REQUEST FOR REGISTRATION OF ONLINE SAFETY CODES

(revised 31 March 2023)

Submitted by:

Australian Mobile Telecommunications Association (AMTA)

BSA | The Software Alliance (BSA)

Communications Alliance Ltd (CA)

Consumer Electronics Suppliers Association (CESA)

Digital Industry Group Inc. (DIGI)

Interactive Games and Entertainment Association (IGEA)

31 March 2023

Contents

1. Purpose of the document

The six industry associations tasked with the development of the Online Safety Codes (the Codes) are seeking registration of the *Consolidated Industry Codes of Practice for the Online Industry (Class 1A and Class 1B Material)* under section 140(1)(c) and 140(2) of the *Online Safety Act 2021*.

For this purpose and accordance with the notices provided to the respective industry associations on 11 April 2022 (varied on 23 June 2022) by the eSafety Commissioner:

1. Communications Alliance Ltd (CA) and the Digital Industry Group Inc. (DIGI) herewith give a copy of the *Consolidated Industry Codes of Practice for the Online Industry (Class 1A and Class 1B Material) Head Terms* and *Schedule 1 – Social Media Services Online Safety Code (Class 1A and Class 1B Material)* to the eSafety Commissioner for consideration for registration;
2. The Australian Mobile Telecommunications Association (AMTA), BSA | The Software Alliance (BSA), CA, DIGI and the Interactive Games and Entertainment Association (IGEA) herewith give a copy of the *Consolidated Industry Codes of Practice for the Online Industry (Class 1A and Class 1B Material) Head Terms* and *Schedule 2 – Relevant Electronic Services Online Safety Code (Class 1A and Class 1B Material* to the eSafety Commissioner for consideration for registration;
3. AMTA, BSA, the Consumer Electronics Suppliers' Association (CESA), CA, DIGI, IGEA herewith give a copy of the *Consolidated Industry Codes of Practice for the Online Industry (Class 1A and Class 1B Material) Head Terms* and *Schedule 3 – Designated Internet Services Online Safety Code (Class 1A and Class 1B Material)* to the eSafety Commissioner for consideration for registration;
4. CA and DIGI herewith give a copy of the *Consolidated Industry Codes of Practice for the Online Industry (Class 1A and Class 1B Material) Head Terms* and *Schedule 4 – Internet Search Engine Services Online Safety Code (Class 1A and Class 1B Material)* to the eSafety Commissioner for consideration for registration;
5. CA, DIGI and IGEA herewith give a copy of the *Consolidated Industry Codes of Practice for the Online Industry (Class 1A and Class 1B Material) Head Terms* and *Schedule 5 – App Distribution Services Online Safety Code (Class 1A and Class 1B Material)*
6. BSA and CA herewith give a copy of the *Consolidated Industry Codes of Practice for the Online Industry (Class 1A and Class 1B Material) Head Terms* and *Schedule 6 – Hosting Services Online Safety Code (Class 1A and Class 1B Material)* to the eSafety Commissioner for consideration for registration;
7. CA herewith gives a copy of the *Consolidated Industry Codes of Practice for the Online Industry (Class 1A and Class 1B Material) Head Terms* and *Schedule 7 – Internet Carriage Services Online Safety Code (Class 1A and Class 1B Material)* to the eSafety Commissioner for consideration for registration; and
8. AMTA and CA herewith give a copy of the *Consolidated Industry Codes of Practice for the Online Industry (Class 1A and Class 1B Material) Head Terms* and *Schedule 8 – Equipment Online Safety Code (Class 1A and Class 1B Material)* to the eSafety Commissioner for consideration for registration.

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

1. Request for registration of Online Safety Codes including Appendix A **(new)** and Annexures 1- 5 (this document[1]);
2. Submissions log and associated responses for the first round of public consultation (September 2022);

[1] This document is the revised version of the Request for registration of Online Safety Codes document submitted to eSafety on 18 November 2022. Revisions in the documents reflect changes made to the Codes by the industry associations in response to preliminary feedback by the Office of the eSafety Commissioner provided in letters of 9 February 2023. They document has also been updated to reflect the Codes development process since 18 November 2022.

3. Submissions log and associated responses for the second round of public consultation (March 2023) **(new)**; and
4. *Consolidated Industry Codes of Practice for the Online Industry (Class 1A and Class 1B Material)* (consisting of the nine parts, i.e., Head Terms and 8 Schedules, as listed above)[2].

2. Background and current regulatory arrangements

Prior to the Online Safety Codes now submitted for registration to the eSafety Commissioner (eSafety), the Internet Industry Association, the responsibilities of which were absorbed by Communications Alliance in 2014, had developed and registered with the regulator, the Australian Communications and Media Authority (ACMA), 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)*.

The *Online Safety Act 2021* (OSA), (together with the *Online Safety (Transitional Provisions and Consequential Amendments) Act 2021*), repealed and replaced the existing online content schemes of the *Broadcasting Services Act 1992* (BSA), Schedules 5 and 7, with the Online Content Scheme in Part 9 of the OSA. With the repeal of Schedule 5 of the BSA, the legal basis for 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)* ceased to exist, and the two codes, the content of which was already long outdated, equally ceased to apply to the industry.

In addition, offline content is subject to the National Classification Scheme which is a cooperative arrangement between the Australian Government and state and territory governments for the classification of films, publications, and computer games. The National Classification Code and the guidelines for the classification of films, computer games and publications were designed primarily for the assessment of commercially produced material before its release into the community.[3] Under the Scheme, the content is largely classified having regard to its 'offensiveness'.[4] The National Classification Code, guidelines for the classification of films, computer games and publications provide the principles and criteria for making classification decisions.[5] Under the OSA , class 1 and class 2 material "is defined by reference to:

- the classification it has received by the Classification Board under the Classification Act (where the material has been classified), or
- eSafety's assessment of "the classification the material would likely be given by the Classification Board under the Classification Act (where the material has not been classified)."[6]

Accordingly, to fill the void created by the repeal of Schedules 5 and 7 of the BSA and driven by a desire to create greater online-offline regulatory parity, section 134 of the 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.

3. Outline of Codes development and registration process

Industry associations, individual participants of relevant industry sections, other stakeholders and eSafety met several times (and held four formal meetings) in the time from May 2021 to September 2021. During that time, industry and eSafety closely engaged over possible code development models, suitable engagement models (given the large number of industry participants involved and breadth of sections covered), potential code architectures, code content and other related matters. The industry associations

[2] further revised following a second round of public consultation between 10 March and 23 March 2023.
[3] p. 18, eSafety Commissioner, *Development of industry codes under the Online Safety Act, Position Paper*, September 2021
[4] pp 20/21, ibid
[5] refer to https://www.classification.gov.au/about-us/legislation as accessed on 18 Nov 2022.
[6] p. 19, eSafety Commissioner, *Development of industry codes under the Online Safety Act, Position Paper*, September 2021

involved (at that time mostly Communications Alliance, DIGI, IGEA and BSA) provided responses to several sets of questions from eSafety to assist eSafety with the development of what would become the Position Paper (see below).

On 29 September 2021, eSafety released the *Development of industry codes under the Online Safety Act, Position Paper* (Position Paper), which conveyed eSafety's understanding and expectation of the scope of material to be covered in the Codes and the underlying Objectives and Outcomes to be achieved through the Codes. The Position Paper explained that the substance of the Codes should address the issues of access, exposure and distribution that are related to class 1 and class 2 material, and also contained a detailed list of example measures of how eSafety proposed its preferred Outcomes for the Codes could be achieved.

In addition, the Position Paper also set out eSafety's eleven positions on codes development.

In October 2021, a Steering Group of six industry associations formally formed and engaged with eSafety on the development of the Codes. Those associations are:

1. Australian Mobile Telecommunications Association (AMTA),
2. BSA | The Software Alliance (BSA),
3. Communications Alliance Ltd (CA),
4. Consumer Electronics Suppliers Association (CESA),
5. Digital Industry Group Inc. (DIGI), and
6. Interactive Games and Entertainment Association (IGEA).

In addition, under the guidance of the Steering Group, industry formed several working groups to develop the Codes. To ensure broad coverage within and across all relevant industry sections, the industry associations reached out to members and non-members of their organisations and invited participation (free of charge, no membership requirement) in the Codes development process. (Also refer to section 4.7 further below.)

The Steering Group agreed with eSafety on the sequential development of two sets of Codes to cover different types of online material:

1. A first set of Codes to cover class 1A and class 1B material[7]. The Position Paper explains that sub-category class 1A material includes child sexual exploitation, pro-terror material, material in relation to extreme crime and violence, and the sub-category of class 1B materials includes crime and violence and drug related material.
2. A second set of Codes to cover class 1C and class 2 material. The sub-category of class 1C material includes fetish-related pornographic material.

The Steering Group also committed to working with eSafety's eleven positions on codes development[8]. These positions are reproduced at Annex 1.

The Steering Group and eSafety constructively engaged over the Objectives and Outcomes put forward in the Position Paper. The original Objectives and Outcomes were adopted, or consensus could be reached for ten of the eleven Outcomes, with the Outcome 1 being adopted by the Steering Group with modifications. A list of the Objectives and Outcomes is provided at Annex 2.

On 11 April 2022, the eSafety Commissioner gave notice to the six industry associations above (each for their respective industry section(s)) under section 141 of the OSA, requesting the development of industry codes, by 9 September 2022, in relation to class 1A and 1B material with measures directed at achieving the Outcomes and Objectives stated in the Position Paper.

On 23 June 2022, these notices were varied to request those codes be now submitted for registration by 18 November 2022.

[7] Refer to p.21, eSafety Commissioner, *Development of industry codes under the Online Safety Act, Position Paper*, September 2021, which further explains that class 1A, class I B and class1C categories of online materials are sub-categories of material created by eSafety based on the National Classification Code and related classification guidelines.

[8] Noting that positions 5 (timeframe for finalisation of codes) and 6 (limitation of number of codes) were later varied (in agreement with the Steering Group) by eSafety.

The giving of notice to industry associations under section 141 of the OSA is a pre-condition to the exercise of the eSafety Commissioner's discretionary powers under sections 145 of the OSA to make (an) industry standard(s).

Sections 140(1) and (3) of the OSA contain the criteria that need to be satisfied prior to the Codes being able to be registered by the eSafety Commissioner. Draft Codes were submitted to eSafety on 18 November 2022, together with supporting documentation including an earlier version of this document.

eSafety shared its preliminary assessment of the draft Codes, including areas of concern in eight letters (one for each Code) sent to the respective industry associations on 9 February 2023, requesting industry provide a response/and or resubmit revised Codes to the eSafety Commissioner by 9 March. The industry associations asked eSafety for an extension to conduct a second 30-day consultation on the draft Codes to give the community and stakeholders an opportunity to express their views on the newly revised codes following eSafety's feedback. A short extension was granted until 31 March 2023.[9]

Part 4 of this document sets out the criteria for registration and how industry has addressed the criteria in the process of developing the codes, including the measures contained in each Code. Where appropriate, the respective positions of eSafety in the eSafety Position Paper, and letters of 9 February 2023 are also referenced.

4. Criteria for registrable Codes – sections 140(1) and (3) of the OSA

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

On 11 April 2022[10], the eSafety Commissioner gave notice to the six industry associations to develop codes pursuant to section 141 of the OSA. The industry associations each received notices to develop codes that apply to participants in the online sections as per the table in section 4.2 below.

By giving notice to the six industry associations pursuant to section 141 of the OSA, the eSafety Commissioner expressed satisfaction that these associations represent the respective sections of the industry for which they have received the notices. All sections of the industry that the OSA seeks to cover through industry codes as listed in section 135 of the OSA were represented by at least one of the industry associations that received the notices.

We note that Communications Alliance was the only association to receive a notice for the online section for 'Providers of internet carriage services, so far as those services are provided to customers in Australia', despite this section being also strongly represented by the Australian Mobile Telecommunications Association (AMTA). We believe this to be an oversight.

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

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

Those Codes are (contained in the *Consolidated Industry Codes of Practice for the Online Industry (Class 1A and Class 1B Material)*):

[9] Email by eSafety to DIGI, CC Communications Alliance, IGE, BSA, AMTA, CESA dated 28 February 2023.

[10] The notice was varied on 23 June 2022 to give effect to a new due date for submission for registration of the Codes.

Title	**section of the online industry to which the code applies**	**Industry association representative as per s141 notice**
Social Media Services Online Safety Code (Class 1A and Class 1B 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 1A and Class 1B Material)	Providers of relevant electronic services, so far as those services are provided to end-users in Australia	● Australian Mobile Telecommunications Association (AMTA) ● BSA | The Software Alliance (BSA) ● CA ● DIGI ● Interactive Games and Entertainment Association (IGEA)
Designated Internet Services Online Safety Code (Class 1A and Class 1B 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 ● BSA ● Consumer Electronics Suppliers’ Association (CESA) ● CA ● DIGI ● IGEA
Internet Search Engine Services Online Safety Code (Class 1A and Class 1B Material)	Providers of internet search engine services, so far as those services are provided to end-users in Australia	● CA ● DIGI
App Distribution Services Online Safety Code (Class 1A and Class 1B 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 1A and Class 1B Material)	Providers of hosting services, so far as those services host material in Australia	● BSA ● CA
Internet Carriage Services Online Safety Code (Class 1A and Class 1B Material)	Providers of internet carriage services, so far as those services are provided to customers in Australia	● CA

Title	section of the online industry to which the code applies	Industry association representative as per s141 notice
Equipment Online Safety Code (Class 1A and Class 1B 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 1A and Class 1B Material))	● AMTA ● CA ● CESA ● IGEA (Operating systems providers were not covered in any s141 notice.)

The Codes deal with matters listed as examples that may be dealt with by industry codes and standards under section 138(3)(a) to (zj) of the OSA and in Schedule A of the notice given to industry associations by eSafety on 11 April 2022 and varied on 23 June 2022.

4.3. Industry associations to give a copy of the Codes to the Commissioner [OSA, section 140(1)(c)]

The industry associations herewith provide eSafety with a copy of the revised Codes, with request for registration pursuant to section 140(2) of the OSA and in accordance with the notice given to industry associations by eSafety on 11 April 2022 and varied on 23 June 2022 and in response to the eight letters sent by eSafety to industry associations on 9 February 2023, inviting eSafety to respond/ and or resubmit Codes for registration by 9 March 2023, and subsequent email from eSafety extending the date for response/resubmission to 31 March 2023[11].

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

The revised Codes deal with matters of substantial relevance to the community. We note that the Position Paper outlines the policy intent for the Codes, i.e., “[t]o ensure that participants of the online industry provide appropriate community safeguards for Australians in relation to class 1 materials.”[12] The section 141 notices stipulate that the Codes contain community safeguards for the matters listed in Schedule A of the notices. The Outcomes of the revised Codes correlate with the matters in the section 141 notices, with some minor changes. (Please refer to Annex 2 and footnote 5 below.) Appendix A outlines the industry associations’ response to each area of concern outlined in eSafety's eight letters to the industry associations dated 9 February 2023.

Matter 1

Measures directed towards achieving the objective of ensuring that industry participants have scalable and effective policies, procedures, systems and technologies in place to take reasonable and proactive steps to **detect and** prevent[13]:

[11] Email by eSafety to DIGI, CC Communications Alliance, IGE, BSA, AMTA, CESA dated 28 February 2023.

[12] p.7, eSafety Commissioner, *Development of industry codes under the Online Safety Act, Position Paper*, September 2021

[13] Note that Matter 1 in Schedule 1 of the notices (and in line with Outcome 1 as proposed by eSafety) reads: “Measures directed towards achieving the objective of ensuring that industry participants have scalable and effective policies, procedures, systems and technologies in place to take reasonable and proactive steps to **detect and** prevent [...]” [emphasis added]. Also refer to Annex 2 for

- access or exposure to,
- distribution of, and
- online storage of

class 1A material.

Matter 2

Measures directed towards achieving the objective of ensuring that industry participants have scalable and effective policies, procedures, systems and technologies in place to take reasonable and proactive steps to prevent or limit:

- access or exposure to, and
- distribution of

class 1B material.

Matter 4[14]

Measures directed towards achieving the objective of ensuring that industry participants have scalable and effective policies, procedures, systems and technologies in place to take reasonable and proactive steps to limit the hosting of class 1A material and class 1B material in Australia.

Matter 5

Measures directed towards achieving the objective of ensuring that industry participants have effective and scalable policies and procedures in place to facilitate consultation, cooperation and collaboration with other industry participants in respect of the removal, disruption and/or restriction of class 1A material and class 1B material, as well as accounts associated with this material.

Matter 6

Measures directed towards achieving the objective of ensuring that industry participants have effective and scalable policies and procedures in place which ensure communication and cooperation with the eSafety Commissioner with respect to matters about class 1A material and class 1B material, including complaints.

Matter 7

Measures directed towards achieving the objective of providing people with a range of technical tools and/or information to limit their access and exposure, and the access and exposure of children in their care, to class 1A material and class 1B material.

Matter 8

Measures directed towards achieving the objective of providing people with clear, easily accessible and effective:

- reporting mechanisms for class 1A material and class 1B material, as well as associated user accounts, and
- complaints mechanisms to address complaints about the handling of reports about class 1A material and class 1B material and codes compliance.

a comparison of the Objectives and Outcomes as proposed by the Position Paper/per consensus between eSafety and Objectives and Outcomes adopted by the Codes.

[14] **Matter 3** has been deliberately omitted as it pertains to class 2 material only which is not subject to the Codes.

Matter 9

Measures directed towards achieving the objective of ensuring that industry participants have scalable and effective policies, procedures, systems and technologies in place to effectively respond to:

- reports about class 1A material and class 1B material, as well as associated user accounts, and
- complaints about the handling of reports about class 1A material and class 1B material and codes compliance.

Matter 10

Measures directed towards achieving the objective of ensuring that industry participants publish easily accessible and plain language policies, procedures and guidelines that set out how they handle class 1A material and class 1B material.

Measures directed towards achieving the objective of ensuring that industry participants provide end-users with information about the safety issues associated with class 1A material and class 1B material.

Matter 11

Measures directed towards achieving the objective of ensuring that industry participants publish annual reports about class 1A material and class 1B material, and their compliance with industry codes.

4.4.1. How the Codes provide appropriate community standards for Matters in section 141 notices

The Codes provide safeguards for end-users in Australia in relation to class1 materials:

The question of whether the jurisdictional scope of the Codes should extend to end-users geographically present in Australia or be focused on Australians was extensively discussed with eSafety during the Codes development process.

Determining the appropriate jurisdictional scope of these Codes is complex given the varying ways the OSA deals with the issue. The Section 141 notices from eSafety to industry associations requesting that the Codes 'apply to participants in the group consisting of providers of social media services, so far as those services are provided to end-users in Australia'. The list of Matters to be addressed by the Codes in the section 141 notices does not stipulate the jurisdictional scope of measures in the Codes.

There is also a distinction drawn in the OSA between the application of the Codes to industry participants that conduct relevant activities and the safeguards they must contain. Section 137(1) of the OSA contains a statement of parliamentary intent that industry codes apply to relevant sections of the online industry in relation to their online activities. Section 134 defines some of these activities as entailing the provision of the service to end-users in Australia (e.g., providing a social media service, relevant electronic service, designated internet service or app distribution service to end-users in Australia). Other activities have a different jurisdictional nexus (e.g., hosting services, internet service providers). The term end-users in Australia is undefined in the OSA. In contrast section 140(1)(d) of the Act, requires that Codes provide appropriate community safeguards for matters of substantial relevance to the community. The term community is also undefined in the OSA.

The initial drafts of the Codes submitted for registration on 18 November 2022 limited the safeguards provided by the measures in the Code to Australian end-users, defined to mean end-users ordinarily resident in Australia. In the initial application for registration document submitted on 18 November 2022, the industry associations explained their view that this approach was consistent with the policy intent outlined in the Position Paper, i.e., "[t]o ensure that participants of the online industry provide appropriate community safeguards for Australians in relation to class 1 materials"[15] and that "[t]he codes be directed to ensuring that class 1 material is prevented, or limited, on services accessible to Australian end-users."[16] The associations further noted that this policy intent aligns with the overall objectives of the

[15] p.7, eSafety Commissioner, *Development of industry codes under the Online Safety Act, Position Paper*, September 2021

[16] p.38, ibid

OSA, as set out in section 3 of the OSA, which are to improve and promote online safety for Australians – relevantly defined in section 5 as individuals who are ordinarily resident in Australia. The scope to which complaints can be made about the industry codes was also noted to be a relevant practical consideration underpinning this approach. Section 40 of the OSA requires that complaints about breaches of an industry code are made by individuals that reside in Australia or bodies corporate that carry on activities in Australia or the Commonwealth, a State or Territory.

The issue of jurisdiction has been extensively discussed with eSafety, including the practical challenges of implementing content regulations that apply to end-users geographically present in Australia. We note in many cases end-users of online services will have signed up to terms of service that have been drafted to comply with the laws of the country where they are ordinarily resident. eSafety's most recent response in relation to this topic was as follows:

> *"eSafety understands that online service providers which are subject to these codes will typically have access to various data/signals, including geolocation indicators, in relation to their end users in the course of providing such services. eSafety considers it reasonable for services to take appropriate steps to consider how relevant data/signals can be used to determine whether an end-user is using the service from within Australia in order to comply with the industry codes (if registered)*.
>
> *One of the most common examples will be the use of IP addresses with an online service provider able to filter IP Addresses that do not match known IP addresses registered to Australia. Participants in different industry sections may have different capabilities to determine a user's general location based on what data/signals are collected.*
>
> *eSafety recognises there is no single method of determining whether a user is accessing a service from Australia with perfect accuracy. However, eSafety's preliminary view is that most service providers will have access to data/signals which enables the service provider to approximate whether a typical user is accessing the service from within Australia."*[17]

In the eight letters sent by eSafety to the industry associations dated 9 February 2023, eSafety made clear that it rejected industry's proposed approach to the scope of the Codes. The Commissioner stated that the Codes as drafted would not satisfy section 140(1)(b) of the Act as those were expressed to apply in respect of 'Australian end-users' and not to the relevant group of providers, described in section 135(2)(e), or to the relevant online activity, described in section 134(e). In response to eSafety's assessment that the eSafety Commissioner would not register the Codes unless the scope of the Codes was to be expressed to apply to 'end-users in Australia', the measures in the revised Codes have now been amended to satisfy this requirement, i.e., to provide safeguards for Australian end-users; defined as end-users in Australia under section 2.1 of the Head Terms.

Overlapping activities by industry participants

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

The eight Codes (and Head Terms) provide appropriate community safeguards for those matters in relation to each industry section that is the subject of a section 141 notice in the manner explained in the remainder of this section.

1. Social Media Services Online Safety Code (Class 1A and Class 1B Material)

Code structure

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

[17] Email by eSafety to DIGI dated 21 February 2023.

Approach to risk assessment

As a general principle, all social media services must assess their risk under this Code, except for:

- a limited category of social media services that meet requirements regarding their purpose, functionality, and reach, which 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 who notify eSafety on or before the date that the Code comes into effect that they have a Tier 1 risk profile. This exception is to encourage services to proactively notify eSafety that they have a Tier 1 risk profile, providing clarity to the eSafety of these services' status.

The approach to assessment of risk, and in particular the guidance on risk assessment criteria, draws from the suggestions made in the Position Paper for assessing risk, and subsequent feedback provided by eSafety to industry associations in its letter to industry associations concerning this Code dated 9 February 2023 (see Appendix A, item 6). In particular, the Code now contains mandatory requirements concerning risk assessment in Clause 5(b) and Clause 5(c) including a requirement that should a risk assessment indicate that the service may be in-between risk tiers, the provider must assign a higher risk profile to that service.

The criteria for a social media service may be altered by legislative rules and the types of services that fall within this category may further be expanded by legislative rules.[18] The functionality of these services may also change in future, e.g., with the advent of Metaverse technologies. In this context, industry is unable to prescribe a definitive methodology for the assessment of risk given the highly indeterminate nature of this service category. The risk methodology set out in the table to this Code in Clause 5 is, therefore, provided as guidance to providers of social media services. Our discussions to date with industry participants suggest that they will either declare themselves Tier 1, use this table to ascertain their risk category, or adopt a risk assessment approach closely modelled on the table.

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 social media services (including future and developing social media services) than the existing range of social media service providers that currently adopt best industry practices in respect of those matters. In particular, most of the minimum compliance measures apply to services that are assessed as Tier 1 (highest risk) and Tier 2 (moderate risk) (i.e., the majority of publicly accessible social media services). Both the scope and the substance of the measures provide a greater range of safeguards to Australians concerning harmful online material than comparable industry codes such as the *UK interim code of practice on online child sexual exploitation and abuse and the Interim code of practice on terrorist content and activity online*.

We note that the Position Paper proposed an approach to risk assessment under which medium risk industry participants would be able to set their own compliance measures based on their risk profile. Over the course of code development, eSafety provided feedback that it expected Tier 2 (moderate risk) and Tier 3 (lower risk) social media services to be subject to minimum compliance measures. This Code, therefore, includes minimum compliance measures for both these risk profiles.

Matter 1 Measures directed towards achieving the objective of ensuring that industry participants have scalable and effective policies, procedures, systems and	**Objective 1: Industry participants will take reasonable and proactive steps to create and maintain a safe online environment for Australian end-users.** **Outcome 1: Industry participants take reasonable and proactive steps to prevent access or exposure to, distribution of, and online storage of class 1A material.**

[18] Section 13(1)(iv), OSA

technologies in place to take reasonable and proactive steps to **detect and** prevent: ● access or exposure to, ● distribution of, and ● online storage of class 1A material. l	**Note: Outcome 1 does not refer to the detection of class 1A material as an entire class, noting that there are no systems and processes that can be reliably deployed to detect the range of real or simulated extreme crime and violence materials that fall within Class 1A. Instead, this Code includes measures that require the detection of specific categories of Class1 materials i.e., known CSAM and certain pro-terror materials: videos and imagery that depict and promote terrorist acts.** **MCM 1:** All social media services must notify appropriate entities – as defined in the Code - about CSEM or pro terror class 1A material on their services, if they identify this material and form a good faith belief that the CSEM or pro terror material is evidence of serious and immediate threat to the life or physical health or safety of an adult or child in Australia. This must be done within 24 hours or as soon as reasonably practicable. Note: this measure is supplementary to existing obligations that may be imposed on social media services under State or Territory or foreign laws. The disclosure of Class 1A material may involve the disclosure of personal information that identifies an individual and will be subject to the *Privacy Act 1988*. This obligation has been drafted to comply with the requirements of that Act concerning such disclosure. See section 16A(1), item 1 of the *Privacy Act 1988*. It is based on the example measure for this outcome in the Position Paper (p.68). Note also the addition in the revised Code, of additional guidance concerning the time critical nature of this measure. **MCM 2:** Tier 1 and Tier 2 social media service providers must implement systems, processes and technologies that enable the provider to take appropriate enforcement action against end-users who breach terms and conditions, community standards and/or acceptable use policies that prohibit class 1A material. At a minimum, they must have standard operating procedures that: - Specify the role of personnel in reviewing and responding to reports of class 1A materials by Australian end-users, - Include clear internal channels for personnel in escalating, prioritising and assessing reports of class 1A material by Australian end-users, - Provide operational guidance to personnel in relation to steps that should be taken when the service receives reports of class 1A materials by Australian end-users, including steps that must be taken concerning the removal of class 1A materials. Note: this measure makes best practice operating procedures for enforcement of policies enforceable for Tier 1 and Tier 2 social media services. **MCM 3:** Tier 1 and Tier 2 social media service providers must take appropriate enforcement action against end-users that breach terms and conditions, community standards, or acceptable use policies prohibiting class 1A material that is reasonably proportionate to the level of harm associated with the relevant breach. Note: this measure builds on the example measures outlined in the Position Paper (p68) by requiring proportionate enforcement action against users that breach terms of service etc. This measure's drafting provides some discretion to social media services in relation to the enforcement action they take for breaches of policies prohibiting class 1A materials, based on providers' experience. For example, some end-users (especially younger end-users) may share Class 1A images without being aware of the potential harm it may cause to victims depicted in images.

End-users may also be coerced into sharing Class 1A materials. The appropriate response will not always be to remove an end-users account. The guidance for this measure elaborates relevant considerations for the development of appropriate enforcement approaches. Note the revised Codes contain additional guidance that in circumstances where an account should be removed this should occur without delay.

Additionally, MCM 3 requires a Tier 1 and Tier 2 social media service providers to:

(a) Remove instances of CSEM or pro-terror materials that are identified to be accessible or distributed by an Australian end-user on the service, within 24 hours or as soon as reasonably practicable thereafter, unless otherwise required to deal with such material by law enforcement,

(b) Remove other instances of class 1A materials that are identified to be accessible or distributed by an Australian end-user, as soon as reasonably practicable unless otherwise required to deal with unlawful class 1A materials by law enforcement,

(c) Terminate an end-user's account as soon as reasonably practicable in the event the end-user is:

   a. Distributing CSEM or pro-terror material to Australian end-users with the intention to cause harm,
   b. Known to be using the account in breach of age restrictions concerning use of the service by an Australian child,
   c. Has repeatedly breached terms and conditions, community standards, and/or acceptable use policies prohibiting class 1A material on the service, and

(d) Take reasonable steps to prevent an end-user that meets requirements of 3 c) i) as above, from creating a new account for use of the service.

In addition, guidance provided by this measure says that a Tier 1 or Tier 2 social media service providers should consider implementing a strike or penalty, restriction, or suspension on an end-user account as an enforcement action for less serious violations of terms and conditions, community standards and/or acceptable use policies prohibiting class 1A material (other than CSEM or pro-terror materials). They should have clear, documented policy outlining the criterion that will be used when/if applying any of these measures.

Note: this measure and accompanying guidance makes industry best practice operating procedures for enforcement of policies enforceable for Tier 1 and Tier 2 social media services.

MCM 4: Tier 1 and Tier 2 social media service providers must ensure they are resourced with reasonably adequate personnel to oversee the safety of the service, with personnel to have clearly defined roles and responsibilities, including for the operationalisation and evaluation of the systems and processes required under this Code.

Note: this measure addresses the need for human resources that have specific safety responsibilities, which was reinforced by feedback from the public consultation process.

MCM 5: All social media service providers must re-assess their risk profile in accordance with this Code following the introduction or implementation of a significant new feature to their social media service. They must take reasonable steps to mitigate any additional risks to Australian end-users concerning material covered by this Code that result from the new feature.

MCM 6: Tier 1 and Tier 2 social media service providers must adopt appropriate features and settings that are designed to mitigate the risks to Australian end-users related to class 1A material, including by anticipating and detecting safety risks posed by such material. At a minimum, they must:

(a) Implement measures to ensure that material can only be uploaded to or distributed on the service by a registered accountholder,

(b) Make clear in terms and conditions, community standards and/or acceptable use policies the minimum age an Australian end-user is permitted to hold an account on the service,

(c) Take reasonable steps to prevent an Australian child that is known to be under the minimum age permitted on the service from holding an account on the service, and to remove them from the service as set out in measure 3), and

(d) Have settings that are designed to prevent account-holders from unwanted contact from other end-users.

The provider should also take reasonable steps to ensure that an Australian child that is less than the minimum age set by the provider is not using its service.

Note: this measure makes best practice operating procedures for enforcement of policies including those relating to child users enforceable for Tier 1 and Tier 2 social media services. We note that eSafety's Age Verification Roadmap and proposed Privacy Act 1988 reforms may supersede this measure.

MCM 7: Tier 1 social media service providers that permit a young Australian child (under age 16) to hold an account on the service must additionally have – at a minimum:

(a) Default settings designed to prevent a child in Australia from unwanted contact from unknown end-users, including settings which prevent the location of the child being shared with other accounts by default,

(b) Easy to use tools and functionality that can help parents or carers safeguard the safety of children using the service.

Note: this measure makes best practice operating procedures for enforcement of policies relating to young child users enforceable for Tier 1 social media services. This measure is consistent with similar requirements in comparable codes such as the *Age-appropriate design code of practice in the UK*, noting that the industry has sought not to pre-empt the outcome of other policy processes concerning protection of children online that are currently underway, including eSafety's Age Verification Roadmap and the review of the *Privacy Act 1988*.

MCM 8: Tier 1 social media service providers must deploy systems, processes and /or technologies designed to detect, flag and/or remove from the service instances of known CSAM, for example using hashing, machine learning, artificial intelligence, or other safety technologies. At a minimum, they must ensure their services use tools and technology that:

(a) Automatically detect and flag known CSAM, such as hash-matching technologies (for example, PhotoDNA, CSAI Match, and equivalent technology),

	(b) limit end-users' ability from to distribute known CSAM (for example, by 'black-holing' known URLs for such material or blocking or removing such material, or preventing users from publicly posting detected material (prior to moderation); and (c) identify phrases or words commonly linked to CSAM and linked activity to enable the provider to deter and reduce the incidence of such material and linked activity. Note: this provision addresses the matter of proactive detection of known CSAM and is based on the example measure suggested for this outcome in the Position Paper (p. 68). This measure applies to all Tier 1 social media service providers for so long as the Code is in force and is being proposed by industry in advance of regulations requiring proactive detection of CSAM in the UK and EU. In contrast to proposed regulations in the EU, the measure is not limited by any requirement that eSafety issue a proactive detection notice of limited duration and applies to a category of providers (rather than individually named providers). **MCM 9:**Tier 1 social media service providers must implement systems, processes and/or technological tools designed to detect, flag and/or remove instances of known pro-terror material from the service, for example, through the use of keyword searches, text signals, hashing, machine- learning, or artificial intelligence that scans for material that may, depending on the context, be known pro-terror material and/or systems and processes that limits users' ability to publicly post such content on their service. Note: this measure is based on the example measure suggested for this outcome in the Position Paper (p. 68) and has been revised in response to eSafety's letter of 9 February (see Appendix A, item 2). It applies to known pro-terror material which has been defined in the Head Terms and as requested by eSafety picks up the GIFCT taxonomy for classifying material that may be terrorist related. Note: We understand that eSafety's preliminary view is that measures in this Code should require proactive detection of pro-terror materials /TVEC online by Tier 1 social media services. e Safety suggests that this can be done via resources provided by the NGOs GIFCT and Tech against Terror. This concept of TVEC (Terrorist Violent Extremist Content) does not exist in Australian law, and was not referenced in the eSafety Position Paper which refers to material that advocates the doing of a terrorist act (including terrorist manifestos). To ensure industry participants are clear on the type of materials subject to this measure, the Code uses the term pro-terror material as defined in the National Classification Scheme. The challenge of identifying pro-terror material online has been extensively discussed by the Code drafters and eSafety. It should be noted that materials potentially within the scope of this measure requires careful human moderation because such material requires highly nuanced context-based judgments to determine if it is in fact pro-terror material within the meaning of the National Classification Scheme (and not for example, used for permissible purposes such as public discussion or debate or as entertainment or satire).[19] We note that it is important that hashes are not misused in a way that could compromise human rights, for example, against vulnerable and marginalised groups (a concern of GIFCT). We also note that there are other ways pro-terror material can potentially be identified by services such as via text based searches and that in future, new tools may be developed for this purpose. The choice of tools requires careful consideration of what will work best based on how their platform operates and what sort of signals they have access to on the service in order to assess materials on the service.

[19] see for example section 9A of the Classification (Publications, Films and Computer Games Act 1995.

	Measure 10 encourages investment in approaches to counter pro-terror materials on services. We note that the availability of reliable hashes for the purpose of proactive detection of such material is currently dependent on voluntary international industry cooperation through NGOs such as the GIFCT. Our understanding is that the GIFCT does not use the approach of the National Classification Scheme to classify visual hashes on its hash sharing database but uses its own set of classifiers it has developed for material that may signal Terrorist Violent Extremist Content (TVEC) online[20]. GIFCT members share signals about TVEC they have identified on their platform so that other members can quickly identify if the same content is shared on their platform and assess it in line with their policies and terms of service, often with reference to legal requirements in a given country where the company is operating. Tools provided by GIFCT and Tech Against Terrorism may signal online imagery that would be Class1 material under the National Classification Scheme. **MCM 10:** Tier 1 social media service providers must take actions that aim to disrupt and deter end-users from using the service to create, post or disseminate CSAM and pro-terror material. At a minimum, a Tier 1 social media service must: (a) implement appropriate techniques that enable the provider to identify and monitor the nature of the threat and the areas of highest foreseeable risk on its services; and (b) implement systems, processes and/or technologies that aim to detect and remove CSAM and pro-terror material from the service. They must also invest in systems, processes and/or technologies that aim to detect, disrupt and/or deter end-users from using the service to create, post or disseminate CSAM and pro-terror materials . Examples of appropriate actions and investments are also provided. Note: this measure has been revised to focus on CSAM and pro-terror materials in response to feedback provided by eSafety in the 9 February 2023 letter on the SMS Code to industry associations. (see Appendix A, item 2)
Matter 2 Measures directed towards achieving the objective of ensuring that industry participants have scalable and effective policies, procedures, systems and technologies in place to take reasonable and proactive steps to prevent or limit: ● access or exposure to, and ● distribution of class 1B material.	**Outcome 2: Industry participants take reasonable and proactive steps to prevent or limit access or exposure to, and distribution of class 1B material.** **MCM 11:** Tier 1 and Tier 2 social media service providers must implement scalable, effective systems, processes and technologies that enable the provider to take appropriate enforcement action against end-users who are known to have breached policies concerning class 1B material. At a minimum, they must have standard operating procedures that (a) Include clear internal channels for personnel to escalate and prioritise reports of class 1B materials, (b) Provide operational guidance to personnel in relation to steps that should be taken when the service receives reports of class 1B materials by Australian end-users, including the steps that must be taken concerning the removal of materials. **MCM 12:** Tier 1 and Tier 2 social media service providers must take enforcement action against end-users who breach terms and conditions, community standards or acceptable use policies

[20] GIFCT does not define the concept of Terrorist Violent Extremist Content.

	prohibiting class 1B material that is proportionate to the level of harm associated with the relevant violation. As soon as reasonably practicable, they must: (a) Remove items of class 1B material identified on the service (b) Terminate an end-user's account in the event the end-user has repeatedly breached terms and conditions, community standards or acceptable use policies prohibiting class 1B material. Tier 1 and Tier 2 social media services should also consider implementing a strike or penalty, restriction, or suspension on an end-user account as an enforcement action for less serious breaches of terms and conditions, community standards and/or acceptable use policies prohibiting class 1B material. They should have clear, documented policy outlining the criterion that will be used when/if applying any of these measures. Note: measures 11 and 12 and accompanying guidance under this Outcome make industry best practice operating procedures for enforcement of policies enforceable for Tier 1 and Tier 2 social media services. **MCM 13:** All social media service providers must re-assess their risk profile in accordance with this Code following the introduction or implementation of a significant new feature to their social media service. They must take reasonable steps to mitigate any additional risks to Australian end-users concerning material covered by this Code that result from the new feature. **MCM 14:** Tier 1 social media service providers must make ongoing investments in tools and personnel that support the capacity of the provider to detect and take enforcement action under this Code concerning class 1B material, proportional to the incidence of class 1B materials on the service. Note: we note, in particular, that measures 13 is designed to ensure that Tier 1 and Tier 2 social media services are committed to ongoing systematic review of the design of their services to safeguard end-users' safety.
Matter 4 Measures directed towards achieving the objective of ensuring that industry participants have scalable and effective policies, procedures, systems and technologies in place to take reasonable and proactive steps to limit the hosting of class 1A material and class 1B material in Australia.	**Outcome 4: Industry participants take reasonable and proactive steps to limit hosting of class 1A and 1B material in Australia.** This outcome does not require additional measures for social media services as the measures in the Code that are designed to limit online storage of class 1A material by a social media service address the first party hosting of this material by such services.
Matter 5 Measures directed towards achieving the objective of ensuring that industry participants have effective and scalable policies and procedures in place to facilitate consultation, cooperation and collaboration with other industry	**Outcome 5: Industry participants consult, cooperate and collaborate with other industry participants in respect of the removal, disruption and/or restriction of class 1A and class 1B material.** **MCM 15:** Tier 1 social media service providers must take part in an annual forum organised or facilitated by any industry association - referred to in the Head Terms - to discuss and evaluate the effectiveness of measures implemented under this

participants in respect of the removal, disruption and/or restriction of class 1A material and class 1B material, as well as accounts associated with this material.	Code and share best practice in implementing the Code and online safety in general with other industry participants. **MCM 16:** Tier 1 social media service providers must implement procedures for collaborating with eSafety, law enforcement, non-governmental or cross industry organisations, that have established systems and processes that facilitate the safe, secure and lawful sharing of information that enables providers of social media services to detect and remove CSEM and pro-terror materials. Note: this measure is based on example measures suggested in the Position Paper (p. 70). The measures and accompanying guidance under this outcome make industry best practice operating procedures for enforcement of policies enforceable for Tier 1 and Tier 2 social media services. It is noted that the achievement of the Outcomes under this Code will require information sharing mechanisms with organisations that are tasked with combatting CSEM and pro-terror materials online. This measure requires that Tier 1 social media services have such mechanisms in place, noting that these must comply with laws such as the *Privacy Act 1988*. **(Optional) Measure 17:** Tier 1 and Tier 2 social media service providers may provide support such as funding and/or access to data for good faith research into the prevalence, impact, and appropriate responses that providers of social media services may adopt in relation to class 1A and class 1B materials and the subcategories of class 1A and class 1B materials, such as CSEM and pro terror material.
Matter 6 Measures directed towards achieving the objective of ensuring that industry participants have effective and scalable policies and procedures in place which ensure communication and cooperation with the eSafety Commissioner with respect to matters about class 1A material and class 1B material, including complaints.	**Outcome 6: Industry participants communicate and cooperate with eSafety in respect of matters relating to class 1A and class 1B material, including complaints.** **MCM 18:** Tier 1 social media service providers must refer to eSafety complaints from the public concerning the providers non-compliance with this Code, where the provider is unable to resolve the complaint within a reasonable time frame. **MCM 19:** Tier 1 social media service providers 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, and online storage of class 1A or class 1B materials by Australian end-users. Note: these measures respond to the Position Paper (see examples measures p. 70) and feedback received by eSafety in the course of developing the Code, noting that these are proactive obligations supplementary to eSafety's power to respond directly to complaints about breaches of the Codes and to issue a reporting notice or make a reporting determination for all social media service providers about their compliance with the BOSE. See also incentives on providers to engage with eSafety expectations 7, 18, 19 and 20 of the BOSE.
Matter 7 Measures directed towards achieving the objective of providing people with a range of technical tools and/or information to limit their access and exposure, and the access and exposure of children in	**Objective 2: Industry participants will empower people to manage access and exposure to class 1A and class 1B material.** **Outcome 7: Industry participants provide tools and/or information to limit access and exposure to class 1A and class 1B material.** **MCM 20:** Tier 1 and Tier 2 social media service providers that permit account holders who are young Australian children under 16 must provide clear and easily accessible information to parents

their care, to class 1A material and class 1B material.	and carers about how to manage the child's access and exposure to class 1A and class 1B material as well as information about safety tools and settings that are accessible to all ages permitted on the service. **MCM 21:** Tier 1 and Tier 2 social media service providers 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. Note: these measures respond to the Position Paper (see example measures for this outcome on p. 70) See also section 7.4 of the Head Terms, which further strengthens these requirements concerning the handling of reports. **MCM 22:** Tier 1 social media service providers must establish a location on the service dedicated to providing online safety information for Australian end-users. At a minimum, it will contain information required under measure 20, 21, 23, 24 and 25, and include information about how Australian end-users can contact third party services that may provide counselling and support. Note: this measure is designed to enhance accessibility of safety information that Tier 1 social media service providers make available to Australian end-users, including information that is required to be provided under other minimum compliance measures.
Matter 8 Measures directed towards achieving the objective of providing people with clear, easily accessible and effective: ● reporting mechanisms for class 1A material and class 1B material, as well as associated user accounts, and ● complaints mechanisms to address complaints about the handling of reports about class 1A material and class 1B material and codes compliance.	**Outcome 8: Industry participants provide clear and effective reporting and complaints mechanisms for class 1A and class 1B material.** **MCM 23:** Tier 1 and Tier 2 social media service providers must provide tools which enable Australian end-users to report, flag and/or make a complaint about class 1A and class 1B material accessible on the service. These must be easily accessible and easy to use, accompanied by clear instructions on how to use them, as well as an overview of the reporting process, and the identity of the reporter must be protected from the reported end-user or account holder. **MCM 24:** Tier 1 and Tier 2 social media service providers must provide tools which enable Australian end-users to make a complaint about: a) The provider's handling of reports about class 1A or class 1B material that is accessible on the service; or b) Any other aspect of the provider's compliance with this Code. **MCM 25:** Tier 1 social media service providers must ensure that the reporting tools referred to in measure 24 above are available and accessible to Australian end-users on-platform (i.e., they should be integrated within the functionality of the social media service in a manner that is visible and accessible). Note: these measures build upon example measures set out in the Position Paper (see p. 71). See also section 7.4 of the Head Terms, which further strengthens these requirements concerning the handling of reports.
Matter 9 Measures directed towards achieving the objective of ensuring that industry participants have scalable and effective policies,	**Outcome 9: Industry participants effectively respond to reports and complaints about class 1A and 1B material.** **MCM 26:** Tier 1 and Tier 2 social media service providers must take appropriate steps to promptly respond to Australian end-users that have made reports referred to in measure 23 or

procedures, systems and technologies in place to effectively respond to: ● reports about class 1A material and class 1B material, as well as associated user accounts, and ● complaints about the handling of reports about class 1A material and class 1B material and codes compliance.	complaints referred to in measure 24. At a minimum a provider of a Tier 1 or Tier 2 social media service must ensure that an Australian end-user who makes a report or complaint is informed in a reasonably timely manner of the outcome of the report or the complaint. **MCM 27**: Tier 1 and Tier 2 social media service providers must implement and document policies and procedures which detail how it gives effect to the requirements in measure 26. **MCM 28:** Tier 1 and Tier 2 social media service providers must ensure that personnel responding to reports are trained in the social media service's policies and procedures for dealing with reports. **MCM 29:** Tier 1 and Tier 2 social media service providers must review the effectiveness of its reporting systems and processes to ensure reports are assessed and material removed or otherwise actioned (if necessary) within reasonably expeditious timeframes, based on the level of harm the material poses to Australian end-users. Such review must occur at least annually. Note: these measures and accompanying guidance under this outcome build on example measures suggested in the Position Paper (p. 72) and make industry best practice operating procedures for establishing accessible and effective reporting mechanisms class1 materials enforceable for Tier 1 and Tier 2 social media services. Please also see section 7.4 of the Head Terms.
Matter 10 Measures directed towards achieving the objective of ensuring that industry participants publish easily accessible and plain language policies, procedures and guidelines that set out how they handle class 1A material and class 1B material. Measures directed towards achieving the objective of ensuring that industry participants provide end-users with information about the safety issues associated with class 1A material and class 1B material.	**Objective 3: Industry participants will strengthen transparency of, and accountability for, class 1A and class 1B material.** **Outcome 10: Industry participants provide clear and accessible information about class 1A and class 1B material.** **MCM 30:** Tier 1 and Tier 2 social media service providers must publish clear and easily accessible terms and conditions, community standards, and/or acceptable use policies, which make clear to Australian end-users that the broad categories of class 1A and class 1B material are prohibited on the service. **MCM 31:** Tier 1 social media service providers must publish clear and accessible information that explains the actions it takes to reduce the risk of harm to Australian end-users caused by the distribution of class 1A and class 1B material on its service. Note: these measures and accompanying guidance under this Outcome build on examples for this outcome in the Position Paper (p. 73) and make industry best practice for documenting policies concerning Class1 materials and providing transparency about the actions taken to address online harms enforceable for Tier 1 and Tier 2 social media services.
Matter 11 Measures directed towards achieving the objective of ensuring that industry participants publish annual reports about class 1A material and class 1B material, and their compliance with industry codes.	**Outcome 11: Industry participants publish annual reports about class 1A and 1B material and their compliance with this Code.** **MCM 32:** Tier 1 social media service providers must submit a Code report which as a minimum contains the following information: a) Details of the risk assessment it has carried out (if the Tier 1 provider is required to undertake a risk assessment), together with information about the risk assessment methodology adopted,

	b) The steps that the provider has taken to comply with the applicable minimum compliance measures, c) the volume of CSEM or pro-terror material removed by the provider of the social media service; d) An explanation as to why these measures are appropriate. **MCM 33:** On request by eSafety, Tier 2 social media service providers must submit to eSafety a Code report which includes the following information: a) Details of the risk assessment it has carried out pursuant to the Code, together with information about the risk assessment methodology adopted, b) The steps that the provider has taken to comply with their applicable minimum compliance measures, c) An explanation as to why these measures are appropriate. Code reports must be submitted within 2 months of a request (no earlier than 12 months after the code has come into effect). Note: these measures contain reporting obligations on Tier 1 and Tier 2 social media services that are supplementary to eSafety's power to investigate breaches of the Codes and to issue a reporting notice or make reporting determinations from all social media service providers about their compliance with the BOSE. The revised Code reduced the time frame for Tier 2 providers to respond to a request from 6 months to 2 months (see Appendix A, item 4).
Additional Matters: review of codes	Position 11 of the Position Paper outlines eSafety's expectation that the Codes will include a statement about how and when they will be reviewed. eSafety also referred to the role of industry associations in the Position Paper (see p.62, 63) These matters are addressed in section 7 of the Heads of Terms, taking into account additional feedback provided by eSafety during the Code development process.
Additional Matters: limitations in Head terms	See Appendix A, item 5.

2. Relevant Electronic Services Online Safety Code (Class 1A and Class 1B Material)

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).

Approach to risk of relevant electronic services This approach to risk in this Code has been extensively revised to address feedback provided by e Safety in its letter of 9 February (see Appendix A, item 21).

Main categories of relevant electronic services

The main categories of all providers of relevant electronic services are not required to assess their risk under this Code:

The industry defines relevant electronic services as including the following main categories:

- pre-assessed relevant electronic service meaning:

    - a closed communication relevant electronic service;
    - a dating service;
    - an encrypted relevant electronic service;
    - a gaming service with communications functionality; or
    - an open communication relevant electronic service.
- an enterprise relevant electronic service; or
- a gaming service with limited communications functionality[21].

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[22].

Such services 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 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 the suggestions made by eSafety in the Position Paper for assessing risk. Similar changes were made to the approach to assessment of risk adapted for social media services to respond to eSafety's letter of 9 February concerning this Code (see Appendix A, item 21). It is difficult to prescribe a definitive methodology for the assessment of risk for indeterminate service categories. The risk methodology set out in the table to this Code in Clause 6 is, therefore, provided as guidance to providers of relevant electronic services.

The Code now also contains a requirement concerning risk assessment in Clause 5.3(a) that make it mandatory for a provider to assign a higher risk profile to a service, should a risk assessment indicate that the assessed service may be in-between risk tiers.

Approach to measures

General

This Code codifies industry best practices that provide safeguards for the community in respect of the matters set out in the section 141 notice. The Code applies these safeguards to a much broader range of relevant electronic services (including future and developing relevant electronic services) than the existing range of relevant electronic service providers that currently adopt best industry practices in respect of those matters. Both the scope and the substance of the measures provide greater safeguards to Australians concerning harmful online material than comparable industry codes such as the *UK interim code of practice on online child sexual exploitation and abuse and the Interim code of practice on terrorist content and activity onlin*e.

We note that the Position Paper proposed an approach to risk assessment under which medium risk industry participants would be able to set their own compliance measures based on their risk profile. However, the definition of relevant electronic services captures a broad range of services with diverse functionalities, purposes, and scale, as well as indeterminate future services specified by legislative rules. This, combined with the need to take into account considerations of user privacy on many of these services and compliance with other legislative requirements, necessitated an approach which combined specific measures for certain service categories but provided flexibility for future categories of services to perform a risk assessment in order to determine if they have a Tier 1, Tier 2 or tier 3 risk status. This Code, therefore, contains specific measures for specific service categories and for services that have a Tier 1 and Tier 2 risk status.

[21] This covers services that fall within section 13A(a) to (f), OSA

[22] Section 13A(g), OSA.

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

This Code provides an explanation of the role of relevant electronic services within the digital ecosystem to provide context for the approach to measures. Clause 4(c) explains:

> *"The variety of relevant electronic services within the scope of this Code have varying capabilities to assess the materials contained in end-user communications. The types of measures that may be possible and/or appropriate for one type of relevant electronic service, will not be appropriate for others. For example, providers of an SMS or email service may not be able to (re)view and/or assess and, therefore, determine whether materials communicated by end-users are class 1A or class 1B materials or be capable of removing such materials from the service. Consequently, the measures in this Code have been designed to take into account the differences between the purpose, functionality and user-base of each type of service; and the need for flexibility in the implementation."*

In the light of this context, the structure of this Code has been revised to take into account the different capacity of services to assess, review, and remove materials. We note that this approach is consonant with the regulatory context of these Codes: the OSA does not penalise services that are not capable of removing material to do so, where eSafety issues a removal notice.[23] 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."*

A new clause 5.2 has been added that requires a provider of a pre-assessed relevant electronic service or a Tier 1 or Tier 2 relevant electronic service to, at eSafety's request, notify eSafety if it is capable of reviewing and assessing material or capable of removing material, or not capable of doing so. See Appendix A, item 21.

Matter 1 Measures directed towards achieving the objective of ensuring that industry participants have scalable and effective policies, procedures, systems and technologies in place to take reasonable and proactive steps to **detect and** prevent: ● access or exposure to, ● distribution of, and ● online storage of class 1A material.	**Objective 1: Industry participants will take reasonable and proactive steps to create and maintain a safe online environment for Australian end-users.** **Outcome 1: Industry participants take reasonable and proactive steps to prevent access or exposure to, distribution of, and online storage of class 1A material.** **Note: Outcome 1 does not refer to the detection of class 1A material as an entire class, noting that there are no systems and processes that can be reliably deployed to detect the range of real or simulated extreme crime and violence materials that fall within class 1A. Instead, this Code includes measures that require the detection of specific categories of class1 materials by very large Tier 1 relevant electronic services i.e., CSAM and certain pro-terror materials: videos and imagery that depict and promote terrorist acts.** **MCM 1:** Enterprise-relevant electronic service providers must have an agreement in place with the enterprise customer, requiring the enterprise customer to ensure the service is not used to distribute illegal materials, and to take appropriate action to enforce breaches of that agreement by the enterprise customer. Note: this measure is the primary obligation of enterprise service providers. As explained in the guidance, these providers of enterprise-relevant electronic services do not have the technical, legal, or practical

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

	ability to exercise control over materials distributed by the enterprise customers' end-users and do not have an effective ability to engage with the enterprise customers' end-users. Instead, providers of enterprise relevant electronic services have a relationship with enterprise customers, who themselves have relationships with their end-users. Accordingly, the types of measures that can be taken by providers of enterprise relevant electronic services to limit the use of their services are primarily contractual. **MCM 2:**,pre-assessed relevant electronic services, Tier 1 or Tier 2 relevant electronic services, gaming service with limited communications functionality providers must notify appropriate entities – as defined in the Code - about CSEM and pro terror class 1A material on their services, if they identify this material and form a good faith belief that the CSEM or pro terror material is evidence of serious and immediate threat to the life or physical health or safety of an adult or child in Australia. This must be done within 24 hours, or as soon as reasonably practicable. Note: this measure is supplementary to existing obligations that may be imposed on relevant electronic services under State or Territory or foreign laws. The disclosure of class 1A material may involve the disclosure of personal information that identifies an individual and will be subject to the *Privacy Act 1988*. This obligation has been drafted to comply with the requirements of that Act concerning such disclosure. See section 16A(1), item 1 of the *Privacy Act 1988*. It is based on the example measure for this outcome in the Position Paper (p. 68). See revisions to guidance that make clear that referral of materials under this measure to appropriate authorities is time critical and should be actioned without delay. **MCM 3**: Pre-assessed relevant electronic services and Tier 1 and Tier 2 relevant electronic service providers must implement systems, processes and technologies that enable the provider to take appropriate enforcement action against end-users who breach terms and conditions, community standards and/or acceptable use policies relating to Class 1A materials. A provider of a pre-assessed relevant electronic service or a Tier 1 or Tier 2 relevant electronic service that is capable of reviewing and assessing materials and removing materials must at a minimum, have standard systems and processes that: (a) enable the review by the provider of reports by Australian end-users of Class 1A materials, (b) enable the prioritisation and, where necessary, escalation of reports of Class 1A materials by Australian end-users. Note: this measure makes best practice operating procedures for enforcement of policies enforceable for Tier 1 and Tier 2 relevant electronic services. We note that this measure has been revised to cover 'extreme crime and violence material' which is not per se illegal under Australian law (See Appendix A, item10). **MCM3**: To the extent providers a pre-assessed relevant electronic service or a Tier 1 or Tier 2 relevant electronic service are not capable of either reviewing and assessing materials or removing material they must have standard operating procedures that: (i) Refer Australian reporters of Class 1A materials to eSafety resources, or (ii) Enable the provider to take appropriate action in response to breaches of terms and conditions, community standards, and/or acceptable use policies relating to Class 1A materials

	Note: this more limited measure was considered appropriate for providers that cannot assess/review relevant content in order to determine whether materials reported to them are in fact class 1A material.. **MCM 4:** To the extent that providers of a pre-assessed relevant electronic service or a Tier 1 or Tier 2 relevant electronic service that is capable of reviewing and assessing material they must implement appropriate systems and processes that enable the provider to take appropriate action in response to breaches of terms and conditions, community standards, and/or acceptable use policies relating to class 1A materials. A provider that is subject to this measure must: a) where capable of removing materials, remove instances of Class 1A materials identified by the provider on the service within 24 hours or as soon as reasonably practicable, unless otherwise required to deal with such material by law enforcement; b) take appropriate steps designed to deter an end-user who has violated breached the relevant terms and conditions, community standards and/or acceptable use policies regarding class 1A materials from additional breaches of these specific policies and standards. Appropriate steps may include (depending on the service and material in question): i) issuing warnings to account holders; ii) restricting the end-user's use of their account (e.g., preventing the end user from being able to send material using the service); iii) suspending the end-user's account for a defined period; iv) terminating the end-user's account; and/or v) taking reasonable steps to prevent end-users who repeatedly breach terms and conditions, community standards and/or acceptable use policies regarding class 1A material who have had their user account terminated from creating a new account. Note: measure has been revised in response to eSafety feedback (See Appendix A, item 9). **MCM 5:** providers of a Tier 1 or Tier 2 relevant electronic service; dating service; an open-communications relevant electronic service; an encrypted relevant electronic service or a gaming service with communications functionality must ensure that they are resourced with reasonably adequate personnel to oversee the safety of the service. Such personnel must have clearly defined roles and responsibilities, including for the operationalisation and evaluation of their systems and processes required under this Code. Note: this measure addresses the need for human resources that have specific safety responsibilities, which was reinforced by feedback from the public consultation process. **MCM 6:** providers of Tier 1 or Tier 2 relevant electronic services; dating services, open communication relevant electronic services;; encrypted relevant electronic services, or gaming services with communications functionality, must evaluate the types of features and settings they could adopt to minimise risks to Australian end-users related to class 1A material adopt the most appropriate features and/or settings for the type of service offered. At a minimum providers of Tier 1 relevant electronic services, open communications relevant electronic services and gaming services with communications functionality must have the following:

	If the service allows the sending of messages, the service must have settings that allow users to block messages from other users; If the service allows for the display of a user's online status, the service must have tools and settings that enable end-users to be hidden or to appear offline; If the relevant electronic service allows the creation of accounts by a young Australian child, provide settings that are designed to prevent children from unwanted contact from strangers, including settings which: (i) make accounts of a young Australian child private by default; and (ii) prevent the location of a young Australian child using the service being shared with any accounts other than accounts approved by the young Australian child or their parent or guardian. At a minimum a provider of a dating service must: a) have settings that allow users to block messages from another user from interacting with the user; b) require an end-user to register for the service before uploading content or using the communication features, and during the registration process, collect and retain a phone number, email address, social media account or other identifier; and c) take reasonable steps to prevent the creation of accounts by a child under 18. Note: these measures make best practice registration requirements and safety settings for Australian end-users enforceable for different categories of services, based on the varying purposes and capabilities of the relevant electronic services. Note that the industry has sought not to pre-empt the outcome of other policy processes concerning protection of children online that are currently underway including eSafety's Age Verification Roadmap and the review of the *Privacy Act 1988*. At a minimum a provider of a closed communication relevant electronic service; or an encrypted relevant electronic service, must require a user to register for the service using a phone number, email address or other identifier. **MCM 7:** Safety by design assessments are required in certain circumstances including where a services category under the Code may change. **MCM 8:** A provider of a Tier 1 relevant electronic service an open communication relevant electronic service that is not a carriage service provider; a dating service; or a gaming service with communications functionality to the extent that it is capable of reviewing and assessing material on the service and removing material from the service will implement systems, processes and/or technologies designed to detect, flag and/or remove instances of known CSAM from that service, for example, through the use of hashing technologies, machine learning, or artificial intelligence that scans for known CSAM and/or other safety technologies, systems and/or processes designed to detect key words or behavioural signals associated with the distribution of CSAM.

	This minimum measure does not apply to carriage service providers to the extent that they provide relevant electronic services via carriage services. Note: this provision addresses the matter of proactive detection of known CSAM and is based on the example measure suggested for this outcome in the Position Paper (p. 68). This measure has been broadened in response to eSafety feedback (See Appendix A, item 9). In contrast to proposed regulations in the EU, the measure is not limited by any requirement that eSafety issue a proactive detection notice of limited duration and applies to a category of providers (rather than individually named providers). The measure may be satisfied by either systems and processes to detect known CSAM or behavioural signals/key words associated with the distribution of CSAM. **MCM 9.**Providers of a Tier 1 relevant electronic service or an open communication relevant electronic service, to the extent capable of reviewing and assessing material on the service and removing material from the service will implement systems, processes and/or technologies designed to detect, flag and/or remove instances of known pro-terror materials from the service, for example, through the use of hashing, machine learning, or artificial intelligence or that scans for known pro-terror material and/or systems and processes that limits users' ability to publicly post such content on their service. This minimum measure does not apply to carriage service providers to the extent that they provide relevant electronic services via carriage services. Note: this measure is based on the example measure suggested for this outcome in the Position Paper (p. 68). It should be noted that, all material that is potentially in scope of this measure requires careful human moderation because it requires context-based judgments to determine whether it is in fact Class 1A material and not for example material that is permissible in the context of public debate. We also note that hashes of this material depend on international industry cooperation through NGOs, such as GIFCT, that are concerned to ensure that hashes are not misused in a way that could compromise human rights, for example, against vulnerable and marginalised groups. We note the effectiveness of this measure and whether it should be supported by requirements for appeals against enforcement action will be considered as part of the Code review process (see Additional Matters). **MCM 10:** Providers of Tier 1 relevant electronic services, dating services, open communication electronic services, closed communication relevant electronic services and encrypted relevant electronic services must take action to disrupt and deter CSAM and pro-terror material and must invest in systems, processes and /or technologies and/or personnel that aim to disrupt or deter CSEM and pro-terror material. This minimum measure does not apply to carriage service providers to the extent that they provide relevant electronic services via carriage services. Note: this measure extends to new generation CSAM and pro-terror material and focuses both on action and investment on the prevention of material on these services, based on input from eSafety.
Matter 2 Measures directed towards achieving the objective of ensuring that industry participants have scalable and effective policies, procedures, systems and technologies in place to take	**Outcome 2: Industry participants take reasonable and proactive steps to prevent or limit access or exposure to, and distribution of class 1B material.** **MCM 11:** providers of a Tier 1 and Tier 2 relevant electronic service and pre-assessed relevant electronic service to the extent they are capable of reviewing and assessing materials must implement appropriate systems and processes that enable the

reasonable and proactive steps to prevent or limit: ● access or exposure to, and ● distribution of class 1B material.	provider to take appropriate action for violations of terms and conditions, community standards, and/or acceptable use policies in relation to class 1B material. Providers of a Tier 1 and Tier 2 relevant electronic services and pre-assessed relevant electronic services to the extent they are not capable of reviewing and assessing class 1B materials from the service must have standard operating procedures that either: a) Refer Australian reporters of class 1B materials to eSafety resources, or b) Enable the provider to take appropriate action for violations of terms and conditions, community standards, and/or acceptable use policies in relation to class 1B material. **MCM 12:** providers of Tier 1 and Tier 2 relevant electronic service and pre-assessed relevant electronic service to the extent they are capable of reviewing and assessing materials must take appropriate action in response to breaches of terms and conditions, community standards, and/or acceptable use policies that is reasonably proportionate to the level of harm associated with the relevant breach. Examples of appropriate steps include (depending on the service and material in question): a) where the provider is capable of removal of material, removal of the relevant material; b) issuing warnings to account holders; c) restricting the end-user's use of their account (e.g., preventing the end-user from being able to send material using the service); d) suspending the user's account for a defined period; e) terminating the user's account; and/or f) taking reasonable steps to prevent end-users that repeatedly breach terms and conditions, community standards and/or acceptable use policies who have had their user account terminated from creating a new account. Note: this measure builds on the example measures outlined in the Position Paper by requiring proportionate enforcement action against users that breach terms of service etc.
Matter 4 Measures directed towards achieving the objective of ensuring that industry participants have scalable and effective policies, procedures, systems and technologies in place to take reasonable and proactive steps to limit the hosting of class 1A material and class 1B material in Australia.	**Outcome 4: Industry participants take reasonable and proactive steps to limit hosting of class 1A and 1B material in Australia.** This outcome does not require additional measures for relevant electronic services (see preamble to Heads of Terms).
Matter 5 Measures directed towards achieving the objective of ensuring that industry participants have effective and scalable policies and procedures in place to facilitate consultation, cooperation and collaboration with other industry participants in respect of the removal, disruption and/or	**Objective 1: Industry participants will take reasonable and proactive steps to create and maintain a safe online environment for Australian end-users.** **Outcome 5: Industry participants consult, cooperate and collaborate with other industry participants in respect of the removal, disruption and/or restriction of class 1A and class 1B material.** **MCM 15:** providers of a Tier 1 relevant electronic service or a pre-assessed relevant electronic service with more than 1 million monthly active accountholders (or more than 1 million active services in operation (SIO) for closed communication relevant

restriction of class 1A material and class 1B material, as well as accounts associated with this material.	electronic services that are also carriage service providers) in Australia must take part in an annual forum organised or facilitated by any industry association referred to in the Head Terms, to discuss and evaluate the effectiveness of measures implemented under this Code and share best practice in implementing the Code and online safety in general with other industry participants. **(Optional) Measure 16:** a relevant electronic service provider may provide support such as funding and /or access to data for good faith research into the prevalence, impact and appropriate responses that providers of relevant electronic services may adopt in relation to class 1A and class 1B materials and the subcategories of class 1A and class 1B materials such as CSEM, and pro-terror material. Note: given the breadth of this industry section, and the highly competitive nature of their services, we consider that a forum facilitated by industry associations is an effective way to encourage collaboration amongst participants in an open and transparent way, noting that many participants voluntarily contribute to best practice initiatives that are appropriate to their service category such as the work of the Digital Trust & Safety Partnership 'Safe Framework'.
Matter 6 Measures directed towards achieving the objective of ensuring that industry participants have effective and scalable policies and procedures in place which ensure communication and cooperation with the eSafety Commissioner with respect to matters about class 1A material and class 1B material, including complaints.	**Outcome 6: Industry participants communicate and cooperate with eSafety in respect of matters relating to class 1A and class 1B material, including complaints.** **MCM 17:** Tier 1 and encrypted relevant electronic services and open communications relevant electronic service providers must share information with eSafety about significant new features or functions released by the provider of the relevant electronic service that the provider reasonably considers are likely to have a significant effect on the access or exposure to, distribution of, and online storage of class 1A or class 1B materials in the reports it provides in accordance with measure 26. Note: these measures respond to the Position Paper (see examples measures p. 70) and feedback received by eSafety in the course of developing the Code, noting that these are proactive obligations supplementary to the eSafety's power to respond directly to complaints about breaches of the Codes and to issue a reporting notice or make reporting determinations for all relevant electronic service providers about their compliance with the BOSE. See also incentives on providers to engage with eSafety expectations 7, 18, 19 and 20 of the BOSE. See also Appendix A, item A, regarding eSafety feedback on previous stipulation concerning the confidentiality of information provided (now removed).
Matter 7 Measures directed towards achieving the objective of providing people with a range of technical tools and/or information to limit their access and exposure, and the access and exposure of children in their care, to class 1A material and class 1B material.	**Objective 2: Industry participants will empower people to manage access and exposure to class 1A and class 1B material.** **Outcome 7: Industry participants provide tools and/or information to limit access and exposure to class 1A and class 1B material.** **MCM 18:** Providers of Tier 1, Tier 2 relevant electronic service and pre-assessed relevant electronic service must publish clear information that is accessible to Australian end-users regarding the role and functions of eSafety, including how to make a complaint to eSafety, and information about the mechanisms described in measure 19.

	Note: this responds to the Position Paper (see example measures for this outcome on p. 70) See also section 7.4 of the Head Terms, which further strengthens these requirements concerning the handling of reports.
Matter 8 Measures directed towards achieving the objective of providing people with clear, easily accessible and effective: ● reporting mechanisms for class 1A material and class 1B material, as well as associated user accounts, and ● complaints mechanisms to address complaints about the handling of reports about class 1A material and class 1B material and codes compliance.	**Outcome 8: Industry participants provide clear and effective reporting and complaints mechanisms for class 1A and class 1B material.** **MCM 19**: Providers of Tier 1 and Tier 2 relevant electronic service and pre-assessed relevant electronic services that are capable of removing materials must provide a tool, mechanism or other process which enables Australian end-users to report, flag and/or make a complaint about material accessible on the service that breaches the provider's terms and conditions, community standards, and/or acceptable use policies. These must be easily accessible and easy to use, accompanied by clear instructions on how to use them, as well as an overview of the reporting process, and the identity of the reporter must be protected from the reported end-user or account holder. Providers of a Tier 1 or Tier 2 relevant electronic service or a pre-assessed relevant electronic service that is not capable of reviewing and assessing materials must: i. Provide tools, mechanisms or other processes that assist Australian end- users to report, flag or make complaints about materials that breach a service's terms and conditions, community standards, and/or acceptable use policies, ii. Make available, via its website, a link to eSafety's online content reporting form, and iii. Respond promptly to complaints about class 1A or class 1B material made by Australian end-users by either a. responding to the complaint, or b. referring the complainant to eSafety. **MCM 20:** providers of a Tier 1, Tier 2, relevant electronic service a pre-assessed relevant electronic service must provide a tool, mechanism or other process which enable Australian end- users to make a complaint about the provider's compliance with this Code. Note: these measures build upon example measures set out in the Position Paper (see p. 71). See also section 7.4 of the Head Terms, which further strengthens these requirements concerning the handling of reports.
Matter 9 Measures directed towards achieving the objective of ensuring that industry participants have scalable and effective policies, procedures, systems and technologies in place to effectively respond to: ● reports about class 1A material and class 1B material, as well as associated user accounts, and ● complaints about the handling of reports about class 1A	**Outcome 9: Industry participants effectively respond to reports and complaints about class 1A and 1B material.** **MCM 21:** providers of Tier 1 and Tier 2 relevant electronic service a pre-assessed relevant electronic services that are capable of reviewing and assessing material must: a) Take appropriate steps to promptly respond to reports of material that violates the provider's terms and conditions, community standards, and/or acceptable use policies made by Australian end-users, b) Implement and document policies and procedures which detail how it gives effect to the requirement in (a), and c) Ensure that personnel responding to reports are trained in the relevant electronic service's policies and procedures for dealing with reports. Note: these measures build upon example measures set out in the Position Paper (see p. 73). See also section 7.4 of the Head Terms,

material and class 1B material and codes compliance.	which further strengthens these requirements concerning the handling of reports and complaints.
Matter 10 Measures directed towards achieving the objective of ensuring that industry participants publish easily accessible and plain language policies, procedures and guidelines that set out how they handle class 1A material and class 1B material. Measures directed towards achieving the objective of ensuring that industry participants provide end-users with information about the safety issues associated with class 1A material and class 1B material.	**Objective 3: Industry participants will strengthen transparency of, and accountability for, class 1A and class 1B material.** **Outcome 10: Industry participants provide clear and accessible information about class 1A and class 1B material.** **MCM 22:** providers of pre-assessed relevant electronic services, Tier 1 ,Tier 2 relevant electronic services, must publish appropriate terms and conditions, community standards, and/or acceptable use policies, regarding content, which is not acceptable on the service, having regard to the nature of the service. Such terms and conditions, community standards and/or acceptable use policies must make clear that the broad categories of material within class 1A material are prohibited on the service and the extent to which broad categories of materials within class 1B materials are either prohibited or restricted on the service. **(Optional) Measure 23:** relevant electronic services providers may run online safety awareness-raising campaigns for Australian end-users and for public or specific sections of the community such as teachers, parents and carers, older users or vulnerable groups, including in partnerships with eSafety, non-government organisations or others. **MCM 24:** providers of a Tier 1 relevant electronic service, an open communication relevant electronic service, or dating services will establish a dedicated section of the service to house online safety information, such as a safety centre that is accessible to Australian end-users that meets minimum requirements concerning information about safety settings and how end-users can make reports and complaints etc. **MCM 25:** a provider of a Tier 1 or Tier 2 relevant electronic service providers, a dating service, an open communication relevant electronic service; or a gaming service with communications functionality, must publish easily accessible and understandable information that explains the tools and settings they make available under minimum compliance measure 6 (Safety by design). Note: these measures and accompanying guidance under this outcome build on examples for this outcome in the Position Paper (p. 73) and make industry best practice for documenting policies concerning class1 materials and explaining the use of safety by design tools and settings.
Matter 11 Measures directed towards achieving the objective of ensuring that industry participants publish annual reports about class 1A material and class 1B material, and their compliance with industry codes.	**Outcome 11: Industry participants publish annual reports about class 1A and 1B material and their compliance with this Code.** **MCM 26:** a provider of a Tier 1 relevant electronic service or an open communication relevant electronic service must submit a Code report which as a minimum contains the following information: a) Details of the risk assessment it has carried out (if the provider is required to undertake a risk assessment is required under the Code) and information about the risk assessment methodology adopted; b) The steps that the provider has taken to comply with the applicable minimum compliance measures;

	c) the volume of CSEM or pro terror material removed by the provider of the relevant electronic service; and d) An explanation as to why these measures are appropriate. **MCM 27:** On request by eSafety, a provider of a Tier 2 relevant electronic service must submit to eSafety a Code report which includes the following information: a) details of the risk assessment it has carried out if the provider is required to undertake a risk assessment is required under the Code) together with information about the risk assessment methodology adopted; b) the steps that the provider has taken to comply with their applicable minimum compliance measures; c) an explanation as to why these measures are appropriate. **MCM 28:** On request by eSafety, providers of a closed communication and encrypted relevant electronic service, dating services or a gaming service with communications functionality 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. **MCM 31:** On request by eSafety, enterprise relevant electronic service providers must confirm in writing to eSafety that the provider is compliant with MCM 1. Note: these measures contain reporting obligations on Tier 1 and Tier 2 relevant electronic services and compliance confirmation requirements on enterprise relevant electronic services that are supplementary to eSafety's power to investigate breaches of the Codes and to issue a reporting notice or make reporting determinations from all relevant electronic service providers about their compliance with the BOSE. Changes have been made to reduce the response time for reports on request to 2 months after receiving the request, but for the first request no earlier than 12 months after this Code comes into effect. New guidance has also been added about how providers should explain the appropriateness of measures in light of their capability to remove, review and assess materials.
Additional Matters: review of Codes	Position 11 of the Position Paper outlines eSafety's expectation that the Codes will include a statement about how and when they will be reviewed. eSafety also made reference to the role of industry associations in the Position Paper (see p. 62, 63) These matters are addressed in section 7 of the Head Terms, taking into account additional feedback provided by eSafety during the Code development process.
Additional Matters: limitations in Head terms	See Appendix A, item 5.

3. Designated Internet Services Online Safety Code (Class 1A and Class 1B Material)

Code structure

This Code comprises the Head Terms and Schedule 3, covering designated internet services as defined in the OSA. Importantly, the Code also includes safeguards for end-user-managed hosting services. Clause 1 acknowledges the breadth of services that 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. It is also noted that 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, (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.[24]

As a result, the approach of this Code has sought to address these differences and uncertainties.

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 the 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;
- a requirement concerning risk assessment in that makes it mandatory for a provider to assign a higher risk profile to a service, should a risk assessment indicate that the assessed service may be in-between risk tiers.
- operating systems which are dealt with under the Equipment Code (please refer to the Equipment Code for further detail);
- general purpose websites that meet criteria relating to their purpose and functionality, which are automatically accorded Tier 3 status. This limits the compliance burden on a vast range of low-risk services that support commerce, public purposes such as health and support services. A website or app that does not meet this criterion, such as a wiki or news service that allows user-generated commentary would be required to do a risk assessment and determine its risk profile as either Tier 1, 2 or 3;
- classified designated internet services that meet criteria relating to their purpose, the materials they provide and functionality. 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; and
- high impact designated internet services which are automatically accorded a Tier 1 risk profile, e.g., pornography sites or ‘gore’ or ‘shock’ sites[25] that allow end-users to post high impact sexually explicit and/or graphically violent materials.

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. This Code also contains specific measures for end-user-managed hosted services such as consumer file storage services (e.g., Dropbox, Google Drive) and enterprise designated internet services, for example, sites designed for ordering commercial supplies by enterprises etc. Both the scope and the substance of the measures provide greater safeguards to Australians concerning harmful online material than comparable industry

[24] section 14, OSA.

[25] i.e., that contain graphically violent high impact materials.

codes such as the *UK interim code of practice on online child sexual exploitation and abuse and the Interim code of practice on terrorist content and activity online*.

Matter 1 Measures directed towards achieving the objective of ensuring that industry participants have scalable and effective policies, procedures, systems and technologies in place to take reasonable and proactive steps to **detect and** prevent: ● access or exposure to, ● distribution of, and ● online storage of class 1A material.	**Objective 1: Industry participants will take reasonable and proactive steps to create and maintain a safe online environment for Australian end-users.** **Outcome 1: Industry participants take reasonable and proactive steps to prevent access or exposure to, distribution of, and online storage of class 1A material.** **Note: Outcome 1 does not refer to the detection of class 1A material as an entire class, noting that there are no systems and processes that can be reliably deployed to detect the range of real or simulated extreme crime and violence materials that fall within class 1A. Instead, the codes include measures that require the detection of CSAM by Tier 1 designated internet services.** **MCM 1:** Providers of an enterprise designated internet service must: a) have an agreement in place with the enterprise customer requiring the enterprise customer to ensure the service is not used to distribute illegal materials; and b) take appropriate action to enforce breaches of that agreement by the enterprise customer. Note: this measure is the primary obligation of enterprise designated internet service providers. As explained in the guidance, these providers of enterprise designated internet services do not have the technical, legal or practical ability to exercise control over materials distributed by the enterprise customers' end-users and do not have an effective ability to engage with the enterprise customers' end-users. Instead, providers of enterprise designated internet services have a relationship with enterprise customers, who themselves have relationships with their end-users. Accordingly, the types of measures that can be taken by providers of enterprise designated internet services to limit the use of their services are primarily contractual. **MCM 2**: Tier 1 designated internet services must notify appropriate entities – as defined in the Code - about CSEM and/or pro terror class 1A material on their services, if they identify this material and form a good faith belief that the CSEM or pro terror material is evidence of serious and immediate threat to the life or physical health or safety of an adult or child in Australia. This must be done within 24 hours or as soon as reasonably practicable. Note: this measure is supplementary to existing obligations that may be imposed on designated internet services under State or Territory or foreign laws. The disclosure of class 1A material may involve the disclosure of personal information that identifies an individual and will be subject to the *Privacy Act 1988*. This obligation has been drafted to comply with the requirements of that Act concerning such disclosure. See section 16A(1), item 1 of the *Privacy Act 1988*. **MCM 3:** Tier 1 and Tier 2 designated internet service providers and end-user-managed hosting services must implement systems, processes and technologies that enable the provider to take appropriate enforcement action for breaches of terms and conditions, community standards and/or acceptable use policies, prohibiting CSEM and pro-terror material. At a minimum, a Tier 1 designated internet service provider must: a) Remove instances of CSEM and pro-terror materials identified by the provider on the service as soon as reasonably practicable unless otherwise required to deal

	with unlawful CSEM and pro-terror materials by law enforcement. b) Terminate an Australian end-user’s account as soon as reasonably practicable in the event the Australian end-user is: a. distributing CSEM or pro-terror materials to Australian end-users with the intention to cause harm, b. known to be an Australian child, or c. has repeatedly violated terms and conditions, community standards and/or acceptable use policies prohibiting CSEM and pro-terror materials on the service, and c) Take reasonable steps to prevent end-users that repeatedly breach terms and conditions, community standards and/or acceptable use policies prohibiting CSEM and pro-terror material who have had their user account terminated from creating a new account. In the case of providers of <u>end-user-managed hosting services,</u> having standard operating procedures that: i. require the provider to engage with reports of CSEM or pro-terror material received from Australian end-users to help determine whether terms and conditions, community standards and/or acceptable use policies prohibiting CSEM and pro-terror materials on the service have potentially been breached; ii. either, where the provider is not capable of assessing of reviewing and assessing materials, refer Australian end-users who are reporters of CSEM or pro-terror materials to eSafety resources; or where the provider is capable of assessing materials enable the provider to take appropriate action in response to determine and respond to breaches of terms and conditions, community standards, and/or acceptable use policies prohibiting CSEM and pro-terror materials, Examples of appropriate action for a <u>Tier 2 designated internet service</u> include: a) removing instances of CSEM and pro-terror materials identified by the provider on the service as soon as reasonably practicable unless otherwise required to deal with unlawful CSEM and pro-terror materials by law enforcement; b) taking appropriate enforcement action against those who breach terms and conditions, community standards, and/or acceptable use policies prohibiting CSEM and pro-terror material that is reasonably proportionate to the level of harm associated with the relevant breach. Appropriate steps may include: i) issuing warnings to end-users; ii) restricting the end-user's use of the service (e.g., where possible, blocking the end-user from being able to post material using the service); iii) suspending the end-user's account for a defined period; iv) terminating the end-user's account; or

	v) taking reasonable steps to prevent end-users that repeatedly breach terms and conditions, community standards and/or acceptable use policies prohibiting CSEM and pro-terror material who have had their user account terminated from creating a new account. Note: This measure has been updated to respond to the letter by eSafety to industry associations concerning this Code dated 9 February 2023. See Appendix A, item 26. **MCM 4:** providers of a Tier 1 and Tier 2 designated internet service and end-user-managed hosting service must implement appropriate systems and processes that enable the provider to take appropriate action for breaches of terms and conditions, community standards, and/or acceptable use policies, prohibiting class 1A materials (other than CSEM and pro-terror materials). In the case of Tier 1 or Tier 2 designated internet services having processes that: i) include clearly specified internal channels for escalating and prioritising reports of class 1A material (other than CSEM and pro-terror materials) to the designated internet service; and ii) provide operational guidance to personnel as to steps that must be taken within specified time frames to deal with class 1A materials that breach the service provider's policies; In the case of end-user-managed hosting services, having standard operating procedures that: i) require the provider to engage with reports of class 1A material (other than CSEM and pro-terror materials) received from Australian end-users to help determine whether terms and conditions, community standards and/or acceptable use policies relating to Class1A materials (other than CSEM and pro-terror materials) on the service breached; and ii) either, where the provider: a) is not capable of assessing of reviewing and assessing materials, refer Australian reporters of class 1A materials (other than CSEM and pro-terror materials) to eSafety resources; or b) is capable of reviewing and assessing materials, require the provider to take appropriate action to determine and respond to breaches of terms and conditions, community standards, and/or acceptable use policies prohibiting class 1A materials (other than CSEM and pro-terror materials). Note: measures 3 and 4 make best practice operating procedures and policies enforceable for Tier 1 and Tier 2 designated internet services and end-user-managed hosting services. It is noted that these do not deal with restrictions on children accessing Tier 1 designated internet services, noting that the industry has sought not to pre-empt the outcome of other policy processes concerning protection of children online that are currently underway including eSafety's Age Verification Roadmap and the review of the *Privacy Act 1988*. This measure has been updated to

respond to the letter by eSafety to industry associations concerning this Code dated 9 February 2023. See Appendix A, item 26.

MCM 5: A provider of a Tier 1 or Tier 2 designated internet service or an end-user-managed hosting service must take appropriate action in response to a breach of the relevant terms and conditions, community standards, and/or acceptable use policies relating to Class 1A material that is reasonably proportionate to the level of harm associated with the relevant breach.

Note: added in response to eSafety feedback in letters of 9 February concerning this Code See Appendix A, item 26

MCM 6: Tier 1 and Tier 2 designated internet service or end-user-managed hosting service providers must ensure they are resourced with reasonably adequate personnel to oversee the safety of the service.

Note: this measure addresses the need for human resources that have specific safety responsibilities, which was reinforced by feedback from the public consultation process.

MCM 7: Tier 2 and Tier 3 designated internet service or end-user-managed hosting service providers must re-assess their risk profile in accordance with this Code following the introduction or implementation of a significant new feature to their service. They must take reasonable steps to mitigate any additional risks to Australian end-users concerning material covered by this Code that result from the new feature.

Note: this measure is designed to ensure that designated internet services are committed to ongoing systematic review of the design of their services to safeguard end-users' safety. See also clause 4.4.

MCM 8: Tier 1 designated internet service providers must implement systems, processes and technologies designed to detect, flag and/or remove from the service, instances of known CSAM for example, using hashing, machine learning, artificial intelligence or other safety technologies. At a minimum, these providers must ensure their services use tools and technology that:

a) Automatically detect and flag known CSAM such as hash-matching technologies (for example, PhotoDNA, CSAI Match, and equivalent technology),

b) Prevent end-users from distributing known CSAM (for example, by 'black- holing' known URLs for such material or blocking or removing such material or preventing users from publicly posting detected material (prior to moderation); and

c) Identify phrases or words commonly linked to CSEM and linked activity to enable the provider to deter and reduce the incidence of such material and linked activity.

Note: this provision addresses the matter of proactive detection of known CSAM and is based on the example measure suggested for this outcome in the Position Paper (p. 68). This measure applies to Tier 1 designated internet services for so long as the Code is in force and is being proposed by industry in advance of regulations requiring proactive detection of CSAM in the UK and EU. In contrast to proposed regulations in the EU, the measure is not limited by any requirement that eSafety issue a proactive detection notice of limited duration and applies to a category of providers (rather than individually named providers). We think that the outcomes-based approach of the Codes combined with the BOSE

	appropriately incentivises capable designated internet services to deploy these systems, processes, and technologies where reasonable. **MCM 9:** Tier 1 designated internet service providers must make ongoing take action and invest in systems, processes and/or technologies that aim to disrupt and/or deter end-users from using the service to create, post or disseminate CSAM and/or pro-terror material proportionate to the risk of these types of material being accessible to Australian end-users on the service. Note: this measure responds to feedback from eSafety about the need for Tier 1 DIS to take action against and invest in combatting CSAM and pro-terror material.
Matter 2 Measures directed towards achieving the objective of ensuring that industry participants have scalable and effective policies, procedures, systems and technologies in place to take reasonable and proactive steps to prevent or limit: ● access or exposure to, and ● distribution of class 1B material.	**Outcome 2: Industry participants take reasonable and proactive steps to prevent or limit access or exposure to, and distribution of class 1B material.** **MCM 10:** See MCM 7 above. **MCM 11:** Tier 1 and Tier 2 designated internet service and end-user-managed hosting service providers must implement appropriate systems and processes that enable the provider to take appropriate action for breaches of terms and conditions, community standards, and/or acceptable use policies in relation to class 1B material. a) in the case of Tier 1 or Tier 2 designated internet services having: i) processes that include clearly specified internal channels for escalating and prioritising reports of breaches of the provider's terms and conditions, community standards, and/or acceptable use policies to the designated internet service; and ii) processes to provide operational guidance to personnel as to steps that must be taken within specified time frames to deal with the reports referred to in i) above. b) in the case of end-user-managed hosting services having standard operating procedures that: i) require the provider to engage with reports of class 1B material received from Australian end-users to help determine whether a terms and conditions, community standards and/or acceptable use policies relating to Class1B materials on the service have potentially been breached and (ii) either, where the provider: A) is not capable of assessing of reviewing and assessing materials, refer reporters of class 1B materials to eSafety resources; or B) is capable of assessing of reviewing and assessing materials, enable the provider to determine and take appropriate action in response to breaches of terms and conditions, community standards, and/or acceptable use policies prohibiting class 1B materials

	Note: This measure has been updated to respond to the letter by eSafety to industry associations concerning this Code dated 9 February 2023. See Appendix A, item 26. **MCM 12:** A provider of a Tier 1 or Tier 2 designated internet service or an end-user-managed hosting service must take appropriate action in response to breaches of the relevant terms and conditions, community standards, and/or acceptable use policies relating to Class 1B material that is reasonably proportionate to the level of harm associated with the relevant breach. Note: This measure has been added to respond to the letter by eSafety to industry associations concerning this Code dated 9 February 2023. See Appendix A, item 26. **MCM 13:** Tier 1 designated internet service and end-user-managed hosting services providers must adopt appropriate features and settings that are designed to mitigate the risks to Australian end-users related to class 1A material. A provider of a Tier 1 designated internet service must at a minimum: a) Implement measures that ensure that material can only be posted to or distributed on the service by a registered account holder, b) Make clear in terms and conditions, community standards and/or acceptable use policies that an Australian child is not permitted to hold an account on the service; and c) Take reasonable steps to prevent an Australian child from holding an account on the service, and to remove them from the service as set out in measure 3. Note: this measure makes best practice operating procedures to ensure that users that post material on a Tier 1 DIS have an account on the service and take steps to ensure an Australian child does not hold an account. Note that the industry has sought not to pre-empt the outcome of other policy processes concerning protection of children online that are currently underway including eSafety's age verification roadmap and the review of the *Privacy Act 1988*. **MCM 14:** Tier 1 designated internet service providers must make ongoing investments in tools and personnel that support the capacity of the provider to detect and take appropriate action under this Code concerning class 1B material, proportionate to the incidence of class 1B materials on the service and the extent class 1B materials are accessible to Australian end-users. Note: this measure is intended to ensure that providers of Tier 1 designated internet services maintain their investment in technology and human resources in a manner that is proportionate to the risk posed by class 1A materials on the service.
Matter 4 Measures directed towards achieving the objective of ensuring that industry participants have scalable and effective policies, procedures, systems and technologies in place to take reasonable and proactive steps to limit the hosting of class 1A material and class 1B material in Australia.	**Outcome 4: Industry participants take reasonable and proactive steps to limit hosting of class 1A and 1B material in Australia.** **MCM 15:** End-user-managed hosting service providers must have practices and procedures to minimise the likelihood that CSEM and pro-terror material is accessible by Australian end-users on the hosting service including by having policies, agreements, terms of use or other arrangements in place that stipulate that CSEM, and pro-terror material must not be stored on the end-user-managed hosting service. **MCM 16:** End-user-managed hosting service providers must implement systems and processes that enable the provider to

	take appropriate action for breaches of terms and conditions, community standards, and/or acceptable use policies regarding class 1B and non-CSEM/non-pro-terror class 1A material accessible by Australian end-users on the hosting service, noting that where such material is lawful (including in jurisdictions outside of Australia), the manner in which it is dealt with will vary from service to service, and such material may be permissible in certain circumstances depending on the context in which it appears. Note: the approach of this measure recognises that class 1A and class 1B material may be stored on an end-user-managed hosting service for many legitimate reasons such as by a freelance journalist preparing a news story for publication for an international news service, or by an academic for the purpose of research. The purpose for which material is stored will not be known to the provider of an end-user-managed hosting service. Please also see Resolve Strategic research concerning community attitudes concerning class 1 material.
Matter 5 Measures directed towards achieving the objective of ensuring that industry participants have effective and scalable policies and procedures in place to facilitate consultation, cooperation and collaboration with other industry participants in respect of the removal, disruption and/or restriction of class 1A material and class 1B material, as well as accounts associated with this material.	**MCM 17:** A provider of an end-user-managed hosting service must adopt measures to support Outcome 5 in relation to class 1A or class 1B material, including for example: a) joining industry organisations intended to address serious online harms, and/or share information on best practice approaches, that are relevant to the service; b) working with eSafety to share information, intelligence, and/or best practices relevant to addressing certain categories of class 1A or class 1B material, that are relevant to the service; c) collaborating with non-government or other organisations that facilitate the sharing of information, intelligence, and/or best practices relevant to addressing certain categories of class 1A or class 1B material; and/or d) joining and/or supporting global or local multi-stakeholder initiatives that bring together a range of subject matter experts to share information and best practices, collaborate on shared projects, and/or working to reduce online harms. Examples include the WePROTECT Global Alliance. e) taking part in an annual forum organised or facilitated by any industry association referred to in the Head Terms to discuss and evaluate the effectiveness of measures implemented under this Code and share best practice in implementing the Code and online safety in general with other industry participants. **MCM 18:** A provider of a Tier 1 or Tier 2 designated internet service and an end-user-managed hosting service may adopt measures to support Outcome 5 in relation to class 1A or class 1B material, including for example: a) joining industry organisations intended to address serious online harms, and/or share information on best practice approaches, that are relevant to the service; b) working with eSafety to share information, intelligence, and/or best practices relevant to addressing certain categories of class 1A or class 1B material, that are relevant to the service; c) collaborating with non-government or other organisations that facilitate the sharing of information, intelligence, and/or best practices relevant to addressing certain categories of class 1A or class 1B material; and/or

	d) joining and/or supporting global or local multi-stakeholder initiatives that bring together a range of subject matter experts to share information and best practices, collaborate on shared projects, and/or working to reduce online harms. Examples include the WePROTECT Global Alliance.
Matter 6 Measures directed towards achieving the objective of ensuring that industry participants have effective and scalable policies and procedures in place which ensure communication and cooperation with the eSafety Commissioner with respect to matters about class 1A material and class 1B material, including complaints.	**Outcome 6: Industry participants communicate and cooperate with eSafety in respect of matters relating to class 1A and class 1B material, including complaints.** **MCM 19:** Tier 1 designated internet service providers must refer complaints from the public concerning the provider's non-compliance with this Code to eSafety where the provider is unable to resolve the complaint within a reasonable time frame. **MCM 20:** Tier 1 designated internet service providers must share information with eSafety about significant new features or functions released by the provider of the designated internet service that the provider reasonably considers are likely to have a significant effect on the access or exposure to, distribution of class 1A or class 1B materials in Australia. In implementing this measure, industry participants are not required to disclose information to eSafety that is confidential. Note: this measure builds on example measures in the Position Paper (see p. 70) and feedback received by eSafety in the course of developing the Code, noting that these are proactive obligations supplementary to eSafety's power to respond directly to complaints about breaches of the Codes and to issue a reporting notice or make a reporting determination for all designated internet services about their compliance with the BOSE. See also incentives on providers to engage with eSafety in expectations 7, 18, 19 and 20 of the BOSE. **MCM 21:** End-user-managed hosting service providers must implement policies and procedures that ensure it responds in a timely and appropriate manner to communications from the Commissioner about compliance with this Code.
Matter 7 Measures directed towards achieving the objective of providing people with a range of technical tools and/or information to limit their access and exposure, and the access and exposure of children in their care, to class 1A material and class 1B material.	**Objective 2: Industry participants will empower people to manage access and exposure to class 1A and class 1B material.** **Outcome 7: Industry participants provide tools and/or information to limit access and exposure to class 1A and class 1B material.** **MCM 22:** Tier 1 and Tier 2 designated internet service and end-user-managed hosting service providers must provide online safety resources that include clear and accessible information for Australian end-users regarding the role and functions of eSafety, including how to make a complaint to eSafety, and information about the mechanisms in measure 20. Note: the measures for this outcome are focused on the provision of information, noting that tools for these services are dealt with elsewhere in the Code.
Matter 8 Measures directed towards achieving the objective of providing people with clear, easily accessible and effective:	**Outcome 8: Industry participants provide clear and effective reporting and complaints mechanisms for class 1A and class 1B material.** **MCM 23:** Tier 1 and Tier 2 designated internet service and end-user-managed hosting service providers must provide a mechanism which enables Australian end-users to provide feedback to the service, including for the purpose of reporting,

● reporting mechanisms for class 1A material and class 1B material, as well as associated user accounts, and ● complaints mechanisms to address complaints about the handling of reports about class 1A material and class 1B material and codes compliance.	flagging, or complaining about material accessible on the service that breaches the provider’s terms and conditions, community standards, and/or acceptable use policies. These must be easily accessible and easy to use, accompanied by clear instructions on how to use them, as well as an overview of the reporting process, and the identity of the reporter must be protected from the reported end-user or account holder. **MCM 24:** Tier 1 and Tier 2 designated internet service and end-user-managed hosting service providers must provide clear and accessible information on how an Australian end-user can contact eSafety regarding the designated internet service’s compliance with this Code. Note: this measure builds on examples provided by eSafety in the Position Paper (see p. 71)
Matter 9 Measures directed towards achieving the objective of ensuring that industry participants have scalable and effective policies, procedures, systems and technologies in place to effectively respond to: ● reports about class 1A material and class 1B material, as well as associated user accounts, and ● complaints about the handling of reports about class 1A material and class 1B material and codes compliance.	**Outcome 9: Industry participants effectively respond to reports and complaints about class 1A and 1B material.** **MCM 25**: Tier 1 designated internet service providers must: a) Take appropriate steps to promptly respond to reports made by Australian end-users of materials that violate the service’s terms and conditions, community standards, and/or acceptable use policies, and b) Ensure that an Australian end-user who reports class 1A or class 1B materials is: i. informed in a reasonably timely manner of the outcome of the report, ii. able to seek a review of the response in sub-measure i) if the Australian end- user is dissatisfied with the providers' response under sub-measure i), and iii. notified of the outcome of a review under sub-measure ii). **MCM 26:** Tier 1 designated internet service providers must implement and document policies and procedures which detail how they give effect to the requirements in measure 22. **MCM 27:** Tier 1 designated internet service providers must ensure that personnel responding to reports are trained in the designated internet service’s policies and procedures for dealing with reports. **MCM 28:** Tier 1 designated internet service providers must review the effectiveness of their reporting systems and processes to ensure reports are assessed and material removed or otherwise actioned (if necessary) within reasonably expeditious timeframes, based on the level of harm the material poses to Australian end-users. Such review must occur at least annually. **MCM 29:** Tier 2 designated internet service and end-user-managed hosting service providers must take appropriate steps to promptly address reports made by Australian end-users of materials that breach the service’s terms and conditions, community standards, and/or acceptable use policies. **MCM 30:** Tier 2 designated internet service and end-user-managed hosting service providers must implement and document policies and procedures which detail how they give effect to the requirements in measure 26. **MCM 31:** Tier 2 designated internet service and end-user-managed hosting service providers must ensure that personnel

	responding to reports are trained in the designated internet service's policies and procedures for dealing with reports. Note: these measures build on examples provided by eSafety in the Position Paper (p. 72). See also measure 7.2 of the Head Terms.
Matter 10 Measures directed towards achieving the objective of ensuring that industry participants publish easily accessible and plain language policies, procedures and guidelines that set out how they handle class 1A material and class 1B material. Measures directed towards achieving the objective of ensuring that industry participants provide end-users with information about the safety issues associated with class 1A material and class 1B material.	**Objective 3: Industry participants will strengthen transparency of, and accountability for, class 1A and class 1B material.** **Outcome 10: Industry participants provide clear and accessible information about class 1A and class 1B material.** **MCM 32:** Tier 1 and Tier 2 designated internet service and end-user-managed hosting service providers must publish appropriate terms and conditions, community standards, and/or acceptable use policies regarding material, which is not permitted on the service, having regard to the purpose of the service. Such terms and conditions, community standards and/or acceptable use policies must make clear that the broad categories of material within class 1A material are prohibited on the service. **MCM 33:** Tier 1 designated internet service providers must publish clear and accessible information that explains the actions they take to reduce the risk of harm to Australian end-users caused by the distribution of class 1A and class 1B material. Note: these measures and accompanying guidance under this outcome build on examples for this outcome in the Position Paper (p. 73) and make enforceable for Tier 1 and Tier 2 designated internet services industry best practice for documenting policies concerning class1 materials and, in the case of Tier 1 designated internet services, providing transparency about the actions taken to address online harms.
Matter 11 Measures directed towards achieving the objective of ensuring that industry participants publish annual reports about class 1A material and class 1B material, and their compliance with industry codes.	**Outcome 11: Industry participants publish annual reports about class 1A and 1B material and their compliance with this Code.** **MCM 34:** Tier 1 designated internet service providers must submit a Code report which as a minimum contains the following information: a) Details of the risk assessment (if the provider is required to undertake a risk assessment is required under the Code), together with information about the risk assessment methodology adopted, b) The steps that the provider has taken to comply with the applicable minimum compliance measures, c) the volume of CSEM or pro terror material removed by the provider of the designated internet service; and d) An explanation as to why these measures are appropriate. **MCM 35:** On request by eSafety, Tier 2 designated internet service providers must submit to eSafety a Code report which includes the following information: a) Details of the risk assessment it has carried out pursuant to clause 4, together with information about the risk assessment methodology adopted, b) The steps that the provider has taken to comply with their applicable minimum compliance measures, c) An explanation as to why these measures are appropriate.

	MCM 36: On request by eSafety, end-user-managed hosting service providers must submit to eSafety a Code report which includes the following information: a) The steps that the provider has taken to comply with their applicable minimum compliance measures, b) An explanation as to why these measures are appropriate. **MCM 37:** On request by eSafety, an enterprise designated electronic service provider must confirm in writing to eSafety that the provider is compliant with MCM 1. Note: these measures contain reporting obligations on designated internet services that are supplementary to eSafety's power to investigate breaches of the Codes and to issue a reporting notice or make reporting determinations for all designated internet service providers about their compliance with the BOSE. Note also reduced response time for reporting in MCM 36 in response to eSafety letters of (9 February concerning this Code (see Appendix A, item 29)
Additional Matters	Position 11 of the Position Paper outlines eSafety's expectation that the Codes will include a statement about how and when the Codes will be reviewed. eSafety also makes reference to the role of industry associations in the Position Paper (see p. 62, 63) These matters are addressed in section 7 of the Heads Terms, taking into account additional feedback provided by eSafety during the Code development process.

4. Internet Search Engine Services Online Safety Code (Class 1A and Class 1B Material)

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.*

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.

Approach to measures

The Code codifies best practices concerning illegal material surfaced in search engine results. All the measures required of providers of internet search engine service providers are mandatory. Both the scope and the substance of the measures provide transparent safeguards to Australians concerning illegal material online. When compared to other frameworks for governing illegal content, such as the EU Digital Services Act, the Code goes into greater specificity with regard to the obligations required of search engines. For example, the Code includes granular, clear requirements around transparency, policies, trust and safety, and cooperation with the Office of the e-Safety Commissioner.

Matter 1 Measures directed towards achieving the objective of ensuring that industry participants have scalable and effective policies, procedures, systems and technologies in place to take reasonable and proactive steps to **detect and** prevent: ● access or exposure to, ● distribution of, and ● online storage of class 1A material.	**Objective 1: Industry participants will take reasonable and proactive steps to create and maintain a safe online environment for Australian end-users.** **Outcome 1: Industry participants take reasonable and proactive steps to prevent access or exposure to, distribution of, and online storage of class 1A material.** **Note: Outcome 1 does not refer to the detection of class 1A material as an entire class, noting that there are no systems and processes that can be reliably deployed to detect and remove access to class 1A materials from search results.** **MCM 1:** All internet search engine service providers must take appropriate steps to support algorithmic optimisation, with a view to elevating authoritative, relevant and trustworthy information and reducing the accessibility or discoverability of class 1A materials in search results. At a minimum, they must: a) Make available to Australian end-users, information about policies for and approach to indexing web pages, and b) Continually review and/or test the performance of algorithms in meeting the above. c) following review/and or testing in b), adjust ranking algorithms to elevate authoritative, relevant and trustworthy information and reduce the risk that class 1A material is accessible or discoverable in search results by Australian end-users, d) make ongoing investments in technology (for example, machine learning, artificial intelligence or other safety technologies). See Appendix A, item 33 for explanation of regions to this Clause in response to letters of 9 February. See also Appendix A, item 1 for explanation about revised meaning of Australian end-user. **MCM 2:** All internet search engine service providers must implement systems, policies and processes designed to reduce the accessibility or discoverability of class 1A material by Australian end-users. At a minimum, a provider of an internet search engine service must: a) Delist search results that surface known CSAM,

	b) Delist links to class 1A materials pursuant to a legal removal request, c) Prevent links to class 1A material that are removed pursuant to a legal removal request from being retained in cached data, where the search engine has the ability to cache results from searches, d) Ensure that autocomplete or predictive entries that appear on the internet search engine service do not include, without justification, terms that have known associations to CSEM based on keyword searches and input from expert organisations, e) Use best efforts to prevent autocomplete / predictive prompts for questions / phrases that would facilitate an Australian end-users search for material for the purpose of inciting terrorism or extreme crime or violence, f) Provide access to tools, such as 'safe search' functionality, which enable users to limit exposure to explicit and / or graphic content, g) Use best efforts to ensure that search results specifically seeking images of known CSAM are accompanied by deterrent messaging that outlines the potential risk and criminality of accessing images of CSAM; and h) Use best efforts to ensure that search results returned for terms that have known associations to CSEM are accompanied by information or links to services that assist Australian end-users to report CSEM to law enforcement and/or seek support. **MCM 3:** All internet search engine service providers must make corresponding adjustments to relevant policies, systems, processes and technologies required in measure 1) where the results of a review in clause 5 (Regular review of adequacy of policies, processes, systems and technologies) indicate they are reasonably necessary. Note: given the purpose of a search engine, their limited functionality and control over online materials services and the billions of web pages indexed by a search engine worldwide, it is appropriate that these measure focus on elevating authoritative and trustworthy information in search results and reduce the accessibility and discoverability of CSAM and CSEM and material that is subject to a valid legal removal request. **MCM 4:** All internet search engine service providers must ensure that one or more designated personnel have primary responsibility to oversee the safety of the service including compliance with the OSA and this Code. Such personnel must have clearly defined roles and responsibilities, including for the creation, operationalisation and evaluation of the systems and processes required under this Code. Note: this measure addresses the need for human resources that have specific safety responsibilities, which was reinforced by feedback from the public consultation process.
Matter 2 Measures directed towards achieving the objective of ensuring that industry participants have scalable and effective policies, procedures, systems and technologies in place to take	**Outcome 2: Industry participants take reasonable and proactive steps to prevent or limit access or exposure to, and distribution of class 1B material.** **MCM 5:** All internet search engine service providers must implement systems processes and technologies that are designed to limit Australian end-users' exposure to class 1B materials. At a minimum, a provider of an internet search engine service must invest in ongoing improvements to ranking algorithms with the aim of prioritising the accessibility and discoverability of authoritative

reasonable and proactive steps to prevent or limit: ● access or exposure to, and ● distribution of class 1B material.	sources of online information and demoting the accessibility of class 1B materials in search results. **MCM 6:** All internet search engine service providers must make adjustments to relevant policies, systems, processes and technologies in measure 5) where the results of a review under clause 5 (Regular review of adequacy of policies, processes, systems and technologies) indicate they are reasonably necessary. Note: this measure builds on the examples in eSafety's Position Paper (see p.69).
Matter 4 Measures directed towards achieving the objective of ensuring that industry participants have scalable and effective policies, procedures, systems and technologies in place to take reasonable and proactive steps to limit the hosting of class 1A material and class 1B material in Australia.	**Outcome 4: Industry participants take reasonable and proactive steps to limit hosting of class 1A and 1B material in Australia.** This Outcome is not applicable to internet search engine services (See preamble to Head Terms).
Matter 5 Measures directed towards achieving the objective of ensuring that industry participants have effective and scalable policies and procedures in place to facilitate consultation, cooperation and collaboration with other industry participants in respect of the removal, disruption and/or restriction of class 1A material and class 1B material, as well as accounts associated with this material.	**Outcome 5: Industry participants consult, cooperate and collaborate with other industry participants in respect of the removal, disruption and/or restriction of class 1A and class 1B material.** **MCM 7:** Internet search engine service providers with more than 500,000 active monthly Australian end-users must implement procedures for collaborating with eSafety, law enforcement, non-governmental or cross industry organisations that have established systems and processes that facilitate the safe, secure and lawful sharing of information that enables the detection and removal of CSEM. Note: the search engine market is a very small market in Australia. This measure builds on examples in the Position Paper that are appropriate for the search market, being designed to ensure that collaboration is required by the major players only, in an open and transparent manner, to ensure that smaller participants are not discouraged from entering the market.
Matter 6 Measures directed towards achieving the objective of ensuring that industry participants have effective and scalable policies and procedures in place which ensure communication and cooperation with the eSafety Commissioner with respect to matters about class 1A material and class 1B material, including complaints.	**Outcome 6: Industry participants communicate and cooperate with eSafety in respect of matters relating to class 1A and class 1B material, including complaints.** **MCM 8:** All internet search engine service providers must refer to eSafety complaints from the public concerning the provider's noncompliance with this Code, where the provider is unable to resolve the complaint within a reasonable time frame. **MCM 9:** All internet search engine service providers must update eSafety regarding changes to the functionality of internet search engine service that are likely to have a significant positive or negative effect on the access or exposure to, distribution of class 1A or class 1B materials in Australia. Note: this measure builds on example measures in the Position Paper (see p. 70).

Matter 7 Measures directed towards achieving the objective of providing people with a range of technical tools and/or information to limit their access and exposure, and the access and exposure of children in their care, to class 1A material and class 1B material.	**Objective 2: Industry participants will empower people to manage access and exposure to class 1A and class 1B material.** **Outcome 7: Industry participants provide tools and/or information to limit access and exposure to class 1A and class 1B material.** **MCM 10:** All internet search engine service providers must implement the following measures: a) Provide age-appropriate safety settings, b) Make available clear and accessible guidelines about the use and effect of such safety settings, c) Make available clear and accessible information about the use and effect of tools available to Australian end-users, and d) Make available information to Australian end-users about online harms and the measures that users can take to protect themselves and children in their care. Note: this measure builds on examples provided by eSafety in the Position Paper (see p. 71).
Matter 8 Measures directed towards achieving the objective of providing people with clear, easily accessible and effective: ● reporting mechanisms for class 1A material and class 1B material, as well as associated user accounts, and ● complaints mechanisms to address complaints about the handling of reports about class 1A material and class 1B material and codes compliance.	**Outcome 8: Industry participants provide clear and effective reporting and complaints mechanisms for class 1A and class 1B material.** **MCM 11:** All internet search engine service providers must have a process for receiving removal requests from Australian end-users for illegal content linked to from within their search engines. **MCM 12:** All internet search engine service providers must provide tools which enable Australian end-users to provide feedback about the quality of the service, which may include feedback on the accessibility of lawful class 1A and class 1B materials. **MCM 13:** All internet search engine service providers must provide Australian end-users with access on its platform to clear information that explains the service's reporting processes. **Optional measure 14:** All internet search engine service providers should intermittently test the adequacy of Australian end-user use and engagement and awareness of reporting mechanisms required under this Code. Note: these measures build on examples provided by eSafety in the Position Paper (see p. 71). They are focused on enabling users to report illegal materials (this would include CSEM and pro-terror materials) and provide feedback on the service (which can be used to optimise the surfacing of authoritative content by end-users).
Matter 9 Measures directed towards achieving the objective of ensuring that industry participants have scalable and effective policies, procedures, systems and technologies in place to effectively respond to: ● reports about class 1A material and class 1B material, as well	**Outcome 9: Industry participants effectively respond to reports and complaints about class 1A and 1B material.** **MCM 15:** All internet search engine service providers must have appropriate personnel, policies, processes, systems and technologies in place to respond to reports by Australian end-users. At a minimum, a provider of an internet search engine service must implement the following measures to address reports: a) Implement policies, procedures, and systems to enable the automated, human, or hybrid triaging and review and response to reports by Australian end-users,

as associated user accounts, and ● complaints about the handling of reports about class 1A material and class 1B material and codes compliance.	b) Implement processes and, where appropriate, tools to enable the handling of complaints by Australian end-users about the search engines response to reports under Outcome 8, c) Provide clear and easily accessible information on how an Australian end-user can contact eSafety where a report or complaint is not resolved to that end- user's satisfaction, d) Establish standard operating procedures which include clearly specified channels for escalating and/or reporting to an appropriate entity – as soon as reasonably practicable or within 24 hours - if the provider: i) identifies CSEM on its service; and ii) forms a good faith belief that the CSEM presents evidence of serious and immediate threat to the life or physical safety of an Australian adult or child. **MCM 16:** All internet search engine service providers must ensure that personnel responding to reports by Australian end-users pursuant to this Code are trained in the platform's policies, systems and processes for dealing with reports. Note: these measures build on examples provided by eSafety in the Position Paper (see p.71). Measure 15(d) is supplementary to existing obligations that may be imposed on search engine services under State or Territory or foreign laws. The disclosure of class 1A material may involve the disclosure of personal information that identifies an individual and will be subject to the *Privacy Act 1988*. This obligation has been drafted to comply with the requirements of that Act concerning such disclosure. See section 16A(1), item 1 of the *Privacy Act 1988*.
Matter 10 Measures directed towards achieving the objective of ensuring that industry participants publish easily accessible and plain language policies, procedures and guidelines that set out how they handle class 1A material and class 1B material. Measures directed towards achieving the objective of ensuring that industry participants provide end-users with information about the safety issues associated with class 1A material and class 1B material.	**Objective 3: Industry participants will strengthen transparency of, and accountability for, class 1A and class 1B material.** **Outcome 10: Industry participants provide clear and accessible information about class 1A and class 1B material.** **MCM 17:** All internet search engine service providers must publish easily accessible and plain language information on their approaches to class 1A and class 1B material. An internet search engine service provider must at a minimum implement the following measures: a) Provide information to Australian end-users about the ways in which the internet search engine service ranks information, b) Provide information on the actions that may be taken to report links to illegal materials, c) Implement processes and, where appropriate, tools to enable the handling of complaints by Australian end-users about the provider's response to reports under Outcome 8, 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 online safety information, e) Provide information to Australian end-users about online safety risks and guidance on how to mitigate these risks, 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.

	Note: these measures and accompanying guidance under this outcome build on examples for this outcome in the Position Paper (p. 73) and make enforceable industry best practice for documenting information about how providers of internet search engines handle and reports from end-users concerning content surfaced in search results online safety risks, including additional obligations regarding how Australian end-users can make a complaint to eSafety.
Matter 11 Measures directed towards achieving the objective of ensuring that industry participants publish annual reports about class 1A material and class 1B material, and their compliance with industry codes.	**Outcome 11: Industry participants publish annual reports about class 1A and 1B material and their compliance with this Code.** **MCM 18:** On request**,** all internet search engine service providers must submit to eSafety a Code report which includes the following information about: a) The steps that the provider has taken to comply with their applicable minimum compliance measures, b) An explanation as to why these measures are appropriate, and c) annual updates about the volume of CSEM or pro-terror material flagged and responded to by the internet search engine service. d) number of complaints about Code compliance and information about the provider's responses; and e) data and information about algorithmic optimisation and other safety innovations that address the discoverability or accessibility of class1A and class 1B materials on the service Note: these reporting obligations supplement information gathering powers of eSafety under the OSA and respond to feedback provided during the Code development process asking for additional transparency on the detection and response of industry participants to CSEM and po-terror materials. See also Appendix A, item 34 about revisions made to this measure in response to eSafety letter of 9 February to industry associations concerning this Code.
Additional Matters: review of codes	Position 11 of the Position Paper outlines eSafety's expectation that the Codes will include a statement about how and when the Codes will be reviewed. eSafety also makes reference to the role of industry associations in the Position Paper (see p. 62, 63) These matters are addressed in section 7 of the Heads Terms, taking into account additional feedback provided by eSafety during the Code development process.
Additional Matters: limitations in Head terms	See Appendix A, item 5.

5. App Distribution Services Online Safety Code (Class 1A and Class 1B Material)

Structure of Code

This Code covers providers of app distribution services as defined in the OSA.

The Code 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 such apps (including their supply/distribution).

As the 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.

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.

Approach to risk

Clause 4 of the Code explains the role of app distribution services in the digital ecosystem. 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.

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.

Matter 1 Measures directed towards achieving the objective of ensuring that industry participants have scalable and effective policies, procedures, systems and technologies in place to take reasonable and proactive steps to **detect and** prevent: ● access or exposure to, ● distribution of, and ● online storage of class 1A material.	**Objective 1: Industry participants will take reasonable and proactive steps to create and maintain a safe online environment for Australian end-users.** **Outcome 1: Industry participants take reasonable and proactive steps to prevent access or exposure to, distribution of, and online storage of class 1A material.** **Note: Outcome 1 does not refer to the detection of class 1A material as an entire class, noting that there are no systems and processes that can be reliably deployed to detect the range of real or simulated extreme crime and violence materials that fall within class 1A.** **MCM 1:** All app distribution service providers must: a) Have agreements in place with third-party app providers that require the third- party app provider to comply with applicable Australian content laws and regulations, b) Have systems, policies and/or procedures in place that enable an app distribution service provider to enforce the provisions in the agreements referred to in a) when there is a breach of such agreements that relates to the access or exposure to, distribution of, or online storage of class 1A material; c) take appropriate action pursuant to the systems, policies and/or procedures referred to in sub-measure 1) b) when there is a breach of the agreement referred to in sub-measure 1) a) that is reasonably proportionate to the

	nature of the third-party app provider's breach of the agreement; d) 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 access or exposure to, distribution of, or online storage of class 1A material via the third-party app; e) Review, to the extent reasonably practicable, third-party apps that may be provided to Australian end-users via the app distribution service provider before those third-party apps are released on the app distribution service, and f) Take steps to ensure all third-party app providers providing third-party apps to the app distribution service are made aware of other industry codes made under the OSA that may apply to them in their role as the app provider. Note: The example measures provided in the Position Paper for this matter assume that services can moderate and report Class 1 materials. Over the course of the code development process industry advised eSafety that app distribution services have a very limited ability to deal with material that end-users may access via a third-party app downloaded from an app distribution service, other than via agreements with third party app providers and through the raising of awareness of the obligations imposed on app providers under the Codes. Whilst app distribution service providers can review apps, where practicable, prior to release, much of the content of many apps is populated after download or shared between end-users after download at which point the app distribution service provider will have limited visibility or control. This measure has been designed with those practical considerations in mind. **MCM 2:** All app distribution service providers must ensure that they are reasonably resourced with personnel to oversee the safety of their app distribution services. Such personnel must have clearly defined roles and responsibilities, including for the operationalisation and evaluation of the systems and processes required under this Code. Note: this measure addresses the need for human resources that have specific safety responsibilities, which was reinforced by feedback from the public consultation process. See Appendix A, item 36 for discussion of revisions made to this measure in response to letters from eSafety to industry associations dated February 9 2023 concerning the app distribution services Code.
Matter 2 Measures directed towards achieving the objective of ensuring that industry participants have scalable and effective policies, procedures, systems and technologies in place to take	**Outcome 2: Industry participants take reasonable and proactive steps to prevent or limit access or exposure to, and distribution of class 1B material.** **MCM 3:** All app distribution service providers must make age and/or content ratings information about third-party apps available on the app distribution service to Australian end-users at the time those third-party apps are released on the app distribution service.

reasonable and proactive steps to prevent or limit: ● access or exposure to, and ● distribution of class 1B material.	Note: this measure builds on best practice by app providers to inform users about the suitability of apps for different age groups.
Matter 4 Measures directed towards achieving the objective of ensuring that industry participants have scalable and effective policies, procedures, systems and technologies in place to take reasonable and proactive steps to limit the hosting of class 1A material and class 1B material in Australia.	**Outcome 4: Industry participants take reasonable and proactive steps to limit hosting of class 1A and 1B material in Australia.** This Outcome is not applicable to app distribution service providers. (See preamble to Head Terms.)
Matter 5 Measures directed towards achieving the objective of ensuring that industry participants have effective and scalable policies and procedures in place to facilitate consultation, cooperation and collaboration with other industry participants in respect of the removal, disruption and/or restriction of class 1A material and class 1B material, as well as accounts associated with this material.	**Outcome 5: Industry participants consult, cooperate and collaborate with other industry participants in respect of the removal, disruption and/or restriction of class 1A and class 1B material.** **MCM 4:** All app distribution service providers must take part in an annual forum, organised or facilitated by any industry association referred to in the Head Terms, to discuss and evaluate the effectiveness of measures in this Code and share best practice in implementing this Code and online safety in general with other industry participants. Note: given the role of app providers in the digital ecosystem, an annual forum is an appropriate vehicle for cooperation and collaboration concerning online safety. **MCM5:**An app distribution service provider must notify eSafety in writing if it removes a third-party app from its app distribution service as part of the action taken by the app distribution service provider pursuant to measure 1) c) in relation to the access or exposure to, distribution of, or online storage of class 1A material. See Appendix A, item 36 for explanation of the introduction of this measure in response to eSafety letter of 9 February concerning the app distribution services Code.
Matter 6 Measures directed towards achieving the objective of ensuring that industry participants have effective and scalable policies and procedures in place which ensure communication and cooperation with the eSafety Commissioner with respect to matters about class 1A material and class 1B material, including complaints.	**Outcome 6: Industry participants communicate and cooperate with eSafety in respect of matters relating to class 1A and class 1B material, including complaints.** **MCM 6:** All app distribution service providers must share information with eSafety about significant new features or functions released by the app distribution service provider that the app distribution service provider reasonably considers are likely to have a significant effect on the access or exposure to, distribution of, and online storage of class 1A or class 1B materials in Australia. Note: this creates a new obligation on app distribution service providers to proactively update eSafety on new features that may impact on the distribution of class 1A or class 1b materials in Australia.

Matter 7 Measures directed towards achieving the objective of providing people with a range of technical tools and/or information to limit their access and exposure, and the access and exposure of children in their care, to class 1A material and class 1B material.	**Objective 2: Industry participants will empower people to manage access and exposure to class 1A and class 1B material.** **Outcome 7: Industry participants provide tools and/or information to limit access and exposure to class 1A and class 1B material.** **MCM 7:** <u>All app distribution service providers</u> 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) Steps that parents and guardians may take to supervise and manage children's use of apps, c) Information about the ability of Australian end-users to report or complain about content on a third-party app to the third-party app provider (being information that can help Australian end-users to report or complain about class 1A or class 1B material), d) Information about the mechanisms in measure 7, and e) The role and functions of eSafety, including how to make a complaint to eSafety. <u>Note:</u> these measures and accompanying guidance under this outcome build on examples for this outcome in the Position Paper (p. 73) and make enforceable industry best practice for documenting information that supports online safety of end-users including information about how end-users can make a complaint to eSafety.
Matter 8 Measures directed towards achieving the objective of providing people with clear, easily accessible and effective: ● reporting mechanisms for class 1A material and class 1B material, as well as associated user accounts, and ● complaints mechanisms to address complaints about the handling of reports about class 1A material and class 1B material and codes compliance.	**Outcome 8: Industry participants provide clear and effective reporting and complaints mechanisms for class 1A and class 1B material.** **MCM 8:** <u>All app distribution service providers</u> 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 concerning class 1A or class 1B material on 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: a) Be easily accessible and easy to use; and b) Be accompanied by plain language instructions on how to use it, as well as an overview of the reporting process. <u>Note</u>: This measure has been drafted to take into account that app distribution service providers cannot directly take action in relation to class 1A and class 1B material that is accessible on a third-party app, but can consider complaints about their own

	breach of the Code and are able to follow up complaints made to third-party app providers regarding class 1A or class 1B material on their third party-apps (see MCM1).
Matter 9 Measures directed towards achieving the objective of ensuring that industry participants have scalable and effective policies, procedures, systems and technologies in place to effectively respond to: ● reports about class 1A material and class 1B material, as well as associated user accounts, and ● complaints about the handling of reports about class 1A material and class 1B material and codes compliance.	**Outcome 9: Industry participants effectively respond to reports and complaints about class 1A and 1B material.** By complying with the minimum compliance measures under Outcome 8, app distribution service providers will also meet the requirements of this Outcome.
Matter 10 Measures directed towards achieving the objective of ensuring that industry participants publish easily accessible and plain language policies, procedures and guidelines that set out how they handle class 1A material and class 1B material. Measures directed towards achieving the objective of ensuring that industry participants provide end-users with information about the safety issues associated with class 1A material and class 1B material.	**Objective 3: Industry participants will strengthen transparency of, and accountability for, class 1A and class 1B material.** **Outcome 10: Industry participants provide clear and accessible information about class 1A and class 1B material.** By complying with the minimum compliance measures under Outcome 7, app distribution service providers will also meet the requirements of this Outcome.
Matter 11 Measures directed towards achieving the objective of ensuring that industry participants publish annual reports about class 1A material and class 1B material, and their compliance with industry codes.	**Outcome 11: Industry participants publish annual reports about class 1A and class 1B material and their compliance with this Code** **MCM 8:** On request, all app distribution service providers must submit to eSafety a Code report which includes the following information: a) the steps that the provider has taken to comply with their applicable minimum compliance measures, b) an explanation as to why these measures are appropriate. Note: App distribution service providers do not have the ability to remove material from third-party apps, and therefore cannot publish annual reports in relation to such material. This measure aims at providing eSafety with information about compliance with this Code, supplementary to the Commissioner's power to investigate breaches of the Codes. See also Appendix A, item 39 regarding the revision to the response times for provision of reports. These must now be provided

	within 2 months of receiving the request, but for the first request no earlier than 12 months after this Code comes into effect.
Additional Matters: review of materials	Position 11 of the Position Paper outlines eSafety's expectation that the codes will include a statement about how and when they will be reviewed. eSafety also makes reference to the role of industry associations in the Position Paper (see p. 62, 63) These matters are addressed in section 7 of the Head Terms, taking into account additional feedback provided by eSafety during the code development process.
Additional Matters: limitations in Head terms	See Appendix A, item 5.

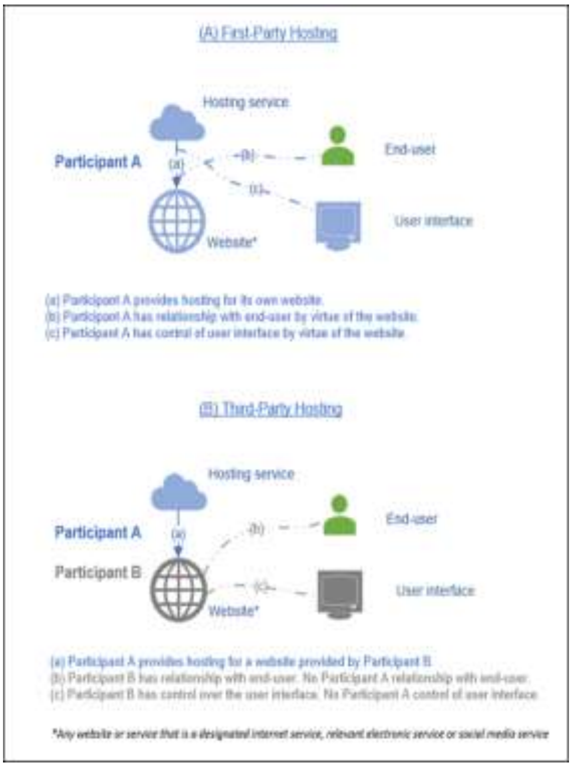
6. Hosting Services Online Safety Code (Class 1A and Class 1B Material)

Code structure

This Code comprises the Head Terms and Schedule 6, 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.

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



(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.

(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.

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.

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. Notwithstanding, both the scope and the substance of the measures in this Code provide greater safeguards to Australians concerning harmful online material than comparable industry codes such as the *UK interim code of practice on online child sexual exploitation and abuse and the Interim code of practice on terrorist content and activity online*.

Matter 1 Measures directed towards achieving the objective of ensuring that industry participants have scalable and effective policies, procedures, systems and technologies in place to take reasonable and proactive steps to **detect and** prevent: ● access or exposure to, ● distribution of, and ● online storage of class 1A material.	**Objective 1: Industry participants will take reasonable and proactive steps to create and maintain a safe online environment for Australian end-users.** **Outcome 1: Industry participants take reasonable and proactive steps to prevent access or exposure to, distribution of, and online storage of class 1A material.** **Note: Outcome 1 does not refer to the detection of class 1A material as an entire class, noting that there are no systems and processes that can be reliably deployed to detect the range of real or simulated extreme crime and violence materials that fall within class 1A.** <u>Note:</u> the appropriate measures for this outcome are the same as those addressing outcomes 4 and 5.

Matter 2 Measures directed towards achieving the objective of ensuring that industry participants have scalable and effective policies, procedures, systems and technologies in place to take reasonable and proactive steps to prevent or limit: ● access or exposure to, and ● distribution of class 1B material.	**Outcome 2: Industry participants take reasonable and proactive steps to prevent or limit access or exposure to, and distribution of class 1B material.** Note: the appropriate measures for this outcome are the same as those addressing outcomes 4 and 5.
Matter 4 Measures directed towards achieving the objective of ensuring that industry participants have scalable and effective policies, procedures, systems and technologies in place to take reasonable and proactive steps to limit the hosting of class 1A material and class 1B material in Australia.	**Outcome 4: Industry participants take reasonable and proactive steps to limit hosting of class 1A and 1B material in Australia.** **MCM 1:** All Third-Party Hosting Service providers 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 1A and class 1B material. Note: this measure is one of the primary obligations of providers of Third-Party Hosting Services. As explained above, providers of Third-Party Hosting Services do not have an effective ability to engage with end-users. Instead, providers of Third-Party Hosting Services have a relationship with other service providers, who themselves have relationships with their end-users. Accordingly, the types of measures that can be taken by providers of enterprise relevant electronic services to prevent and/or limit access or exposure to, distribution of, and/or online storage or hosting of class 1A or 1B material are primarily contractual. **MCM 2:** All Third-Party Hosting Service providers must enforce (also see Appendix A, item 40) the following policies and/or contractual terms to ensure appropriate and proportionate enforcement action with respect to customers of the service that violate its policies prohibiting class 1A and class 1B material: a) Standard operating procedures which include channels for prioritising and escalating reports of class 1A and class 1B material on a customer’s service that makes use of the Third-Party Hosting Service, b) Standard operating procedures to enforce their policies when they become aware of class 1A and class 1B material on a customer’s service that makes use of the Third-Party Hosting Service, such as by notifying, warning, suspending, or terminating the account(s) of the customer in question, and c) Policies and procedures that take into account the application of Australian laws that oblige the participant to report certain categories of material to law enforcement bodies, as well as the application of criminal offences relating to possession and distribution of material, so as to ensure that all appropriate escalations and referrals occur as necessary and appropriate in accordance with such laws.

	Note: this measure supplements MCM 1 and requires providers of Third-Party Hosting Services to ensure they have measures in place to take appropriate and take enforcement action with respect to customers of the service. Due to the inherent lack of control and visibility that providers of Third-Party Hosting Services have over individual pieces of hosted material of their customers, such providers' responses will generally be limited to notifying, warning, suspending, or terminating the customers in question. This measure nonetheless allows providers of Third-Party Hosting Services to ensure that their responses are proportionate, as having a 'one-size-fits-all' approach to enforcement presents several public interest and technical challenges, including the disruption of critical private, commercial and government operations. **MCM 3:** All Third-Party Hosting Service providers must ensure that end-users can contact the participant in relation to class 1A and class 1B material provided on a customer's service where such material is hosted by the Third-Party Hosting Service. Note: this measure has been included in response to feedback provided by eSafety during the Code development process. For larger Third-Party Hosting Service providers this codifies existing practice but for smaller providers this may extend existing practices and, therefore, adds to existing safeguards.
Matter 5 Measures directed towards achieving the objective of ensuring that industry participants have effective and scalable policies and procedures in place to facilitate consultation, cooperation and collaboration with other industry participants in respect of the removal, disruption and/or restriction of class 1A material and class 1B material, as well as accounts associated with this material.	**Outcome 5: Industry participants consult, cooperate and collaborate with other industry participants in respect of the removal, disruption and/or restriction of class 1A and class 1B material.** **MCM 4:** All Third-Party Hosting Service providers must ensure that it takes appropriate steps or adopt measures that are designed to support outcome 5 in relation to class 1A or class 1B material, including for example: a) Establishing clear channels of communication between the Third-Party Hosting Service provider and other Third-Party Hosting Service providers, as well as participants in different sectors of the online industry, b) Joining industry organisations intended to address serious online harms, and/or share information on best practice approaches, which are relevant to Third-Party Hosting Services, c) Working with eSafety to share information, intelligence, and/or best practices relevant to addressing certain categories of class 1A or class 1B material, that are relevant to Third-Party Hosting Services, d) Collaborating with non-government or other organizations that facilitate the sharing of information, intelligence, and/or best practices relevant to addressing certain categories of class 1A or class 1B material, and/or e) Joining and/or supporting global or local multi-stakeholder initiatives that bring together a range of subject matter experts to share information and best practices, collaborate on shared projects, and/or working to reduce online harms. Examples include the WePROTECT Global Alliance. Note: this measure also supplements the measures addressing Outcome 4 and requires providers of Third-Party Hosting Services to take appropriate steps or adopt measures with respect to consulting, cooperating and collaborating with other industry participants in preventing and/or limiting access or exposure to, distribution of, and/or online storage or hosting of class 1A or 1B material.

Matter 6 Measures directed towards achieving the objective of ensuring that industry participants have effective and scalable policies and procedures in place which ensure communication and cooperation with the eSafety Commissioner with respect to matters about class 1A material and class 1B material, including complaints.	**Outcome 6: Industry participants communicate and cooperate with eSafety in respect of matters relating to class 1A and class 1B material, including complaints.** **MCM 5:** All Third-Party Hosting Service providers must implement policies and procedures that ensure it responds in a timely and appropriate manner to communications from eSafety about compliance with this Code. Note: this measure is based on one of the example measures suggested for this Outcome in the Position Paper (p. 70).
Matter 7 Measures directed towards achieving the objective of providing people with a range of technical tools and/or information to limit their access and exposure, and the access and exposure of children in their care, to class 1A material and class 1B material.	**Objective 2: Industry participants will empower people to manage access and exposure to class 1A and class 1B material.** **Outcome 7: Industry participants provide tools and/or information to limit access and exposure to class 1A and class 1B material.** **MCM 6:** All Third-Party Hosting Service providers must offer customers of the service: a) Tools, settings or information (e.g., privacy and online safety settings), appropriate to the nature and function of the Third-Party Hosting Service, that are capable of enabling customers to address material, including class 1A and class 1B material, on the customer's service; and b) Clear and accessible guidance about how to use and the effect of any such tools, settings or information. Note: as outlined above, monitoring individual pieces of material within customer-hosted environments is beyond the technical, legal and practical abilities of providers of Third-Party Hosting Services. However, such providers should be able, and are required under this measure, to offer customers of their services tools, settings or information to enable customers to address class 1A/1B material on the customers service, as well as clear guidance to accompany such tools, settings or information.
Matter 8 Measures directed towards achieving the objective of providing people with clear, easily accessible and effective: ● reporting mechanisms for class 1A material and class 1B material, as well as associated user accounts, and ● complaints mechanisms to address complaints about the handling of reports about class 1A material and class 1B material and codes compliance.	**Outcome 8: Industry participants provide clear and effective reporting and complaints mechanisms for class 1A and class 1B material.** **MCM 3:** All Third-Party Hosting Service providers must ensure that end-users can contact the participant in relation to class 1A and class 1B material provided on a customer's service where such material is hosted by the Third-Party Hosting Service. Note: please see the note on MCM 3 in respect of Outcome 4 above.
Matter 9 Measures directed towards achieving the objective of ensuring that industry participants have scalable and effective policies,	**Outcome 9: Industry participants effectively respond to reports and complaints about class 1A and 1B material.** **MCM 3:** All Third-Party Hosting Service providers must ensure that end-users can contact the participant in relation to class 1A

procedures, systems and technologies in place to effectively respond to: - reports about class 1A material and class 1B material, as well as associated user accounts, and - complaints about the handling of reports about class 1A material and class 1B material and codes compliance.	and class 1B material provided on a customer's service where such material is hosted by the Third-Party Hosting Service. **MCM 6:** All Third-Party Hosting Service providers must offer customers of the service: a) Tools, settings or information (e.g., privacy and online safety settings), appropriate to the nature and function of the Third-Party Hosting Service, that are capable of enabling customers to address material, including class 1A and class 1B material, on the customer's service; and b) Clear and accessible guidance about how to use and the effect of any such tools, settings or information. Note: please see the notes on MCMs 3 and 6 in respect of Outcome 4 and 7 above.
Matter 10 Measures directed towards achieving the objective of ensuring that industry participants publish easily accessible and plain language policies, procedures and guidelines that set out how they handle class 1A material and class 1B material. Measures directed towards achieving the objective of ensuring that industry participants provide end-users with information about the safety issues associated with class 1A material and class 1B material.	**Objective 3: Industry participants will strengthen transparency of, and accountability for, class 1A and class 1B material.** **Outcome 10: Industry participants provide clear and accessible information about class 1A and class 1B material.** **MCM 7:** All Third-Party Hosting Service providers must provide information or links to information about online safety issues with respect to class 1A and class 1B material, and the role and functions of eSafety, including how to make a complaint to eSafety under the OSA. Examples in the Code include: i. Establishing a dedicated hub, portal or other location that houses online safety information for users or refers users to where they can find online safety information (e.g., the eSafety website); and ii. Running online safety awareness-raising campaigns in Australia, including in partnerships with one or more other organisations including government and non-government organisations or others. Note: Outcome 10 is also partially addressed through the measures addressing Outcome 4 above.
Matter 11 Measures directed towards achieving the objective of ensuring that industry participants publish annual reports about class 1A material and class 1B material, and their compliance with industry codes.	**Outcome 11: Industry participants publish annual reports about class 1A and 1B material and their compliance with this Code.** **MCM 8:** On request, all third-party hosting service providers must submit to eSafety a Code report which includes the following information: a) The steps that the provider has taken to comply with their applicable minimum compliance measures, b) An explanation as to why these measures are appropriate. c) the number of reports in relation to class 1A or class 1B material received by the Third-Party Hosting Service under minimum compliance measure 3. (Also see Appendix, item 47.) Note: this measure is supplementary to eSafety's power under the OSA to issue a reporting notice or make reporting determinations for all hosting service providers about their compliance with the BOSE.
Additional Matters	Position 11 of the Position Paper outlines eSafety's expectation that the codes will include a statement about how and when they

	will be reviewed. eSafety also makes reference to the role of industry associations in the Position Paper (see p62, 63) These matters are addressed in section 7 of the Heads of Terms, taking into account additional feedback provided by eSafety during the Code development process.

7. Internet Carriage Services Online Safety Code (Class 1A and Class 1B Material)

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.

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[26]: 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. ISPs are distinct from hosting services.

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, 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.

Matter 1 Measures directed towards achieving the objective of ensuring that industry participants have scalable and effective policies, procedures, systems and technologies in place to take reasonable and proactive steps to **detect and** prevent: ● access or exposure to, ● distribution of, and ● online storage of class 1A material.	**Objective 1: Industry participants will take reasonable and proactive steps to create and maintain a safe online environment for Australian end-users.** **Outcome 1: Industry participants take reasonable and proactive steps to prevent access or exposure to, distribution of, and online storage of class 1A material.** **Note: Outcome 1 does not refer to the detection of Class 1A material as an entire class, noting that there are no systems and processes that can be reliably deployed to detect the range of real or simulated extreme crime and violence materials that fall within Class 1A.** **MCM 1:** All internet service providers must inform its Australian end-users that they must not produce online material that is in contravention of any Australian State, Territory, or Commonwealth law, including the OSA. Note: ISPs cannot control the content that traverses their networks and are by law prohibited to monitor content. This measure aims to ensure that those who are in control of content are aware of their legal requirements.
Matter 2 Measures directed towards achieving the objective of ensuring	**Outcome 2: Industry participants take reasonable and proactive steps to prevent or limit access or exposure to, and distribution of class 1B material.**

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

that industry participants have scalable and effective policies, procedures, systems and technologies in place to take reasonable and proactive steps to prevent or limit: ● access or exposure to, and ● distribution of class 1B material.	This Outcome does not have any separate measures as ISPs cannot see, inspect or differentiate between the material that traverses their networks.
Matter 4 Measures directed towards achieving the objective of ensuring that industry participants have scalable and effective policies, procedures, systems and technologies in place to take reasonable and proactive steps to limit the hosting of class 1A material and class 1B material in Australia.	This outcome is not applicable to internet service providers. Where an internet service provider is also offering third-party hosting services, these services are subject to the Hosting Services Online Safety Code (Class 1A and Class 1B Material).
Matter 5 Measures directed towards achieving the objective of ensuring that industry participants have effective and scalable policies and procedures in place to facilitate consultation, cooperation and collaboration with other industry participants in respect of the removal, disruption and/or restriction of class 1A material and class 1B material, as well as accounts associated with this material.	**Outcome 5: Industry participants consult, cooperate and collaborate with other industry participants in respect of the removal, disruption and/or restriction of class 1A and class 1B material.** **MCM 2:** All internet service providers must notify a hosting service provider within 3 business days if the internet service provider becomes aware that the hosting service provider is hosting alleged class 1A material. This notification requirement will only apply if the internet service provider is aware of the identity and email address of the hosting service provider. However, an internet service provider must take reasonable steps to identify and obtain the email address of the hosting service provider. Note: ISPs almost never become aware of hosting providers hosting such material (no known case so far) but will take reasonable steps to identify a hosting provider if they did. ISPs do not have any other means to identify hosting providers than the general public.
Matter 6 Measures directed towards achieving the objective of ensuring that industry participants have effective and scalable policies and procedures in place which ensure communication and cooperation with the eSafety Commissioner with respect to matters about class 1A material and class 1B material, including complaints.	**Outcome 6: Industry participants communicate and cooperate with eSafety in respect of matters relating to class 1A and class 1B material, including complaints.** **MCM 3:** Upon request by eSafety, all internet service providers must sign the *Protocol Governing ISP Blocking Under Part 8 of the Online Safety Act 2021*, which deals with the blocking of domains for certain Class 1A material upon request by the eSafety Commissioner. Note: this measure aims at increasing the number of ISPs that participate in the Protocol. Currently, the six largest ISPs voluntarily participate in the Protocol, thereby covering well over 90% of Australian subscribers. Note that ISPs were ready to engage further: at eSafety's request, this Code does not include a minimum compliance measure to require ISPs to engage with eSafety on the development of a protocol to govern requests from eSafety to block access to certain domains which contain CSEM.

Matter 7 Measures directed towards achieving the objective of providing people with a range of technical tools and/or information to limit their access and exposure, and the access and exposure of children in their care, to class 1A material and class 1B material.	**Objective 2: Industry participants will empower people to manage access and exposure to class 1A and class 1B material.** **Outcome 7: Industry participants provide tools and/or information to limit access and exposure to class 1A and class 1B material.** **MCM 4:** All internet service providers must make information available to Australian end- users on filtering products and how they can be obtained at or close to the time of sale (also see Appendix A, item52). This information must be easily accessible. **MCM 5:** All internet service providers 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. Note: this measure aims at providing end-users with the choice to use filters to limit access to certain materials for children, including tested FFF, without overloading end-users with information at or close to point of sales when they are unlikely to take in more information (noting consumer complains about 'information overload' at or close to point of sale).
Matter 8 Measures directed towards achieving the objective of providing people with clear, easily accessible and effective: ● reporting mechanisms for class 1A material and class 1B material, as well as associated user accounts, and ● complaints mechanisms to address complaints about the handling of reports about class 1A material and class 1B material and codes compliance.	**Outcome 8: Industry participants provide clear and effective reporting and complaints mechanisms for class 1A and class 1B material.** **MCM 6:** All internet service providers must make available information to Australian end-users on their right to complain to a content provider and eSafety (including where a complaint to a content provider remains unresolved) about class 1A and class 1B material, or unsolicited electronic messages that promote such material. **MCM 7:** All internet service providers must make available, via their website, a link to eSafety's online content complaints reporting process. Note: this measure achieves the objective by pointing end-users to the most useful avenues to pursue their complaints, which are with the content provider or eSafety, given that the ISP cannot control, i.e., detect or remove, content or exert any control over the owner of the content.
Matter 9 Measures directed towards achieving the objective of ensuring that industry participants have scalable and effective policies, procedures, systems and technologies in place to effectively respond to: ● reports about class 1A material and class 1B material, as well as associated user accounts, and	**Outcome 9: Industry participants effectively respond to reports and complaints about class 1A and 1B material.** **MCM 8:** All internet service providers must either respond to any complaint it receives from an Australian end-user about class 1A and class 1B material or refer the complainant to eSafety. Note: also see above. ISPs will usually not be well-placed to respond to a complaint directly and the complainant may often be better served through other industry participants in the supply chain or eSafety. However, end-users can always complain to an ISP and can also complain to the TIO about an ISPs conduct and will, upon contacting an ISP and expressing dissatisfaction be advised of their rights to contact the TIO in accordance with the rules of the *Telecommunications Consumer Protections Code* (enforced by the ACMA).

● complaints about the handling of reports about class 1A material and class 1B material and codes compliance.	
Matter 10 Measures directed towards achieving the objective of ensuring that industry participants publish easily accessible and plain language policies, procedures and guidelines that set out how they handle class 1A material and class 1B material. Measures directed towards achieving the objective of ensuring that industry participants provide end-users with information about the safety issues associated with class 1A material and class 1B material.	**Objective 3: Industry participants will strengthen transparency of, and accountability for, class 1A and class 1B material.** **Outcome 10: Industry participants provide clear and accessible information about class 1A and class 1B material.** **MCM 9:** All internet service providers must make easily accessible to Australian end-users, plain-language information (also see Appendix A, item 53) on online safety in respect of class 1A and class 1B material, including information for parents/carers about how to supervise and control children's access and exposure to class 1A and class 1B material, and provide Australian- end-users information about the role and functions of the eSafety Commissioner. Note: ISPs do not handle class 1A/1B material as they have no control or visibility of such material and, consequently, do not publish such policies. However, this measure aims at that end-users can also find information on an ISP website that assists them with understanding which measures they can take to protect them and their children against such material as well as information about eSafety.
Matter 11 Measures directed towards achieving the objective of ensuring that industry participants publish annual reports about class 1A material and class 1B material, and their compliance with industry codes.	**Outcome 11: Industry participants publish annual reports about class 1A and 1B material and their compliance with this Code.** **MCM 10:** On request, all internet service providers must submit to eSafety a Code report which includes the following information: a) The steps that the provider has taken to comply with their applicable minimum compliance measures, b) An explanation as to why these measures are appropriate. c) the number of complaints in relation to class 1A and class 1B material an Internet service provider has responded to under minimum compliance measure 8; and d) the number of complaints received about compliance with this Code. Note: ISP do not remove material and, consequently, cannot publish annual reports in relation to such material. This measure aims at providing eSafety with the information about compliance with this Code without placing unnecessary regulatory burden on ISPs. It is noted that ISPs are also subject to the BOSE and any associated reporting obligations.
Additional Matters	Position 11 of the Position Paper outlines eSafety's expectation that the Codes will include a statement about how and when the Codes will be reviewed. eSafety also makes reference to the role of industry associations in the Position Paper (see p. 62, 63) These matters are addressed in section 7 of the Heads Terms, taking into account additional feedback provided by eSafety during the Code development process.

8. Equipment Online Safety Code (Class 1A and Class 1B Material)

This Code covers manufacturers, suppliers and installers and maintenance providers as defined in the OSA and operating system providers (defined in this Code).

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.

Approach to operating systems:

In addition – and going beyond the requirements and definition of the OSA – this Code also covers operating system providers for certain devices with higher risk profiles. The definitions of 'operating system' and 'OS provider' explain the details around these online participants. While operating systems have been defined as designated internet services, they have been included in this Code due to their logical connection to devices which allow access to online material via an internet carriage service.

Approach to risk of devices:

This Code defines different risk profiles for different categories of equipment. The Code defines devices as either 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. The approach to the risk profiles for equipment reflects subsequent feedback provided by eSafety to industry associations in the letter to industry associations dated 9 March 2023 (see Appendix A, item 56). For example, the definition of interactive (Tier 1) devices has been amended to make clear that displays for immersive environments are covered by the definition (see Appendix A, item 56). Importantly, this definition also puts beyond doubt that gaming devices with general internet browsing functionality are deemed interactive (Tier 1) devices and, therefore, must comply with the minimum measures assigned to this risk tier (see Appendix A, item 56).

The Code also contains specific measures for 'gaming devices' (devices designed to enable end-users to play online games with other end-users) and 'children's interactive devices' (devices targeted at children). The approach balances the need to appropriately identify devices that have the highest likelihood that class 1A and 1B material will be accessed on or distributed from those devices with the need to ensure that an inappropriate regulatory burden is imposed for low or no risk internet-connected devices with some form of browsing capability, which would include many IoT and semi-industrial devices/application (e.g., cars with typical touch screens to access radio, music, navigation etc. services).

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 1A/B 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.

Matter 1 Measures directed towards achieving the objective of ensuring that industry participants have scalable and effective policies, procedures, systems and technologies in place to take	**Objective 1: Industry participants will take reasonable and proactive steps to create and maintain a safe online environment for Australian end-users.** **Outcome 1: Industry participants take reasonable and proactive steps to prevent access or exposure to, distribution of, and online storage of class 1A material.** **Note: Outcome 1 does not refer to the detection of class 1A material as an entire class, noting that there are no systems and processes that can be**

reasonable and proactive steps to **detect and** prevent: ● access or exposure to, ● distribution of, and ● online storage of class 1A material.	**reliably deployed to detect the range of real or simulated extreme crime and violence materials that fall within class 1A.** By complying with the minimum compliance measures under Outcome 7, equipment providers will also meet the requirements of this Outcome.
Matter 2 Measures directed towards achieving the objective of ensuring that industry participants have scalable and effective policies, procedures, systems and technologies in place to take reasonable and proactive steps to prevent or limit: ● access or exposure to, and ● distribution of class 1B material.	**Outcome 2: Industry participants take reasonable and proactive steps to prevent or limit access or exposure to, and distribution of class 1B material.** By complying with the minimum compliance measures under Outcome 7, equipment providers will also meet the requirements of this Outcome.
Matter 4 Measures directed towards achieving the objective of ensuring that industry participants have scalable and effective policies, procedures, systems and technologies in place to take reasonable and proactive steps to limit the hosting of class 1A material and class 1B material in Australia.	**Outcome 4: Industry participants take reasonable and proactive steps to limit hosting of class 1A and 1B material in Australia.** This Outcome is not applicable to equipment providers and OS providers.
Matter 5 Measures directed towards achieving the objective of ensuring that industry participants have effective and scalable policies and procedures in place to facilitate consultation, cooperation and collaboration with other industry participants in respect of the removal, disruption and/or restriction of class 1A material and class 1B material, as well as accounts associated with this material.	**Outcome 5: Industry participants consult, cooperate and collaborate with other industry participants in respect of the removal, disruption and/or restriction of class 1A and class 1B material.** **MCM 1:** A manufacturer of an interactive (Tier 1) device, a manufacturer of a gaming device or an OS provider must take part in an annual forum organised and facilitated by one of the industry associations responsible for the development of this Code (as listed in the Head Terms) to discuss and share relevant issues, advances and best practice in online safety with other industry participants. **(Optional) Measure 2:** An industry participant who is: 1. a manufacturer of a secondary (Tier 2) device or a non-interactive (Tier 3) device. 2. a supplier, 3. a maintenance provider, or 4. an installation provider, may choose to attend the industry forum referred to in measure 1. Note: given the breadth of this industry section, a forum facilitated by industry associations is an effective way to encourage collaboration amongst participants in an open and transparent manner. This is most

	effectively targeted at manufacturers and OS providers given the vast numbers of suppliers.
Matter 6 Measures directed towards achieving the objective of ensuring that industry participants have effective and scalable policies and procedures in place which ensure communication and cooperation with the eSafety Commissioner with respect to matters about class 1A material and class 1B material, including complaints.	**Outcome 6: Industry participants communicate and cooperate with eSafety in respect of matters relating to class 1A and class 1B material, including complaints.** **MCM 3:** A manufacturer or supplier of an interactive (Tier 1) device 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. **MCM 4:** A manufacturer or an OS provider must share information with eSafety about material new features or functions released by the manufacturer or OS provider that the manufacturer or OS provider reasonably considers are likely to have a material positive or negative effect on the access or exposure to, distribution of, and online storage of class 1A or class 1B materials in Australia. Note: these measures respond to the Position Paper (see example measures p. 70) and feedback received by eSafety in the course of developing the Code (for example, see Appendix A, item 62), noting that these are proactive obligations supplementary to eSafety's power to respond directly to complaints about breaches of the Codes.
Matter 7 Measures directed towards achieving the objective of providing people with a range of technical tools and/or information to limit their access and exposure, and the access and exposure of children in their care, to class 1A material and class 1B material.	**Objective 2: Industry participants will empower people to manage access and exposure to class 1A and class 1B material.** **Outcome 7: Industry participants provide tools and/or information to limit access and exposure to class 1A and class 1B material.** **MCM 5:** A manufacturer of an interactive (Tier 1) device or gaming device must ensure that easily accessible information with respect to the safe use of those devices online by Australian end-users is available in the form of online safety resources. This information must include the role of eSafety, including a link to eSafety's complaints forms, and how Australian end-users can limit access to class 1A and class 1B materials when using that equipment. A manufacturer of children's interactive devices or gaming devices must ensure that easily accessible information is made available to Australian end-users about how to support online safety in a child's use of those devices. A supplier of interactive (Tier 1) devices (including children's interactive devices) and gaming devices must provide easily accessible information with respect to the safe use of that device (including how to support online safety in a child's use of that device) at or around the time of a sale, including at a minimum information about the role of eSafety, including a link to eSafety's complaints forms, and how Australian end-users can limit access to class 1A and class 1B materials when using that equipment. A maintenance provider or installation provider of interactive (Tier 1) devices must provide information with respect to the safe use of interactive (Tier 1) devices online by Australian end-users upon request.

	A manufacturer of gaming devices that enable Australian end-users to freely browse the internet must provide easily accessible information that this functionality exists. **MCM 6:** a) OS providers must develop and implement relevant tools where appropriate within operating systems that allow Australian end-users to help reduce the risk of harm to children when using interactive (Tier 1) devices. b) OS providers for a children's interactive device must set default safety settings for Australian end-users for children's interactive devices to the most restrictive privacy and location settings provided for on that device. c) OS providers must make tools available to Australian end-users to assist in restricting the unauthorised access to and operation of an adult's interactive (Tier 1) device by a child. d) A manufacturer or gaming devices must develop and implement appropriate tools that allow Australian end-users to help reduce the risk of harm to children when using the device. **MCM 7:** Suppliers interactive (Tier 1) devices must provide tools or training to staff to enable staff to appropriately respond to questions from Australian end-users regarding online safety, including available complaints mechanisms. **(Optional) Measure 8:** An industry participant who is a manufacturer of interactive (Tier 1) devices may provide additional information with respect to the safe use of interactive (Tier 1) devices online by Australian end-users. **(Optional) Measure 9:** A manufacturer of secondary (Tier 2) devices may take reasonable steps to consider features and/or settings that are designed to mitigate the risks to children when accessing material via the secondary (Tier 2) device. A manufacturer of secondary (Tier 2) devices may take reasonable steps to develop and implement tools that permit the use of online content filtering technologies and other safety features to help reduce the risk of harm to children. Note: these measures build upon example measures set out in the Position Paper (see p. 71) and are designed to enhance accessibility of safety tools and information made available to Australian end-users. In respect of safety information, the obligations in MCM 5 and 7 are targeted to the specific role played by participants in the supply chain to ensure that end-users are provided with relevant safety information so they can make informed purchasing decisions and are provided with after-sales support should they require it. In respect of safety tools, MCM 6 builds upon the example measures set out in the Position Paper with respect to default settings for children's interactive devices (see pp. 68-69 and 74), providing additional safeguards for this vulnerable end-user group and recognises the role that OS providers and manufacturers of gaming devices can play in providing safety tools and settings for all interactive (Tier 1) devices and gaming devices (respectively), noting these devices have higher risk profiles. MCM 5 and 6 have been revised in response to eSafety's letter of 9 February 2023 (see Appendix A, items 57-61).
Matter 8 Measures directed towards achieving the objective of providing	**Outcome 8: Industry participants provide clear and effective reporting and complaints mechanisms for class 1A and class 1B material.**

people with clear, easily accessible and effective: ● reporting mechanisms for class 1A material and class 1B material, as well as associated user accounts, and ● complaints mechanisms to address complaints about the handling of reports about class 1A material and class 1B material and codes compliance.	**MCM 10:** A manufacturer or supplier of interactive (Tier 1) devices must make available information to Australian end users on their right to complain to a content provider and/or eSafety (including where a complaint to a content provider remains unresolved) about class 1A and 1B material, or unsolicited electronic messages that promote such material. **MCM 11:** A manufacturer or supplier of interactive (Tier 1) devices must make available, via their online safety resources, a link to eSafety's online content complaints reporting form. Note: The measures for this matter take into consideration the inability of manufacturers and suppliers of interactive (Tier 1) devices to control the content accessible to end-users on their devices. These measures achieve the objective of Outcome 8 by pointing end-users to the most useful avenues to pursue their complaints, which are with the relevant content provider(s). These measures also build upon example measures set out in the Position Paper (see p. 71). See also section 7.4 of the Head Terms, which further strengthens these requirements concerning the handling of reports.
Matter 9 Measures directed towards achieving the objective of ensuring that industry participants have scalable and effective policies, procedures, systems and technologies in place to effectively respond to: ● reports about class 1A material and class 1B material, as well as associated user accounts, and ● complaints about the handling of reports about class 1A material and class 1B material and codes compliance.	**Outcome 9: Industry participants effectively respond to reports and complaints about class 1A and 1B material.** **MCM 12:** A manufacturer of interactive (Tier 1) devices or an OS provider must have a complaints mechanism to deal with complaints of potential Code breaches from Australian end-users. Note: also see above. These measures build upon example measures set out in the Position Paper (see p. 72). See also section 7.4 of the Head Terms, which further strengthens these requirements concerning the handling of reports.
Matter 10 Measures directed towards achieving the objective of ensuring that industry participants publish easily accessible and plain language policies, procedures and guidelines that set out how they handle class 1A material and class 1B material. Measures directed towards achieving the objective of ensuring that industry participants provide end-users with information about the safety issues associated with class 1A material and class 1B material.	**Objective 3: Industry participants will strengthen transparency of, and accountability for, class 1A and class 1B material.** **Outcome 10: Industry participants provide clear and accessible information about class 1A and class 1B material.** By complying with the minimum compliance measures under Outcome 7, equipment providers will also meet the requirements of this Outcome.
Matter 11	**Outcome 11: Industry participants publish annual reports about class 1A and 1B material and their compliance with this Code.**

Measures directed towards achieving the objective of ensuring that industry participants publish annual reports about class 1A material and class 1B material, and their compliance with industry codes.	**MCM 13:** A manufacturer of interactive (Tier 1) devices and/or OS providers must submit a Code report which as a minimum contains: a) The number of complaints from Australian end-users received by the manufacturer or OS provider about compliance with this Code through the complaint mechanisms implemented under MCM 12; b) The steps that the manufacturer and/or OS provider has taken to comply with the applicable minimum compliance measures; and c) An explanation as to why these measures are appropriate. **MCM 14:** On request by eSafety, a manufacturer of secondary (Tier 2) devices must submit a Code report which includes the following formation: a) An explanation as to why the manufacturer considers the device to be a secondary (Tier 2) device, b) The steps that the manufacturer has taken to comply with their applicable minimum compliance measures, and c) An explanation as to why these measures are appropriate. Note: manufacturers and OS providers cannot remove material, and, consequently, cannot publish annual reports in relation to such material. These measures provide eSafety with information about compliance with this Code and, for manufacturers of interactive (Tier 1) devices and OS providers, Code complaints, without placing unnecessary regulatory burden on manufacturers and OS providers. The revised Code introduced the requirement for manufacturers of interactive (Tier 1) devices to report on Code complaints and reduced the time frame for manufacturers of secondary (Tier 2) devices to respond to a request from 6 months to 2 months (see Appendix A, item 66).These measures are also supplementary to the Commissioner's power to investigate breaches of the Codes and to issue a reporting notice or make reporting determinations from all equipment providers and OS providers about their compliance with the BOSE.
Additional Matters	Position 11 of the Position Paper outlines eSafety's expectation that the codes will include a statement about how and when they will be reviewed. eSafety also makes reference to the role of industry associations in the Position Paper (see p62,63) These matters are addressed in section 7 of the Heads of Terms, taking into account additional feedback provided by eSafety during the code development process.

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

4.5.1. First public consultation: September 2022

In accordance with the requirement of section 140(1)(e)((i) and (3)of the OSA, the industry association facilitated a first public consultation of 30 days from 1 September to 2 October 2022.

4.5.2. Website / social media / general online communications for first public consultation

The industry associations published the first version of the draft Codes at the purpose-built website https://onlinesafety.org.au/ and accepted submissions through upload of submissions to this website from

1 September to 2 October 2022. Upon request, an extension for the first round of submissions was granted until 9 October 2022, and no submission received after this date has been declined or not been considered.

Submitters were required to accept the associations' Privacy Policy and could choose to consent to/decline publication of their respective submission.

Publication for public consultation of the draft Codes was advertised by the associations through various means, including social media channels, online newsletters and general communications to association members and non-members.[27]

The publication of the draft Codes was accompanied by an Explanatory Paper that provided a plain language:

- Executive Summary
- Background on the
  - Online Safety Act;
  - Parameters set out by the eSafety Commissioner's Position Paper;
  - Material covered by the Codes; and
  - Development process.
- Industry's approach to the Codes for class 1A and class 1B material, including the
  - Structure of the Codes;
  - Different requirements based on functionality of industry sectors; and
  - Requirements for proactive detection of class 1 materials.
- Next steps, including key submission dates and information; and
- Online safety objectives and outcomes as used in the Codes.

For further information, eSafety's Position Paper was published alongside the draft Codes and Explanatory Paper.

The website also contained short FAQ that anticipate some key questions in relation to the Codes and their operation.

All documents produced by the industry associations (draft Codes and Explanatory Paper) were available for download as a PDF and in Word format.

4.5.3. Targeted invitations for submissions to the first public consultation

In addition, the associations have emailed more than 200 individuals across the following organisations directly to invite submissions on the Codes (noting that the stakeholder list did at times include multiple representatives from some organisations). The invitations contained links to the publication websites with explanations as to how submitter could contribute to the Codes development process:

Organisations working to counter children's exploitation / terrorism:

1. Alannah & Madeleine Foundation
2. Australian Centre to Counter Child Exploitation (ACCCE)
3. Bravehearts
4. Global Internet Forum to Counter Terrorism (GIFCT)
5. Inhope

[27] Also refer to section 4.7 on consultation with the sections of the industry further below.

6. International Center for Missing & Exploited Children (ICMEC)
7. National Center for Missing & Exploited Children (NCMEC)
8. Tech Against Terrorism
9. The Carly Ryan Foundation
10. The Daniel Morcombe Foundation
11. WeProtect Global Alliance

Organisations representing children and young people:

12. Australian Research Alliance for Children and Youth
13. Australian Youth Affairs Coalition
14. Commissioner for Children and Young People South Australia
15. Multicultural Youth Advocacy Network (MYAN) NSW
16. National Children's Commissioner, Australian Human Rights Commission
17. Office of the Advocate for Children and Young People NSW
18. The Children and Young People Commissioner Australian Capital Territory
19. The Children's Commissioner Northern Territory
20. The Commission for Children and Young People Victoria
21. The Commissioner for Children and Young People Western Australia
22. The Commissioner for Children Tasmania
23. The Office of the Guardian for Children and Young People South Australia
24. The Office of the Public Guardian Queensland
25. UNICEF (United Nations Children's Fund)
26. Yourtown
27. Youth Affairs Council of Victoria
28. Youth Affairs Council of Western Australia

Organisations representing parents, carers, teachers and educators:

29. Australian Education Union (AEU) NT Branch
30. Australian Education Union (AEU) SA Branch
31. Australian Education Union (AEU) TAS Branch
32. Australian Education Union (AEU)ACT Branch
33. Australian Education Union Victoria
34. New South Wales Teachers Federation
35. Queensland Teachers Union
36. State School Teachers Union of Western Australia

Women's advocacy groups:

37. Communicare
38. Domestic and family violence groups
39. Domestic Violence Service Management (DVSM)
40. DVConnect Queensland
41. Economic Abuse Reference Group

42. Katherine Women's Legal Service
43. National Council of Women Australia
44. Relationships Australia
45. Safe Steps
46. United Nations (UN) Women
47. White Ribbon Australia
48. Women’s Legal Service NSW
49. Women's Services Network (WESNET)

Organisations representing sex workers:

50. Assembly Four
51. Australian Queer Archives
52. Eros Association
53. LGBTIQ+ Health Australia
54. Scarlett Alliance

Organisations in the area of safety technology / digital trust:

55. Digital Trust & Safety Partnership
56. Family Zone
57. Online Safety Tech Industry Association (OSTIA)
58. Safety Tech Innovation Network

Organisations representing consumers:

59. Australian Communications Consumer Action Network (ACCAN)
60. Choice
61. Consumer Action
62. Consumer Action Law Centre
63. Consumer Policy Research Centre
64. Consumers Association of South Australia
65. Consumers Federation of Australia
66. Queensland Consumers Association

Organisations representing legal interests and other advocacy areas:

67. Community Legal Centres Australia
68. Darwin Community Legal Service
69. Law Council of Asia & the Pacific
70. Law Council of Australia
71. Law Society of Australian Capital Territory
72. Law Society of New South Wales
73. Law Society of Tasmania
74. Law Society of the Northern Territory
75. Law Society of Victoria
76. Law Society of Western Australia

77. Public Interest Advocacy Centre
78. Queensland Law Society

Representatives from academia:

79. Allens Hub for Technology, Law and Innovation
80. Australian National University (ANU) College of Law
81. Australian National University (ANU) Tech Policy Design Centre
82. Australian Research Council (ARC) Centre of Excellence for the Digital Child
83. Australian Strategic Policy Institute (ASPI)
84. Berkeley University
85. Canberra University
86. Charles Sturt University, Centre for Law and Justice
87. Harvard University
88. Latrobe University
89. Minderoo Tech & Policy Lab
90. Queensland University of Technology (QUT) Digital Media Research Centre
91. Royal Melbourne Institute of Technology (RMIT) University
92. Stanford University
93. Swinburne University
94. University of California, Irvine
95. University of Melbourne
96. University of New South Wales (UNSW), School of Law, Society & Criminology
97. University of Ottowa
98. University of Technnology Sydney (UTS)
99. University of the Sunshine Coast
100. University of Western Australia
101. Western Sydney University (UWS) Young & Resilient Centre

Organisations representing user and/or producers of services and devices affected by the Codes:

102. .auDA
103. ACT | The App Association
104. Asia Internet Coalition (AIC)
105. Australian Banking Association
106. Australian Chamber of Commerce and Industry
107. Australian Copyright Council
108. Australian Industry Group
109. Australian Information Industry Association
110. Australian Society of Authors
111. Business Council of Australia
112. Computer & Communications Industry Association (CCIA)
113. Council of Small Business Organisations Australia (COSBOA)
114. Information Technology Industry Council (ITIC)

115. Internet Association of Australia
116. IoT Alliance Australia
117. Music Australia
118. Screen Australia
119. Standards Australia
120. Tech Council of Australia
121. Tech UK
122. The Australian Digital Alliance
123. Universities Australia

Civil society organisations (digital rights and policy separately below):

124. Australian Community Managers
125. Australian Council for Civil Liberties
126. Australian Privacy Foundation
127. IIS Partners
128. Reset Australia

Organisations working in the area of digital rights / policy:

129. AccessNow
130. American Civil Liberties Union
131. Australia’s Internet Governance Forum
132. Australian Seniors Computer Clubs Association (ASCCA)
133. Brookings Institute
134. Center for Democracy & Technology (CDT)
135. Center for Information Policy Leadership
136. Centre for Digital Wellbeing
137. Centre for Responsible Technology
138. Digital Rights Watch
139. Electronic Frontier Foundation
140. Electronic Frontiers Australia
141. Future of Privacy Forum
142. Global Network Initiative (GNI)
143. Human Rights Watch
144. Index on Censorship
145. Internet Australia
146. Internet Society
147. Knight First Amendment Institute
148. LGBT Tech
149. Ranking Digital Rights

Australian Government agencies/departments (if not already listed):

150. Australian Communications and Media Authority

151. Australian Human Rights Commission
152. Australian Institute of Criminology
153. Department of Home Affairs
154. Department of Infrastructure, Transport, Regional Development, Communications and the Arts
155. Office of the Australian Information Commissioner

4.5.4. Roundtable first public consultation

Furthermore, during the second period of public consultation, on 13 September 2022, the six associations convened a Stakeholder Roundtable to discuss key aspects and questions in relation to the draft Codes published for public consultation. The following stakeholders were considered to have particular expertise relevant to those questions and were invited to attend the Roundtable:

1. .auDA
2. Access Now
3. Alannah & Madeleine Foundation
4. Assembly Four
5. Australian Communications Consumer Action Network (ACCAN)
6. Business Council of Australia (BCA)
7. Consumer Action
8. Council of Small Business Organisations Australia (COSBOA)
9. Daniel Morcombe Foundation
10. Digital Rights Watch
11. Digital Trust & Safety Partnership
12. Electronic Frontiers Australia
13. Global Network Initiative (GNI)
14. International Center for Missing & Exploited Children (ICMEC)
15. Law Council of Asia & the Pacific
16. Law Council of Australia
17. Queensland University of Technology (QUT) Digital Media Research Centre
18. Scarlett Alliance
19. Swinburne University
20. Tech Against Terrorism
21. The Carly Ryan Foundation
22. University of New South Wales (UNSW), School of Social Sciences
23. Western Sydney University (UWS) Young & Resilient Centre

As observers:

24. Department of Infrastructure, Transport, Regional Development, Communications and the Arts
25. Office of the eSafety Commissioner

4.5.5. Research commissioned by Communications Alliance and DIGI

To further strengthen insights from consultation and in line with the Position Paper's recommendations15, DIGI and Communications Alliance commissioned research undertaken by Resolve Strategic, to provide an evidence-base of the expectations of the general Australian public. A nationally representative study on issues relevant to the Codes was undertaken during the consultation period from 13 to 18 September 2022.16 The research results were presented to a group of Government stakeholders on 10 October 2022 and the full report and methodology published, alongside the submissions received (with permission to publish), on https://onlinesafety.org.au/submissions/.

4.5.6. Response to first public consultation

The industry associations received 88 submissions of which 41 were from organisations/government agencies/companies and 47 from the general public.

The industry associations published 63 submissions on their website https://onlinesafety.org.au/: 34 submissions from organisations/government agencies/companies (i.e., 7 declined permission to publish) and 29 from the general public (16 declined permission to publish, 2 contained abusive language and expletives).

4.5.7. Second public consultation: 9 March to 23 March 2023

In response to the feedback received in the letters by eSafety dated 9 February 2023, the industry associations made substantial revisions to the draft Codes that were submitted to eSafety in November 2022.

The industry associations asked eSafety for an extension to conduct a second 30-day consultation on the draft Codes to give the community and stakeholders an opportunity to express their views on the newly revised Codes. A short extension was granted until 31 March 2023 which allowed for a 14-day consultation period.

4.5.8. Website / social media / general online communications for second round of public consultation

Revised versions of the Codes (with revisions marked up in the text) were published on https://onlinesafety.org.au/. The industry associations accepted feedback through upload of submissions to this website from 9 March to 31 March 2023.

As for the first round of public consultation, submitters to the second public consultation were required to accept the associations' Privacy Policy and could choose to consent to/decline publication of their respective submission.

Prior to the commencement of the second round of public consultation, the industry associations published the version of the draft Codes submitted to eSafety on 18 November 2022 , together with eSafety's letters to industry dated 9 February 2023 and the application for registration on https://onlinesafety.org.au/ to provide interested stakeholders with additional transparency over the process.

The publication of the draft Codes was accompanied by a Supplementary Explanatory Paper that provided a plain language explanation of the key revisions made to the Codes in response to eSafety's feedback dated 9 February 2023.

Publication of the revised draft Codes was advertised by the associations through various means, including social media channels, online newsletters and general communications to association members and non-members.[28]

All documents produced by the industry associations (revised Codes and Supplementary Explanatory Paper) were available for download as a PDF and in Word format.

4.5.9. Targeted invitations for submissions to the first public consultation

Prior to the second public consultation, all invitees to the Roundtable during the first public consultation (refer to section 4.5.4) and all 88 individuals/organisations/government agencies that made a submission during the first public consultation (refer to section 4.5.6) were emailed nine days in advance of the commencement of the second public consultation to make them aware of the upcoming consultation (including dates). The notice of the upcoming consultation contained links to the publication websites with a brief summary on the process between November 2022 and the commencement of the second public consultation and explanations as to how submitter could further contribute to the Codes development process.

In addition, on commencement of the second public consultation, the associations emailed all 88 submitters of the previous public consultation as well as the same 200 individuals across the 155 organisations listed in section 4.5.3 above (first public consultation) to invite submissions on the revised Codes. Emails were also sent to all invitees of the Roundtable during the first public consultation (with the exception of eSafety as the Office was well-informed about the process). The invitations contained, in essence, the same information as the advance notices described above.

4.5.10. Briefing Session/Q & A for second public consultation

During the period of the second public consultation, the industry associations invited the same expert stakeholders that were invited to the Roundtable during the first public consultation (refer to section 4.5.4) to a Briefing Session/Q & A for expert stakeholders. eSaftey attended as an observer.[29]

A Summary of Discussion was provided to all stakeholders for review and, subsequently, as a final record of the meeting.

4.5.11. Response to second public consultation

The industry associations received 25 submissions of which 23 were from organisations/government agencies/companies and 2 from the general public.

The industry associations published 24 submissions on their website https://onlinesafety.org.au/: 22 submissions from organisations/government agencies/companies (i.e., 1 declined permission to publish) and 2 from the general public.

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

All submissions to the first and second public consultation were given due consideration in the same manner by the industry associations and the members of the working groups that drafted the Codes through the following process:

- All submissions were read, and all key feedback was extracted into a submissions log.

[28] Also refer to section 4.7.3 on consultation with the sections of the industry further below.
[29] DITRDCA did not attend but had been briefed separately by DIGI and Communications Alliance.

- Subsequently, the industry participants previously involved in the drafting of the Codes methodically considered the feedback (by subject matter) and made changes to the Codes, where deemed appropriate.
- Industry members provided commentary against all feedback received (also where no change to the Codes was made in response to the submitter's feedback), seeking to address the feedback.
- The second submissions log and associated responses were published on https://onlinesafety.org.au/submissions/ along with the submissions).

Please refer to the enclosed documents '*Submission log and associated responses for 1st public consultation'* and *'Submission log and associated responses for 2nd public consultation'* for a complete overview of the submissions logs and associated industry responses. Please note that these logs and associated responses do not include submissions for which the submitter has declined permission to publish. However, we assure eSafety that all submissions have been considered in the same manner and with the same rigour.

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

4.7.1. Website / social media / general online communications

Please refer to section 4.5.2 and 4.5.6 above.

4.7.2. Development of the Codes through a broad cross-section of participants in the respective sections of the online industry

The industry associations developed the Codes through a highly collaborative process. The following steps were taken to ensure broad participation in the development process, including beyond the membership of the six industry associations:

- The industry associations invited their respective members to participate in the Codes development process.
- Where gaps in membership were identified, industry associations reached out to invite non-members to the Codes development process (at no cost or membership requirements).
- 65 industry participants either directly participated in the drafting of the Codes or were regularly engaged during the development of the Codes, with a further 220 member organisations being consulted via their respective industry association in the drafting process (i.e., not included in the list of organisations consulted above). 14 industry participants directly involved in the drafting of the Codes are not members of one of the six industry associations that received a section 141 notice.

  It should be noted that industry participants usually provide several services (sometimes more than 40) across different industry sections (often across different brands), thereby necessitating the involvement of many more individuals than the number of industry participants indicated above. The industry associations estimate the number of services covered by the directly involved industry participants to be in excess of 350 (excluding services represented by consulting firms or industry associations). A list of the industry participants (i.e., organisations) involved in the process (outside public consultation) is provided at Annex 4.

[30] The industry associations requested that eSafety allow time for a 30-day consultation on the revised Codes, following receipt of the letters of 9 February 2023. eSafety responded that the Codes must be resubmitted by 31 March 2023. This meant that the time for consultation was reduced to 14 days, taking into account the need for industry to develop revised Codes for public consultation, respond to submissions and submit Codes for registration along with the required registration documentation.)

- In the period from mid-May 2021(with the most intensive work commencing after the publication of the Position Paper in late September) to 18 November 2022, the industry participants met (usually in working groups, not counting smaller informal meetings) 154 times for a total of more than 182 hours to develop the Codes for public consultation, consider eSafety's (at all stages of the process) and consider feedback from other stakeholders.
- In addition, in the same time period, the Steering Group comprised of key representatives of the six industry associations met more than 40 times for more than 42 hours (excluding hours the Steering Group met with eSafety) to guide the Codes development process, coordinate communication with stakeholders, including eSafety, ensure consistency of approach and oversee the governance of the process.
- In the period between 9 February and 31 March 2023, the industry participants met in working groups for a total of more than 20 hours to consider eSafety's feedback, develop the revised Codes for the second public consultation and consider the feedback received from other stakeholders. This time does not include time spent on informal sessions or individually assigned drafting tasks.
- In that same period, members of the Steering Group met with eSafety twice (not counting the Briefing Session/Q&A) for a further in-depth discussion of specific, critical issues.

4.7.3. Consultation with participants in the respective sections of the online industry

In addition to the Codes drafting process itself, which given the broad reach with which it was conducted arguably already constitutes a form of consultation[31], the industry associations undertook the following measures to repeat or amplify the invitation to make a submission to the first and second round of public consultation in response to the draft Codes:

- At the beginning of the consultation period, which ran concurrently to the consultation for the public, the industry associations again invited their members to make a submission in relation to the published draft Codes.
- In addition, at the same time, the industry association reached out to other organisations/associations that were reasonably believed to be able to assist with amplifying the invitation for submissions.
- The industry associations also re-connected with individual non-member participants in the respective online sections to again invite submissions and address potential questions.

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

The same process as in section 4.6 above was followed for submissions received from the first and second round of public consultation. The submissions and associated responses are recorded in the two logs for submissions received from the public.

Where changes to the Codes were being proposed that specifically affected industry participants not represented by the industry associations, the industry associations sought to contact those industry participants and seek their input to the extent possible.

[31] Refer to p. 56/57, eSafety Commissioner, *Development of industry codes under the Online Safety Act, Position Paper*, September 2021

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

The eSafety Commissioner and/or the Office of the eSafety Commissioner were extensively consulted during the development of the Codes and included the following key engagement points:[32]

- Representatives of the associations repeatedly sought engagement with eSafety to develop early thinking on draft Codes as early as 1 March 2021.
- Industry associations, individual participants of relevant industry sections and stakeholders and eSafety continued to engage and participated in four formal meetings – in addition to any informal meetings or email correspondence – in the time from May to September 2021:
  - 21 May 2021
  - 25 June 2021
  - 5 Aug 2021
  - 28 Sept 201
- Those engagements covered areas of possible code development models, suitable engagement models given the large number of industry participants involved and the breadth of sections covered, potential code architectures, code content and other related matters. The industry associations involved (at that time mostly Communications Alliance, DIGI, IGEA and BSA) provided responses to several sets of questions from eSafety to assist eSafety with the development of the Position Paper.
- On 29 September 2022, eSafety released its Position Paper which conveyed eSafety's understanding and expectation of the scope of material to be covered in the Codes and the underlying Objectives and Outcomes. The Position Paper also contained a detailed list of example measures of how eSafety proposed those Outcomes could be achieved.
- Subsequent to the release of the Position Paper - and in parallel to already ongoing drafting work - the Steering Group and eSafety constructively engaged over the Objectives and Outcomes put forward in the Position Paper. In late December 2021, the original Objectives and Outcomes were adopted, or consensus could be reached for ten of the eleven Outcomes, with the Outcome 1 being adopted by the Steering Group with modifications.
- The Steering Group also committed to working with eSafety's eleven positions on codes development, thereby again demonstrating a general willingness to engage with the ex-ante expectations of the regulator.
- The Steering Group agreed with eSafety on the sequential development of two sets of Codes to cover different types of online material: a first set of Codes to cover class 1A and class 1B material, and a second set of Codes to cover class 1C and class 2 material.
- The Steering Group agreed to a timeline[33] (provided at Annex 3) for the delivery of the Codes by 21 July 2022, including interim milestones and deliverables, with eSafety and provided frequent updates about progress upon request.
- On 14 February 2022, as agreed per the (updated) timeline, the Steering Group provided a first complete draft set of Codes (including Head Terms) to eSafety.
- Feedback on the first draft Codes (including Head Terms) was received in tranches in the period 11 March to 31 March 2022.
- The Steering Group and industry participants closely engaged with eSafety over the following weeks over the feedback provided and the way forward, including in formal meetings on 25

[32] The consultation with eSafety (as the regulator of the Codes, if registered) has been substantially more extensive than what some of the participating industry associations have ever undertaken in comparable Code development scenarios. In its history, Communications Alliance has developed and revised more than 80 Codes.

[33] Timeline later revised upon mutual agreement with eSafety (after variation of notice).

February, 25 March and 1 April 2022. It was noted that, as the complexity of the first draft had necessitated a longer than anticipated feedback period, additional time would be required for industry to deliver the final Codes. eSafety agreed to vary the notices to the respective industry associations to provide for a new due date for registration, contingent on a second pre-public consultation draft of the Codes being provided to eSafety.

- On 11 April 2021, the Commissioner issued all six industry associations with the respective section 141 notices with a due date for Code submission by 9 September 2022.
- The Steering Group agreed a revised timeline (also provided at Annex 3) with eSafety, including the delivery of a second pre-public consultation draft of the Codes to eSafety.
- The Steering Group provided the second set of draft Codes in tranches in the period from 13 May to 6 July 2022. This draft was accompanied by detailed tables (on a per Code basis) outlining how the industry associations had considered the feedback provided by eSafety on the first draft Codes.
- On 23 June 2022, the eSafety Commissioner formally varied the notices with a new due date for Codes submission by 18 November 2022. No new formal timeline was agreed thereafter. However, the Steering Group kept eSafety regularly informed about its proposed next milestones, particularly the release of the Codes for public consultation.
- To provide further opportunity for discussion and clarification of the drafting submitted with the second draft Codes, the Steering Group, select expert industry participants and eSafety engaged in special workshops on key areas of interest, i.e.,:
    - 1 July 2022: Classification (2 hours)
    - 4 July 2022: Equipment, internet service providers (2 hours)
    - 21 July 2022: Relevant electronic services, designated internet services, hosting services (3 hours)
    - 22 July 2022: Proactive detection (2 hours)
- Feedback on the second draft Codes was received from 27 May, with the majority being provided on 12 August 2022. This feedback was considered as part of the feedback received during public consultation (1 September - 2 October) to ensure a balanced consultation process.
- On 13 September 2022, the Steering Group facilitated a Stakeholder Roundtable (also refer to section 4.5.4), with eSafety and the Department of Infrastructure, Transport, Regional Development, Communications and the Arts as observers.
- On 10 October 2022, DIGI and Communications Alliance convened a Roundtable to brief Government stakeholders, including eSafety, on the research commissioned by DIGI and Communications Alliance on the expectations of the general Australian public in relation to issues relevant to the Codes. eSafety was provided with the full report and methodology on 25 October 2022.
- In late October 2022, the Steering Group and individual industry participants considered substantial feedback provided by eSafety in relation to key issues and concepts.
- On 21 March 2023, DIGI and Communications Alliance convened a Briefing Session/Q & A to brief expert stakeholders, including eSafety, on the most recent revisions to the draft Codes and to offer an opportunity to ask questions on those revisions.
- On 22 March and 27 March, DIGI and Communications Alliance met with eSafety to discuss the revised Codes and areas of specific concern.
- Excluding informal conversations and email correspondence, smaller informal meetings and Roundtables, the Steering Group and/or the Steering Group together with industry participants have met with eSafety for a combined total of more than 33 hours (in addition to the 42 hours of Steering Group meetings mentioned above) during the development of the Codes.

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

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

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

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

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

Position 5: Industry associations will prepare all codes for registration by July 2022 or adopt a phased approach to codes development. Under the phased approach, codes dealing with the most harmful content must be lodged for registration by July 2022, and codes dealing with content which is inappropriate for children must be lodged for registration by December 2022.[34]

Position 6: Industry associations will limit the number of codes developed.[35]

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

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

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

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

Position 11: The codes will include a review mechanism.

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

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

Annex 2: Objectives and Outcomes as per Position Paper/per consensus between eSafety and industry and as adopted throughout the Codes

Objectives and Outcomes in Position Paper/revised Outcomes as per consensus between eSafety and industry	**Objectives and Outcomes as adopted throughout the Codes**
Objective 1: Industry participants will take reasonable and proactive steps to create and maintain a safe online environment for Australian end-users.	**Objective 1:** Industry participants will take reasonable and proactive steps to create and maintain a safe online environment for Australian end-users.
Outcome 1: Industry participants take reasonable and proactive steps to detect and[36] prevent access or exposure to, distribution of, and online storage of class 1A material.	**Outcome 1:** Industry participants take reasonable and proactive steps to prevent access or exposure to, distribution of, and online storage of class 1A material.
Outcome 2: Industry participants take reasonable and proactive steps to prevent or limit access or exposure to, and distribution of class 1B material.	**Outcome 2:** Industry participants take reasonable and proactive steps to prevent or limit access or exposure to, and distribution of class 1B material.
Outcome 4[37]: Industry participants take reasonable and proactive steps to limit hosting of class 1A and 1B material in Australia.	**Outcome 4:** Industry participants take reasonable and proactive steps to limit hosting of class 1A and 1B material in Australia.
Outcome 5: Industry participants consult, cooperate and collaborate with other industry participants in respect of the removal, disruption and/or restriction of class 1A and class 1B material.	**Outcome 5:** Industry participants consult, cooperate and collaborate with other industry participants in respect of the removal, disruption and/or restriction of class 1A and class 1B material.
Outcome 6: Industry participants communicate and cooperate with eSafety in respect of matters relating to class 1A and 1B material, including complaints.	**Outcome 6:** Industry participants communicate and cooperate with eSafety in respect of matters relating to class 1A and 1B material, including complaints.
Objective 2: Industry participants will empower Australian end-users to manage access and exposure to class 1A and class 1B material.	**Objective 2:** Industry participants will empower Australian end-users to manage access and exposure to class 1A and class 1B material.
Outcome 7: Industry participants provide tools and/or information to limit access and exposure to class 1A and 1B material.	**Outcome 7:** Industry participants provide tools and/or information to limit access and exposure to class 1A and 1B material.

[36] The Codes do not include blue language in Outcome 1.

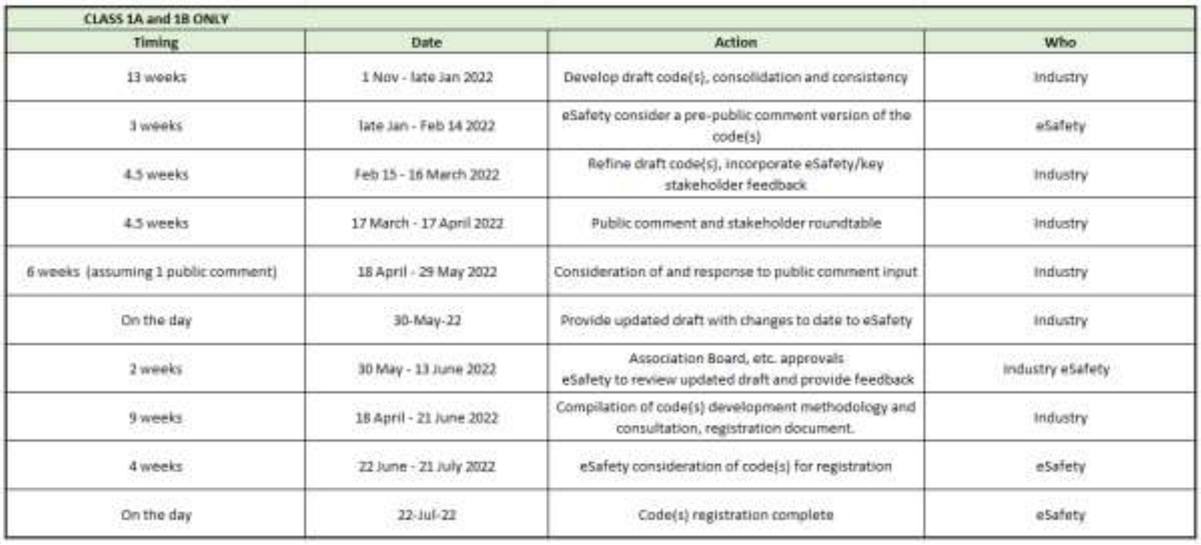
[37] **Outcome 3** has been deliberately omitted as it pertains to Class 2 material only which is not subject to the Codes.

Outcome 8: Industry participants provide clear and effective reporting and complaints mechanisms for class 1A and 1B material.	**Outcome 8**: Industry participants provide clear and effective reporting and complaints mechanisms for class 1A and 1B material.
Outcome 9: Industry participants effectively respond to reports and complaints about class 1A and 1B material.	**Outcome 9:** Industry participants effectively respond to reports and complaints about class 1A and 1B material.
Objective 3: Industry participants will strengthen transparency of, and accountability for class 1A and class 1B material.	**Objective 3:** Industry participants will strengthen transparency of, and accountability for class 1A and class 1B material.
Outcome 10: Industry participants provide clear and accessible information about class 1A and class 1B material	**Outcome 10:** Industry participants provide clear and accessible information about class 1A and class 1B material
Outcome 11: Industry participants publish annual reports about class 1A and 1B material and their compliance with this Code.	**Outcome 11:** Industry participants publish annual reports about class 1A and 1B material and their compliance with this Code.

Annex 3: Timelines

Timeline 1:

Timeline as agreed between eSafety and the Steering Group in mid-December 2021. In January 2022, it was agreed to push the delivery date of the draft Codes to eSafety to 14 Feb 2022 (but maintain the deadline of 21 July 2022).

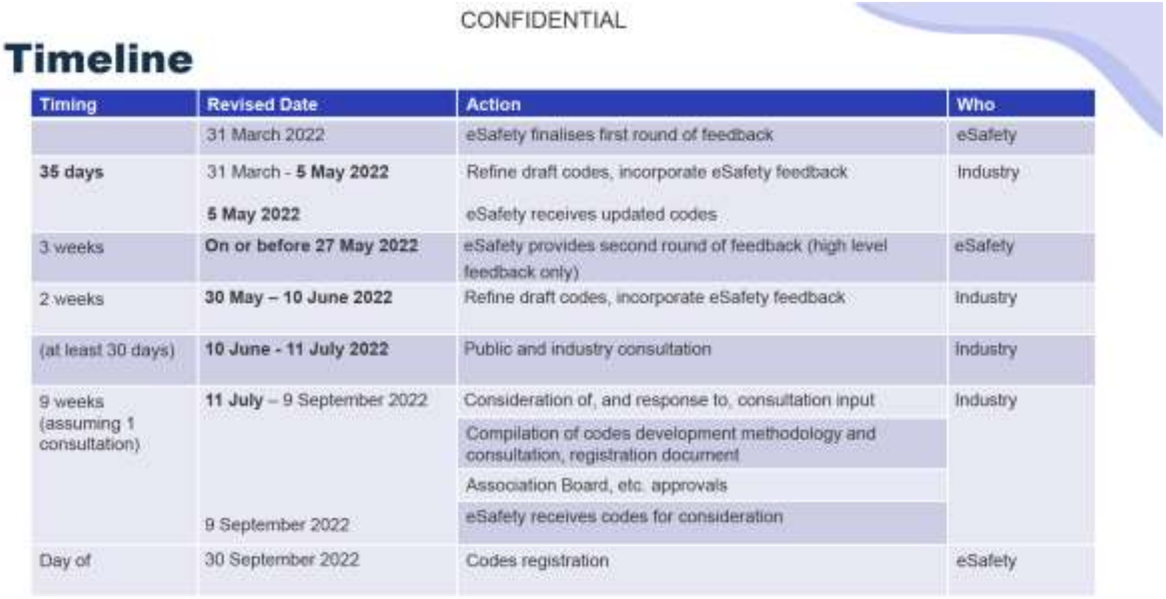


CLASS 1A and 1B ONLY

Timing	Date	Action	Who
13 weeks	1 Nov - late Jan 2022	Develop draft code(s), consolidation and consistency	Industry
3 weeks	late Jan - Feb 14 2022	eSafety consider a pre-public comment version of the code(s)	eSafety
4.5 weeks	Feb 15 - 16 March 2022	Refine draft code(s), incorporate eSafety/key stakeholder feedback	Industry
4.5 weeks	17 March - 17 April 2022	Public comment and stakeholder roundtable	Industry
6 weeks (assuming 1 public comment)	18 April - 29 May 2022	Consideration of and response to public comment input	Industry
On the day	30-May-22	Provide updated draft with changes to date to eSafety	Industry
2 weeks	30 May - 13 June 2022	Association Board, etc. approvals eSafety to review updated draft and provide feedback	Industry eSafety
9 weeks	18 April - 21 June 2022	Compilation of code(s) development methodology and consultation, registration document.	Industry
4 weeks	22 June - 21 July 2022	eSafety consideration of code(s) for registration	eSafety
On the day	22-Jul-22	Code(s) registration complete	eSafety

Timeline 2:

Timeline as agreed between eSafety and the Steering Group on 26 April 2022.



CONFIDENTIAL

Timeline

Timing	Revised Date	Action	Who
	31 March 2022	eSafety finalises first round of feedback	eSafety
35 days	31 March - **5 May 2022** **5 May 2022**	Refine draft codes, incorporate eSafety feedback eSafety receives updated codes	Industry
3 weeks	**On or before 27 May 2022**	eSafety provides second round of feedback (high level feedback only)	eSafety
2 weeks	**30 May – 10 June 2022**	Refine draft codes, incorporate eSafety feedback	Industry
(at least 30 days)	**10 June - 11 July 2022**	Public and industry consultation	Industry
9 weeks (assuming 1 consultation)	**11 July** – 9 September 2022 9 September 2022	Consideration of, and response to, consultation input Compilation of codes development methodology and consultation, registration document Association Board, etc. approvals eSafety receives codes for consideration	Industry
Day of	30 September 2022	Codes registration	eSafety

Note subsequent extension (and consequential changes to timelines) of the deadline for submission for registration of the Codes as per revised section 141 notice.

Annex 4: List of industry participants that either directly participated in drafting of the Codes or were regularly engaged during the development of the Codes

***** These organisations are not members of one of the six industry associations that received a section 141 notice.

AARNet	NBN Co
Adobe	*Netflix
Amazon	NEXTDC
Amazon Web Services	*Nextdoor
Apple	Nintendo
auDA	Oppo Mobile
Aussie Broadband	Optus
*****Auttomatic	Oracle
Baker McKenzie	Panasonic
*****Bumble	*****Pinterest
*****Cloudflare	*****Reddit
Dropbox	Salesforce
eBay	Samsung
Electronic Arts	Snap
Foxtel	Sony
*****Glassdoor	Sony Interactive Entertainment
Google	*****Spotify
Hisense	Symbio
HMD Global	Telstra
IBM	Tiktok
IoT Alliance Australia	TPG Telecom
KPMG	Twilio

*Lego Life	Twitch
Lenovo	Twitter
LG	*Uber
LinkedIn	Ubisoft
Linktree	Vocus
*LITT	*Wikimedia
Macquarie Telecom	Woolworths
*Match Group	Yahoo
Meta	Zoom
Microsoft	ZTE

Appendix A: Industry associations response to areas of concern as communicated by eSafety in letters to industry associations dated 9 March 2023

Relevant part of Code/ sections/outcomes	eSafety feedback	Industry response to feedback
Social Media Services		
1. Scope	eSafety considers it is unlikely the draft SMS Code would satisfy s 140(1)(b) of the Act because the code is expressed to apply in respect of 'Australian end-users' and not to the relevant group of providers, described in s 135(2)(a), or to the relevant online activity, described in s 134(a).	Section 2.1 of the Head Terms has amended the definition of Australian end-user to mean end user in Australia.
2. Matter 1: **Measures directed towards achieving the objective of ensuring that industry participants have scalable and effective policies, procedures, systems and technologies in place to take reasonable and proactive steps to access or exposure to, distribution of, and online storage of class 1A material.**	eSafety considers that in order to provide appropriate community safeguards for Matter 1, the draft SMS Code would need to ensure, at a minimum: (a) all Tier 1 SMS (regardless of whether they meet the definition of Very large SMS) use systems, processes and/or technologies to detect and remove known pro-terror material/ Terrorist and Violent Extremist Content (TVEC); and (b) Tier 1 SMS make ongoing investment in systems and processes and technologies in relation to class 1A material (including first generation CSAM2	In relation to a) Clause 9 has been redrafted to extend to all Tier 1 SMS services. A new definition has been added to the definition of known pro-terror material. Note that eSafety was asked to provide feedback to industry about the term TVEC and advised as follows: *eSafety recognises that there is no universally accepted definition of TVEC but have previously suggested to the industry associations that it may be a useful term because it is used by both the GIFCT and Tech Against Terrorism*[38]. While the terms TVEC is used by GIFCT and Tech against Terrorism they do not define this term and it is not used in the National Classification Schemes. As suggested by eSafety we have included reference to indicators of terrorist material in the GIFCT taxonomy for its database of hashed material. The definition of known pro-terror material in section 2.1 has been revised to ensure that known material may include Class 1A material that are associated with: i. terrorist and violent extremist activity on the United Nations List of Imminent Credible Threats may be taking place online; ii. content produced by terrorist entities on the United Nations Security Council's Consolidated Sanctions List; It should be noted that whether materials on these databases is in fact Class 1 A material is an assessment that must be made in accordance with the National Classification Scheme which in turn refers to terrorist acts within the meaning of the Criminal Code. Industry considers this is necessary to ensure the Codes are consistent with the Classification scheme (and the approach that was set out in the Position Paper). Industry considers that it is critical any changes to the basic concept of pro-terror material should be made as part of the review of the National Classification scheme so that they are transparent to the public.

[38] Email eSafety to DIGI 21 February 2023

		In relation to b) see revised Clause 10 that required Tier 1 SMS providers to take action and invest in systems, technologies and processes to disrupt and deter CSAM and pro-terror material. This commitment requires SMS providers to invest in systems processes and technologies that aim to prevent end-users from using social media services to create, post or disseminate CSAM and pro-terror material. These obligations extend to first generation CSAM and pro-terror materials.
3. Matter 4: **Measures directed towards achieving the objective of ensuring that industry participants have scalable and effective policies, procedures, systems and technologies in place to take reasonable and proactive steps to limit the hosting of class 1A material and class 1B material in Australia.**	Having regard to the measures proposed for Matter 1 and Matter 2 and the concerns set out above, our preliminary view is that in order to provide appropriate community safeguards for Matter 4, the draft SMS Code would need to ensure it contains, at a minimum, the steps in paragraph 16 above.	See response in 2.
4. Matter 11: **Measures directed towards achieving the objective of ensuring that industry participants publish annual reports about class 1A material and class 1B material, and their compliance with industry codes.**	eSafety’s preliminary view is that the proposed 6 months’ response timeframe in MCM 33 is likely to prevent MCM 33 from providing appropriate community safeguards in relation to this matter, and suggests that a response timeframe of 2 months would be appropriate.	MCM 33 has been amended to provide a response timeframe of 2 months.
5. Limitation clause in the head terms	There is a risk that as drafted, clause 6.1(c) could create broad exclusions from code commitments. eSafety considers it important that service providers consider how code compliance could be achieved by alternative mechanisms or by remedying the design. Clause 6.1 (e)(iii), (h), (i) and (j) and clause 6.2 each limit the codes from requiring industry participants to take action or engage in conduct that would violate other laws. As previously communicated to Industry Bodies, eSafety considers that the blanket exclusions are not desirable and it would be more appropriate for service providers to communicate specific concerns to eSafety when a specific issue arises as to how compliance with a code requirement may breach a law and/or explore alternative approaches to meeting the minimum compliance measures of the code while still meeting other legal requirements.	Section 6.1 has been revised so that it is not phrased as a limitation on compliance i.e., this Code does not require any industry participant to undertake steps that could do the listed acts including undermining encryption. 6.2 has been added to make clear this does not mean participants are exempt from complying with the Code but aids their interpretation of measures. Where Industry has concerns it can raise these with eSafety or take an alternative approach to compliance In relation to the second point it is important that it is clear to industry participants that the Code is a subsidiary regulatory instrument and does not override other Australian laws. This is standard in other industry Codes. See for example, 1.1.2 of the Telecommunications Consumer Protections Code’ If there is a conflict between the requirements of the Code and any requirement imposed on a Supplier by statute or by a Regulator, the Supplier will not be in breach of the Code by complying with the statute or the requirements of the Regulator’. This provision is particularly important in the context of the ongoing review of the National Classification Scheme, which contains the fundamental regulatory principles upon which this Code depends and the widely scoped review of the Privacy Act 1988 (Cth) that includes proposals that would potentially restrict providers from collecting and using some categories of data for the purpose of complying with this Code..
6. Risk assessment	In relation to the risk assessment	We note that the risk assessment methodology was

methodology	methodology in the draft SMS Code, eSafety is concerned that SMS providers may underestimate their risk level if application of the tiers and relative weighting of the factors listed in the table is left to industry participants to determine without further guidance. The process to identify applicable compliance measures is entirely reliant on an effective risk assessment. While SMS providers are required to demonstrate that the compliance measures they have adopted are reasonable, it would be difficult for eSafety to critically assess risk profile assigned by the SMS provider to the online activity if those risk factors are open to broad interpretation and the risk profile adopted do not accurately reflect the risk of harm.	designed to take into account eSafety's guidance in the Position paper and specifically the risk factors listed on page 50/51. We have made various changes throughout the Code development process to strengthen these provisions. The SMS Code has now been further amended so that the previous guidance in Clause 5 is now mandatory except for the table of risk factors. This ensures that eSafety has a list of clear criteria against which it can test whether the risk assessments of individual providers accurately reflect the risk of harm. In addition, a provision in Clause 5 (c) has been added that requires participants to choose a higher risk tier when a service may be in-between risk tiers, the provider must assign a higher risk profile to that service. The risk methodology set out in the table is provided as guidance to service. Industry's view is that it is not possible to prescribe a methodology for social media services as the criteria for a social media service may be altered by legislative rules and the types of services that fall within this category may further be expanded by legislative rules. We have also added a guidance note that the risk factors in the Table should be given equal weighting and provided some clarifications about the purpose criteria and the meaning of video streaming and interactive video streaming.
7. 'Appropriate steps' in MCM 26	eSafety recognises that the timeliness of the actions required under this measure will depend on a number of factors such as those set out in the guidance note in MCM 26. However, eSafety considers it reasonable for MCM 26 to provide greater clarity about what 'appropriate' steps entail because there is risk arising from the uncertain language where some service providers may take ineffective steps and/or respond in an unreasonable time frame, which will undermine the effectiveness of MCM 26 to deliver appropriate community safeguards.	We are unclear as to the nature of the concern here as the measure specifies that at minimum end-users must be informed in a reasonably timely manner of the outcome of a complaint. The guidance is clear about the factors that are relevant to assessing what is 'reasonably timely in this context.

Relevant part of Code/ sections/outcomes	eSafety feedback	Industry response to feedback
Relevant Electronic Services		
8. Scope	eSafety considers it unlikely that the draft RES Code would satisfy s 140(1)(b) of the Act because the code is expressed to apply in respect of 'Australian end-users' and not to the relevant group of providers, described in s 135(2)(b), or to the relevant online activity, described in s 134(b).	See response in 1. above
9. Matter 1:	In order to provide appropriate	In relation to (a) minimum compliance measure 5 is

Measures directed towards achieving the objective of ensuring that industry participants have scalable and effective policies, procedures, systems and technologies in place to take reasonable and proactive steps to detect and prevent access or exposure to, distribution of, and online storage of class 1A material.	community safeguards for Matter 1, the draft RES Code would need to ensure, at a minimum, that: (a) the commitment in MCM 5 for Tier 1 and Tier 2 RES to take appropriate action in response to breaches of policies for prohibiting Child Sexual Exploitation Material (CSEM) and pro-terror material should require appropriate action to be taken in relation to breaches of policies prohibiting other class 1A material; (b) Closed Communication RES and Encrypted RES should also be subject to MCM 5; (c) all Tier 1 RES (regardless of whether they meet the definition of Very Large RES), should commit to use appropriate systems, processes and technologies to detect and remove known CSAM (MCM 9) (d) Closed Communication RES and Encrypted RES should commit to use appropriate systems, processes and/or technologies to detect and remove known CSAM (MCM 9) (recognising that services using carrier networks are limited in their ability to deploy relevant technologies but other technologies, systems or processes could be implemented to detect and remove known CSAM and known pro-terror material); (e) all Tier 1 RES (regardless of whether they meet the definition of Very Large RES), Closed Communication RES and Encrypted RES should commit to use appropriate systems, processes and/or technologies to detect and remove known pro-terror material/Terrorist and Violent Extremist Content (TVEC) where available (MCM 10); (f) Tier 1 RES and Dating services should commit to ongoing investment in systems and process and technologies in relation to the detection of class 1A material (including first generation CSAM). The commitment should not be limited to a commitment to invest in the safe design of its services to 'provide appropriate support for the provider's compliance with this Code' in order to ensure there is ongoing investment to address the broader risk of class 1A content on services (including first generation CSAM); and (g) Closed Communication RES and Encrypted RES should commit to ongoing investment in systems, process and/or technologies in relation to the detection of class 1A material (including first generation CSAM). The	now MCM 4 has been revised to extend this MCM to all pre-assessed electronic services and Tier 1 and Tier 2 RES. See definition of pre-assessed relevant electronic service in Clause 3. A pre-assessed relevant electronic service means: (i) a closed communication relevant electronic service; (ii) a dating service; (iii) an encrypted relevant electronic service; (iv) a gaming service with communications functionality; or (v) an open communication relevant electronic service. This new category of service extends to all types of existing services that could potentially be classified as Tier 1 or tier 2 under the previous code drafts. See also corresponding edits to measure 3. The type of action that services are required to take will depend on whether they are able to determine whether a user has breached their policies, i.e., where the provider is capable of reviewing and assessing and/or removing materials. See new definition of 'capable of reviewing and assessing materials' in Clause 3, with notes. See also Clause 5.2 which explains how relevant measures apply where a provider is partially capable of reviewing materials. This capability to assess and review materials is critical for providers to assess materials in accordance with the Classification Scheme. In addition, the drafting of MCM 4 a) makes clear that the ability of providers to remove materials is contingent on their having the capability to do so. In relation to (b) MCM 3 and 4 now applies to all pre-assessed relevant electronic services or a Tier 1 or Tier 2 relevant electronic service and all types of class 1A material. In relation to (c) and (d) MCM 8 (previously MCM 9) now extends to Tier 1 RES and also an open communication relevant electronic service that is not a carriage service provider; a dating service; or a gaming service with communications functionality. Note that Encrypted RES are not subject to this Clause but are now subject to revised MCM 10: Actions to be taken by Tier 1 relevant electronic services, dating services, open communication electronic services, closed communication relevant electronic services and encrypted relevant electronic services to disrupt or deter CSEM and pro-terror material. In relation to (e) revised MCM 9 (previously MCM 10) requires) a Tier 1 relevant electronic service; or open communication relevant electronic services excluding carriage service providers, that is capable of reviewing and assessing material on the service and removing material from the service to implement systems, processes and/or technologies designed to detect, flag and/or remove instances of known pro-terror materials from the service. See definition of known pro-terror material in section 2.1 of the Head Terms discussed in 2. above. In relation to (f) see revised MCM 10: Actions to be taken by Tier 1 relevant electronic services, dating services, open communication electronic services, closed communication relevant electronic services and encrypted relevant electronic services to disrupt or deter CSEM and pro-terror materials. This extends obligations to take action and invest in the prevention

	commitment should not be limited to a commitment to invest in the safe design of its services to ‘provide appropriate support for the provider’s compliance with this Code’ in order to ensure there is ongoing investment to address the broader risk of class 1A content on services (including first generation CSAM).	of CSAM and pro-terror materials (including first generation materials) to a broad range of services that might be categorised as Tier 1 or Tier 2 under the previous Code drafts.
10. MCM 5: scope	While eSafety recognises that CSEM and pro-terror material are different to other types of class 1A material (in both the nature and extent of the harms and also the ability of this material to be more easily defined and/or identified), eSafety disagrees with the limited application of MCM 5, which requires action in response to breaches of policies prohibiting CSEM and pro-terror material, to a subset of class 1A material. Under the Act, eSafety is empowered to issue removal notices for the removal of all class 1 material with a requirement to comply within 24 hours. In order to provide appropriate community safeguards, the draft RES Code should complement this complaints and removal scheme; confining the commitment in MCM 5 to CSEM and pro-terror material risks undermining it.	Revised MCM 4 (previously MCM 5) now applies to all Class 1A materials.
11. MCM 5: scope	In order to provide appropriate community safeguards, MCM 5 should also apply to Closed Communication RES and Encrypted RES.	See response in 9.
12. MCM 9: scope	Further, eSafety considers that all Tier 1 RES (regardless of whether they meet the definition of Very Large RES) could reasonably comply with a requirement to use appropriate systems, processes and technologies to detect and remove known CSAM (MCM 9).	See response in 9.
13. MCM 9: scope	Recognising that encrypted services and services using carrier networks may be limited in their ability to deploy relevant technologies, eSafety considers that Encrypted RES and Closed Communication RES could reasonably comply with a requirement to use systems, processes and/or technologies to detect and remove known CSAM (MCM 9) and that such a commitment is important to provide appropriate community safeguards.	See response in 9. We think that the revised MCM 10 is a more appropriate measure for Encrypted RES and Closed Communication RES, that recognizes their limited ability to deploy some technologies but provides flexibility for such services to take actions that can deter and disrupt CSAM and pro-terror material and will provide appropriate community safeguards. Additionally new MCM 10 also includes a commitment to invest in disrupting and deterring CSAM and pro-terror material per 9. above.
14. MCM 10: scope	eSafety considers that Tier 1 RES (regardless of whether they meet the definition of Very Large RES), Closed Communication RES and Encrypted	See response in 9 and 13 above.

	RES should use appropriate systems, processes and/or technologies to detect and remove known TVEC/pro-terror material (MCM 10). While this commitment would not require providers to use all three of systems and processes and technologies, eSafety notes that in practice, some RES providers may use the same systems, processes and technologies to detect and remove known TVEC as they do for known CSAM (while using different datasets).	
15. MCM 11: scope	MCM 11 does not include Closed Communication RES, Encrypted RES and Dating services. eSafety considers it reasonable for these services to commit to making ongoing investments, particularly given the flexibility the guidance of MCM 11 provides to make ongoing investments that vary depending on the type of service. Without such commitments, eSafety is concerned that appropriate community safeguards may not be provided.	See response in 9. to point (f) and 13 regarding revisions to MCM 10 (previously MCM 11)
16. Matter 2: **Measures directed towards achieving the objective of ensuring that industry participants have scalable and effective policies, procedures, systems and technologies in place to take reasonable and proactive steps to limit access or exposure to, and distribution of class 1B material.**	eSafety is concerned with the scope and application of MCM 14. While this measure does not list class 1B material specifically it refers generally to 'breaches of terms and conditions, community standards, and/or acceptable use policies' eSafety recognises that these measures in the draft RES Code are designed to be proportionate to the relative harmfulness of class 1B material compared to class 1A. However, eSafety is concerned with MCM 14's limited application to Tier 1 and Tier 2 RES to take action in response to breaches of policies and the absence of such a commitment on Closed Communication RES and Encrypted RES. In addition to this concern with MCM 14, eSafety is concerned with the omission of a specific reference to class 1B material and the range of examples of appropriate steps provided. eSafety is concerned that steps taken in accordance with this MCM will not work to complement eSafety's power under the Act to issue removal notices requiring removal of all material that is or would be classified as class 1.	See revised MCM 12 (previously MCM 14) which now applies to Class 1B materials. Note similar adjustments in scope to MCM 4 to a broader range of categories of service, taking into account, where relevant, the capability of providers to review and assess materials and their capability to remove materials.
17. Matter 6: **Measures directed towards achieving the objective of**	The commitment in MCM 19 to share information with eSafety is limited to Tier 1 RES and Encrypted RES and it is not clear to eSafety why MCM 19	See revised MCM 17 which now applies to A provider of: a Tier 1 relevant electronic service; b) an encrypted relevant electronic service., c) an open communication relevant electronic service and d) a

ensuring that industry participants have effective and scalable policies and procedures in place which ensure communication and cooperation with the eSafety Commissioner with respect to matters about class 1A material and class 1B material, including complaints.	does not also include Closed Communication RES, given new features or functions could also change the risk profile for these services. eSafety's preliminary view is that, in order for MCM 19 to provide appropriate community safeguards, MCM 19 should be extended to Closed Communication RES.	gaming service with communications functionality. We consider that the kinds of changes to Closed Communications RES that would likely have a significant impact on a services risk in relation to Class 1 materials would result in a change of category for closes comms services (for example, adopting encryption). This is adequately dealt with by other Code requirements for example, to conduct a safety by design assessment.
18. MCM 19: Confidentiality	eSafety's preliminary view is that the carve-out in MCM 19 excusing industry participants from providing confidential information in code reports is not appropriate and notes clause 7.3 (b) of the head terms. Clause 7.3(b) provides relevantly that 'if an industry participant identifies any material in a Code report as the industry participant's confidential information, eSafety must maintain such material in confidence'. Such information may clearly be of significance to eSafety's understanding of the risk of a service and eSafety would be expected to maintain the confidentiality of such information.	This carve out has been removed in revised MCM 17 (previously MCM19).
19. Matter 11: **Measures directed towards achieving the objective of ensuring that industry participants publish annual reports about class 1A material and class 1B material, and their compliance with industry codes.**	eSafety's preliminary view is that the proposed 6 months' response timeframe in MCMs 29 and 30 is likely to prevent these MCMs providing appropriate community safeguards in relation to this matter and suggests that a reasonable response timeframe of 2 months would be appropriate.	The reporting measures have been revised. For those services that report on request of eSafety (services that likely be equivalent to Tier 2 service categories under previous drafts), the response timeframe has been reduced to 2 months. See also additional guidance about capability to assess and review/and or remove materials.
20. Limitations clause in Head Terms	Clause 6.1 (c) limits the codes from requiring any industry participant to 'render methods of encryption or other information security measures less effective'. As previously communicated to Industry Bodies, eSafety has concerns that rendering 'other information security measures less effective' is too broad and is a very low bar. There is a risk that as drafted, clause 6.1(c) could create broad exclusions from code commitments. eSafety considers that service providers consider how code compliance could be achieved by alternative mechanisms or by remedying the design. Clause 6.1 (e)(iii), (h), (i) and (j) and clause 6.2 each limit the codes from requiring industry participants to take action or engage in conduct that would violate other laws. As previously communicated to Industry Bodies, eSafety considers that the blanket exclusions are not desirable and it would be more appropriate for service providers to communicate specific	See response in 5.

	concerns to eSafety when a specific issue arises as to how compliance with a code requirement may breach a law and/or explore alternative approaches to meeting the minimum compliance measures of the code while still meeting other legal requirements.	
21. Risk assessment methodology	In relation to the risk assessment methodology in the draft RES Code, eSafety is concerned that RES providers may underestimate their risk level if application of the tiers and relative weighting of the factors listed in the table is left to industry participants to determine without further guidance. It would be difficult for eSafety to critically assess the risk profile assigned by the RES provider to its online activity(ies) if those risk factors are open to broad interpretation and the risk profile adopted does not accurately reflect the risk of harm.	The RES category is a highly diverse and open-ended category of services and may encompass as yet undeveloped future services, including future services prescribed by legislative instrument. This makes it impossible to prescribe an appropriate risk assessment approach for this section of the industry. The RES Code has therefore been restructured to define the categories of services that currently would be categorized as RES under the OSA and allocate appropriate measures for each category. Some measures e.g. around enforcement have also been revised to consider the different capacity of services to assess, review, and remove materials. See new clause 5.2 that requires a provider of a pre-assessed relevant electronic service or a Tier 1 or Tier 2 relevant electronic to, at eSafety's request, notify eSafety if it is capable of removing, reviewing and assessing material or capable of removing material, or not capable of doing so. We have retained the need for services that do not fall within these categories to assess their risk. The risk factors in the table in Clause 6 are based on the guidance in the Position paper at p.50 and 51 . We have made various changes throughout the Code development to strengthen the risk assessment approach. The RES code has now been further amended so that the previous guidance in Clause 6 is now mandatory except for the table of risk factors. This ensures that eSafety has a list of clear criteria against which it can test whether the risk assessments of individual providers accurately reflect the risk of harm. In addition, a provision in Clause 5.3 (iii) has been added that requires participants to choose a higher risk tier when a service may be in-between risk tiers, the provider must assign a higher risk profile to that service.
Relevant part of Code/ sections/outcomes	**eSafety feedback**	**Industry response to feedback**
Designated Internet Services		
22. Scope	eSafety considers it is unlikely that the draft DIS Code would satisfy s140(1)(b) of the Act because the code is expressed to apply in respect of 'Australian end-users' and not to the relevant group of providers, described in s 135(2)(c), or to the relevant online activity, described in s 134(c).	See response in 1. above.
23. Matter 1:	eSafety considers that in order to provide appropriate community	Industry has very carefully considered eSafety's views on this issue. As previously noted to eSafety,

Measures directed towards achieving the objective of ensuring that industry participants have scalable and effective policies, procedures, systems and technologies in place to take reasonable and proactive steps to detect and prevent access or exposure to, distribution of, and online storage of class 1A material.	safeguards for Matter 1, the draft DIS Code would need to ensure that, at a minimum: (a) end-user managed hosting services use systems, processes and technologies to detect and remove known child sexual abuse materials (CSAM); and (b) Tier 1 DIS and end-user managed hosting services use systems, processes and/or technologies to detect and remove known pro-terror material/ Terrorist and Violent Extremist Content (TVEC); and (c) Tier 1 DIS and end-user managed hosting services make ongoing investment in systems, processes and technologies in relation to class 1A material (including first generation CSAM). eSafety does not agree with Industry Bodies' submission that the requirement to deploy technology to detect certain material should not extend to end-user managed hosting services due to potential user privacy concerns. Online file/photo storage sites have been found to be commonly used to facilitate dissemination of CSAM and TVEC.	Industry has sought to develop measures that include proactive steps to detect and/or deter and disrupt end-users access or exposure to, distribution of, and online storage of pro-terror materials that are appropriate for different service types. In the case of the DIS Code, Industry was unable to agree with an eSafety 's suggested approach on these three measures for end-user hosting services in relation to CSAM and pro-terror material, due to privacy concerns and key differences in service offerings. We turn to each of the measures proposed by eSafety in turn ((a) to (c)): a) The Code does not include obligations on end-user managed hosting services to detect Known CSAM for the reasons outlined above. b) The Code now includes obligations on Tier 1 DIS to take action and invest in deterring and disrupting CSAM and pro-terror material (including first generation materia) in a manner that is proportionate to the risk of that material being accessible to Australian end-users . c) See (b)
24.	Further, eSafety considers that Tier 1 DIS and end-user managed hosting services could reasonably comply with a requirement to use systems, processes and/or technologies to proactively detect known TVEC. While this commitment would not require providers to use all three of systems and processes and technologies, eSafety notes that in practice, Tier 1 DIS and end-user managed hosting services providers may use the same systems, processes and technologies to detect and remove known TVEC as they do for known CSAM (while using different datasets).	See response in 23.
25.	eSafety's current views is that it is not reasonable or appropriate to curtail the ongoing investment requirement in MCM 8 to known CSAM, due to the immensely harmful consequences associated with the creation, distribution and dissemination of first generation CSAM. Technologies and processes aimed at detecting first generation CSAM are increasingly being developed and also deployed on a range of services. eSafety considers that commitments by Tier 1 DIS and end-user managed hosting services to invest in the development of systems, processes and technologies is critical	See response in 23.

	in order to provide appropriate community safeguards.	
26. Matter 2: **Measures directed towards achieving the objective of ensuring that industry participants have scalable and effective policies, procedures, systems and technologies in place to take reasonable and proactive steps to detect and prevent access or exposure to, distribution of, and online storage of class 1B material.**	eSafety has concerns that the lack of an explicit requirement to adhere to and enforce their policies will undermine the effectiveness of MCM 10, as well as making it potentially unenforceable from a compliance perspective. This is because DIS providers could demonstrate compliance with MCM 10 by publishing and maintaining such policies without taking action to enforce the policies. eSafety notes that requiring DIS providers to apply or enforce their own policies does not remove service providers' ability to exercise discretion. Nor does it mean the service provider would be required to take certain action in all circumstances (such as terminating the provision of a service). Service providers have the flexibility to design and implement their policies to allow appropriate and proportionate responses to potential breach scenarios. Further, as it is currently drafted, MCM 10(b)(i) appears to suggest that the standard operating procedures should require an end-user managed hosting service to refer reporters of class 1B materials to eSafety resources at first instance. As previously communicated to Industry Bodies, eSafety suggests all DIS providers respond to reports of class 1A and 1B material under their complaints mechanism before referring unresolved complaints to eSafety.	Amendments have been made to revised MCM 3 ,4, 5 and MCM 11 and 12 that make clear DIS providers must take enforcement action for breach of policies concerning Class 1A and Class1 B materials. For end-user hosting services the appropriate enforcement action will vary depending on whether they are capable or not capable of assessing and reviewing materials (see definition of capable of reviewing and assessing materials in clause 3. A note has been added to explain that due to the nature of some designated internet services, and the manner in which they are otherwise regulated, providers of these services may not be capable of reviewing and assessing content stored or shared by end-users on their services. This can impact a provider's ability to review and assess material. A provider's ability to access and view material, and the provider's ability to view content and end user activity, will therefore depend on whether the provider has both the legal and technical capacity to do so. If a provider is prohibited by law from undertaking such activity, or such activity is not technically feasible (e.g., due to the nature and functionality of the designated internet service), then the provider will not be capable of reviewing and assessing material. In circumstances where a provider cannot review and assess material that is the subject of the complaint we consider that the most active response is to refer the complainant to eSafety who has powers to order end-users to remove Class 1 materials.
27. Matter 4: **Measures directed towards achieving the objective of ensuring that industry participants have scalable and effective policies, procedures, systems and technologies in place to take reasonable and proactive steps to limit the hosting of class 1A material and class 1B material in Australia.**	eSafety's preliminary view is that in order for the draft DIS Code to provide appropriate community safeguards in relation to Matter 4, it would need to ensure: it contains the steps in paragraph 16 above (which are also necessary in order to provide appropriate community safeguards in relation to Matters 1 and 2); and greater clarity in MCMs 13 and 14 to include an obligation to apply and enforce policies and terms of use agreements.	See response in 26.
28. Matter 5: **Measures directed towards achieving the objective of ensuring that industry participants have effective and scalable policies and procedures in place to**	eSafety recognises the diverse range of services covered under the DIS Code and the potential practical difficulties in requiring all Tier 1 or 2 DIS providers to make this a minimum compliance measure. However, eSafety considers that end-user managed hosting services are a	See m MCM 17 that makes industry collaboration of end-user hosting service providers mandatory.

facilitate consultation, cooperation and collaboration with other industry participants in respect of the removal, disruption and/or restriction of class 1A material and class 1B material, as well as accounts associated with this material.	category of DIS providers where collaboration is reasonable and appropriate. This could take place, by example, via an annual industry forum, information sharing with eSafety, contribution to cross-sector online safety groups and/or supporting research and innovation. Proactive engagement within and across industry will complement the other compliance measures and help address displacement effects where bad actors find shelter in smaller or less mainstream platforms to host and disseminate harmful content. eSafety suggests revising the measure to be a mandatory obligation for end-user managed hosting service.	
29. Matter 11: **Measures directed towards achieving the objective of ensuring that industry participants publish annual reports about class 1A material and class 1B material, and their compliance with industry codes.**	eSafety's preliminary view is that the proposed 6 months' response timeframe in MCMs 32 and 33 is likely to prevent the measures from providing appropriate community safeguards in relation to this matter, and suggests that a reasonable response timeframe of 2 months would be appropriate.	Se revised MCM 35 (previously MCM 32) and MCM 36 t(previously MCM 33) that reduce the response times for annual reports to 2 months
30. Limitations clause in Head Terms	Clause 6.1 (e)(iii), (h), (i) and (j) and clause 6.2 each limit the codes from requiring industry participants to take action or engage in conduct that would violate other laws. As previously communicated to Industry Bodies, eSafety considers that the blanket exclusions are not desirable and it would be more appropriate for service providers to communicate specific concerns to eSafety when a specific issue arises as to how compliance with a code requirement may breach a law and/or explore alternative approaches to meeting the minimum compliance measures of the code while still meeting other legal requirements.	See response in 5.
31. Risk assessment	In relation to the risk assessment methodology in the draft DIS Code, the demographics of the actual user base of a service is not listed as a factor in the risk assessment. eSafety considers the extent to which a DIS attracts a large number of child users to be relevant to the risk profile, particularly if a chat/messaging function that is not limited to private messages within the service is offered. Such services have a relatively high risk of exposure to online predators and the risk of unwanted contact and grooming. eSafety suggests that DIS providers be required to factor in the age of their actual users in order to ensure a more accurate evaluation of potential online	See amendment to guidance in clause 5 9 regarding demographics that makes clear this includes the age of users (noting that ascertaining age will not always be possible on publicly accessible websites) We note that the risk assessment methodology was designed to take into account eSafety's guidance in the Position paper and specifically the risk factors listed on page 50/51. Designing a risk methodology is difficult for this category since designated internet services since the scope of services in scope is left open by the OSA. This category is also highly diverse including file storage services, publicly accessible websites, apps, subscription services, and unknown types of future services that conduct online activities that do not fall within other industry sections. Determining the relative scale of such services is also difficult as not all types e.g. public websites,

	risks that could be enabled or facilitated by the online platform or service. The process to identify applicable compliance measures is entirely reliant on an effective risk assessment. While DIS providers are required to demonstrate that the compliance measures they have adopted are reasonable, it would be difficult for eSafety to critically assess risk profile assigned by the DIS provider to the online activity if those risk factors are open to broad interpretation and the risk profile adopted does not accurately reflect the risk of harm.	require users to register to use their services We note that eSafety has not given the industry specific feedback on how the current approach can be improved to ensure providers' risk profiles adequately reflect the risk of harm. We have strengthened the risk assessment approach by making the guidance in 5 (b) mandatory.
Relevant part of Code/ sections/outcomes	**eSafety feedback**	**Industry response to feedback**
Search Engine Services		
32. Scope	eSafety considers it is unlikely that the draft SES Code would satisfy s 140(1)(b) of the Act because the code is expressed to apply in respect of 'Australian end-users' and not to the relevant group of providers, described in s 135(2)(d), or to the relevant online activity, described in s 134(d).	See response in 1.
33. MCM 1: Algorithmic optimisation	eSafety considers it is unclear how adherence to the minimum requirements identified in MCM 1 will, in themselves, effectively ensure 'ongoing investments to support algorithmic optimisation'. This presents a risk of the measure being implemented by SES Providers without action taken to improve ranking algorithms following the review or testing envisaged, and/or expenditure in research and development in technology to reduce the accessibility or discoverability of class 1A material.	See revised MCM 1 that now makes clear that following review/and or testing in SES providers must, adjust ranking algorithms to elevate authoritative, relevant and trustworthy information and reduce the risk that class 1A material is accessible or discoverable in search results by Australian end-users.
34. Matter 11: **Measures directed towards achieving the objective of ensuring that industry participants publish annual reports about class 1A material and class 1B material, and their compliance with industry codes**.	eSafety's preliminary view is that the proposed 6 months' response timeframe in MCM 18 is likely to prevent this MCM from providing appropriate community safeguards in relation to this matter and suggests that a reasonable response time frame of 2 months would be appropriate. eSafety also considers that the reporting requirements under MCM 18 are unlikely to be sufficient for the purposes of providing appropriate community safeguards. While eSafety recognises that in many cases an internet search engine provider will not regularly receive reports of class 1A and class 1B material, eSafety considers that service providers should	See measures in MCM 18 that reduce the response time frame for reports to 2 months and provide for additional data to be provided in the report.

	collect further relevant information, for inclusion in a report to eSafety which could include the: • number of reports received for class 1A and class 1B material; • number of complaints received in respect of the handling of class 1A and class 1B material; • number of complaints related to code compliance; • an explanation of the appropriateness of those measures and responses; and • data and information on safety innovations, investments and third-party engagements	
Relevant part of Code/ sections/outcomes	**eSafety feedback**	**Industry response to feedback**
App Distribution Services		
35. Scope	eSafety considers it is unlikely the draft App Distribution Code would satisfy s 140(1)(b) of the Act because the code is expressed to apply in respect of 'Australian end-users' and not to the relevant group of providers, described in s 135(2)(e), or to the relevant online activity, described in s 134(e).	See response in 1.
36. Matter 1: **Measures directed towards achieving the objective of ensuring that industry participants have scalable and effective policies, procedures, systems and technologies in place to take reasonable and proactive steps to detect and prevent access or exposure to, distribution of, and online storage of class 1A material.**	eSafety's preliminary view is that MCM 1, as currently drafted, is insufficient to provide appropriate community safeguards for Matter 1 because: (a) there is no clear commitment by app distribution service providers to apply or enforce their terms of agreements with third-party app providers where they fail to comply with Australian content laws; and (b) there is insufficient specificity on the review process that app distribution service providers are required to undertake before third-party apps are released on the service (for example specific material and/or policies).	See revised MCM 1 and corresponding guidance that contains a clear commitment by app distribution service providers to take enforcement action in relation to beaches of agreements with third party app providers that is reasonably proportionate to the nature of the third-party app provider's breach of the agreement; and new sub-measure 1 d) that requires providers to 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 access or exposure to, distribution of, or online storage of class 1A material via the third-party app.
37. Enforcement actions by app distribution service providers	eSafety has previously identified in earlier versions of the code a lack of clarity on the enforcement action to be taken by app distribution service providers where third-party app providers fail to comply with Australian content laws. In response, the Steering Group raised concerns that requiring enforcement of policies risked being too prescriptive on enforcement measures and interfering with parties' freedom to contract.	See response in 36 plus the addition of new MCM 5 requiring providers to notify eSafety when apps are removed as part of the action taken by the app distribution service provider pursuant to measure 1) c) in relation to the access or exposure to, distribution of, or online storage of class 1A material. This can assist eSafety coordinate with other providers if the removal of an app raises safety concerns about equivalent apps on other sites.

	eSafety recognises the importance of proportionality in responding to potential breaches of policies. However, eSafety considers it reasonable and appropriate for MCM 1 to include a commitment on app distribution service providers to apply and enforce the terms of their agreements with third-party app providers, which cover compliance with Australian content laws and regulations. eSafety also has concerns that the absence of such commitment may impact the effectiveness of the reporting mechanism under MCM 8. This is because an app distribution service provider's reporting requirement will not include reporting on enforcement action taken under their agreements in response to third-party app providers' failure to comply with Australian content laws (as regards class 1 material). This omission may affect the ability of the code to provide transparency of and accountability for class 1 material.	
38. Matter 5: **Measures directed towards achieving the objective of ensuring that industry participants have effective and scalable policies and procedures in place to facilitate consultation, cooperation and collaboration with other industry participants in respect of the removal, disruption and/or restriction of class 1A material and class 1A material, as well as accounts associated with this material.**	eSafety's preliminary view is that, in order to provide appropriate community safeguards for Matter 5, the draft App Distribution Code should include a commitment from app distribution service providers to communicate in a timely manner in order to collaborate on the removal of apps as a result of class 1A and 1B material. eSafety considers this more effective than relying on direction from law enforcement or on eSafety exercising its formal app removal power under the Act. eSafety's Position Paper set out a number of examples of such active collaboration measures.	The new MCM 5 provides information that can be used by eSafety to publicise app removals by participants. Industry is concerned that industry wide collaboration regarding apps removal is best coordinated by eSafety to avoid the risk that such action would contravene competition laws.
39. Matter 11: **Measures directed towards achieving the objective of ensuring that industry participants publish annual reports about class 1A material and class 1B material, and their compliance with industry codes.**	eSafety's preliminary view is that the proposed 6 months' response timeframe in MCM 8 is likely to prevent this MCM from providing appropriate community safeguards in relation to this matter, and suggests that a reasonable response time frame of 2 months would be appropriate.	The response time frame in revised MCM 9 (previously MCM 8) has been reduced to 2 months.

Relevant part of Code/ sections/outcomes	eSafety feedback	Industry response to feedback
Hosting services		
40. Matter 1: **Measures directed towards achieving the objective of ensuring that industry participants have scalable and effective policies, procedures, systems and technologies in place to take reasonable and proactive steps to detect and prevent access or exposure to, distribution of, and online storage of class 1A material.** **41. Matter 2:** **Measures directed towards achieving the objective of ensuring that industry participants have scalable and effective policies, procedures, systems and technologies in place to take reasonable and proactive steps to prevent or limit access or exposure to, and distribution of, class 1B material.** **42. Matter 4:** **Measures directed towards achieving the objective of ensuring that industry participants have scalable and effective policies, procedures, systems and technologies in place to take reasonable and proactive steps to limit the hosting of class 1A material and class 1B material in Australia.**	eSafety considers that MCMs 1 and 2 are unlikely to provide appropriate community safeguards in their current form. Although MCM 1 sets out a requirement to have clear contractual terms and/or policies with regard to unlawful content, MCM 2 does not require that relevant terms and policies be enforced, applied or adhered to by the hosting service provider. A requirement that these terms and policies be 'in place' may potentially be met by a service provider having these documents prepared, published and/or executed as applicable.	MCM 2 has been amended to make clear that relevant terms and policies are to be enforced.
43.	eSafety is concerned that a hosting service provider will be able to establish that it has complied with its obligations if it can demonstrate that it has published and/or executed relevant terms and policies regarding class 1A and class 1B material (MCM 1) and has also published policies or executed terms which set out the procedures for considering reports and enforcing such policies (MCM 2) without requiring the service provider to actually apply or enforce those policies and/or terms.	See response in 40.
44.	eSafety notes that requiring hosting service providers to apply or enforce their own policies and terms does not remove service providers' ability to exercise discretion, nor does it mean the service provider would be required to take certain action in all	See response in 40. Guidance similar to the feedback provided has been included in MCM 2.

	circumstances (such as terminating the provision of a service). Service providers remain able to design these terms and policies to allow appropriate and proportionate responses to potential breach scenarios.	
45.	eSafety considers it unlikely that measures which fail to require a hosting service provider to adhere to, apply or enforce their terms or conditions where their service is being used to store class 1A or class 1B material would provide appropriate community safeguards.	See response in 40.
46. Matter 11: **Measures directed towards achieving the objective of ensuring that industry participants publish annual reports about class 1A material and class 1B material, and their compliance with industry codes.**	eSafety has concerns that the timeframe for responding to requests for reports under MCM 8 will impact eSafety's ability to consider a service provider's compliance with code commitments, as well as eSafety's ability to provide constructive input into the first review of the Hosting Code. Without an effective review process, the capability of the Hosting Code to provide appropriate community safeguards may be compromised. eSafety's preliminary view is that the proposed 6 months' response timeframe in MCM 8 is likely to prevent this MCM from providing appropriate community safeguards in relation to this matter and suggests that a reasonable response timeframe of 2 months would be appropriate.	The response timeframe in revised MCM 9 (previously MCM 8) has been reduced to 2 months.
47.	eSafety also considers that the reporting requirements under MCM 8 are unlikely to be sufficient for the purposes of providing appropriate community safeguards. While eSafety recognises that in many cases a hosting service provider will not regularly receive reports of class 1A and class 1B material, eSafety considers that service providers should collect further information, for inclusion in a report to eSafety which could include: • number of reports received for class 1A and class 1B material; • number of complaints received in respect of the handling of class 1A and class 1B material; • number of complaints related to code compliance; • an explanation of the appropriateness of those measures and responses; and • data and information on safety innovations, investments and third-party engagements etc.	MCM 8 has been amended to include a requirement for Third-Party Hosting Services to also report, upon request, the number of reports in relation to class 1A or class 1B material received by the Third-Party Hosting Service under MCM 3. Given these services are likely to receive a very limited number of reports due to their secondary nature in the supply chain and the fact that end-users usually do not know the hosting provider (and may even have difficulty of finding out who the hosting provider for a given website is), the number of reports for class 1A/B material received does not appear a useful metric. Similarly, due to the secondary nature in the supply chain and difficulty of being known to end-users, the number of complaints related to code compliance does not appear meaningful. It is unclear how 'an explanation of the appropriateness of those measures and responses' materially differs from the existing requirements of MCM 8. The request for 'data and information on safety innovations, investments and third-party engagements etc.' fails to acknowledge the supply chain and the fact that these services will not scan for material etc., i.e., what types of investments or

		innovations would be expected? As noted further below, it is also not clear how third-party engagements would be measured.
48. Limitations in head terms		See response in 5
49. Scope		See response in 1

Relevant part of Code/ sections/outcomes	eSafety feedback	Industry response to feedback
Internet Service Provider (ISP)		
50.	eSafety considers it unlikely the draft ISP Code would satisfy s 140(1)(b) of the Act because the code is expressed to apply in respect of 'Australian end-users' and not to the relevant group of providers, described in s 135(2)(g), or to the relevant online activity, described in s 134(g).	Section 2.1 of the Head Terms has amended the definition of Australian end-user to mean end user in Australia.
51.	eSafety considers that the draft ISP Code is unlikely to meet the requirement under s 140(1)(d)(i) of the Act, because it does not provide appropriate community safeguards for Matters 7, 10 and 11 for the reasons outlined below.	
52. Matter 7: **Measures directed towards achieving the objective of providing people with a range of technical tools and/or information to limit their access and exposure, and the access and exposure of children in their care, to class 1A material and class 1B material.**	eSafety's preliminary view is that, while the proposed MCMs are positive steps towards providing people with a range of technical tools and/or information, the commitments as currently drafted are insufficient to provide appropriate community safeguards under Matter 7 for the following reasons: • Timing and availability of information – as eSafety has previously communicated to industry, eSafety considers the information to be provided under MCMs 4 and 5 important and, in order to help safeguard end-users, ISPs should provide this information at or close to the point of sale. While industry has raised concerns that this may lead to 'information overload', eSafety considers that a commitment to provide information on filters 'at, or close to the time of sale' is sufficiently flexible to avoid the risk of information overload at sign-up. Clear communication with links to more detailed information may also help address the risk of information overload. eSafety considers it important to provide information 'at, or close to the time of sale' as this is the time when end-users are likely most interested, and most motivated to explore the adoption of a filter. eSafety also considers it	See proposed change for MCM 4 - now including a requirement to "providing at or close to the time of the sale". ISPs maintain that the investment in and monitoring of the development of filtering and other user-safety tools is not part of their business activities and, importantly, well performed by the safety tech sector. eSafety states that it "considers monitoring developments in filtering technology or other tools designed to protect users is important to help ensure there are technologies and systems available to remove, disrupt and/or restrict class 1A and class 1B material." We note that the availability of the tools is unrelated to ISPs performing the investment or monitoring function as can be seen by the availability of those tools without ISPs currently engaging in those activities. In fact, have increased in the past years. Importantly, the number of filters accredited under the Family Friendly Filter scheme has increased substantially from around 4 to currently 10 over the past two years. The additional requirement to now provide information about filtering products and how to obtain those at or close to the time of sale may drive the uptake of filtering products which is, so we understand, the outcome that eSafety wants to achieve rather than specific new filtering products. MCM 7 proposed a change to link to the eSafety complaints reporting process rather than the form, as a form may change over time and as the process may also require the user to select the appropriate

	important that, in ensuring this commitment remains effective, the information remains easy to navigate to and accessible on the ISP's website. • Monitoring the development of filtering and other user-safety tools – The draft ISP Code does not contain any commitment requiring ISPs to invest in, or monitor the development of, filters or other technology designed to increase user safety. eSafety notes previous comments made by the Industry Body that ISPs have limited expertise in filtering products, and that there are significant costs related to developing filtering products. However, eSafety considers monitoring developments in filtering technology or other tools designed to protect users is important to help ensure there are technologies and systems available to remove, disrupt and/or restrict class 1A and class 1B material. eSafety considers it reasonable and appropriate that the ISP code contain such a commitment from large ISPs (for example, those ISPs with over 1 million end-users in Australia).	form, e.g., cyber-bulling of a child, adult cyber abuse, image-based abuse etc., (e.g., refer to https://www.esafety.gov.au/report/forms)
53. Matter 10: **Measures directed towards achieving the objective of ensuring that industry participants publish easily accessible and plain language policies, procedures and guidelines that set out how they handle class 1A material and class 1B material; and Measures directed towards achieving the objective of ensuring that industry participants provide end-users with information about the safety issues associated with class 1A material and class 1B material.**	The draft ISP Code includes MCM 9 which requires ISPs to make information on online safety in respect of class 1A and 1B material accessible to end-users, including information for parents/carers about how to supervise and control children's access and exposure to class 1A and 1B material, and to provide end-users with information about the role and functions of eSafety. eSafety considers that the information required to be provided by ISPs should be easily accessible and understandable in order for this commitment to operate effectively and provide appropriate community safeguards.	See proposed change to MCM 9 to include "easily" accessible and "plain language" requirement for information.
54. Matter 11: **Measures directed towards achieving the objective of ensuring that industry participants publish annual reports about class 1A material and class 1B material, and their compliance with industry codes.**	eSafety has concerns that the timeframe for responding to requests for reports under MCM 10 will impact eSafety's ability to consider a service provider's compliance with code commitments, as well as eSafety's ability to provide constructive input into the first review of the ISP Code. Without an effective review process, the capability of the ISP Code to provide appropriate community safeguards may be compromised. eSafety's preliminary view is that the proposed 6 months' response timeframe in MCM 10 is likely to prevent this MCM from providing appropriate community safeguards in	The response timeframe in revised MCM 10 has been reduced to 2 months. MCM 10 has also been revised to now include the a) the number of complaints in relation to class 1A and class 1B material an Internet service provider has responded to under minimum compliance measure 8 above; and b) the number of complaints received about compliance with this Code. With regard to the feedback to report the number of complaints received in respect of the handling of class 1A and class 1B material, it is noted that ISPs from all experience and in all likelihood to not receive complaints about the material in the first place, but if they were to receive such a complaint, they do not

	relation to this matter and suggests that a reasonable response timeframe of 2 months would be appropriate. eSafety also considers that the reporting requirements under MCM 10 are unlikely to be sufficient for the purposes of providing appropriate community safeguards. While eSafety recognises that in many cases an internet service provider will not regularly receive reports of class 1A and class 1B material, eSafety considers that service providers should collect further relevant information, for inclusion in a report to eSafety that could include: the: • number of reports received for class 1A and class 1B material; • number of complaints received in respect of the handling of class 1A and class 1B material; • number of complaints related to code compliance; • an explanation of the appropriateness of those measures and responses; and • data and information on safety innovations, investments and third-party engagements etc.	'handle' the material as they have no visibility of the material. With regard to the reporting on an explanation of the appropriateness of those measures and responses, against the background of the above, we do not see how this would be different to the already existing reporting obligation 10 (b) (previously 10 (a)). With regard to the reporting on data and information on safety innovations, investments and third-party engagements etc., we refer in part to our commentary in relation to Matter 7 (investment into filtering) but also note more generally that the approach is flawed for a sector that has no technical ability to detect and remove content (we note our earlier comments on the differences to 'Cleaner Pipes') and is legally prohibited from inspection, interception, use or disclosure of the communications that travel over the networks in question. Further, we question what metric would be applied to third-party engagements. Overall, we do not believe that this reporting metric is useful for ISPs.

Relevant part of Code/ sections/outcomes	eSafety feedback	Industry response to feedback
Equipment		
55. Scope	Accordingly, eSafety considers it unlikely that the draft Equipment Code will satisfy s 140(1)(b) of the Act. This is because the scope of the Equipment Code, via the definitions above, are linked to equipment used by Australian end-users and not to the group of persons described in s 135(2)(h) or the to the relevant online activity, described in s 134(h).	Section 2.1 of the Head Terms has amended the definition of Australian end-user to mean end user in Australia.
56. Risk methodology	eSafety's preliminary view is that the risk methodology in the draft Equipment Code results in meaningful compliance measures being placed on a too narrow group of devices which is not commensurate with their risk profiles. eSafety is also concerned with the significant weight in the risk assessment given to the presence or absence of a screen, which means some devices for use in immersive environments may potentially be excluded from Tier 1 where they do not make use of a 'screen' in the traditional sense (such as VR or AR goggles).	A new definition for gaming device has been added (term 'primarily' removed post 2nd public consultation). In addition, the definition for interactive Tier 1 device definition has been amended to include internet browsing via a display to capture immersive environments (alongside existing concept of browsing via a screen). The fourth limb of the definition (general internet browsing) has been amended with a removal of the term 'primary'. However, it is important to keep the terminology of 'intended significant' as both together are required to facilitate general internet browsing. The mere existence of the facility to generally browse the internet could be seen as stating an intention when, in reality, it's intended purpose was different.

	eSafety considers that, in order to provide appropriate community safeguards, the Equipment Code should: • assign risk assessment categories that are based on objective, readily ascertainable factors; • broaden the definition of Tier 1 to include devices that have general web browsing functionality; and • be drafted in a way that both existing devices which have a material degree of risk attached to them (including equipment for use in immersive environments that may not make use of a screen in the traditional sense) and those devices which are likely to be made available in Australia in the foreseeable future will be required to comply with appropriate compliance measures.	Consequently, the purpose needs to be 'intended' and 'significant'. Further guidance on the intention of the operation of this limb is provided in the table at clause 5. Importantly, the note under the definition of interactive Tier 1 device makes clear that gaming devices with general internet browsing functionality are considered interactive Tier 1 devices, provided that the functionality is not attained through unauthorised third-party software, modifications, tools, 'hacks', or other methods that may breach any applicable terms of use. As indicated above, the table in clause 5 has been amended to provide further clarification on the definition of interactive Tier 1 device We also sought feedback from the IoT Alliance Australia which agreed that a broadening of the definition of interactive Tier 1 devices to include devices that have a general web browsing functionality (i.e,, without limitation to intended, significant purpose) would broaden the scope to include a vast number of IoT devices that have no or only a theoretical harm risk associated with them.
57. Matter 1: **Measures directed towards achieving the objective of ensuring that industry participants have scalable and effective policies, procedures, systems and technologies in place to take reasonable and proactive steps to detect and prevent access or exposure to, distribution of, and online storage of class 1A material.** **58. Matter 2:** **Measures directed towards achieving the objective of ensuring that industry participants have scalable and effective policies, procedures, systems and technologies in place to take reasonable and proactive steps to prevent or limit access or exposure to, and distribution of class 1B material.** **59. Matter 7:** **Measures directed towards achieving the objective of providing people with a range of technical tools and/or information to limit their access and exposure, and the access and exposure of children in their care, to class 1A material and class 1B material.**	As set out above, the risk assessment methodology in the draft Equipment Code relies on subjective factors such as intended significant functions or primary design purpose. This means actual usage or secondary functions which may be associated with material risks will not be part of the risk assessment. eSafety considers that the minimum compliance measures (MCMs) proposed in the draft Equipment Code to address Matters 1, 2 and 7 (namely, MCMs 5-7) are together unlikely to provide appropriate community safeguards for those matters due to their limited application based on these risk categories. There is a significant risk that the current methodology will exclude devices (currently or likely to be supplied in the foreseeable future) that carry material risks for end-users from code requirements to have in place appropriate measures concerning class 1A or 1B materials, or to provide appropriate information or tools.	MCM 5 and 6 have been updated to include obligations on manufacturers of the newly defined term gaming devices. This includes a new provision that manufacturers of gaming devices with functionality that enables Australian end-users to freely browse the internet must provide easily accessible information that this functionality exists. Suppliers of interactive (Tier 1) devices, including children's interactive devices, and gaming devices must also provide accessible information on how to support online safety in a child's use of those devices.
60.	eSafety also notes that even for devices that are covered (Tier 1 and Gaming Devices), MCM 5 does not	See above regarding MCM 5 We note that the above information (MCM 5 (c), how to support online safety in a child's use of those

	require suppliers to provide information on children's online safety at or about the time of sale. eSafety's preliminary view is that making relevant resources available online to end-users is unlikely in itself to provide appropriate community safeguards. eSafety considers it important to provide. information 'at or about the time of sale' as this is the time when end-users are likely most interested, and most motivated, to investigate relevant safety resources.	devices) must be made available at or around the time of sale. (As per Nov 2022 draft.)
61.	eSafety also notes that there is no requirement under MCM 6 for OS Providers to develop and implement relevant tools within operating systems to assist in reducing the risk of harm to children using Tier 1 devices. The commitment on OS Providers is to take 'reasonable steps' towards this outcome. eSafety considers a commitment to take 'reasonable steps' is unlikely to be effective or measurable.	This MCM has now been amended to provide that an OS provider must develop and implement relevant tools where appropriate. There is also a new obligation in MCM 6 on manufacturers of gaming devices to develop and implement appropriate tools that allow Australian end-users to help reduce the risk of harm to children when using the devices.
62. Matter 6: **Measures directed towards achieving the objective of ensuring that industry participants have effective and scalable measures in place which ensure communication and cooperation with the eSafety Commissioner with respect to matters about class 1A and class 1B material, including complaints.**	The draft Equipment Code includes MCMs 3 and 4 to deal with this matter. MCM 3 applies to manufacturers and suppliers of Tier 1 devices, while MCM 4 applies to manufacturers of Tier 1 devices and OS Providers. As noted above, eSafety's preliminary view is that the draft Equipment Code's risk assessment methodology may exclude devices from Tier 1 that carry significant online safety risks for end-users. The limitation of MCM 4 in particular to Tier 1 devices leaves manufacturers of many devices without obligations to advise eSafety about new functions or features that may have a 'significant' effect on end-users' access or exposure to, distribution of, and online storage of class 1A or 1B material. While eSafety recognises that such developments are more likely to occur for devices that belong in Tier 1, eSafety's preliminary view is that in order for appropriate community safeguards to be provided, any relevant development with a 'significant' impact on end-users' safety in this respect should be communicated to eSafety, regardless of the nature of the device.	The limitation in MCM 4 regarding Interactive Tier 1 devices has been removed and now applies to all manufacturers.
63. Matter 8 **Measures directed towards achieving the objective of providing people with clear,**	Reflecting eSafety's preliminary views concerning the risk assessment methodology, eSafety considers that, to ensure proper community	Industry considers the proposed measures reasonably and proportionate as they target the devices and providers most likely to receive complaints. Overall, it is also important to bear in

easily accessible and effective: reporting mechanisms for class 1A and class 1B material, as well as associated user accounts; and complaints mechanisms to address complaints about the handling of reports about class 1A material and class 1B material and code compliance. **64. Matter 9** **Measures directed towards achieving the objective of ensuring that industry participants have scalable and effective policies, procedures, systems and technologies in place to effectively respond to: reports about class 1A and class 1B material, as well as associated user accounts; and complaints about the handling of reports about class 1A material and class 1B material and codes compliance.**	safeguards are provided with respect to Matters 9 and 10, these MCMs should apply to a broader range of devices than those currently captured by Tier 1, noting that end-users of a wide range of devices may need information about making complaints or seeking assistance from eSafety in connection with their devices (for instance, Gaming Devices falling outside of Tier 1 and devices with general web browsing functionality which may not be considered a 'primary' or 'significant' function).	mind that equipment providers are not content providers, which again reduces the likelihood that end-users turn to equipment providers in relation to class 1A/B materials. If they were to receive such complaints, they are not in a position to remove material.
65. Matter 10 **Measures directed towards achieving the objective of ensuring that industry participants publish easily accessible and plain language policies, procedures and guidelines that set out how they handle class 1A material and class 1B material. Measures directed towards achieving the objective of ensuring that industry participants provide end-users with information about the safety issues associated with class 1A material and class 1B material.**	MCMs 5-7 are considered above with respect to Matters 1, 2 and 7, and eSafety's assessment of MCMs 5-7 in relation to Matter 10 largely aligns with the analysis above. eSafety's preliminary view is that, in order to provide appropriate community safeguards, the range of devices to which MCMs 5-7 apply should be broader than is the case under the Code's risk allocation methodology, covering for example devices with general web browsing functionality and ensuring information about children's online safety is provided at or about the time of sale where appropriate.	See response to 57 and 60
66. Matter 11 **Measures directed towards achieving the objective of ensuring that industry participants publish annual reports about class 1A material and class 1B material, and their compliance with industry codes.**	eSafety's concerns with the limited definition of Tier 1 devices (described above) increases eSafety's concerns with the effectiveness of MCM 14. eSafety's preliminary view is that the proposed 6 months' response timeframe in MCM 14 for Tier 2 devices is likely to prevent this MCM from providing appropriate community safeguards in relation to this matter. eSafety suggests that a reasonable response timeframe of 2 months would be appropriate. eSafety also considers that the reporting requirements listed under MCMs 13 and 14 are unlikely to be sufficient for the purposes of providing appropriate community safeguards. While eSafety recognises that in many	The response timeframe in revised MCM 14 has been reduced to 2 months. MCM 13 has been amended to include the number of complaints from Australian end-users received by the manufacturer of an interactive Tier 1 device or the OS provider about Code compliance. For reasons outlined above, the first two proposed metrics do not appear useful in an equipment context. The fourth requested metric is, in our view, not substantially different to the measure as already drafted. In relation to the fifth metric, industry notes MCM 4 which provides for transparency of any features that negatively impacts on potential harms to end-users in this area.

	cases OS Providers and device manufacturers will not receive reports of class 1A and class 1B material, eSafety considers that these participants should collect further relevant information for inclusion in a report to eSafety that could include the: • number of reports received for class 1A and class 1B material; • number of complaints received in respect of the handling of class 1A and class 1B material; • number of complaints related to code compliance; • an explanation of the appropriateness of those measures and responses; and • data and information on safety innovations, investments and third-party engagements etc.	