Discussion Paper: Draft Phase 2 online safety codes

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)

22 October 2024

Contents

1. Introduction

The Online Safety Act 2021 (Cth) (the OSA), which commenced on 23 January 2022, provides for the establishment of new, enforceable industry codes and standards for eight sections of the online industry to regulate the most harmful types of online content. This discussion paper is about the eight draft industry codes (the Codes) developed by industry associations at the request of the eSafety Commissioner under the OSA to address Class 1C and Class 2 materials. **These draft Codes are primarily designed to protect children from exposure to online pornography and other harmful content such as "self harm material" that encourages, promotes or provides instruction for suicide, an act of deliberate self-injury or an eating disorder or behaviour associated with an eating disorder**. The draft Codes also include measures that outline how relevant digital services propose to approach age assurance.

Table 1 : Draft Codes

Title	Section of the online industry to which the code applies	Industry associations tasked with developments of Code
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
Internet Search Engine Services	Providers of internet search engine services, so far as	● CA ● DIGI

Title	Section of the online industry to which the code applies	Industry associations tasked with developments of Code
Online Safety Code (Class 1C and Class 2 Material)	those services are provided to end-users in Australia	
App Distribution Services Online Safety Code (Class 1C and Class 2 Material)	Providers of app distribution services, so far as those services are provided to end-users in Australia	● CA ● DIGI ● IGEA
Hosting Services Online Safety Code (Class 1C and Class 2 Material)	Providers of hosting services, so far as those services host material in Australia	● BSA ● CA
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 (Operating systems providers were not covered in any s141 notice.)

The industry associations developing the codes are seeking the views of the online industry, advocacy groups, the general public and other interested stakeholders on the drafts of the

Codes which are are (contained in the Consolidated Industry Codes of Practice for the Online Industry (Class 1C and Class 2 Material):available at https://onlinesafety.org.au/.

This discussion paper:

- sets out the background to the development of the Codes;
- explains the public consultation process;
- explains how to make a submission;
- sets out questions for discussion that are relevant to the Codes; and
- provides an explanation of the approach of industry associations to the development of the Codes, including the proposed measures.

2. Background to the development of the Phase 2 Codes

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 will take 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 s141 notices request the relevant industry associations to develop a Phase 2 Code or Codes that deal with matters in similar terms to the following:**

> ***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.***

Additionally the notices require that that relevant industry associations submit draft Codes to eSafety for final consideration by 19 December 2024. In July 2024, the eSafety Commissioner published a supplementary position paper that outlined eSafety's expectations for developing Phase 2 Codes (**July 2024 Position Paper**) that included suggested measures for the Codes[1].

[1] available at https://www.esafety.gov.au/sites/default/files/2024-07/Development-of-Phase-2-Industry-Codes-under-the-Online-Safety-Act-eSafety-position-paper.

3. Public consultation on the draft

The following timeline outlines the key steps that industry will take take to finalise draft Codes for submission to the eSafety Commissioner from this point forward:

Table 2: Timeline for consultation and key steps in finalising draft Codes:

Date	Key steps
22 October 2024	Public consultation on the Phase 2 Codes opens (for 31 days)
22 November 2024	Public consultation closes
25 November 2024	Review public submissions and amend Codes in response
19 December 2024	Planned lodgement of Codes with request for registration with the Commissioner

Part 7 of this document sets out how industry has approached the development of the draft Codes, including the measures contained in each Code. Where appropriate, the respective positions of eSafety in the eSafety July 2024 Position Paper, are also referenced.

4. Submissions

The industry associations invite submissions from industry and the public on the draft Codes.

Submissions, can be made via Email: hello@onlinesafety.org.au

Each submission should be accompanied by:

- the name of the individual or organisation making the submission
- a name for publication purposes (this can be the name of the individual or organisation, or a pseudonym, or 'anonymous')
- contact details (such as a telephone number, postal address or email address)

A submitter may claim confidentiality over their name or contact details.

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

The closing date for submissions is 11:59pm AEDT, Friday 22 November.

The industry associations recognises that the timeline may be challenging for some participants. Due to the statutory deadline, we may not be able to accommodate requests for extensions. However, please contact us at **hello@onlinesafety.org.au** if you require an alternative method of making a submission or we can otherwise assist you with making a submission.

In the interests of transparency, the industry associations intend to publish submissions we receive on our website **www.onlinesafety.org.au**, including any personal information in the submissions. Submissions will be made public. Please ensure that you do not include any personal information in your submission that you do not want published.

5. Privacy information

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

6. Discussion questions

The Industry associations are seeking views on the effectiveness of the draft Codes in providing appropriate community safeguards for class 1C and class 2 material. We are also seeking submissions on some live policy questions on which we welcome views during public consultation. We have provided discussion questions in this paper to assist in focusing submissions. They are a guide only and not intended to limit the scope of submissions. Responses can be provided to all, any or none of the questions.

Question 1: The materials subject to these Codes (Class 1C and Class 2 materials) is material which should be restricted to users under the age of 18, based on the criteria of the National Classification Scheme, but is primarily lawful for adults to view. These categories include high impact pornography, high-impact nudity, self-harm material, or material that describes or depicts high-impact violence and themes of crime and drug and alcohol dependency. The Codes have been drafted to differentiate between services based on:

- The extent users would reasonably expect to be able to securely and privately use certain types of service to store/access/share Class 1C or Class 2 materials provided that it is lawful. So for example, the draft Codes do not require file storage (user-managed hosting services) or communication services such as email, messaging services , sms or messaging services to prohibit Class 1C or Class 2 materials or to scan/remove these materials.
- Whether the purpose of the service is to distribute certain Class 1C or Class 2 materials e.g the Codes require pornography sites and generative AI services that are designed to generate high impact pornography to implement age assurance measures.
- Whether the service allows/prohibits 'high priority materials' including pornography and self harm materials, to better align these Codes with international approaches e.g under the UK Online Safety Act e.g social media services that allow high impact online pornography must implement age assurance measures to prevent child end-users from accessing that content whereas social media services that prohibit high impact online pornography are required to implement other appropriate measures to limit the risk of child end-users accessing or being exposed to high-impact online pornography, subject to their risk profile.

Do you agree with this approach?

Question 2: Do you think the Codes strike an appropriate balance between user privacy, data security, freedom of expression and online safety, particularly around services used for private communication and storage of material such as file storage services? Should providers of most relevant electronic services that allow users under 18 (such as email and private messaging services) be required to scan all Australian user's communications and messages to detect and remove lawful Class 1C and Class 2 materials?

Question 3 : It is the industry's view that age assurance should be both effective, privacy preserving and data minimising. Therefore, the question of when and where age assurance should take place is inextricably linked with the question of how age assurance should be implemented:

a. Where should age assurance measures be introduced in relation to these Codes ? Should for example, all users of Tier 1 and Tier 2 equipment be subject to age assurance measures? Should users of email, messaging services an other types of private communication services and file storage services be subject to age assurance or other kinds of measures that restrict access to content?
b. What kinds of information gathering requirements and processes should be implemented by relevant industry participants to conduct age assurance?

Question 4: Should all Australian end-users who engage with online devices or services generally be required to undergo age assurance processes, or only those Australian end-users who wish to access high impact services (such as, for example, services that have the predominant purpose of high impact pornography)?

Industry associations request that submitters provide reasons to support any views expressed. We welcome practical examples, research and other evidence.

7. Approach to the development of the Consolidated Phase 2 Codes

The section 141 notices issued by the eSafety Commissioner stipulate that the Codes contain community safeguards that:

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

In this section we explain the approach the industry associations have taken to designing the Codes and the measures they contain.

A note on the proposal by some Australian governments to introduce age restrictions for social media and other digital services.

Industry notes that since the eSafety Commissioner has issued the s141 notices there have been additional policy developments at both the State and Federal level that impact on the development of the Phase 2 Codes, including announcements by the South Australian State government, the Victorian State government and the Federal government that each will introduce age restrictions on the use of social media by users under the age of 16.

In the case of South Australia, the scope of the proposed age restrictions extend to a wide range of services in scope of these Codes, not only social media services as defined under the OSA including all DIS services that allow user to user communications or user-generated materials and a large range of RES services such as sms, mms, vms, gaming services, dating services, messaging services and email services, all of which would need to restrict access to these services by under 16 year old users. The scope of the services to be subject to age restrictions by the Federal government is as yet unclear.

In making a submission, submitters should therefore be aware that the Codes are being developed at the request of the eSafety Commissioner while development of key elements of the national framework are being progressed concurrently or are under consideration, including critical work by the Federal government on a national approach to age requirements and age assurance. Despite the uncertainty around the regulatory framework , we consider that the Codes can serve to bolster and complement other measures that may be introduced, being targeted in specific risks and harms relating to Class 1C and Class 2 materials.

7.1. Structure

The Head Terms contain common terms that apply to each industry Code. The eight 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 eight 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) and 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.

7.2. 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.

7.3. Age assurance

7.3.1. 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*[2] (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 .

7.3.2. Additional consideration*s*

Industry has received various suggestions from eSafety, both from the July 2024 Position Paper and in our meetings, 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[3]. Given the current immature state of age assurance technology and rapid developments in the sector, industry believes it is better to preserve flexibility for service providers required to introduce age assurance under the Codes.

While there are a range of online services that are using age assurance for limited jurisdictions or limited services to date there is limited independent or regulatory assessment of their appropriateness[4]. It is hoped that international standards, such as the *ISO standard for age assurance (ISO/IEC 27566 – Information security, cybersecurity and privacy protection – age assurance systems)* 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.

The content in scope of the Phase 2 Codes is also an important factor in devising an appropriate approach to age assurance. The measures under these Codes must be directed at preventing children from accessing 'class 1C and class 2 materials'. This scope of content within these Codes is broad and is based on the National Classification Scheme. The classification process requires nuanced, context-based judgments of materials, which are very difficult to do accurately

[2] eSafety Commissioner, *Roadmap for age verification and complementary measures to prevent and mitigate harms to children from online pornography,* (March 2023).

[3] *July 2024 Position paper* p 83.

[4] eSafety, *Tech Trends Issues Paper Age assurance*, July 2024 p.7

at scale for the vast range and diversity of online material. Following the suggestions in the July 2024 Position Paper 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).

In this context, 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 instead apply a layered set of protections at every stage of the tech stack – including obligations for app stores, devices, ISPs and other categories of services – that provide a meaningful uplift in preventing underage access to inappropriate content. Although industry has not prescribed how age assurance must be implemented, we have set out a variety of practical and realistic methods, based on our experience to date. This approach allows for 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).

7.4. 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.

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[5]. 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 ge range of a given user). The introduction of these definitions is consistent with the Ofcom approach to implementing age assurance measures, recognition that age

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

	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: **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 class1 C materials. **class 2B materia**l 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 describes or 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, as and could for example include news footage, historical footage, research and educational materials. **class 2C 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 describes or depicts high-impact violence and themes of crime and drug and alcohol dependency; but (b) excludes class 2A material, class 2B material, self-harm material and simulated gambling material. **high impact online pornography** means class 1C and class 2A material. This definition is intended to capture materials that are ordinarily understood to be pornography in a manner that is consistent with eSafety's approach to pornography in developing the Roadmap and its Young people's encounters with pornography research high-priority restricted category of material means high impact online pornography and self-harm material.

	self-harm material 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 loop 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 at a minimum include reasonable age assurance measures to help the provider to identify whether an Australian end-user is a child; (iii) it is recognised that some end-users may be able to circumvent such measures, although a provider should seek to limit this where reasonably possible;

	(iv) it is recognised that some measures may not always accurately identify whether an Australian end-user is a child and a provider will take reasonable steps to improve the accuracy of its measures over time; (v) the effectiveness and impact on user privacy of appropriate age assurance measures for a service must be proportionate to the risk of harm to Australian children from class 1C and class 2 material on the service. 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 or guardian 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, 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[6].
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 Bill 2024* (which would introduce, amongst other things, 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 led 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 mandatory compliance measure identified in the Schedule; and (ii) to the extent that the Schedule identifies possible alternative actions that may be taken, 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. 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

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

	eSafety Commissioner, consistent with the recommendations in the July 2024 Position paper.

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

7.5.1. Code structure

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

7.5.2. Services that allow a high-priority restricted category of material.

If the posting of material in a given high-priority restricted category is allowed under the applicable terms of use for the social media service, then the service provider will need to comply with compliance measures for that restricted category of material as set out in clause 6 and the table in clause 7 of the Schedule. The service provider will also need to comply with certain general supporting compliance measures, as set out in the table in clause 9 of the Schedule.

7.5.3. Services that prohibit a high-priority restricted category of material

If the posting of material in a given high-priority restricted category is not allowed under the applicable terms of use for the social media service, then the service provider must assess the risk that material in that high-priority restricted category will be accessed, distributed or stored by an Australian child on that service. Based on the risk assessment, the service provider will need to comply with compliance measures for that high- priority restricted 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 harmful 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.

7.5.4. 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 posting of material in a given high-priority restricted category 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)).

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

Consistent with the Phase 1 Codes:

- a limited category of social media services that meet requirements regarding their purpose, functionality, and reach, are automatically accorded Tier 3 status. This exception is intended to reduce the compliance burden on services that are low risk e.g., teaching and learning platforms in schools and universities that allow students to interact with each other and teachers via a blog or discussion board, but do not allow users to create a profile; and

- providers of social media services that 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.

7.5.6. 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 high priority restricted materials, and in the case of a service that prohibits such materials, the service's risk tiering. Some measures apply to specific types of high priority restricted 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.

7.5.7. Compliance measures where high-priority restricted category material is allowed on a social media service

Objective 1: Protect and prevent children in Australia from accessing or being exposed to class 1C and class 2 material.	See Matter 1 s141 notice
Age assurance	**MCM 1.1** A provider of a service must, to the extent technically feasible and reasonably practicable, take steps to implement: (a) implement appropriate age assurance measures; and (b) access control measures, before providing access to high impact online pornography and/or self-harm material; All service providers that allow any high priority restricted category of material are required to restrict access to that material to under age users.

Default safety and security settings	**MCM 1.2** A service provider must ensure that default safety settings for child end-users are appropriately robust to protect children from being exposed to high impact online pornography and self-harm material. The July 2024 Position paper recommends that social media 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. We have made this measure mandatory for all social media services that allow high impact online pornography and self-harm material (N.B we suggest the concept of safety setting is more apt here than privacy setting and we have used the concept of 'appropriately robust' to reflect that there may be even stricter settings available to deal with other types of material, which may not necessarily be appropriate to apply by default).
Appropriate measures to prevent child end-users from accessing or being exposed to high-impact online pornography or self-harm material	**MCM 1.3** A service provider must, to the extent technically feasible and reasonably practicable, implement appropriate measures to prevent child end-users from accessing or being exposed to high-impact online pornography or self-harm material. Appropriate measures may include: (a) implementing age-gates on entire services where the primary purpose or function is providing high-impact online pornography or self-harm material; or, on identified areas of services with the primary purpose of providing high-impact online pornography or self-harm material; (b) implementing interstitial notices or functions e.g. warning labels, blurring, halting autoplay, and notice screens on high-impact online pornography or self-harm material which is distributed to child end-users through news and discovery feeds, and, to the extent messaging features are not covered by another Code, through private messaging; (c) filtering high-impact online pornography or self-harm material out of news and discovery feeds by downlisting, deprioritising or quarantining, so that it is not brought to the attention of child end-users; (d) ensuring that recommender systems, algorithms, and other choice architecture, do not promote high-impact online pornography or self-harm material to child end-users; (e) ensuring that end-users are able to report or flag content which they consider may be contrary to a service's terms and conditions, or is not appropriately tagged as being unsuitable for child end-users, and take appropriate steps to respond to such reports; and (f) ensuring compatibility with third-party filtering software or tools which may be installed on devices, or provided by internet carriage services. This measure replicates the suggestion made by eSafety in 3.1 of the table of Suggested measures in the July 2024 Position paper p 85.

Terms and conditions relating to high-impact online pornography and self-harm material	**MCM 1.4** A service provider must have, and enforce, clear actions, policies or terms and conditions relating to high-impact online pornography and self-harm material, which will include to the extent applicable terms and conditions dealing with types of high-impact online pornography and self-harm material that are allowed or not allowed to be posted on their social media service. See suggested measure in 1.1 of the table of suggested measures in the July 2024 Position paper p 82
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.	
Opt-in safety tools	**MCM 1.5** Except where the predominant purpose of the service is to provide access to high impact online pornography and/or self-harm material, a service provider must allow all end-users to opt-in at any time to safety tools which may limit their access or exposure to high impact online pornography on the service and are appropriate for the service. Appropriate safety tools may include solutions for: (a) filtering material; (b) blocking material; (c) blurring material; (d) halting autoplay of material; (e) placing interstitial notices on material so that users can click through to view if they wish. 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	**MCM 1.6** To the extent relevant, a service provider must publish clear and accessible information to Australian end-users about the tools and settings available to reduce the occurrence of high impact online pornography and self-harm material in their news and discovery feed. This measure is complementary to measure 1.5.
Updates and consultation with eSafety about relevant changes to technology	**MCM 1.7** 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 high impact online pornography or self-harm 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 the equivalent measure in the Phase 1 Codes for class 1A and class 1B material to high priority restricted categories of material.
Reporting and complaints mechanisms	**MCM 1.8** A service provider must provide tools which enable Australian end-users to report, flag and/or make a complaint about high impact online pornography or self-harm material which they consider may be contrary to the social media service's terms and conditions, and that these reports are considered and actioned appropriately. Such reporting mechanisms must: (a) be easily accessible and easy to use; (b) be accompanied by clear instructions on how to use them. This measure ensures that end-users can report those categories of high priority restricted materials that breach terms of use.
On-platform reporting tools for high impact online pornography	**MCM 1.9** A service provider must ensure that the reporting tools referred to in measure 1.8 above for high impact online pornography or self-harm material are available and accessible to Australian end-users on the interface of the social media service. This measure compliments measure 1.8 by ensuring that reporting tools are readily accessible on a service.
Training	**MCM 1.10** A service provider must ensure that personnel responding to reports referred to in compliance measure 1.8 are trained in the social media service's policies and procedures for dealing with reports. This measure is also complementary to measures 1.8, and 1.9.
Reviews of compliance of personnel with systems and processes	**MCM 1.11** A service provider 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 is also complementary to measures 1.8, 1.9, and 1.10, and is consistent with best industry compliance practice.

Information about how services deal with high impact online pornography and/or self- harm material	**MCM 1.12** A service provider 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 high impact online pornography and/or self-harm material on its service. This measure extends the equivalent measure in the Phase 1 Codes for class 1A and class 1B material to high priority restricted categories of material.
Annual reporting to eSafety on Code compliance	**MCM 1.13** A service provider 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 high impact online pornography and/or self-harm material; (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 measures 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. This measure extends reporting obligations in the Phase 1 Codes to high impact restricted materials.
Information for Australian end-users about the role and functions of eSafety, including how to make a complaint to eSafety	**MCM 1.14** 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 this obligation in the Phase 1 Codes to all providers that allow a high priority restricted category material.
Location on service that is dedicated to providing online safety information	**MCM 1.15** Service providers 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 Codes to this Code.

7.5.8. Other material-specific compliance measures

Note: These compliance measures apply to the extent a high-priority restricted category of material is not allowed to be posted on a social media service under the applicable terms of use and to other class 2 material that may be posted on the social media service (irrespective of whether it is allowed under the applicable terms of use).

Objective 1: Protect and prevent children in Australia from accessing or being exposed to class 1C and class 2 material.	See Matter 1 s141 notice
Terms and conditions relating to class 1C and class 2 material Tier 1 and Tier 2 services.	**MCM 2.1** A service provider must have, and enforce, clear actions, policies or terms and conditions relating to class 1C and class 2 material. Relevant policies and actions should 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.
Appropriate measures to prevent child end-users from accessing or being exposed to high-impact online pornography or self-harm material, Tier 1, and Tier 2 services.	**MCM 2.2** A service provider must, to the extent technically feasible and reasonably practicable, implement appropriate measures to prevent child end-users from accessing or being exposed to high-impact online pornography or self-harm material. This measure reflects the suggestion made by eSafety in 4.1 of the table of Suggested measures in the July 2024 Position paper p 87. Given the examples in the Position paper are mainly directed at situations where these materials are allowed, we would appreciate further eSafety's suggestions as to what example compliance measures would be appropriate for services that prohibit these materials (other than MCM 2.1 above and MCM 2.3 below).
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.	
Continuous improvement for systems regarding high impact online pornography, Tier 1 and Tier 2 services.	**MCM 2.3** A service provider must invest in and aim to continuously improve systems which can detect high impact online pornography and automatically action that material before it is encountered by end-users. This should include increasing the capability of automated tools to make determinations about material which may be high impact online pornography.

	This measure takes into account eSafety' suggestion in 6.1 of the table of suggested measures in the July 2024 Position paper p.89
Continuous improvement for systems regarding self-harm material, Tier 1 services.	**MCM 2.4** A service provider must invest in and aim to continuously improve systems which can detect self-harm material and automatically action that material before it is encountered by end-users. This should include increasing the capability of automated tools to make determinations about material which may be self-harm material. This measure takes into account eSafety' suggestion in 6.1 of the table of suggested measures in the July 2024 Position paper p.89
Updates with eSafety about relevant changes to technology, Tier 1 services	**MCM 2.5** 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 high impact online pornography or self-harm 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 the equivalent measure in the Phase 1 Codes to high impact restricted categories of materials.
Reporting and complaints mechanisms, Tier 1 and Tier 2 services.	**MCM 2.6** A service provider must provide tools which enable Australian end-users to report, flag and/or make a complaint about class 1C and class 2 material which they consider may be contrary to the social media service's terms and conditions, and that these reports are considered and actioned appropriately. Such reporting mechanisms must: (a) be easily accessible and easy to use; (b) be accompanied by clear instructions on how to use them. This measure extends equivalent measures for class 1A and 1B materials in the Phase 1 Codes to class 1C and class 2 Materials.
On-platform reporting tools for high impact online pornography, Tier 1 and Tier 2 services.	**MCM 2.7** A service provider must ensure that the reporting tools referred to in measure 2.6 above 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 the measure in 2.6 by ensuring tools are accessible to users.

Training for personnel responding to reports, Tier 1 and Tier 2 services.	**MCM 2.8** A service provider must ensure that personnel responding to reports referred to in compliance measure 2.6 are trained in the social media service's policies and procedures for dealing with reports. This measure compliments the measure in 2.6 and 2.7 by ensuring tools are accessible to users.
Reviews of compliance of personnel with systems and processes, Tier 1 and Tier 2 services.	**MCM 2.9** A service provider 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 is complementary to measures 2.6, 2.7, and 2.8.
Information about how services deal with high impact online pornography, Tier 1 and Tier 2 services.	**MCM 2.10** A service provider 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 high impact online pornography on its service.
Information about how services deal with self-harm material, Tier 1 services.	**MCM 2.11** A service provider 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 self-harm material on its service.
Reporting to eSafety on Code compliance (high impact online pornography), Tier 1 and Tier 2 services.	**MCM 2.12** 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 high impact online pornography; (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 measures 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.

	This measure extends reporting obligations of Tier 1 services in the Phase 1 Codes to high impact online pornography materials. Given that eSafety will require periodic reporting under the BOSE , which can cover the measures taken in the Phase 2 Codes, we have made this report on request.
Reporting to eSafety on Code compliance (self-harm material), Tier 1 and Tier 2 services.	**MCM 2.13** 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 self harm material; (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 measures 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. This measure extends reporting obligations of Tier 1 services in the Phase 1 Codes to self harm materials. Given that eSafety will require periodic reporting under the BOSE , which can cover the measures taken in the Phase 2 Codes, we have made this report on request.
Engagement, Tier 1 services	**MCM 2.14** A service provider must appropriately engage with safety and community organisations (such as civil society groups, public interest groups and representatives of marginalised communities) 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. 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, Tier 1 and Tier 2 services	**MCM 2.15** 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 this obligation in the Phase 1 Codes to all Tier 1 and Tier 2 services.

Location on service that is dedicated to providing online safety information, Tier 1 services	**MCM 2.16** 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 Codes to this Code.

7.5.9. Other supporting compliance measures

Note: These compliance measures apply to all social media services that allow high-priority restricted category of material and to other social media services with a Tier 1 or Tier 2 risk profile for a high-priority restricted category of material.

Objective 1: Protect and prevent children in Australia from accessing or being exposed to class 1C and class 2 material.	See Matter 1 s141 notice
Trust and safety function	**MCM 3.1** 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.
Complaints tools	**MCM 3.2** 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: (c) be easily accessible and simple to use; and (d) be accompanied by plain language instructions on how to use them. This measure extends the equivalent measure in the Phase 1 Codes to this Code.
Timely referral of unresolved complaints to eSafety	**MCM 3.3**

	A service provider must 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 the equivalent measure in the Phase 1 Codes to this Code.

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

7.6.1. Code structure

This Code comprises the Head Terms and Schedule 2, covering relevant electronic services as defined in the OSA. The Code also includes safeguards for the community for providers of first party hosting services and first party app distribution services to the extent that there is an overlap between these activities and the provision of a relevant electronic service (see Preamble to Head Terms). This Code has also adopted key features of the RES standard, including definitions to promote a consistent approach between Codes and Standards.

7.6.2. Approach to risk of relevant electronic services

Main categories of relevant electronic services

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

- is required to assess the risk that a high-priority restricted category of material (impact online pornography and/or self-harm material) will be accessed or, distributed, or stored on that service and determine a risk profile; or
- 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 4.43.

The main categories of all providers of relevant electronic services are not required to assess their risk under this Code, consistent with the approach of the RES standard.:

- an enterprise relevant electronic service;
- a gaming service with limited communications functionality;
- a telephony relevant electronic service; and
- pre-assessed relevant electronic service meaning:
  - a communication relevant electronic service;
  - a dating service;
  - a gaming service with communications functionality.

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

Other categories of relevant electronic services

The definition of relevant electronic services is broad and may include services that may in future be specified as relevant electronic services in legislative rules[7].

Such services that do not fall into one of the categories set out in clause 4.3 assess their risk under this Code except for providers of Tier 1 relevant electronic services who notify eSafety on or before the commencement date of the Code that they have a Tier 1 risk profile. This exception

[7] s13 A, OSA.

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

The approach to assessment of risk for other relevant electronic services , and in particular the guidance on risk assessment, draws from section 9 of the Standard for Relevant Electronic Services. Note that for those services that must conduct a risk assessment 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 (cl4.3(a)).

7.6.3. 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.

This Code explains in Cl 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 the 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 penalise services that are not capable of removing material to do so, where eSafety issues a removal notice.[8] 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.

7.6.4. Compliance measures that apply to all RES:

This section requires age assurance measures based on the purpose of the service, consistent with 1.1 of the suggested measures in the Table in the July 2024 Position paper. We have required age assurance to RES services that fall into certain high risk categories (as opposed to general purpose RES which are often critical communications tools). Those high risk RES are those that have the sole or predominant purpose of distributing high impact online pornography or simulated gambling materials . See the discussion on age assurance and restriction of access to class 1C and class 2 materials above.

[8] see for example, section 80, section 91,section 111, section 121 OSA.

Objective 1: Protect and prevent children in Australia from accessing or being exposed to class 1C and class 2 material.	See Matter 1 s141 notice
Age assurance measures for high impact pornography	**MCM 1** A provider who provides a relevant electronic service with the sole or predominant purpose of permitting end-users to share high impact online pornography must, to the extent technically feasible and reasonably practicable, implement: a) appropriate age assurance measures; and b) access control measures, before providing access to that service. This measure requires age assurance measures for services that actively solicit pornographic materials on their services .e.g Chaturbate.
Age assurance measures for gaming services	**MCM 2** A provider who provides a gaming service that enables end-users to play a computer game that is, or would likely be, classified as R18+, because it constitutes simulated gambling material must, to the extent technically feasible and reasonably practicable, implement: a) appropriate age assurance measures; and b) access control measures, before providing access to that computer game. This measure requires age assurance measures for simulated gambling games.

7.6.5. Compliance measures for communication relevant electronic services

Objective 1: Protect and prevent children in Australia from accessing or being exposed to class 1C and class 2 material.	See Matter 1 s141 notice
Terms and conditions prohibiting illegal activity	**MCM 3** A provider of a communication relevant electronic service must: a) have terms and conditions in place with 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 agreement terms and conditions; and d) if the provider becomes aware of a breach of the prohibition described in a), take appropriate and proportionate action. 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). Most communications relevant electronic 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 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 will inevitably 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*[9]. 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 communication RES falling in certain high risk categories to implement age assurance measures and access controls (see table at 7.7.4 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 high impact pornography (see measure 7 below); and

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

	(iii) included measures 3 and 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.
Contact mechanisms	**MCM 4** A provider of a communication relevant electronic service must ensure that Australian end-users can contact the provider in relation to breaches of the prohibitions described in measure 3 a) by end-users of the service. A provider of a communications relevant electronic service must consider information provided by Australian end-users pursuant to this contact mechanism and take action as appropriate pursuant to measure 3 d). The contact mechanism must: a) be easily accessible and easy to use; b) where the mechanism does not involve use of a widely used communication mechanism (eg phone or email), have clear instructions on how to use it; and c) 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 contacts made through this mechanism. This measure supports MCM 3.
Training for personnel responding to contact	**MCM 5** A provider of a communications relevant electronic service must ensure that personnel responding to contacts made by Australian end-users under measure 4 are trained in the communications relevant electronic service's policies and procedures for dealing with such contacts. This measure supports MCM 4.
Review of compliance personnel with systems and processes	**MCM 6** A provider of a communications relevant electronic service must review the effectiveness of its contact mechanism (as required by measure 4) and processes to ensure information received via the contact mechanism is considered and actioned (if necessary) as appropriate pursuant to measure 3 d). Such review must occur at least annually. This measure supports MCM 4 and 5.

Objective 2: Provide Australian end-users with effective information, tools and options to limit access and exposure to class 1C and class 2 material.	See s141 notices Matter 2
Tools, features and/or settings	**MCM 7** A provider of a communication relevant electronic service must ensure that it has appropriate tools, or features and/or settings available to assist Australian end-users to limit receipt of unsolicited high impact pornography. 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; b) tools, features and/or settings that automatically blur images detected as containing nudity on receipt. This measure is intended to ensure all end-users can limit receipt of unsolicited high impact pornography. See comments on MCM 3 regarding the combined approach taken in this regard.
Blocking mechanisms and group chats	**MCM 8** A provider of a communication relevant electronic service the predominant purpose of which is: a) to enable Australian end-users to view, search for or communicate with other end-users (target end-users) on the service without knowing the target end-users' phone numbers or email addresses; or b) to recommend target end-users to Australian end-users, based on interests or connections common to the end-users, must ensure that: c) if the service allows the sending of messages between end-users – it has tools and settings that allow Australian end-users to block messages from other end-users; and d) if the service allows the sending of messages in a group chat between three or more end-users – it has tools and settings that allow Australian end-users to leave that group chat. This measure is intended to ensure that all Australian end-users can limit exposure to unsolicited or unwanted contact.
Updates to eSafety about relevant changes to technology	**MCM 9** A provider of a communication relevant electronic service must take reasonable steps to ensure eSafety receives updates regarding significant changes to the functionality of their service that are likely to have a material positive or negative effect on the

	risk of sharing of high impact online pornography or self-harm material to an Australian child. A provider may choose to provide this information in a Code 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 extends obligations in the Relevant Electronic Services standard to update eSafety on changes to the functionality of their services to changes that increase the risk of sharing of high impact online pornography or self-harm material to an Australian child This mirrors the update obligations included across relevant Phase 2 Codes.
Significant changes to the service	**MCM 10** A provider of a communication relevant electronic service must ensure that before it makes a significant change to the service (including any significant new feature of the service enabled by generative artificial intelligence) that is likely to have a material negative effect on the risk of sharing of high impact online pornography or self-harm material to an Australian child, 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 review and update whether new features (including generative AI features) are safe in relation to the risk of high impact restricted materials on its service and make appropriate adjustments to mitigate risk where required.
Improvement	**MCM 11** Where appropriate and technically feasible, a provider of a communication relevant electronic service must either take reasonable steps to further develop and improve tools, features, settings and/or measures (as relevant) it has in place under measures 7, 8 or 10 (as applicable) over time, or otherwise contribute to industry safety initiatives that aim to improve online safety outcomes for Australian children. Examples of activities that a provider may engage in to meet this measure include: a) any activities designed to further develop the effectiveness of the settings and tools; b) joining relevant industry organisations or other third party organisations and sharing information on best practice approaches; c) contributing to industry initiatives (including initiatives lead by industry associations or other third party organisations);

	d) conducting or supporting research into and development of online safety settings and tools and approaches; e) providing support, either financial or in kind, to organisations the functions of which are or include protection of children online; f) extending the application of a feature or tool applied under another industry code or standard to operate in connection with its service; and g) activities that aim to refine algorithms or inputs into tools to improve their effectiveness. 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 Relevant Electronic Services 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 MCM 16 in this regard.
Information about tools and contact mechanisms	**MCM 12** A provider of a communication relevant electronic service must provide clear and accessible information to Australian end-users regarding: a) the tools, features, settings and/or measures required by measures 7, 8, 10 and 11 (as relevant); and b) how to contact the provider as required by measure 4. 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 7, 8,10 and 11. 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	**MCM 13** 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 MCM's in SMS code. This incorporates suggestions from the Position Paper that the Code contains measures requiring providers to make information available.
Location on or via service that is dedicated to providing online safety information	**MCM 14** A provider of a communications relevant electronic 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) include 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. See equivalent measure in SMS code.
Reporting to eSafety on Code compliance	**MCM 15** Where eSafety issues a written request to a provider of a communication relevant electronic 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. See equivalent measure in SMS code. This mirrors the Code reporting obligations included across relevant Phase 2 Codes and also extends the reporting requirements of section 17 of the Relevant Electronic Services Standards for RES services, as appropriate for Phase 2.
Trust and safety function	**MCM 16** A provider of a communications relevant electronic service 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 requirements in section 17 of the Relevant Electronic Services Standard to this Code, as appropriate for Phase 2. See also the comment on MCM 11 above.
Engagement	**MCM 17** A provider of a communications relevant electronic service must either: (a) appropriately engage with safety and community organisations (such as civil society groups, public interest groups and representatives of marginalised communities) 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 materia; 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 Australian**s.** This provision is also supplementary to section 22 of the Relevant electronic Services Standard. This mirrors the engagement obligations included across relevant Phase 2 Codes.
Complaints tools	**MCM 18** A provider of a communications relevant electronic service must provide tools which enable Australian end-users to make a complaint about 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 conforms with section 28 of the Relevant electronic Services Standard
Timely referral of unresolved complaints to eSafety	**MCM 19** A provider of a communications relevant electronic service must refer to eSafety complaints from Australian end-users concerning the provider's 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 Relevant Electronic Services Standard to this Code, as appropriate for Phase 2.

7.6.6. Compliance measures for dating services: measures 20-35

In general dating services have the same obligations in this Code as Communications Relevant Electronic Services. It does not include an equivalent to measure 8. Measure 26 is also different to MCM 10:

Significant changes to the service, Dating services	**MCM 25** Unless it has implemented: a) appropriate age assurance measures; and b) access control measures, before providing access to its dating service, a provider of a dating service must ensure that before it makes a significant change to the service (including any significant new features of the service enabled by generative artificial intelligence) that is likely to have a material negative effect on the risk of sharing of high impact online pornography or self-harm material to an Australian child, it must: c)carry out an assessment of the kinds of features and settings measures that could reasonably be incorporated into the service to minimise that risk; and d) where appropriate, apply features and settings measures so identified to help to mitigate that risk. This measure is intended to limit the requirement of risk assessments following changes to the service, where the service has assured that users are over 18 years of age.

7.6.7. Compliance measures for gaming services with communications functionality: measures 36-51

As for the Relevant Electronic Services Standard this Code distinguishes between gaming services with limited communications functionality and gaming services with communications functionality. Gaming services with communication functionality have generally equivalent obligations to communications relevant electronic services (including a requirement to implement blocking mechanisms for group chats ; see MCM 40) . There are no compliance requirements for the former due to the low risk of this service.

7.6.8. Compliance measures for telephony RES: measures 52 -57

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

Email systems provided by carriage service providers (CSPs) run on networks and systems that were not designed to provide these services. They are ancillary to the services of internet access and the provision of a mobile/fixed network. Many have been built to global standards, past or still applicable. Consequently, these networks and systems are far less adjustable (i.e. there are no simple ‘bolt-ons’ or network upgrades that could be used). Measures to ‘scan’ messages for class 2 material would most likely require a ‘rebuild’ of systems associated with multi-year change programs and leading to unmanageable costs

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

For email services (provided by CSPs) many users are of an older demographic as younger generations tend to OTT email services.

7.6.9. Compliance measures for Tier 1 – Tier 3 MCM 58 to 71

The compliance measures are for categories of services that are presently unknown. Services with a Tier 1 -2 risk profile are subject to measures that apply to Communications Relevant Electronic Services.

7.6.10. Compliance measures for enterprise relevant electronic service

There are no additional compliance measures for these services in these Codes.

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

7.7.1. 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.

eSafety will be aware that a broad range of services are captured by the definition of designated internet services 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 and social media service, the Minister can in future specify services as designed internet services by legislative instrument.[10]

7.7.2. 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) high impact online pornography; and/or

[10] section 14, OSA.

(B) self-harm material; and

(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 high impact online pornography; 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.

7.7.3. Approach to risk assessment

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

- 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, a model distribution platform, and an enterprise DIS 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 criterion, 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 would be classified a certain way under the Classification Act. A website or app that does not meet the criteria for this category, for example, a fanfiction site that allows end-users to post self-authored publications to the service, 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; and
- high impact class 2 DIS, which are services that have the sole or predominant purpose of enabling end users to access any restricted category of material (such as porn 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, which are services that have the sole or predominant purpose of being used to generate high impact online pornography (such as 'nudify me' apps.)
- end-user managed hosting services.

Similar to the approach in the SMS Code, a provider of a DIS 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 Designate Internet Services Standard.

7.7.4. 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 was 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 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 porn site) apply in the same way to the classified DIS.

7.7.5. Measures for providers of a high impact class 2 DIS.

Objective 1: Protect and prevent children in Australia from accessing or being exposed to class 1C and class 2 material.	See matter 1 s141 notice
Age assurance measures	**MCM1.1:** The provider of the service must, to the extent technically feasible and reasonably practicable implement: a) appropriate age assurance measures; and b) access control measures, before providing access to the designated internet service. As this measure applies to services with the predominant purpose of providing access to a restricted category of material, it is a service level restriction (i.e. age assurance and access control must occur prior to the service being accessed by any Australian end-users). As this measure is designed to ensure that no child can access the service, subsequent measures are intended to complement this measure or are directed at ensuring the safety of all users of the service and not specifically child end users.
Default safety and security settings	**MCM 1.2:** The provider of the service must ensure that default safety and security settings for child end-users are appropriately robust to protect children from being exposed to high impact online pornography and self-harm material. The July 2024 Position paper 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 a service whose predominant purpose is with respect to a high-priority restricted category of material, this measure requires mandatory default

	settings where a user fails age assurance and is intended to complement the requirement for access controls in MCM 1.1.
Objective 2: provide Australian end-users with effective information, tools and options to limit access and exposure to class 1C and class 2 material.	See Matter 2 s141 notice.
Terms and conditions relating to class 1C and class 2 material	**MCM 1.3** The provider of the service must have, and enforce, clear actions, policies or terms and conditions relating to class 1C and class 2 material, which will include, to the extent applicable, terms and conditions dealing with the types of high-impact online pornography and self-harm material that are allowed or not allowed on the designated internet service. Relevant policies and actions must be implemented according to a graduated, risk-based approach. This approach may be different for different types of material. This replicates the equivalent measure for higher risk services in the SMS Code.
Reporting and complaints mechanism	**MCM 1.4** 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 material 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. See suggested measure in 1.1 of the table of suggested measures in the July 2024 Position paper p 82
On interface reporting tools	**MCM1.5** The provider of the service must ensure that the reporting tools referred to in measure 1.4 above are available and accessible to Australian end-users on-the interface of the designated internet service. This measure compliments measure 1.4 by ensuring that reporting tools are readily accessible on a service. See equivalent measure in SMS.
Information about how services deal with high impact online pornography and/or self-harm material	**MCM 1.6** 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 high impact online pornography and/or self-harm material This measure complements measure 1.1
Trust and safety function	**MCM 1.7** The provider of the service 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 requirements in section 19 of the Standard for Designated Internet Services to this code.
Timely referral of unresolved complaints to eSafety	**MCM 1.8** The provider of the service must 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 equivalent requirements in the s29 and s30 of the Designated Internet Standard to complaints concerning a material non-compliance with this Code.
Updates to eSafety about relevant changes to technology	**MCM 1.9** The provider of the service 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 high impact online pornography and/or self-harm material by an Australian child. The provider of the service may choose to provide this information in an annual report to eSafety under this Code. In implementing this measure, a provider of a service is not required to disclose information to eSafety that is confidential. This measure extends measures requiring notification of changes to a service that are analogous to section 34 of the Designated Internet Services Standard to this code.
Information for Australian end-users about the role and functions of eSafety, including how to make a complaint to eSafety	**MCM 1.10** 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 the equivalent requirement under section 26 of the Standard for Designated Internet Services to this Code.

Location on or via service that is dedicated to providing online safety information	**MCM 1.11** 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 the equivalent requirement under section 26 of the Standard for Designated Internet Services to this Code.
Engagement	**MCM1.12** 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) 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. This measure compliments section 1.3 of the Head Terms.
Complaints tools	**MCM1.13** The provider of the service must provide tools which enable Australian end-users to make a complaint about the provider's compliance with this Code. Such reporting mechanisms must: a) be easily accessible and easy to use; and b) be accompanied by clear instructions on how to use them. This measure extends the equivalent requirement under section 27 of the Standard for Designated Internet Services to apply to this Code.
Training for personnel responding to reports	**MCM 1.14** The provider of the service must ensure that personnel responding to reports are trained in the designated internet service's policies and procedures for dealing with reports. This measure replicates the equivalent requirement in the SMS Code for higher risk services
Review of compliance personnel with systems and processes	**MCM 1.15** 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
Significant changes to services	**MCM 1.16** The provider of the service must ensure that before it makes a significant change to the service that is likely to have a material negative effect on the risk of sharing of high impact online pornography and/ or self-harm 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 the requirements in s 24 of the Standard for Designated Internet Services to this Code.
Reporting to eSafety on Code compliance	**MCM 1.17** Where eSafety issues a written request to the 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) details of any risk assessment it is required to undertake pursuant to this Code; 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 measures 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 similar reporting requirements in sections 31 and 36 of the Designated Internet Services Standard to this Code.

7.7.6. measures for providers of – Designated Internet Service with a Tier 1-Tier 3 risk profile.

Objective 1: Protect and prevent children in Australia from accessing or being exposed to class 1C and class 2 material.	See matter 1 s141 notice
Appropriate measures to limit the risk of child end-users	**MCM 2.1:**

accessing or being exposed to high-impact online pornography and/or self-harm material, Tier 1 DIS	The provider of the service must, to the extent technically feasible and reasonably practicable, implement appropriate measures that limit the risk of Australian child end-users accessing or being exposed to high impact online pornography and self-harm material. Examples of appropriate measures may include: a) implementing interstitial notices or functions e.g. warning labels, b) blurring, halting autoplay, and notice screens on High Impact Online Pornography and/or self-harm material which is made available to end-users. This includes through private messaging (where available) and only to the extent messaging features are not covered by another Code; or c) filtering high impact online pornography and/or self- harm material out of news and discovery feeds by downlisting, deprioritising or quarantining, so that it is not brought to the attention of child end- users; or d) ensuring that recommender systems, algorithms, and other choice architecture, do not promote high impact online pornography and/or self-harm material to child end-users; or e) ensuring compatibility with third-party filtering software or tools which may be installed on devices, or provided by internet carriage services; or f) enabling child profiles on the service that are set by default at the highest safety settings available to limit children's exposure to high impact online pornography and/or self-harm materials. This measure largely replicates the suggestion made by eSafety in 3.1 of the table of suggested measures in the July 2024 Position paper p 85. It also replicates the equivalent measures in the SMS Code for Tier 1 and Tier 2 services.
Continuous improvement for systems regarding high impact online pornography and/or self-harm material Tier 1 services.	**MCM 2.2:** A provider of a service that does not allow high impact pornography and/or self- harm material on its service must invest in and aim to continuously improve systems which can detect high impact online pornography and/or self-harm material and automatically action that material before it is encountered by end-users. This should include increasing the capability of automated tools to make determinations about material which may be high impact online This measure takes into account eSafety' suggestion in 6.1 of the table of suggested measures in the July 2024 Position paper p.89 and replicates the equivalent measures in the SMS Code for Tier 1 and Tier 2 SMS.
Reporting and complaints mechanisms, Tier 1 and Tier 2 services	**MCM 2.3** 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 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. This extends equivalent measures in section 27 of the Designated Internet Services Standard to this Code.
Objective 2: provide Australian end-users with effective information, tools and options to limit access and exposure to class 1C and class 2 material.	See Matter 2 s141 notice.
Opt-in safety tools, Tier 1 services	**MCM 2.4** The provider of 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 high impact online pornography and/or self-harm material on the service. Appropriate safety tools may include solutions for: a) filtering material; b) blocking material; c) blurring material; d) halting autoplay of material; e) placing interstitial notices on material so that users can click through to view if they wish. This measure replicates equivalent measures for higher risk categories of social media services in the SMS Code.
Terms and conditions relating to class 1C and class 2 material, Tier 1 services.	**MCM 2.5** The provider of the service must have, and enforce, clear actions, policies or terms and conditions relating to class 1C and class 2 material, which will include, to the extent applicable, terms and conditions dealing with the types of high-impact online pornography and self-harm material that are allowed or not allowed to be posted on the designated internet service. Relevant policies and actions must be implemented according to a graduated, risk-based approach. This approach may be different for different types of material. This measure replicates equivalent measures for higher risk categories of social media services.
Trust and safety function, Tier 1 and Tier 2 services	**MCM 2.6** The provider of the service 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 requirements in section 19 of the Standard for Designated Internet Services to this Code.
Information about how services deal with high impact online pornography and/or self-harm material, Tier 1 services.	**MCM 2.7** 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 high impact online pornography and/or self-harm material on its service. This measure is complementary to MCM 2.1
Timely referral of unresolved complaints to eSafety, Tier 1 services.	**MCM 2.8** The provider of the service must 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 time frame. This measure extends equivalent requirements in s29 and s30 of the Designated Internet Standard to complaints concerning a material non-compliance with this Code.
Updates to eSafety about relevant changes to technology, Tier 1 services	**MCM 2.9** The provider of the service 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 high impact online pornography and/or self- harm materials by an Australian child. The provider of the service 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 measures requiring notification of changes to a service that are analogous to section 34 of the Designated Internet Services Standard to this code.
Information for Australian end-users about the role and functions of eSafety, including how to make a complaint to eSafety, Tier 1 services	**MCM 2.10** The provider of the service must publish clear information that is accessible toAustralian end-users which explains the role and functions of eSafety, including how to make a complaint to eSafety. This measure extends the equivalent requirement under section 26 of the Standard for Designated Internet Services to this Code.
Location on or via service that is dedicated to providing online safety information, Tier 1 services.	**MCM 2.11**

	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-user can contact third party services that may provide counselling and support; and c) is accessible to Australian end-users. This measure extends the equivalent requirement under section 26 of the Standard for Designated Internet Services to this Code.
Complaints tools	**MCM 2.12** The provider of the service must provide tools which enable Australian end-users to make a complaint about: a) the provider’s handling of reports about high impact 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: c) be easily accessible simple to use; and d) be accompanied by plain language instructions on how to use them. This measure extends the equivalent requirement under section 27 of the Standard for Designated Internet Services to apply to this Code.
Training for personnel responding to reports, Tier 1 and Tier 2 services	**MCM 2. 13** The provider of the service must ensure that personnel responding to reports are trained in the designated internet service’s policies and procedures for dealing with reports. This measure replicates the equivalent requirement in the SMS Code for higher risk services
Review of compliance personnel with systems and processes	**MCM 2.14** 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

Reporting to eSafety on Code compliance, Tier 1 and Tier 2 services.	**MCM 2.15** Where eSafety issues a written request to the 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) details of any risk assessment it is required to undertake pursuant to this Code; 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 measures 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 similar reporting requirements in sections 31 and 36 of the Designated Internet Services Standard to this Code.

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

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

7.7.8. 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.

Reporting and complaints mechanisms	**MCM 4.1** 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. This measure distinguishes between DIS that only provide materials that are classified under the National Scheme e.g films, and video and DIS which may have unclassified and classified materials.

Trust and safety function	**MCM 4.2** The provider of the service 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 requirements in section 19 of the Standard for Designated Internet Services to this code.
Reporting to eSafety on Code compliance	**MCM 4.3** 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 measures 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 similar reporting requirements in sections 31 and 36 of the Designated Internet Services Standard to this Code.
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) 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 1: 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. (iii) self-harm material; and

	(iv) Computer games that have been or would be classified R18+ by the Classification Board under the Classification Act due to the presence of class 2E material (R18+ simulated gambling computer games)
Appropriate measures to limit the risk of child end-users accessing or being exposed to other 2A and/or self-harm material	**MCM 4.4** 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 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; or b) implementing notices or functions e.g., warning labels, blurring,halting autoplay, and notice screens on other class 2A material and self-harm material; or c) filtering other 2A material and self- harm material out of discovery feeds by downlisting, deprioritising or quarantining such material; or d) ensuring that recommender systems, algorithms, and other choice architecture, do not promote other 2A material or self- harm material; 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 or self- harm materials. This measure deals with 2A materials that are not films (e.g. publications) as well as self-harm material, and are designed to restrict and limit the exposure of users to these materials via its service.
Age assurance measures	**MCM 4.5** A provider of a classified DIS 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 X18+ material and/or R18+ simulated gambling computer games. Age assurance measures are required where a classified DIS makes certain high impact restricted categories of material available via its service.
Information about tools and settings	**MCM 4.6** To the extent a provider of a classified DIS implements features, functionalities or settings that require user action to comply with measures 4.4 and 4.5, 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.

7.7.9. High Impact generative AI DIS

Measures for this service category largely replicate measures for a High Impact DIS, save that they apply to the creation of pornographic materials only.

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

7.8.1. 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.
>
>> 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.

7.8.2. 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. Clause 4 of the Code elaborates on this rationale for this approach. Additionally, the Code requires providers to review their risk following material changes in their functionality, and at least once a year. This ensures that providers of internet search engine services are committed to ensure their continued compliance with the safeguards required by the Codes.

7.8.3. Approach to measures

The Code codifies best practices concerning pornographic material, which is the only category of high impact restricted material for which providers are currently able to identify and implement access restrictions. We note that in this respect search engines are designed to not include links to pornographic material in search results unless the user is intentionally searching for it. The likelihood of accidental or unintentional encounters with pornographic material via search engines is low. Both the scope and the substance of the measures provide transparent safeguards to children and adult Australians concerning pornography. When compared to other international regulations governing pornographic material encountered via search the Code goes into greater specificity with regard to the obligations required of search engines.

Objective 1: Protect and prevent children in Australia from accessing or being exposed to class 1C and class 2 material.	See Matter 1 in s141 notice.
Policies relating to high impact online pornography	**MCM1** A provider of an internet search engine service must have and enforce policies around: a) how high impact online pornography is to be dealt with on the service, including whether or not access to any kinds of high impact online pornography are or are not allowed on the service via search results; and b) how the provider reduces the risk of Australian Children accessing or being exposed to high impact online pornography in search results. A provider of an internet search engine service must have, and implement, processes, systems and technologies to apply such policies to reduce the accessibility or discoverability of high impact online pornography by Australian Children in search results. This measure takes into account the recommendation in PCS B3.2 of the OFcom Online Safety Children's search code.
Age assurance or defaults	**MCM 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 Measure 4; or b) implement defaults in accordance with Measure 5. Note: Internet search engine services are designed for general public use, with or without an account. Providers of internet search engine services are not required to implement age assurance measures for users who are not logged into an account. This measure provides a mechanism via which users can receive a safer search experience by default without requiring that all users identify themself to the search engine provider by logging in to support age assurance. This preserves adults' ability to access information and lawful content without identifying themselves to the search engine provider

	while providing an appropriate level of default protection against children accessing pornography. This takes into account the suggestions of eSafety in 2.1 of the Table in the July 2024 Position Paper p84 that defaults be applied to all users for whom age assurance is not completed.
Default settings for Australian Children where age assurance is adopted	**MCM 3** A provider of an internet search engine service must apply safety tools and settings, like 'SafeSearch', 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 high impact online pornography in search results. This measure together with MCM3 ensures that children that are logged into an account receive, by default, a safe search experience that restricts access to pornography.
Defaults where age assurance is not adopted	**MCM 4** Where a provider of an internet search engine service cannot reasonably ascertain whether an Australian end-user is an Australian Child, or otherwise chooses not to implement appropriate age assurance measures in accordance with Measure 3, the provider must apply measures, by default: a) to reduce the risk of Australian Children accessing or being exposed to high impact online pornography in search results, and b) to protect and prevent an Australian end-user from being unintentionally exposed to high impact online pornography via search results. For example, appropriate measures may include: ● blurring high impact pornography material that appears in search results by default; or ● designing search algorithms to reduce the risk of material appearing in search results for search queries not intended to solicit the material. This measure together with MCM3 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 pornography.
Parental controls	**MCM 5** As a complement to age assurance measures and any default settings which a provider of a search engine service is required to implement under this code, a provider of an internet search engine service must make parental controls available to the parent or carer of an Australian child under the age of thirteen to limit or alter access to high impact online pornography. This measure reflects the suggestions of eSafety in 2.1 of the Table in the July 2024 Position Paper p84 that parental controls apply as a complement to age assurance and default settings.

Search advertising	**MCM 6** A provider of an internet search engine service must take appropriate steps to ensure that advertising for high impact online pornography is not served in search results for an account holder its systems indicate is likely to be an Australian Child. This measure reflects the suggestions of eSafety in 3.2 of the Table in the July 2024 Position Paper p86.
Safety tools for Australian end-users	**MCM 7** A provider of an internet search engine service must allow all Australian end-users to opt-in at any time to appropriate safety tools, such as 'SafeSearch' functionality, which restrict their access and exposure to high impact online pornography being accessed via search results. This measure reflects the suggestions of eSafety in 4.1 of the Table in the July 2024 Position Paper p88.
User choice about algorithms	**MCM 8** Providers of internet search must take appropriate steps, such as filtering, to empower Australian end-users to make choices about algorithms which may reduce the occurrence of high impact online pornography being accessed via search results. This takes into account the suggestions of eSafety in 5.1 of the Table in the July 2024 Position paper p89.
Information for end users	**MCM 9** Providers of internet search engine services must publish easily accessible and plain language information on their approaches to the safety features that are the subject of this Code. A provider of an internet search engine service must at a minimum implement the following measures as they relate to high impact online pornography: a) make available to Australian end-users clear and accessible information about settings and tools made available by the provider to reduce access to high impact online pornography via search results; b) provide information to Australian end-users about the actions they may take to provide feedback about the service, report illegal materials and report high impact online pornography despite safety tools under Measures 10, 11 and 12; c) where relevant, provide information to Australian 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 high impact online pornography; d) establish or maintain a hub, portal or other online location that houses online safety information that can be accessed by Australian end-users or refers Australian end-users to where they can find appropriate online safety information;

	e) provide clear and accessible information on how an Australian end-user can make a complaint under Measure 17 and contact eSafety where a complaint made under Measure 17 is not resolved to that end-user's satisfaction; and f) provide information to Australian end-users about the role and functions of eSafety, including how to make a complaint to eSafety under the OSA. This takes into account the suggestions of eSafety in the July 2024 Position Paper p 80 and extends relevant measures in the Phase 1 Code to online pornography.
User feedback	**MCM 10** A provider of an internet search engine service must provide tools which enable Australian end-users to provide feedback about the accessibility of class 1C and class 2 material in search results. This measure extends equivalent measures in the Phase 1 Code to class 1C and class 2 materials.
Delisting request process for illegal content	**MCM 11** A provider of an internet search engine service must have a process for receiving delisting requests from Australian end-users for pages that contain class 1C or class 2 material that is illegal and which the end-user has accessed via search results of the internet search engine. This measure extends equivalent measures in the Phase 1 Code to class 1C and class 2 materials.
Process to report high impact online pornography appearing despite safety tools	**MCM 12** A provider of an internet search engine service must have a process for receiving reports from Australian end-users that pages that contain high impact online pornography are included in search results of the internet search engine when safety tools, such as 'SafeSearch', are on. This measure ensures users are able to report websites which contain high impact online pornography and are not appropriately restricted by safety tools.
Responding to reports and legal delist requests	**MCM 13** A provider of an internet search engine service must have appropriate personnel, policies, processes, systems and technologies in place to consider and take appropriate action in response to reports by Australian end-users concerning high impact online pornography being available to Australian Children in search results and to legal delist requests. At a minimum, a provider of an internet search engine service must implement the following measures to address such reports and legal delist requests: a) implement policies, processes, systems and technologies to enable the automated, human or hybrid triaging, and

	review and response to reports by Australian end-users and legal delist requests; and b) 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 complaints under Measure 17. This measure extends equivalent measures in the Phase 1 Code to class 1C and class 2 materials.
User complaints	**MCM 14** A provider of an internet search engine service must provide tools which enable Australian 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. This takes into account the suggestions of eSafety in the July 2024 Position Paper p80 and extends relevant measures in the Phase 1 Code to online pornography.
Timely referral of unresolved complaints to eSafety	**MCM 15** A provider of an internet search engine service must refer to eSafety complaints from Australian end-users concerning a material non-compliance with this Code by the service 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 as in general these materials are lawful and there is significantly greater difficulty of classifying materials under this Code.
New features or functionality posing increased risk	**MCM 16** A provider of an internet search engine service must: a) conduct additional reviews of the risk posed to Australian Children that high impact online pornography is accessible in search results prior to implementing any new feature or functionality of the service that significantly increases that risk; and b) take reasonable steps to mitigate any additional risks to Australian Children concerning material covered by this Code that result from the new feature or functionality that significantly increases risk, subject to the limitations in section 6.1 of the Head Terms. This measure extends equivalent obligations in the Phase 1 Codes to online pornography.
Update eSafety on changes	**MCM 17**

	A provider of an internet search engine service must take reasonable steps to ensure eSafety receives updates regarding 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 high impact online pornography by Australian Children, such as significant changes to its machine learning algorithms and/or models (including large language models and multimodal foundation models) that increase the risk that high impact online pornography is accessible in search results. A provider of an internet search engine service may choose to provide this information as part of the provider's report under Measure 23. This extends equivalent measures in the Phase 1 Codes to this code.
Engagement	**MCM 18** A provider of an internet search engine service must appropriately engage with safety and community organisations (such as civil society groups, public interest groups and representatives of marginalised communities) 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. This measure further supports the commitment in section 1.3 of the Head Terms
Invest in ongoing improvements	**MCM 19** A provider of an internet search engine service must invest in ongoing improvements to its systems to automatically detect high impact online pornography and automatically action that material according to user preferences such as those expressed through 'SafeSearch' functionality. This should include increasing the capability of automated tools to make determinations about material which may be high impact online pornography, incorporating factors like context. This measure further supports the commitment in section 1.3 of the Head Terms
Invest in and adequately resource teams	**MCM 20** A provider of an internet search engine service must measurably invest in and adequately 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 flagged material and can consider material including factors like context while automated consideration of these factors is not technically feasible or reasonably practicable.

Reporting on Code compliance	**MCM 21** 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 their applicable mandatory compliance measures; and b) an explanation as to why these measures are appropriate. This extends equivalent measures in the Phase 1 codes to this code.

7.9. Schedule 5 App Distribution Services Online Safety Code (Class 1C and Class 2 Material)

7.9.1. Structure of Code

This Code covers providers of app distribution services as defined in the OSA. Owing to the overlap between app distribution services and the provision of other service categories regulated by the OSA, the Code follows the approach of the Phase 1 Code and is limited to the distribution of third-party apps on these services. This is because, where an app distribution service provider is distributing its own first-party apps, the provider will already be subject to other Codes that apply to services that can be accessed via such apps (including their supply/distribution).

7.9.2. App distribution services/providers of third party apps

Following the approach in the Phase 1 Codes, this Code is limited to the distribution of third-party apps. There is a structural distinction made in the Code between the provider of the app distribution service itself, and the third-party providers of the apps that are placed on the app distribution service for distribution. The third-party app providers are not subject to the requirements of this Code. They are already regulated separately under the OSA and under the Codes that apply to their apps. The focus of this Code is therefore not on the provision of the apps themselves (given the apps are already regulated under the OSA and the other Codes applicable to their third-party app providers) but on the role of the app distribution service provider in providing an additional line of protection for Australian end-users including children. That said, we have distinguished between apps that are obviously predominately for the purpose of distributing high impact materials and simulated gambling materials which present the highest risk to children and other apps. Please note the introduction of a new definition for this purpose:

> **high impact app** means a third-party app that has the sole or predominant purpose of enabling end-users to access any or all of the following types of materials:
>
> (a) high impact online pornography; or
>
> (b) self-harm material.
>
> **simulated gambling app** means a third-party app that contains or provides access to any computer game that is, or would likely be, classified as R18+, because it constitutes simulated gambling material.third-party app means an app that is:
>
> (a) provided by a person other than the app distribution service provider for that app; and
>
> (b) standalone in nature (i.e., not separate components of a program).

Age assurance obligations for app stores sit with those app stores who choose to make available high impact or simulated gambling apps, given it is obvious predominantly for the purpose of distributing class 2 material. For other apps, it is not obvious to the app store owner the prevalence of class 2 material or the extent to which users may be under 18. For that reason, it is primarily the obligation of those app developers to undertake age assurance in line with their commitments under other Codes, but with obligations triggered for app stores if developers of high impact or simulated gambling apps fail to do so (in addition to the other proportionate obligations sitting with app stores).

7.9.3. Enterprise app distribution

The Code does not apply to internal distribution of apps within an enterprise or other organisation, where there is no external supply to an Australian end-user. It also does not apply where the apps distributed on a service are exclusively apps that have already been classified by the National Classification Scheme. This is consistent with the approach in the Phase 1 Code.

7.9.4. Approach to risk

Clause 4 of the Code explains the role of app distribution services in the tech stack. As app distribution service providers are not the providers of the apps themselves, they do not directly control or have full visibility of all content shared via apps.

The measures in the Code are designed to be proportionate and appropriate to the role of app distribution service providers.

Given the nature of app distribution service providers' role, all app distribution services are treated as having a similar risk profile under the Code.

7.9.5. 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 for app distribution services. The Code applies these safeguards and makes them enforceable for a much broader range of app distribution services (including future and developing app distribution services) than the existing range of app distribution service providers that currently adopt best industry practices in respect of those matters.

Objective 1: Protect and prevent children in Australia from accessing or being exposed to class 1C and class 2 material.	
Terms, enforcement, actions and policies relating to high impact apps and simulated gambling apps	**MCM 1** An app distribution service provider that includes any high-impact apps or simulated gambling apps on its app distribution service must: a) have agreements in place with third-party app providers of any high-impact apps and simulated gambling apps on the app distribution service that require those third-party app providers to implement appropriate age assurance measures and access control

	measures to the extent required by any industry codes registered under the OSA; b) have systems, policies and/or procedures in place that enable an app distribution service provider to: i) where the app distribution service provider becomes aware of a breach of the contractual provisions described in sub-measure a) due to a failure to implement age assurance measures or access control measures, take appropriate and proportionate action; and ii) take at least one of the options described in c) ii) below; c) if the app distribution service provider becomes aware of a breach of the contractual provisions referred to in sub-measure a): i) take appropriate action pursuant to the systems, policies and/or procedures referred to in sub-measure b) (i) that is reasonably proportionate to the nature of the third-party app provider's breach; and ii) if, after a reasonable period has elapsed, the third-party app provider still has not complied with the contractual provisions, either: A. remove the high-impact app or simulated gambling app from the app distribution service; or B. to the extent technically feasible and reasonably practicable implement appropriate age assurance measures and access control measures prior to permitting download of the high-impact app or simulated gambling app. It is not necessary that a particular form of words be used in the agreement so long as the contractual effect of the agreement is as required by sub-measure (a). This measure sets out how app distribution providers will incentivise certain app providers to meet age assurance and access control requirements under the various Phase 2 Codes, and provide protections where there are failures to do so. The Position Paper indicates that the appropriateness of age assurance measures should be proportionate to risk. Measure 1 is focused on high risk apps - namely, high-impact apps and simulated gambling apps . This involves an approach to apps that is proportionate to risk, but also one that focuses on apps where it should be reasonably clear to the app distribution service provider that the apps in question fall within the high-risk categories. For other apps, the risk associated with class 1C and class 2 material may not be obvious to an app distribution service provider given (as outlined in section 4 of the Code) app distribution service providers do not directly control or have visibility of all content shared via third-party apps. The measure obliges app distribution service providers to contractually require third-party app providers to implement appropriate age assurance measures and access control measures. If third-party app providers breach these requirements then after attempts to resolve the issue, the app distribution service provider must either remove the

	relevant app from the app distribution service or implement age assurance solutions to prevent children downloading the app. The Code does not require app providers to age-gate all services as this would subject users to multiple barriers to accessing services which are more efficiently implemented at the service level. In the case of some services under these Codes, content services providers will need to take measures to prevent children accessing specific content but not the service itself, in order to ensure that age assurance is proportional to the matters set out in the s141 notice.
App review	**MCM2** An app distribution service provider must: a) have systems, policies and/or procedures in place for the review of third-party apps that may be provided to Australian end-users via the app distribution service before those third-party apps are released on the app distribution service, with the aim of reducing the risk of children being exposed to class 1C and class 2A material via the third-party app; b) review, to the extent reasonably practicable, third-party apps that may be provided to Australian end-users via the app distribution service pursuant to the systems,policies and/or procedures referred to in sub-measure a). This measure enhances the measures for app review in the Phase 1 Code. This measure mirrors but extends MCM 1d) and 1e) of the Phase 1 Code to cover class 1C and class 2A material. Again, this focuses on a risk that is more likely to be identifiable to an app distribution service provider during app review (noting that app distribution service providers will not always have full visibility of the content that will be available to end-users on the app during the review process).
Age and/or content ratings	**MCM3** An app distribution service provider must: a) ensure that age and/or content ratings information includes information that will assist Australian end-users to make decisions about a third-party app's suitability for children; b) to the extent that an age and/or content rating outcome has been provided to the app distribution service provider by a third-party app provider, have a policy and/or procedure to consider the appropriateness of that age and/or content rating outcome given the potential for class 1C or class 2A material on the third-party app; and c) have a policy and/or procedure in place to: A. if an age and/or content rating outcome was determined by the app distribution service provider, ensure that the app distribution service provider will re-consider the appropriateness of the age and/or content rating outcomes as appropriate; and

	B. if an age and/or content rating outcome was provided to the app distribution service provider by a third-party app provider, request that the third-party app provider will re-consider the appropriateness of the age and/or content rating outcomes as appropriate and if not satisfied with their response to that request, raise that concern with the third-party app provider and take appropriate action; and d) implement the policies and/or procedures described in (b) and (c). This measure builds on MCM 3 of the Phase 1 Code. It addresses eSafety's suggestion on page 86 of the Position Paper that app distribution services consider the appropriateness of any developer-submitted age rating as part of any app review process. In combination with measure 9 (user feedback) it incorporates eSafety's suggestion that users be given a means to provide feedback on apps which may have been inappropriately age rated. Guidance on measure 9, and measure 3, makes clear that a significant volume of such feedback should trigger a reconsideration of the appropriateness of an age rating (or a request to the relevant third-party app provider to do so). It also goes beyond this to more generally require app distribution service providers to re-consider the appropriateness of age rating outcomes as appropriate.
Objective 2: Provide Australian end-users with effective information, tools and options to limit access and exposure to class 1C and class 2 material.	
Safety tools and/or features	**MCM 4** An app distribution service provider must provide appropriate safety tools and/or features for its app distribution service that assist Australian end-users to make decisions about third-party apps that are only suitable for adults. Examples of appropriate safety tools and/or features may include: a) parental controls; b) tools or features that require parental/guardian approval for child purchases or categories of child purchases; c) features that promote and/or provide information about the age and/or content ratings used, and apps that fall within different age and/or content ratings used for children; d) child friendly tabs (or sections of the app distribution service) with curated content; e) tools or features that enable parents/guardians to block download of apps or categories of apps by children.

	This measure incorporates suggestions by eSafety on page 87 of the Position Paper regarding safety tools, with examples relevant to an app distribution service included. Such requirements for safety tools are in addition to measures such as measure 1 above which supports and encourages age assurance protections for high-risk apps.
Recommender systems	**MCM 5** If there are both high impact apps and other third-party apps available on an app distribution service, the app distribution service provider must take appropriate steps to ensure that any recommender systems in the app distribution service minimise the promotion of those high impact apps to Australian end-users who are children. This incorporates some suggestions from page 86 of the Position Paper that app distribution services should not serve details of age inappropriate apps to child end-users (via search results and advertisements) and also on page 87 regarding recommender systems, with a focus on high-risk apps. The provision has been tied to recommender systems for promotion of apps (as opposed to recommender systems in relation to news and content discovery feeds) given that app distribution services may not have news and content discovery feeds.
Improvement of safety tools	**MCM 6** An app distribution service provider must take steps to further develop and improve the tools it has in place under measure 4 over time. Examples of activities that a provider may engage in to meet this measure include: a) any activities designed to further develop the effectiveness of the tools; b) sharing information with third-party app developers to assist them to understand how tools will interact with their apps; c) joining industry organisations intended to address online harm to children and sharing information on best practice approaches; d) conducting or supporting research into and development of online safety tools and approaches; e) providing support, either financial or in kind, to organisations the functions which are or include protection of children online; f) extending the application of a feature or tool applied under another industry code or standard under the OSA to operate in connection with its app distribution service; g) activities that aim to refine algorithms or inputs into tools to improve their effectiveness.

	This incorporates suggestions for improvement of protective tools on page 88 of the Position Paper with examples of relevant activity that may contribute to this. The suggestion for a measure regarding resourcing trust and safety functions was not included given this is already required under the Phase 1 Code.
Online safety resources	**MCM 7** An app distribution service provider must provide online safety resources that include clear and accessible information for Australian end-users regarding: a) the age and/or content ratings approach used by the app distribution service provider pursuant to measure 3 b) safety tools and/or features used by the app distribution service provider pursuant to measure 4; c) the ability of Australian end-users to report or complain about content on a third-party app to the third-party app provider; d) the mechanisms in measure 8; and e) the role and functions of eSafety, including how to make a complaint to eSafety about class 1C or class 2 material. This incorporates suggestions from the Position Paper that the Code contains measures requiring providers to make information available about safety features, educational resources, and links to complaint systems (both those administered by industry participants and by eSafety). Note that this provision builds on existing information requirements already included in the Phase 1 Code, and therefore does not repeat all of those requirements.
Enabling reporting by end-users	**MCM 8** An app distribution service provider must provide a mechanism that enables Australian end-users to report or make a complaint about: a) a failure by a third-party app provider to satisfactorily resolve a report or a complaint by the Australian end-user relating to a third-party app distributed by the app distribution service provider; and b) a breach of this Code by the app distribution service provider. The reporting tool and complaints mechanism must: c) be easily accessible and easy to use; and d) be accompanied by plain language instructions on how to use it. A failure by a third-party app provider to satisfactorily resolve a report or a complaint as required by a), means a failure to resolve

	a report or a complaint that the third-party app provider is obliged to handle under the industry code applicable to the relevant third-party app. This measure strengthens the reporting requirements for the Phase 1 Codes and extends these to this Code.
User feedback	**MCM 9** An app distribution service provider must: a) provide a means for Australian end-users to provide; and b) accept and consider; feedback from Australian end-users on the age and/or content ratings applied to any third-party app on the app distribution service. In combination with measure 3 (age and/or content ratings) this incorporates suggestions from the Position Paper that users be given a means to provide feedback on apps which may have been inappropriately age rated. Guidance on measure 9, and measure 3, makes clear that a significant volume of such feedback should trigger a reconsideration of the appropriateness of an age rating (or a request to the relevant third-party app provider to do so).
Engagement	**MCM 10** An app distribution service provider must appropriately engage with safety and community organisations (such as civil society groups, public interest groups and representatives of marginalised communities) to gather information to help inform the measures taken for the purposes of protecting or preventing children from accessing high impact apps or simulated gambling apps).
Updates to eSafety about relevant changes to technology	**MCM 11** An app distribution service provider must take reasonable steps to ensure eSafety receives updates regarding significant changes to the functionality of their app distribution service that are likely to have a material positive or negative effect on the risk of children accessing high impact apps or simulated gambling apps. An app distribution service provider may choose to provide this information in a Code report to eSafety under this Code. In implementing this measure, industry participants are not required to disclose information to eSafety that is confidential**.** This mirrors the engagement obligations included across relevant Phase 2 Codes.
Reporting to eSafety on Code compliance	**MCM 12** Where eSafety issues a written request to a provider of an app distribution 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 compliance measures under this Code; b) an explanation as to why these measures are appropriate. A provider of an app distribution service who has received such a request from eSafety must 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 app distribution service 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.

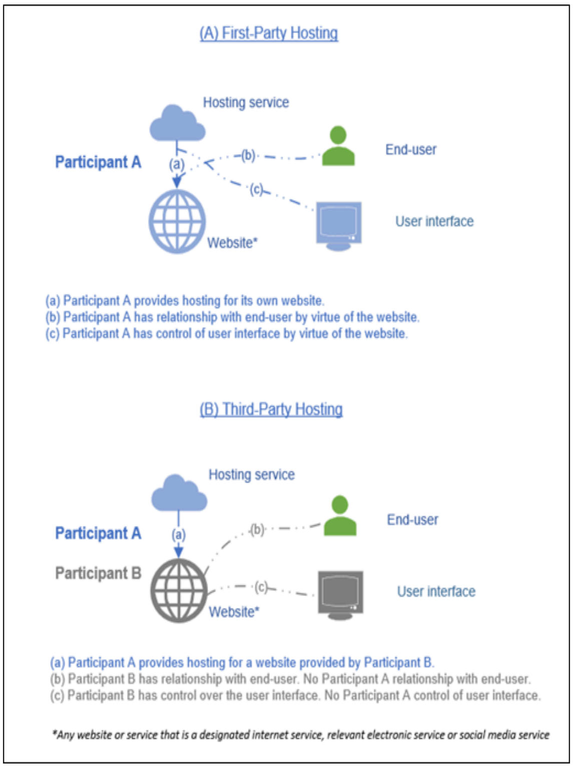
7.10. Schedule 5 Hosting Services Online Safety Code (Class 1C and Class 2 Material)

7.10.1. 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.

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.

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


(A) First-Party Hosting
Hosting service
Participant A
(a)
(b)
(c)
End-user
User interface
Website*
(a) Participant A provides hosting for its own website.
(b) Participant A has relationship with end-user by virtue of the website.
(c) Participant A has control of user interface by virtue of the website.
(B) Third-Party Hosting
Hosting service
Participant A
(a)
Participant B
(b)
(c)
End-user
User interface
Website*
(a) Participant A provides hosting for a website provided by Participant B.
(b) Participant B has relationship with end-user. No Participant A relationship with end-user.
(c) Participant B has control over the user interface. No Participant A control of user interface.
*Any website or service that is a designated internet service, relevant electronic service or social media 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.

7.10.2. 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.

7.10.3. 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.

Objective 1: Protect and prevent children in Australia from accessing or being exposed to class 1C and class 2 material.	See Matter 1, section 141 notice.
Policies and contractual terms relating to applicable Australian content laws	**MCM 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 suggestion by eSafety in the 6.1 of the July 2024 Position paper p.86
Enforcement action relating to customer breaches of policies and contractual terms	**MCM 2** A provider of a third-party hosting service must 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. This measure supports MCM1.
Objective 2 :Online industry must provide Australian end-users with effective information, tools and options to limit access and exposure to high impact online pornography, class 2D and other class 2 material	

Contact Mechanisms	**MCM 3** A provider of a third-party hosting service must ensure that end-users can contact the provider in relation to breaches of applicable Australian content laws and regulations by customers including industry codes or standards made pursuant to the OSA, that create legal obligations for customers relating to class 1C and class 2 material of the third party hosting service. This extends equivalent provisions in the Phase 1 Codes to the Phase 2 Codes.
Policies and procedures relating to Code compliance	**MCM 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 Phase 1 Codes to the Phase 2 Codes
Other supporting Measures	
Reporting to eSafety on Code compliance.	**MCM 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 minimum compliance measures;and b) an explanation as to why these measures 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 annual reporting measures in the Phase 1 Codes to the Phase 2 Codes.

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

7.11.1. Approach

This Code comprises the Head Terms and Schedule 7 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.

This Code expands upon the requirements previously imposed on ISPs through the *Content Services Code 2008 (Version 1.0)* and the *Codes for Industry Co-regulation in the Areas of Internet* *and Mobile Content 2004 (Version 10.4)* (which ceased to exist with enactment of the OSA). 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[11]: ISPs cannot control content accessible using their services. The only way to potentially limit access to material accessible using their service is (in some cases) through blocking access to content on a URL/domain basis. ISPs contribute to the safety of end-users through the provision of information and the promotion of filters. They will assist filter providers, where technically possible, with compatibility issues.

ISPs are distinct from hosting services.

7.11.2. Risk

Under this Code, all ISPs have the same risk and are subject to the same minimum compliance measures.

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) a minimum compliance measure requiring ISPs to have processes in place to check that new Australian end-users 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.

Objective 1: Protect and prevent children in Australia from accessing or being exposed to class 1C and class 2 material.	
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.	**MCM 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 and be provided at or close to the time of the sale, as well as at least annually thereafter. This measure has been strengthened to ensure that the required information will now be provided annually, in addition to being easily accessible and at/close to the time of sale. This will assist with bringing filters to the front of mind to end-users. In addition MCM 2 (promotion of the Family Filter Program) remains unchanged:

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

	MCM 2: An internet service provider must 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.
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.	**MCM 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 and be provided at or close to the time of the sale, as well as at least annually thereafter. This measure has been strengthened to now include information (being easily accessible, provided at/close to time of sale and annually) on how end-users could provide feedback should they encounter compatibility issues. This measure is further complemented by additional measures to improve any compatibility issues with ISP proprietary and third-party filter products where they arise for end-users. Please refer to MCMs 7 and 8 (see further below). These measures are in addition to existing measures in relation to information provided on the end-user's right to complain, noting that any complaints to an ISP are subject to an extensive ACMA-enforced Complaint Handling Standard which which sets out detailed rules for the handling of complaints, including timeframes for responding to complaints The Standard 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. Note: 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. Blocks not being applied 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. not all compatibility issues are, or remain, within the control of the ISP. Due to the number of different types of routers available through third parties (even if supplied by the ISP), ISPs would not ever 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, be they proprietary or third-party.
Objective 2: Provide customers in Australia who use internet carriage services with effective information, tools and options	

to limit access and exposure to class 1C and class 2 material.	
Improvement of protective tools Providers should measurably invest in and improve the efficacy and end-user experience with filters and parental controls, to encourage users to adopt these tools and reduce user drop-off from filters as the result of poor service or user experience.	**MCM 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 and be provided at or close to the time of the sale, as well as at least annually thereafter. As indicated above, this measure aims at bringing filtering products to the front of mind of consumers at regular intervals (annually). **MCM 7:** If an internet service provider makes available a proprietary filtering product, the internet service provider must, to the extent technically feasible, ensure compatibility of that filtering product and the internet service it provides. **MCM 8:** Where an internet service provider becomes 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. If technically feasible, 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. 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. They will also attempt to assist the filtering provider to resolve compatibility issues.This aims at further improving the user experience with filtering tools.Currently, there are 11 Family Friendly Filters and a plethora of other filters (which may or may not satisfy the FFF standards if they were to undergo testing). As 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 incorporate user behaviour in relation to potentially unwanted material.

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

7.12.1. Scope

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

This Code codifies industry best practices that provide safeguards for the community in respect of the matters set out in the section 141 notice for equipment providers manufacturers suppliers, installers and maintenance providers, and beyond that, for operating system providers. The Code applies these safeguards and makes them enforceable for a much broader range of equipment providers (which include manufactures, suppliers, installation and maintenance providers) than the existing range of equipment providers that currently adopt best industry practices in respect of those matters.

7.12.2. Approach to risk of devices:

This Code defines devices into three risk tiers: interactive (Tier 1), secondary (Tier 2) or non-interactive (Tier 3), and provides a table with criteria designed to guide industry participants subject to this Code with determining their devices, which reflects the same approach taken in the Phase 1 Codes.

The minimum compliance measures in this Code are focused on interactive (Tier 1) devices (and associated operating systems of these devices), which are differentiated from the other device risk tiers by virtue of the fact that general internet browsing through a screen or display capable of displaying video or images is an intended significant function of the device. It is this element which poses the highest likelihood that a child will be able to access class 1C/2 material. This approach is consistent with the July 2024 Position Paper which outlines the need to account for the likelihood that a child will use a device to access class 2 material on a service, while also ensuring that low or no risk internet-connected devices are not subject to inappropriate regulatory burden.

Unlike the Phase 1 Equipment Code, this Code does not include definitions for 'children's interactive devices' (devices targeted at children) and 'gaming devices', nor are there specific minimum compliance measures targeted at these types of equipment. Instead, the minimum compliance measures apply to all interactive (Tier 1) devices and/or OS providers (as appropriate) regardless of whether the equipment is targeted at children or used for gaming. This approach is consistent with the July 2024 Position Paper 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.[12] Further, this ensures that gaming devices with general internet browsing capability, and therefore the highest risk of enabling access to class 2 material by a child, are subject to the measures in this Code.

7.12.3. Approach to supply chain/equipment providers:

Minimum 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.

[12] *July 2024 Position paper* p 76.

Objective 1: Protect and prevent children in Australia from accessing or being exposed to class 1C and class 2 material	See S141 notice, Matter 1.
On-device measures for child accounts or profiles (OS providers of Tier 1 devices)	**MCM 1** An OS provider must: a) enable Australian end-users to set up child accounts or profiles for use on interactive (Tier 1) devices; b) have appropriate default safety settings applied to such child accounts or profiles that reduce the risk of such accounts or profiles being used to view high impact pornography; and c) only permit those default safety settings to be adjusted via an adult account or profile that is linked to the child account or profile. 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 measures 2 and 5 of this Code which provide for additional safety tools and settings that can be applied to protect child end-users aged thirteen and above.
On-device measures for adult accounts or profiles (OS providers of Tier 1 devices)	**MCM 2** 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 of Tier 1 devices)	**MCM 3** A person who is a manufacturer of an interactive (Tier 1) device must ensure that easily accessible information is made available to Australian end-users about: a) the default safety settings it has applied pursuant to measure 1 above; b) how to adjust those default safety settings; and c) how to adjust any other safety settings on the device. This measure builds on measures 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 of Tier 1 devices)	**MCM 4** A manufacturer of an interactive (Tier 1) device must ensure that the features and settings described in measures 1 and 2 are made available at no additional charge to the end-user. This measure reflects the guidance in the July 2024 Position Paper at p 86 to ensure safety features are free for end-users.
Objective 2: Provide customers in Australia who use internet carriage services with effective information, tools and options to limit access and exposure to class 1C and class 2 material.	
Tools (OS providers of Tier 1 devices)	**MCM 5** In addition to the default settings required by measure 1, an OS provider must develop and implement appropriate tools that assist Australian end-users to help manage the risk of exposure to high impact pornography. 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.
Provision of information about safe use of equipment online (manufacturers of Tier 1 Devices)	**MCM 6** A manufacturer of interactive (Tier 1) devices must ensure that easily accessible information with respect to: a) the tools described in measure 5 (if applicable); 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 high impact pornography through use of those tools when using that equipment. This measure builds on measure 5 of the Phase 1 Equipment Code to ensure manufacturers of certain equipment provide information about the safe use of equipment to end-users, and extends this requirement to tools required by this Code.
Provision of information about safe use of equipment online (suppliers of Tier 1 devices)	**MCM 7** A supplier of interactive (Tier 1) devices must provide easily accessible information about: a) the fact that such devices have some default safety settings that will be applied if a child account or profile is set up; b) the fact that other tools are available that will help Australian end-users manage access to forms of inappropriate material, 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 a) and b).

	This measure builds on measure 5 of the Phase 1 Equipment Code to ensure suppliers of certain equipment provide information about the safe use of equipment to end-users, and extends this requirement to tools required by this Code. 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)	**MCM 8** If a person is a maintenance provider or 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, upon request. This measure builds on measure 5 of the Phase 1 Equipment Code to ensure maintenance and installation providers provide information about the safe use of certain equipment to end-users upon request and extends this requirement to tools required by this Code. This measure also adopts the feedback from eSafety in the July 2024 Position Paper at p 77.
Improvement (OS providers of Tier 1 devices)	**MCM 9** An OS provider must take steps to further develop and improve safety settings and tools it has in place under measures 1 and 5 over time. Examples of activities that a provider may engage in to meet this measure include: a) any activities designed to further develop the effectiveness of the settings and tools; b) joining industry organisations intended to address online harm to children and sharing information on best practice approaches; c) conducting or supporting research into and development of online safety settings and tools and approaches; d) providing support, either financial or in kind, to organisations the functions of which are or include protection of children online; e) extending the application of a feature or tool applied under another industry code or standard under the OSA to operate in connection with its interactive (Tier 1) device; (f) activities that aim to refine algorithms or inputs into tools to improve their effectiveness. 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 Relevant Electronic Services Standard.
Trust and safety function (manufacturers and OS Providers of Tier 1 devices)	**MCM 10** A person who is a manufacturer of interactive (Tier 1) devices or an OS provider must have, or have access to, reasonably adequate 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)	**MCM 11** 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 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)	**MCM 12** 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 the provider's handling of reports about the provider's compliance with this Code. 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. This measure extends the requirement in measure 12 of the Phase 1 Equipment Code to this Code.
Communication with eSafety concerning complaints (manufacturers and supplies of Tier 1 devices)	**MCM 13** 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)	**MCM 14** 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) to gather information to help inform the measures it takes to protect or prevent children from accessing or being exposed to high impact pornography. This measure supports the general commitment made in section 1.6 under the Head Terms.
Staff (suppliers of Tier 1 devices)	**MCM 15**

	A supplier of interactive (Tier 1) devices must provide tools or training to staff to enable staff to appropriately comply with measure 7 (to the extent those staff are involved in meeting measure 7). This complements measure 7 of this Code.
Updates to eSafety about relevant changes in technology (manufacturers and OS providers of Tier 1 devices)	**MCM 16** If a person is a manufacturer of an interactive (Tier 1) device or an OS provider, that person must take reasonable steps to ensure eSafety receives updates regarding 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 high impact pornography in Australia by children. The person may choose to provide this information in a Code report to eSafety under this Code. In implementing this measure, industry participants are not required to disclose information to eSafety that is confidential. This extends obligations requiring notification of significant changes to eSafety that are analogous to MCM 4 of the Phase 1 Equipment Code.
Reporting to eSafety on Code compliance (manufacturers and OS providers of Tier 1 devices)	**MCM 17** 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.