of the public consultation process on the Phase 2 Codes and the industry's responses to that feedback have been documented in the Summary of Industry Response to Submissions on Phase 2 OSA Codes submitted to eSafety with this Request for Registration.

8.3. The Codes have been published and participants of the respective sections of the industry have been invited to make submissions to the associations within no less than 30 days [OSA, section 140(1)(f)(i) & Positions 7 and 8, Position Paper].

The industry associations have developed these Phase 2 Codes through a highly collaborative process with industry participants. The following steps were taken to ensure broad participation in the Codes development process, including beyond the membership of the five industry associations:

a. The industry associations invited their respective members to participate in the Codes development process.

b. Where gaps in membership were identified, industry associations reached out to invite non-members to the Codes development process (at no cost or membership requirements). These included invites to industry participants in the Phase 1 process and additional participants identified by associations.

c. Relevant industry participants either directly participated in the drafting of the Codes or were offered the opportunity to raise issues and contribute suggestions to the development of the draft Codes.

---

24 https://onlinesafety.org.au/wp-content/uploads/2024/10/Discussion-Paper-for-public-consultation_-Phase-2-OSA-Codes-.docx.pdf)

28 February 2025.

d. Industry participants were also invited to make submissions to associations as part of the public consultation process as described in 8.1 above.

8.4. The associations gave consideration to any submissions that were received from participants of the respective sections of the industry [OSA, section 140(1)(f)(ii) & Position 8, Position Paper].

The industry associations have given consideration to all the submissions received as part of the public consultation process and responses to the feedback have been documented in the Summary of Industry Response to Submissions on Phase 2 OSA Codes submitted to eSafety with this Request for Registration. In addition industry participants were invited to participate directly in the drafting of the Phase 2 Codes as outlined in 8.1.

8.5. The Commissioner has been consulted about the development of the Codes [OSA, section 140(1)(g) & Position 9, Position Paper]

The industry associations regularly engaged with the Office of the eSafety Commissioner via face to face meetings and in written correspondence during the development of the Phase 2 Codes. The industry association's response to the additional feedback received from eSafety is documented in the Industry Response to eSafety Feedback provided separately to eSafety with this Request for Registration.

Annex 1: eSafety's positions on codes development (reproduced from Position Paper)

Position 1: The codes will address the issues of access, exposure and distribution that are related to class 1 and class 2 material.

Position 2: The application of the codes will not be limited to services provided from Australia.

Position 3: Industry associations will develop a set of common drafting principles to inform codes development. (p.45)

Position 4: The codes will adopt an outcomes-and risk-based regulatory approach, supported by clear compliance measures which apply to industry participants whose services or devices present the greatest risk in respect of class 1 and class 2 material.

Position 5: Industry associations will prepare all codes for registration by July 2022 or adopt a phased approach to codes development. Under the phased approach, codes dealing with the most harmful content must be lodged for registration by July 2022, and codes dealing with content which is inappropriate for children must be lodged for registration by December 2022.[25]

Position 6: Industry associations will limit the number of codes developed.[26]

Position 7: Industry associations will engage widely with participants within their industry section(s) to ensure they adequately represent each section covered by a code.

Position 8: Industry associations will conduct meaningful industry and public consultation.

Position 9: Industry associations will engage with eSafety throughout the codes development process.

Position 10: Industry participants will handle reports and complaints about class 1 and class 2 material and codes compliance in the first instance. eSafety will act as a 'safety net' if resolution of a complaint is not satisfactory.

Position 11: The codes will include a review mechanism.

[25] The Steering Group and eSafety later agreed that Position 5 would be varied: Industry opted for a two-phased approach (i.e., produce a first set of Codes for class 1 material, followed by a second set of Codes dealing with class 2 material); however, eSafety formally varied the due date for the class 1 Codes to 18 November 2022, with commencement of the class 2 Codes in 2023.

[26] The industry associations had proposed a single class 1 Code with 8 Schedules or Chapters for the respective online sections. eSafety requested eight independent Codes under one consolidated umbrella document, now titled *Consolidated Industry Codes of Practice for the Online Industry (class 1A and class 1B Material)*, to allow for independent registration/refusal of registration. The industry associations accommodate that request and have taken the same approach to the Phase 2 Codes.

Annex 2: List of industry participants that directly participated in drafting of the Codes to date.

18 North
Adobe
Amaysim
Amazon
AMTA
Apple
Aussie Broadband
TCG
Automattic
AV Link
Aylo
Blizzard
BSA
Bumble
Canva
CESA
Change.org.
Communications Alliance
Developers Alliance
DIGI
Discord App
EA
Eros
Free Speech Coalition
Glassdoor
Global Tencent
Go Fund Me
Goodreads
Google
X Hamster

Interactive Games and Entertainment Association (IGEA)
Lego
LGE
Linkedin
Linktr.ee
Match
Meta
Microsoft
Nintendo
Netflix
Next Door
Open AI
Optus
Panasonic
Pinterest
Product Review
PS Engage
Red Bubble
Reddit
Riot Games
Roblox
Samsung
Scarlet Alliance
Snap
Snapchat
Sony
Spotify
Tech Council
Telstra
The Littapp (LITT)
TikTok
TPG Telecom
Trafalgar Strategy
Twitch TV
Uber

Ubisoft
Vocus
Wikimedia
X
Yahoo Inc.
Zenimax
Zoom