# REQUEST FOR REGISTRATION OF ONLINE SAFETY CODES

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)

18 November 2022

# 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 (this document);
2. Submission log and associated responses; and
3. *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. 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.[1] Under the Scheme, the content is largely classified having regard to its 'offensiveness'.[2] The National Classification Code, guidelines for the classification of films, computer games and publications provide the principles and criteria for making classification decisions.[3] 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)."[4]

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 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,

[1] p. 18, eSafety Commissioner, *Development of industry codes under the Online Safety Act, Position Paper*, September 2021
[2] pp 20/21, ibid
[3] Refer to https://www.classification.gov.au/about-us/legislation as accessed on 18 Nov 2022.
[4] p. 19, eSafety Commissioner, *Development of industry codes under the Online Safety Act, Position Paper*, September 2021

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[5]. 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[6]. 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.

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. Those criteria are being addressed in the following. Where appropriate, the respective position from the 'position on development on codes' from the eSafety Position Paper is also referenced.

[5] 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 film classification guidelines.
[6] 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.

# 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[7], 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*):

| **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)<br>● 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)<br>● BSA \| The Software Alliance (BSA)<br>● CA<br>● DIGI<br>● Interactive Games and Entertainment Association (IGEA) |

[7] 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 |
|---|---|---|
| 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<br>● BSA<br>● Consumer Electronics Suppliers' Association (CESA)<br>● CA<br>● DIGI<br>● 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<br>● 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<br>● DIGI<br>● 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<br>● 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 |
| 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)<br>Operating system providers (as defined in the Equipment Online Safety Code (Class 1A and Class 1B Material)) | ● AMTA<br>● CA<br>● CESA<br>● IGEA<br>(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 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.

## 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 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."[8] 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 Codes correlate with the matters in the section 141 notices, with some minor changes. (Please refer to Annex 2 and footnote 5 below.)

**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[9]:

- 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[10]**

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.

[8] p.7, eSafety Commissioner, *Development of industry codes under the Online Safety Act, Position Paper*, September 2021
[9] 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 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.
[10] **Matter 3** has been deliberately omitted as it pertains to class 2 material only which is not subject to the Codes.

**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.

**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

<u>The Codes provide safeguards for Australians in relation to class1 materials:</u>

The measures in the Codes are directed towards providing safeguards for Australian end-users; defined as end-users ordinarily resident in Australia under section 2.1 of the Head Terms. 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.

The jurisdictional scope of regulations concerning internet materials is complex, particularly given the varying ways the OSA deals with the issue. It is noted that the section 141 notices do not specify the jurisdictional scope of the Codes, but that 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). Industry submits that the approach in the Codes is 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"[11] and that "[t]he codes be directed to ensuring that class 1 material is prevented, or limited, on services accessible to Australian end-users."[12] This policy intent aligns with the overall objectives of the 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.

As discussed with eSafety, there are practical challenges for many services to implement content regulations that apply specifically to end-users geographically present in Australia. In particular, to comply with that scope, some services would need to collect significant data to track the geographical movement of their users which is contrary to the principles of data minimisation which is captured in a number of Australian Privacy Principles under the *Privacy Act 1988*. Feedback received during public consultation also indicated that stakeholders are concerned about any further collection of user data. The scope to which complaints can be made about the industry codes is also a relevant practical consideration. 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.

**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.

**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

[11] p.7, eSafety Commissioner, *Development of industry codes under the Online Safety Act, Position Paper*, September 2021
[12] p.38, ibid

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.

**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 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*. 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**<br><br>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:<br><br>● access or exposure to,<br><br>● distribution of, and<br><br>● online storage of<br><br>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.**<br><br>**Outcome 1: Industry participants take reasonable and proactive steps to prevent access or exposure to, distribution of, and online storage of class 1A material.**<br><br>**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.**<br><br>**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 Australian adult or child. This must be done within 24 hours or as soon as reasonably practicable.<br><br>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).<br><br>**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:<br>- Specify the role of personnel in reviewing and responding to reports of class 1A materials by Australian end-users,<br>- Include clear internal channels for personnel in escalating, prioritising and assessing reports of class 1A material by Australian end-users,<br>- 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.<br><br>Note: this measure makes best practice operating procedures for enforcement of policies enforceable for Tier 1 and Tier 2 social media services.<br><br>**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.<br><br>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.<br><br>Additionally, MCM 3 requires a Tier 1 and Tier 2 social media service providers to:<br>(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,<br>(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,<br>(c) Terminate an end-user's account as soon as reasonably practicable in the event the end-user is:<br>i. Distributing CSEM or pro-terror material to Australian end-users with the intention to cause harm,<br>ii. Known to be using the account in breach of age restrictions concerning use of the service by an Australian child, |

| | |
|---|---|
| | iii. Has repeatedly breached terms and conditions, community standards, and/or acceptable use policies prohibiting class 1A material on the service, and<br>(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.<br><br>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.<br><br>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.<br><br>**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.<br><br>Note: this measure addresses the need for human resources that have specific safety responsibilities, which was reinforced by feedback from the public consultation process.<br><br>**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.<br><br>**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:<br><br>(a) Implement measures to ensure that material can only be uploaded to or distributed on the service by a registered account-holder,<br>(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,<br>(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<br>(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.<br><br>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.<br><br>**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:<br><br>(a) Default settings designed to prevent an Australian child from unwanted contact from unknown end-users, including settings which prevent the location of the child being shared with other accounts by default,<br>(b) Easy to use tools and functionality that can help parents or carers safeguard the safety of children using the service.<br><br>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*.<br><br>**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:<br><br>(a) Automatically detect and flag known CSAM, such as hash-matching technologies (for example, PhotoDNA, CSAI Match, and equivalent technology),<br><br>(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<br>(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.<br><br>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). The measure has been limited to known CSAM as the industry considers that mandating the widespread deployment of AI or machine learning to detect new CSAM for Tier 1 social media services is difficult in the absence of any safeguards (such as oversight by an independent regulator as proposed in the EU) that would address stakeholders' concerns that its |

| | |
|---|---|
| | use by some companies may result in the removal of legitimate material on the service. We think that the outcomes-based approach of the Codes, combined with the Basic Online Safety Expectations (BOSE), together appropriately incentivise capable social media services to deploy these systems, processes, and technologies, where reasonable.<br><br>**MCM 9:**Tier 1 very large social media service providers with over 8 million monthly active Australian end users must implement systems, processes and/or technological tools designed to detect, flag and/or remove instances of videos and images that depict and promote a terrorist act from the service, for example, through the use of hashing, machine- learning, or artificial intelligence that scans for videos and images that may, depending on the context, depict and promote a terrorist act and/or systems and processes that limits users' ability to publicly post such content on their service.<br><br>Note: this measure is based on the example measure suggested for this outcome in the Position Paper (p. 68). It applies to very large social media services that can make the investment in systems, processes and human resources required to detect, flag and/or remove instances of videos and images that depict and promote a terrorist act from the service. It should be noted that unlike CSAM, all video or imagery potentially within the scope of this measure requires careful human moderation because such material requires context-based judgments to determine if it is in fact material that depicts and promotes a terrorist act. We also note that hashes of this material depend on international industry cooperation through NGOs such as GIFCT who 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).<br><br>**MCM 10:** Tier 1 social media service providers must make ongoing investments in tools (for example, using hashing, machine learning, artificial intelligence, or other safety technologies) and personnel that support the capacity of the provider to detect, and take enforcement action concerning class 1A material, proportional to the incidence of class 1A material on the service and the extent class 1A materials are accessible to Australian end-users.<br><br>Note: this measure is based on the suggested measure by eSafety in the Position Paper (p68) intended to ensure that providers of Tier 1 social media 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. The guidance for this measure specifically asks that such investments are directed towards improving proactive detection tools. |
| **Matter 2**<br><br>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:<br><br>● access or exposure to, and | **Outcome 2: Industry participants take reasonable and proactive steps to prevent or limit access or exposure to, and distribution of class 1B material.**<br><br>**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 violated policies concerning class 1B material. At a minimum, they must have standard operating procedures that |

| | |
|---|---|
| ● distribution of<br>class 1B material. | (a) Include clear internal channels for personnel to escalate and prioritise reports of class 1B materials,<br>(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.<br><br>**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 prohibiting class 1B material that is proportionate to the level of harm associated with the relevant violation. As soon as reasonably practicable, they must:<br><br>(a) Remove items of class 1B material identified on the service<br>(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.<br><br>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.<br><br>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.<br><br>**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.<br><br>**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.<br><br>Note: we note, in particular, that measures 13 is designed to ensure that Tier1 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**<br><br>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 | **Outcome 4: Industry participants take reasonable and proactive steps to limit hosting of class 1A and 1B material in Australia.**<br><br>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. |

| | |
|---|---|
| limit the hosting of class 1A material and class 1B material in Australia. | |
| **Matter 5**<br><br>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.**<br><br>**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 Code and share best practice in implementing the Code and online safety in general with other industry participants.<br><br>**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.<br><br>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*.<br><br>**(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**<br><br>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.**<br><br>**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.<br><br>**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.<br><br>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**<br><br>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.**<br><br>**Outcome 7: Industry participants provide tools and/or information to limit access and exposure to class 1A and class 1B material.**<br><br>**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 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.<br><br>**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.<br><br>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.<br><br>**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.<br><br>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**<br><br>Measures directed towards achieving the objective of providing people with clear, easily accessible and effective:<br><br>● reporting mechanisms for class 1A material and class 1B material, as well as associated user accounts, and<br><br>● 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.**<br><br>**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.<br><br>**MCM 24:** Tier 1 and Tier 2 social media service providers must provide tools which enable Australian end-users to make a complaint about:<br><br>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.<br><br>**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).<br><br>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**<br><br>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:<br>● reports about class 1A material and class 1B material, as well as associated user accounts, and<br>● 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.**<br><br>**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 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.<br><br>**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.<br><br>**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.<br><br>**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.<br><br>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**<br><br>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.<br><br>Measures directed towards achieving the objective of ensuring | **Objective 3: Industry participants will strengthen transparency of, and accountability for, class 1A and class 1B material.**<br><br>**Outcome 10: Industry participants provide clear and accessible information about class 1A and class 1B material.**<br><br>**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. |

| | |
|---|---|
| that industry participants provide end-users with information about the safety issues associated with class 1A material and class 1B material. | **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.<br><br>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**<br><br>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.**<br><br>**MCM 32:** Tier 1 social media service providers must submit a Code report which as a minimum contains the following information:<br><br>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,<br><br>b) The steps that the provider has taken to comply with the applicable minimum compliance measures,<br><br>c) the volume of CSEM or pro-terror material removed by the provider of the social media service;<br><br>d) An explanation as to why these measures are appropriate.<br><br>**MCM 33:** On request by eSafety, Tier 2 social media service providers must submit to eSafety a Code report which includes the following information:<br><br>a) Details of the risk assessment it has carried out pursuant to the Code, together with information about the risk assessment methodology adopted,<br><br>b) The steps that the provider has taken to comply with their applicable minimum compliance measures,<br><br>c) An explanation as to why these measures are appropriate.<br><br>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. |
| **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 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 Heads of Terms, taking into account additional feedback provided by eSafety during the Code development process. |

## (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 assessment

As a general principle all providers of relevant electronic services must assess their risk under this Code except for providers of:

- 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.
- gaming services with limited communications functionality: a limited category of gaming services that compared to other relevant electronic services have highly restricted functionality that inhibits the ability of users to share material widely with other users.These services are automatically accorded Tier 3 (lowest risk) status. It should be noted that this limitation applies only to a subset of gaming services that meet very narrow and specific criteria, and that gaming services are otherwise required to undertake a risk assessment.
- closed communications services, such as email, SMS (short message service) and MMS.
- encrypted relevant electronic services where encryption prevents the service provider from viewing the material that is conveyed on the service.
- enterprise relevant electronic services, for example, email, messaging, and chat services provided to government and commercial enterprises.
- dating services that are accorded Tier 2 status, noting that these services have a specific purpose that inherently limits their size and reach, comparative to other relevant electronic services.

The approach to assessment of risk, and in particular the guidance on risk assessment criteria draws from the suggestions made by eSafety in the Position Paper for assessing risk.

### 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 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. 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 other categories to perform a risk assessment. This Code, therefore, contains specific measures for services with different risk tiers and for specific service categories: closed communications services, encrypted relevant electronic services, enterprise relevant electronic services and dating services. We note the addition of dating services responds to feedback from eSafety and other stakeholders during the public consultation process about how these services are treated under the Code, noting that the functionality of these services could also fall within the definition of social media service under the OSA.

| | |
|---|---|
| **Matter 1**<br><br>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:<br><br>● access or exposure to,<br><br>● distribution of, and<br><br>● online storage of<br><br>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.**<br><br>**Outcome 1: Industry participants take reasonable and proactive steps to prevent access or exposure to, distribution of, and online storage of class 1A material.**<br><br>**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.**<br><br>**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.<br><br>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 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.<br><br>**MCM 2:** Tier 1, Tier 2 relevant electronic services, closed communication and encrypted relevant electronic service 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 Australian adult or child. This must be done within 24 hours, or as soon as reasonably practicable.<br><br>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).<br><br>**MCM 3:** 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 violate terms and conditions, community standards and/or acceptable use policies that prohibit class CSEM and pro-terror material. At a minimum, they must have standard systems and processes that:<br><br>(a) Enable the review by the provider of reports by Australian end-users of CSEM and pro-terror materials,<br>(b) Enable the prioritisation and, where necessary, escalation of reports of CSEM and pro-terror material 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 does not cover 'extreme crime and violence material' which is not per se illegal under Australian law. Please see the Resolve Strategic research commissioned by DIGI/CA that supports the position taken not to include non-illegal materials for services enabling private communications within the scope of this measure.<br><br>**MCM3**: Closed communication and encrypted relevant electronic service providers must have standard operating procedures that:<br><br>(i) Refer Australian reporters of CSEM and pro-terror materials to eSafety resources, or<br>(ii) Enable the provider to take appropriate action in response to breaches of terms and conditions, community standards, and/or acceptable use policies prohibiting CSEM and pro-terror material review.<br><br>Note: this more limited measure for closed communication relevant electronic services and encrypted relevant electronic services with respect to dealing with class 1A materials was considered appropriate as providers will often not have access to relevant content) needed to make an assessment of whether materials reported to them are in fact class1A material (see guidance for this measure).<br><br>**MCM 4:** Tier 1 and Tier 2 relevant electronic service providers 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 prohibiting class 1A materials (other than CSEM and pro-terror materials).<br><br>Note: see note on MCM 3 above concerning the need for providers of services that enable private communications to take different approaches to CSEM and pro-terror materials and Class 1A materials that generally are not illegal.<br><br>**MCM 4:** Closed communication and encrypted relevant electronic service providers must have standard operating procedures that either:<br><br>i. Refer Australian reporters of class 1A materials (other than CSEM and pro- terror materials) to eSafety resources; or<br><br>ii. Enable the provider to take appropriate action in response to violations of terms and conditions, community standards, and/or acceptable use policies prohibiting class 1A materials (other than CSEM and pro-terror materials).<br><br>Note: see note on MCM 3 above about the limited capacity of many providers of these services to review material on the service.<br><br>**MCM 5:** Tier 1 and Tier 2 relevant electronic service providers must take appropriate action in response to violations of 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. At a minimum, the provider must:<br><br>a) Remove instances of CSEM or pro-terror 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,<br><br>b) Take appropriate steps designed to deter an end-user who has breached the relevant terms and conditions, community standards and/or acceptable use policies regarding CSEM or pro-terror materials from additional violations of these specific policies and standards.<br><br>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. This measure provides some discretion to relevant electronic services in relation to the enforcement action they take for breaches of policies prohibiting class 1A materials. This is based on providers' experience that breaches, especially by younger users, are not always intentional and or may be the result of coercion. The guidance elaborates relevant considerations for the development of appropriate enforcement approaches.<br><br>**MCM 6:** Tier 1, Tier 2 and encrypted relevant electronic service providers 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.<br><br>Note: this measure addresses the need for human resources that have specific safety responsibilities, which was reinforced by feedback from the public consultation process.<br><br>**MCM 7:** Closed communication and encrypted relevant electronic service providers must require a user to register for the service using a phone number, email address or other identifier.<br><br>**MCM 7:** Tier 1 and Tier 2 relevant electronic service providers must evaluate the types of features and settings they could adopt to minimise risks to Australian end-users related to class 1A material and adopt the most appropriate features and/or settings for the type of service offered.<br><br>At a minimum, a provider of Tier 1 relevant electronic service must:<br><br>a) If the service allows the sending of messages, have settings that allow users to block messages from other users,<br><br>b) If the service allows for the display of a user's online status, have tools and settings that enable end-users to be hidden or to appear offline, and<br><br>c) If the relevant electronic service allows the creation of children's accounts provide settings that are designed to prevent children from unwanted contact from strangers, including settings which:<br><br>i. make accounts of children under the age of 16 private by default, and<br><br>ii. prevent the location of child accounts being shared with any accounts other than approved accounts by default.<br><br>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;<br>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<br>c) take reasonable steps to prevent the creation of accounts by a child under 18.<br><br>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 services, including dating 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*.<br><br>**MCM 8:** All relevant electronic 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.<br><br>Note: measure 8 is designed to ensure that all relevant electronic services are committed to ongoing systematic review of the design of their services to safeguard end-users' safety.<br><br>**MCM 9:** A provider of a Tier 1 relevant electronic service with over 8 million active Australian end-users and a provider of a dating 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 behavioural signals associated with the distribution of CSAM.<br><br>This minimum measure does not apply to carriage service providers to the extent that they provide relevant electronic services via carriage services.<br><br>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 very large Tier 1 relevant electronic services and all dating 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). The measure may be satisfied by either systems and processes to detect known CSAM or behavioural signals associated with the distribution of CSAM. We think that the outcomes-based approach of the codes combined with the BOSE appropriately incentivise capable relevant electronic services to deploy these systems, processes, and technologies where reasonable.<br><br>**MCM 10.** A provider of a Tier 1 relevant electronic service with over 8 million monthly active Australian end users will implement systems, processes and/or technologies designed to detect, flag and/or remove instances of videos and images that depict and promote a terrorist act from the service, for example, through the |

| | |
|---|---|
| | use of hashing, machine learning, or artificial intelligence that scans for videos and images that may, depending on the context, depict and promote a terrorist act 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.<br><br>Note: this measure is based on the example measure suggested for this outcome in the Position Paper (p. 68). It applies to very large relevant electronic services that can make the investment in systems, processes and human resources required to detect, flag and/or remove instances of videos and images that depict and promote a terrorist act from the service. It should be noted that unlike CSAM, all video and imagery 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 video or imagery that depicts and promotes a terrorist act. 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).<br><br>**MCM 11:** Providers of Tier 1 relevant electronic services must make ongoing investments in the safe design of its services including in settings, systems, processes and /or technologies and/or personnel that provide appropriate support for the provider's compliance with the Code. This minimum measure does not apply to carriage service providers to the extent that they provide relevant electronic services via carriage services.<br><br>Note: this measure is based on the suggested measure by eSafety in the Position Paper (p. 68) intended to ensure that providers of Tier 1 relevant electronic 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.<br><br>**(Optional) Measure 12**: All relevant electronic service Where the provider has considered it appropriate and/or where it holds data that can be used for such an analysis, a provider of a relevant electronic service may implement systems, processes and/or technologies designed to detect, flag and/or remove instances of known CSAM or videos and images that depict and promote a terrorist act from the service.<br><br>Note: this measure encourages providers to implement systems to detect known CSAM and certain pro-terror material, noting that the outcomes-based approach to the Code in combination with the BOSE contain incentives for capable providers to use this technology where it is reasonable to do so. |
| **Matter 2**<br><br>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.**<br><br>**MCM 13:** Tier 1 and Tier 2 relevant electronic service providers must implement appropriate systems and processes that 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. |

| | |
|---|---|
| reasonable and proactive steps to prevent or limit:<br>● access or exposure to, and<br>● distribution of<br>class 1B material. | **MCM 13**: Closed communication and encrypted relevant electronic service providers must have standard operating procedures that either:<br>a) Refer Australian reporters of class 1B materials to eSafety resources, or<br>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.<br>**MCM 14:** Tier 1 and Tier 2 relevant electronic service providers must take appropriate action in response to violations 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.<br>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. Measure 11 provides an option for providers that may not have visibility over materials to refer reporters of Class1B material to eSafety resources (noting that such material is not illegal and part of a private communication.) See further the Resolve Strategic Research about community views on class1 material online. |
| **Matter 4**<br>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.**<br>This outcome does not require additional measures for relevant electronic services (see preamble to Heads of Terms). |
| **Matter 5**<br>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. | **Objective 1: Industry participants will take reasonable and proactive steps to create and maintain a safe online environment for Australian end-users.**<br>**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.**<br>**MCM 17:** Tier 1, closed communication and encrypted relevant electronic 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 Code and share best practice in implementing the Code and online safety in general with other industry participants.<br>**(Optional) Measure 18:** Tier 1, Tier 2, closed communication and encrypted relevant electronic 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 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.<br><br>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**<br><br>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.**<br><br>**MCM 19:** Tier 1 and encrypted 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 28.<br><br>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. |
| **Matter 7**<br><br>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.**<br><br>**Outcome 7: Industry participants provide tools and/or information to limit access and exposure to class 1A and class 1B material.**<br><br>**MCM 20:** Tier 1, Tier 2, closed communication and encrypted relevant electronic service providers 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 21.<br><br>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**<br><br>Measures directed towards achieving the objective of providing people with clear, easily accessible and effective:<br><br>● reporting mechanisms for class 1A material and class 1B | **Outcome 8: Industry participants provide clear and effective reporting and complaints mechanisms for class 1A and class 1B material.**<br><br>**MCM 21**: Tier 1 and Tier 2 relevant electronic service providers 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 |

| | |
|---|---|
| material, as well as associated user accounts, and<br>● complaints mechanisms to address complaints about the handling of reports about class 1A material and class 1B material and codes compliance. | an overview of the reporting process, and the identity of the reporter must be protected from the reported end-user or account holder.<br>**MCM 21:** Closed communication and encrypted relevant electronic service providers must:<br>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,<br>ii. Make available, via its website, a link to eSafety's online content reporting form, and<br>iii. Respond promptly to complaints about class 1A or class 1B material made by Australian end-users by either<br>a. responding to the complaint, or<br>b. referring the complainant to eSafety.<br>**MCM 22:** Tier 1, Tier 2, closed communication and encrypted 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.<br>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**<br>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:<br>● reports about class 1A material and class 1B material, as well as associated user accounts, and<br>● 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.**<br>**MCM 23:** Tier 1 and Tier 2 relevant electronic service providers must:<br>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,<br>b) Implement and document policies and procedures which detail how it gives effect to the requirement in (a), and<br>c) Ensure that personnel responding to reports are trained in the relevant electronic service's policies and procedures for dealing with reports.<br>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, which further strengthens these requirements concerning the handling of reports and complaints. |
| **Matter 10**<br>Measures directed towards achieving the objective of ensuring that industry participants publish easily accessible and plain language policies, procedures and | **Objective 3: Industry participants will strengthen transparency of, and accountability for, class 1A and class 1B material.**<br>**Outcome 10: Industry participants provide clear and accessible information about class 1A and class 1B material.** |

| | |
|---|---|
| guidelines that set out how they handle class 1A material and class 1B material.<br><br>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. | **MCM 24:** Tier 1, Tier 2 relevant electronic services, closed communication and encrypted relevant electronic service providers 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.<br><br>**(Optional) Measure 25:** Tier 1, Tier 2 relevant electronic services, closed communication and encrypted relevant electronic service 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.<br><br>**MCM 26:** Tier 1 relevant electronic service providers 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.<br><br>**MCM 27:** Tier 1 or Tier 2 relevant electronic service providers must publish easily accessible and understandable information that explains the tools and settings they make available under minimum compliance measure 7 (Safety by design).<br><br>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**<br><br>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.**<br><br>**MCM 28:** Tier 1 relevant electronic service must submit a Code report which as a minimum contains the following information:<br><br>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;<br><br>b) The steps that the provider has taken to comply with the applicable minimum compliance measures;<br><br>c) the volume of CSEM or pro terror material removed by the provider of the relevant electronic service; and<br><br>d) An explanation as to why these measures are appropriate.<br><br>**MCM 29:** On request by eSafety, Tier 2 relevant electronic service providers must submit to eSafety a Code report which includes the following information:<br><br>e) 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;<br>f) the steps that the provider has taken to comply with their applicable minimum compliance measures;<br>g) an explanation as to why these measures are appropriate.<br>**MCM 30:** On request by eSafety, closed communication and encrypted relevant electronic service providers must submit to eSafety a Code report which includes the following information:<br>h) the steps that the provider has taken to comply with their applicable minimum compliance measures; and<br>i) an explanation as to why these measures are appropriate.<br>**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.<br>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. |
| **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 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. |

## (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 is not fixed as it can be amended by the Minister by legislative instrument. 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;
- 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 accorded a Tier 1 risk profile, e.g., pornography sites that allow end-users to post high impact 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, sited 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 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**<br><br>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:<br><br>● access or exposure to,<br><br>● distribution of, and<br><br>● online storage of<br><br>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.**<br><br>**Outcome 1: Industry participants take reasonable and proactive steps to prevent access or exposure to, distribution of, and online storage of class 1A material.**<br><br>**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.**<br><br>**MCM 1:** Providers of an enterprise designated internet service must:<br><br>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<br><br>b) take appropriate action to enforce breaches of that agreement by the enterprise customer.<br><br>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.<br><br>**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 Australian adult or child. This must be done within 24 hours or as soon as reasonably practicable.<br><br>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*.<br><br>**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.<br><br>At a minimum, a Tier 1 designated internet service provider must:<br><br>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<br><br>b) Terminate an Australian end-user's account as soon as reasonably practicable in the event the Australian end-user is:<br><br>a. distributing CSEM or pro-terror materials to Australian end-users with the intention to cause harm,<br><br>b. known to be an Australian child, or<br><br>c. has repeatedly violated terms and conditions, community standards and/or acceptable use policies prohibiting CSEM and pro-terror materials on the service, and<br><br>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.<br><br>d) In the case of end-user-managed hosting services, having standard operating procedures that either refer Australian reporters of class 1A materials to eSafety resources; or enable the provider to take appropriate action in response |

| | |
|---|---|
| | to breaches of terms and conditions, community. standards, and/or acceptable use policies prohibiting CSEM and pro-terror materials.<br><br>Examples of appropriate action for a Tier 2 designated internet service include:<br><br>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;<br><br>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:<br><br>i) issuing warnings to end-users;<br><br>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);<br><br>iii) suspending the end-user's account for a defined period;<br><br>iv) terminating the end-user's account; or<br><br>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.<br><br>**MCM 4:** 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, prohibiting class 1A materials (other than CSEM and pro-terror materials).<br><br>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*.<br><br>**MCM 5:** 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.<br><br>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:** 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.<br><br>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.<br><br>**MCM 7:** 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:<br><br>a) Automatically detect and flag known CSAM such as hash-matching technologies (for example, PhotoDNA, CSAI Match, and equivalent technology),<br><br>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<br><br>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.<br><br>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.<br><br>**MCM 8:** Tier 1 designated internet service providers must make ongoing investments in systems and processes and/or technologies (for example, using hashing, machine learning, artificial intelligence or other safety technologies) and personnel that support the capacity of the provider to detect, and take appropriate action concerning known CSAM, proportionate to the incidence of such materials on the service and the extent such materials are accessible to Australian end-users.<br><br>Note: this measure is based on eSafety's suggested measure in the Position Paper (see p68) and 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 2**<br><br>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:<br><br>● access or exposure to, and<br><br>● distribution of<br><br>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.**<br><br>**MCM 9:** See MCM 6 above.<br><br>**MCM 10:** 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.<br><br>**MCM 11:** 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:<br><br>a) Implement measures that ensure that material can only be posted to or distributed on the service by a registered account holder,<br><br>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<br><br>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.<br><br>Note: this measure makes best practice operating procedures to ensure that users that post material on a Tier 1 service 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*.<br><br>**MCM 12:** 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.<br><br>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**<br><br>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 | **Outcome 4: Industry participants take reasonable and proactive steps to limit hosting of class 1A and 1B material in Australia.**<br><br>**MCM 13:** 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. |

| | |
|---|---|
| limit the hosting of class 1A material and class 1B material in Australia. | **MCM 14:** 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.<br><br>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**<br><br>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.**<br><br>**(Optional) Measure 15:** Tier 1 and Tier 2 designated internet service and end-user-managed hosting service providers may adopt measures to support this matter in relation to class 1A or class 1B material, including for example:<br><br>a) Joining industry organisations intended to address serious online harms, and/or share information on best practice approaches, that are relevant to the service,<br><br>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,<br><br>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<br><br>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.<br><br>Note: this measure provides a range of options for Tier 1 and Tier 2 designated internet services to consult, cooperate and collaborate amongst providers of designated internet services that is appropriate for the very diverse types of businesses that are within the scope of these measures. The outcomes-based approach of the Codes in combination with the BOSE (see expectation 10) incentivises capable providers of Tier 1 and Tier 2 services to adopt measures concerning cooperation and collaboration that are reasonable for their business. |

| | |
|---|---|
| **Matter 6**<br><br>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.**<br><br>**MCM 16:** 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.<br><br>**MCM 17:** 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.<br><br>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.<br><br>**MCM 18:** 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**<br><br>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.**<br><br>**Outcome 7: Industry participants provide tools and/or information to limit access and exposure to class 1A and class 1B material.**<br><br>**MCM 19:** 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.<br><br>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**<br><br>Measures directed towards achieving the objective of providing people with clear, easily accessible and effective:<br><br>● reporting mechanisms for class 1A material and class 1B material, as well as associated user accounts, and | **Outcome 8: Industry participants provide clear and effective reporting and complaints mechanisms for class 1A and class 1B material.**<br><br>**MCM 20:** 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, 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 |

| | |
|---|---|
| ● complaints mechanisms to address complaints about the handling of reports about class 1A material and class 1B material and codes compliance. | 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.<br><br>**MCM 21:** 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.<br><br>Note: this measure builds on examples provided by eSafety in the Position Paper (see p. 71) |
| **Matter 9**<br><br>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:<br><br>● reports about class 1A material and class 1B material, as well as associated user accounts, and<br><br>● 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.**<br><br>**MCM 22**: Tier 1 designated internet service providers must:<br><br>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<br><br>b) Ensure that an Australian end-user who reports class 1A or class 1B materials is:<br><br>i. informed in a reasonably timely manner of the outcome of the report,<br><br>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<br><br>iii. notified of the outcome of a review under sub-measure ii).<br><br>**MCM 23:** 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.<br><br>**MCM 24:** 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.<br><br>**MCM 25:** 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.<br><br>**MCM 26:** 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.<br><br>**MCM 27:** 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 28:** 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.<br><br>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**<br><br>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.<br><br>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.**<br><br>**Outcome 10: Industry participants provide clear and accessible information about class 1A and class 1B material.**<br><br>**MCM 29:** 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.<br><br>**MCM 30:** 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.<br><br>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**<br><br>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.**<br><br>**MCM 31:** Tier 1 designated internet service providers must submit a Code report which as a minimum contains the following information:<br><br>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,<br><br>b) The steps that the provider has taken to comply with the applicable minimum compliance measures,<br><br>c) the volume of CSEM or pro terror material removed by the provider of the designated internet service; and<br><br>d) An explanation as to why these measures are appropriate.<br><br>**MCM 32:** 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,<br><br>b) The steps that the provider has taken to comply with their applicable minimum compliance measures,<br><br>c) An explanation as to why these measures are appropriate.<br><br>**MCM 33:** On request by eSafety, end-user-managed hosting service providers must submit to eSafety a Code report which includes the following information:<br><br>a) The steps that the provider has taken to comply with their applicable minimum compliance measures,<br><br>b) An explanation as to why these measures are appropriate.<br><br>**MCM 34:** On request by eSafety, an enterprise designated electronic service provider must confirm in writing to eSafety that the provider is compliant with MCM 1.<br><br>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. |
| **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**<br><br>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:<br><br>● access or exposure to,<br>● distribution of, and<br>● online storage of<br><br>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.**<br><br>**Outcome 1: Industry participants take reasonable and proactive steps to prevent access or exposure to, distribution of, and online storage of class 1A material.**<br><br>**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.**<br><br>**MCM 1:** All internet search engine service providers must make ongoing investments in technology 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:<br><br>a) Make available to Australian end-users, information about policies for and approach to indexing web pages, and<br><br>b) Continually review and/or test the performance of algorithms in meeting the above objectives.<br><br>**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,<br><br>b) Delist links to class 1A materials pursuant to a legal removal request,<br><br>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,<br><br>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,<br><br>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,<br><br>f) Provide access to tools, such as 'safe search' functionality, which enable users to limit exposure to explicit and / or graphic content,<br><br>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<br><br>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.<br><br>**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.<br><br>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.<br><br>**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.<br><br>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**<br><br>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:<br>● access or exposure to, and<br>● distribution of<br>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.**<br><br>**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 sources of online information and demoting the accessibility of class 1B materials in search results.<br><br>**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.<br><br>Note: this measure builds on the examples in eSafety's Position Paper (see p.69). |
| **Matter 4**<br><br>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.**<br><br>This Outcome is not applicable to internet search engine services (See preamble to Head Terms). |
| **Matter 5**<br><br>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.**<br><br>**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.<br><br>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**<br><br>Measures directed towards achieving the objective of ensuring that industry participants have | **Outcome 6: Industry participants communicate and cooperate with eSafety in respect of matters relating to class 1A and class 1B material, including complaints.**<br><br>**MCM 8:** All internet search engine service providers must refer to eSafety complaints from the public concerning the provider's |

| | |
|---|---|
| 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. | noncompliance with this Code, where the provider is unable to resolve the complaint within a reasonable time frame.<br><br>**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.<br><br>Note: this measure builds on example measures in the Position Paper (see p. 70). |
| **Matter 7**<br><br>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.**<br><br>**Outcome 7: Industry participants provide tools and/or information to limit access and exposure to class 1A and class 1B material.**<br><br>**MCM 10:** All internet search engine service providers must implement the following measures:<br><br>a) Provide age-appropriate safety settings,<br><br>b) Make available clear and accessible guidelines about the use and effect of such safety settings,<br><br>c) Make available clear and accessible information about the use and effect of tools available to Australian end-users, and<br><br>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.<br><br>Note: this measure builds on examples provided by eSafety in the Position Paper (see p. 71). |
| **Matter 8**<br><br>Measures directed towards achieving the objective of providing people with clear, easily accessible and effective:<br><br>● reporting mechanisms for class 1A material and class 1B material, as well as associated user accounts, and<br><br>● 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.**<br><br>**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.<br><br>**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.<br><br>**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.<br><br>**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.<br><br>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**<br><br>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:<br><br>● reports about class 1A material and class 1B material, as well as associated user accounts, and<br><br>● 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.**<br><br>**MCM 15:** <u>All internet search engine service</u> providers must have appropriate personnel, policies, processes, systems and technologies in place to respond to reports by Australian end-users.<br><br>At a minimum, a provider of an internet search engine service must implement the following measures to address reports:<br><br>a) Implement policies, procedures, and systems to enable the automated, human, or hybrid triaging and review and response to reports by Australian end-users,<br><br>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,<br><br>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,<br><br>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:<br><br>i) identifies CSEM on its service; and<br><br>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.<br><br>**MCM 16:** <u>All internet search engine service</u> 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.<br><br><u>Note:</u> 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**<br><br>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 | **Objective 3: Industry participants will strengthen transparency of, and accountability for, class 1A and class 1B material.**<br><br>**Outcome 10: Industry participants provide clear and accessible information about class 1A and class 1B material.**<br><br>**MCM 17:** <u>All internet search engine service</u> providers must publish easily accessible and plain language information on their approaches to class 1A and class 1B material. An internet search |

| | |
|---|---|
| handle class 1A material and class 1B material.<br><br>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. | engine service provider must at a minimum implement the following measures:<br><br>a) Provide information to Australian end-users about the ways in which the internet search engine service ranks information,<br><br>b) Provide information on the actions that may be taken to report links to illegal materials,<br><br>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,<br><br>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,<br><br>e) Provide information to Australian end-users about online safety risks and guidance on how to mitigate these risks, and<br><br>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.<br><br>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**<br><br>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.**<br><br>**MCM 18:** On request**,** all internet search engine service providers must submit to eSafety a Code report which includes the following information:<br><br>a) The steps that the provider has taken to comply with their applicable minimum compliance measures,<br><br>b) An explanation as to why these measures are appropriate, and<br><br>c) annual updates about the volume of CSEM or pro-terror material flagged and responded to by the internet search engine service.<br><br>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. |
| **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. |

## (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**<br><br>Measures directed towards achieving the objective of ensuring that industry participants have | **Objective 1: Industry participants will take reasonable and proactive steps to create and maintain a safe online environment for Australian end-users.** |

| | |
|---|---|
| scalable and effective policies, procedures, systems and technologies in place to take reasonable and proactive steps to **detect and** prevent:<br>● access or exposure to,<br>● distribution of, and<br>● online storage of<br>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.**<br>**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.**<br>**MCM 1:** All app distribution service providers must:<br>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,<br>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 measure 1) a),<br>c) 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<br>d) Take steps to ensure all third-party app providers are made aware of other industry codes made under the OSA that may apply to them in their role as the app provider.<br>Note: The example measures provided in the Position Paper for this matter assume that services are able to 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.<br>**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.<br>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**<br>Measures directed towards achieving the objective of ensuring that industry participants have scalable and effective policies, | **Outcome 2: Industry participants take reasonable and proactive steps to prevent or limit access or exposure to, and distribution of class 1B material.**<br>**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 |

| | |
|---|---|
| procedures, systems and technologies in place to take reasonable and proactive steps to prevent or limit:<br>● access or exposure to, and<br>● distribution of<br>class 1B material. | at the time those third-party apps are released on the app distribution service.<br>Note: this measure builds on best practice by app providers to inform users about the suitability of apps for different age groups. |
| **Matter 4**<br>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.**<br>This Outcome is not applicable to app distribution service providers. (See preamble to Head Terms.) |
| **Matter 5**<br>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.**<br>**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.<br>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. |
| **Matter 6**<br>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.**<br>**MCM 5:** 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.<br>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**<br>Measures directed towards achieving the objective of providing people with a range of technical tools and/or information to limit their | **Objective 2: Industry participants will empower people to manage access and exposure to class 1A and class 1B material.** |

| | |
|---|---|
| access and exposure, and the access and exposure of children in their care, to class 1A material 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.**<br><br>**MCM 6:** All app distribution service providers must provide online safety resources that include clear and accessible information for Australian end-users regarding:<br><br>a) The age and/or content ratings approach used by the app distribution service provider pursuant to measure 3,<br><br>b) Steps that parents and guardians may take to supervise and manage children's use of apps,<br><br>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),<br><br>d) Information about the mechanisms in measure 7, and<br><br>e) The role and functions of eSafety, including how to make a complaint to eSafety.<br><br>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 that supports online safety of end-users including information about how end-users can make a complaint to eSafety. |
| **Matter 8**<br><br>Measures directed towards achieving the objective of providing people with clear, easily accessible and effective:<br><br>● reporting mechanisms for class 1A material and class 1B material, as well as associated user accounts, and<br><br>● 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.**<br><br>**MCM 7:** All app distribution service providers must provide a mechanism that enables Australian end-users to report or make a complaint about:<br><br>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<br><br>b) A breach of this Code by the app distribution service provider.<br><br>The reporting tool and complaints mechanism must:<br><br>a) Be easily accessible and easy to use; and<br><br>b) Be accompanied by plain language instructions on how to use it, as well as an overview of the reporting process.<br><br>Note: 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**<br><br>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:<br><br>● reports about class 1A material and class 1B material, as well as associated user accounts, and<br><br>● 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.**<br><br>By complying with the minimum compliance measures under Outcome 8, app distribution service providers will also meet the requirements of this Outcome. |
| **Matter 10**<br><br>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.<br><br>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.**<br><br>**Outcome 10: Industry participants provide clear and accessible information about class 1A and class 1B material.**<br><br>By complying with the minimum compliance measures under Outcome 7, app distribution service providers will also meet the requirements of this Outcome. |
| **Matter 11**<br><br>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**<br><br>**MCM 8:** On request, all app distribution service providers must submit to eSafety a Code report which includes the following information:<br><br>a) the steps that the provider has taken to comply with their applicable minimum compliance measures,<br><br>b) an explanation as to why these measures are appropriate.<br><br>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. |
| **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 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. |

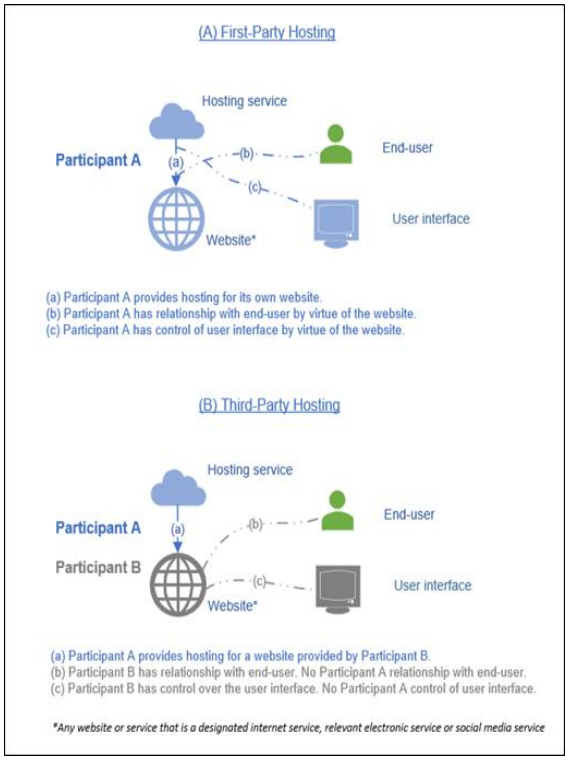
## (6) Hosting Services Online Safety Code (Class 1A and Class 1B Material)

### 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:




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**<br>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:<br>● access or exposure to,<br>● distribution of, and<br>● online storage of<br>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.**<br>**Outcome 1: Industry participants take reasonable and proactive steps to prevent access or exposure to, distribution of, and online storage of class 1A material.**<br>**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.**<br>Note: the appropriate measures for this outcome are the same as those addressing outcomes 4 and 5. |
| **Matter 2**<br>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.**<br>Note: the appropriate measures for this outcome are the same as those addressing outcomes 4 and 5. |

| | |
|---|---|
| reasonable and proactive steps to prevent or limit:<br>● access or exposure to, and<br>● distribution of<br>class 1B material. | |
| **Matter 4**<br>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.**<br><br>**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.<br><br>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.<br><br>**MCM 2:** All Third-Party Hosting Service providers must ensure that the following policies and/or contractual terms are in place to take appropriate and proportionate enforcement action with respect to customers of the service that violate its policies prohibiting class 1A and class 1B material:<br><br>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,<br><br>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<br><br>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.<br><br>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 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 be generally 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.<br><br>**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.<br><br>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**<br><br>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.**<br><br>**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:<br><br>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,<br><br>b) Joining industry organisations intended to address serious online harms, and/or share information on best practice approaches, that are relevant to Third-Party Hosting Services,<br><br>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,<br><br>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<br><br>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.<br><br>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**<br><br>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.**<br><br>**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.<br><br>Note: this measure is based on one of the example measures suggested for this Outcome in the Position Paper (p. 70). |
| **Matter 7**<br><br>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.**<br><br>**Outcome 7: Industry participants provide tools and/or information to limit access and exposure to class 1A and class 1B material.**<br><br>**MCM 6:** All Third-Party Hosting Service providers must offer customers of the service:<br><br>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<br><br>b) Clear and accessible guidance about how to use and the effect of any such tools, settings or information.<br><br>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**<br><br>Measures directed towards achieving the objective of providing people with clear, easily accessible and effective:<br><br>● reporting mechanisms for class 1A material and class 1B material, as well as associated user accounts, and<br><br>● 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.**<br><br>**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.<br><br>Note: please see the note on MCM 3 in respect of Outcome 4 above. |

| | |
|---|---|
| **Matter 9**<br><br>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:<br><br>● reports about class 1A material and class 1B material, as well as associated user accounts, and<br><br>● 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.**<br><br>**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.<br><br>**MCM 6:** All Third-Party Hosting Service providers must offer customers of the service:<br><br>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<br><br>b) Clear and accessible guidance about how to use and the effect of any such tools, settings or information.<br><br>Note: please see the notes on MCMs 3 and 6 in respect of Outcome 4 and 7 above. |
| **Matter 10**<br><br>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.<br><br>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.**<br><br>**Outcome 10: Industry participants provide clear and accessible information about class 1A and class 1B material.**<br><br>**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:<br><br>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<br><br>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.<br><br>Note: Outcome 10 is also partially addressed through the measures addressing Outcome 4 above. |
| **Matter 11**<br><br>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.**<br><br>**MCM 8:** On request, all third-party hosting service providers must submit to eSafety a Code report which includes the following information:<br><br>a) The steps that the provider has taken to comply with their applicable minimum compliance measures,<br><br>b) An explanation as to why these measures are appropriate. |

| | |
|---|---|
| | 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[13]: 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**<br><br>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:<br><br>● access or exposure to,<br><br>● distribution of, and | **Objective 1: Industry participants will take reasonable and proactive steps to create and maintain a safe online environment for Australian end-users.**<br><br>**Outcome 1: Industry participants take reasonable and proactive steps to prevent access or exposure to, distribution of, and online storage of class 1A material.**<br><br>**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.**<br><br>**MCM 1:** All internet service providers must inform its Australian end-users that they must not produce online material that is in |

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

| | |
|---|---|
| ● online storage of<br>class 1A material. | contravention of any Australian State, Territory, or Commonwealth law, including the OSA.<br><br>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**<br><br>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:<br>● access or exposure to, and<br>● distribution of<br>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.**<br><br>This Outcome does not have any separate measures as ISPs cannot see, inspect or differentiate between the material that traverses their networks. |
| **Matter 4**<br><br>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.<br><br>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**<br><br>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.**<br><br>**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.<br><br>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** | **Outcome 6: Industry participants communicate and cooperate with eSafety in respect of matters relating to class 1A and class 1B material, including complaints.** |

| | |
|---|---|
| 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. | **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.<br><br>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.<br><br>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**<br><br>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.**<br><br>**Outcome 7: Industry participants provide tools and/or information to limit access and exposure to class 1A and class 1B material.**<br><br>**MCM 4:** All internet service providers must make information available to Australian end- users on filtering products and how they can be obtained. This information must be easily accessible.<br><br>**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.<br><br>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.<br><br>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**<br><br>Measures directed towards achieving the objective of providing people with clear, easily accessible and effective:<br>● reporting mechanisms for class 1A material and class 1B material, as well as associated user accounts, and<br>● 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.**<br><br>**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.<br><br>**MCM 7:** All internet service providers must make available, via their website, a link to eSafety's online content complaints reporting form.<br><br>Note: this measure achieves the objective by 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**<br><br>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:<br>● reports about class 1A material and class 1B material, as well as associated user accounts, and<br>● 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.**<br><br>**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.<br><br>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). |
| **Matter 10**<br><br>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.<br><br>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.**<br><br>**Outcome 10: Industry participants provide clear and accessible information about class 1A and class 1B material.**<br><br>**MCM 9:** All internet service providers must make accessible to Australian end-users, information 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.<br><br>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**<br><br>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.**<br><br>**MCM 10:** On request, all internet service providers must submit to eSafety a Code report which includes the following information:<br>a) The steps that the provider has taken to comply with their applicable minimum compliance measures,<br>b) An explanation as to why these measures are appropriate.<br><br>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 burdon 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 manufactures, suppliers and installers and maintenance providers as defined in the OSA and operating system providers.

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 Code also contains specific measures for devices designed primarily to enable end-users to play online games with other end-user 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**<br>Measures directed towards achieving the objective of ensuring | **Objective 1: Industry participants will take reasonable and proactive steps to create and maintain a safe online environment for Australian end-users.** |

| | |
|---|---|
| that industry participants have scalable and effective policies, procedures, systems and technologies in place to take reasonable and proactive steps to **detect and** prevent:<br>● access or exposure to,<br>● distribution of, and<br>● online storage of<br>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.**<br>**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.**<br>By complying with the minimum compliance measures under Outcome 7, equipment providers will also meet the requirements of this Outcome. |
| **Matter 2**<br>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:<br>● access or exposure to, and<br>● distribution of<br>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.**<br>By complying with the minimum compliance measures under Outcome 7, equipment providers will also meet the requirements of this Outcome. |
| **Matter 4**<br>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.**<br>This Outcome is not applicable to equipment providers and OS providers. |
| **Matter 5**<br>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 | **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.**<br>**MCM 1:** A manufacturer of an interactive (Tier 1) 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.<br>**(Optional) Measure 2:** An industry participant who is:<br>1. a manufacturer of a secondary (Tier 2) device or a non-interactive (Tier 3) device. |

| | |
|---|---|
| accounts associated with this material. | 2. a supplier,<br>3. a maintenance provider, or<br>4. an installation provider,<br>may choose to attend the industry forum referred to in measure 1.<br>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 given the vast numbers of suppliers. |
| **Matter 6**<br>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.**<br>**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.<br>**MCM 4:** A manufacturer of an interactive (Tier 1) device 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.<br>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, noting that these are proactive obligations supplementary to eSafety's power to respond directly to complaints about breaches of the Codes. |
| **Matter 7**<br>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.**<br>**Outcome 7: Industry participants provide tools and/or information to limit access and exposure to class 1A and class 1B material.**<br>**MCM 5:** A manufacturer of an interactive (Tier 1) device or devices designed primarily to enable end-users to play online games with other end-users 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.<br>A manufacturer of an interactive (Tier 1) device or devices designed primarily to enable end-users to play online games with other end-users 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.<br>A supplier of interactive (Tier 1) devices (incl. children's interactive devices) must provide easily accessible information with respect to the safe use of interactive (Tier 1) devices online by Australian |

| | |
|---|---|
| | end-users 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.<br><br>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.<br><br>**MCM 6:**<br><br>a) OS providers must take reasonable steps to develop and implement tools within operating systems that allow Australian end-users to help reduce the risk of harm to children when using interactive (Tier 1) devices.<br><br>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<br><br>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.<br><br>**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.<br><br>**(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.<br><br>**(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.<br><br>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.<br><br>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 can play in providing safety tools and settings for all interactive (Tier 1) devices, noting these devices have higher risk profiles. |

| | |
|---|---|
| **Matter 8**<br><br>Measures directed towards achieving the objective of providing people with clear, easily accessible and effective:<br><br>● reporting mechanisms for class 1A material and class 1B material, as well as associated user accounts, and<br><br>● 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.**<br><br>**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.<br><br>**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.<br><br>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**<br><br>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:<br><br>● reports about class 1A material and class 1B material, as well as associated user accounts, and<br><br>● 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.**<br><br>**MCM 11:** 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.<br><br>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**<br><br>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.<br><br>Measures directed towards achieving the objective of ensuring that industry participants provide end-users with information about | **Objective 3: Industry participants will strengthen transparency of, and accountability for, class 1A and class 1B material.**<br><br>**Outcome 10: Industry participants provide clear and accessible information about class 1A and class 1B material.**<br><br>By complying with the minimum compliance measures under Outcome 7, equipment providers will also meet the requirements of this Outcome. |

| | |
|---|---|
| the safety issues associated with class 1A material and class 1B material. | |
| **Matter 11**<br><br>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.**<br><br>**MCM 13:** A manufacturer of interactive (Tier 1) devices and/or OS providers must submit a Code report which as a minimum contains:<br><br>a) The steps that the manufacturer and/or OS provider has taken to comply with the applicable minimum compliance measures; and<br><br>b) An explanation as to why these measures are appropriate.<br><br>**MCM 14:** On request by eSafety, a manufacturer of secondary (Tier 2) devices must submit a Code report which includes the following formation:<br><br>a) An explanation as to why the manufacturer considers the device to be a secondary (Tier 2) device,<br><br>b) The steps that the manufacturer has taken to comply with their applicable minimum compliance measures, and<br><br>c) An explanation as to why these measures are appropriate.<br><br>Note: equipment and OS providers cannot remove material, and, consequently, cannot publish annual reports in relation to such material. This measure aims at providing eSafety with information about compliance with this Code without placing unnecessary regulatory burden on equipment and OS providers. 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. Website / social media / general online communications

The industry associations published 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 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.[14]

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.

### 4.5.2. Targeted invitations for submissions

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:**

- Alannah & Madeleine Foundation
- Australian Centre to Counter Child Exploitation (ACCCE)
- Bravehearts
- Global Internet Forum to Counter Terrorism (GIFCT)
- Inhope
- International Center for Missing & Exploited Children (ICMEC)
- National Center for Missing & Exploited Children (NCMEC)
- Tech Against Terrorism

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

- The Carly Ryan Foundation
- The Daniel Morcombe Foundation
- WeProtect Global Alliance

**Organisations representing children and young people:**

- Australian Research Alliance for Children and Youth
- Australian Youth Affairs Coalition
- Commissioner for Children and Young People South Australia
- Multicultural Youth Advocacy Network (MYAN) NSW
- National Children's Commissioner, Australian Human Rights Commission
- Office of the Advocate for Children and Young People NSW
- The Children and Young People Commissioner Australian Capital Territory
- The Children's Commissioner Northern Territory
- The Commission for Children and Young People Victoria
- The Commissioner for Children and Young People Western Australia
- The Commissioner for Children Tasmania
- The Office of the Guardian for Children and Young People South Australia
- The Office of the Public Guardian Queensland
- UNICEF (United Nations Children's Fund)
- Yourtown
- Youth Affairs Council of Victoria
- Youth Affairs Council of Western Australia

**Organisations representing parents, carers, teachers and educators:**

- Australian Education Union (AEU) NT Branch
- Australian Education Union (AEU) SA Branch
- Australian Education Union (AEU) TAS Branch
- Australian Education Union (AEU)ACT Branch
- Australian Education Union Victoria
- New South Wales Teachers Federation
- Queensland Teachers Union
- State School Teachers Union of Western Australia

**Women's advocacy groups:**

- Communicare
- Domestic and family violence groups
- Domestic Violence Service Management (DVSM)
- DVConnect Queensland
- Economic Abuse Reference Group
- Katherine Women's Legal Service
- National Council of Women Australia
- Relationships Australia

- Safe Steps
- United Nations (UN) Women
- White Ribbon Australia
- Women's Legal Service NSW
- Women's Services Network (WESNET)

**Organisations representing sex workers:**

- Assembly Four
- Australian Queer Archives
- Eros Association
- LGBTIQ+ Health Australia
- Scarlett Alliance

**Organisations in the area of safety technology / digital trust:**

- Digital Trust & Safety Partnership
- Family Zone
- Online Safety Tech Industry Association (OSTIA)
- Safety Tech Innovation Network

**Organisations representing consumers:**

- Australian Communications Consumer Action Network (ACCAN)
- Choice
- Consumer Action
- Consumer Action Law Centre
- Consumer Policy Research Centre
- Consumers Association of South Australia
- Consumers Federation of Australia
- Queensland Consumers Association

**Organisations representing legal interests and other advocacy areas:**

- Community Legal Centres Australia
- Darwin Community Legal Service
- Law Council of Asia & the Pacific
- Law Council of Australia
- Law Society of Australian Capital Territory
- Law Society of New South Wales
- Law Society of Tasmania
- Law Society of the Northern Territory
- Law Society of Victoria
- Law Society of Western Australia
- Public Interest Advocacy Centre
- Queensland Law Society

**Representatives from academia:**

- Allens Hub for Technology, Law and Innovation
- Australian National University (ANU) College of Law
- Australian National University (ANU) Tech Policy Design Centre
- Australian Research Council (ARC) Centre of Excellence for the Digital Child
- Australian Strategic Policy Institute (ASPI)
- Berkeley University
- Canberra University
- Charles Sturt University, Centre for Law and Justice
- Harvard University
- Latrobe University
- Minderoo Tech & Policy Lab
- Queensland University of Technology (QUT) Digital Media Research Centre
- Royal Melbourne Institute of Technology (RMIT) University
- Stanford University
- Swinburne University
- University of California, Irvine
- University of Melbourne
- University of New South Wales (UNSW), School of Law, Society & Criminology
- University of Ottowa
- University of Techhnology Sydney (UTS)
- University of the Sunshine Coast
- University of Western Australia
- Western Sydney University (UWS) Young & Resilient Centre

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

- .auDA
- ACT | The App Association
- Asia Internet Coalition (AIC)
- Australian Banking Association
- Australian Chamber of Commerce and Industry
- Australian Copyright Council
- Australian Industry Group
- Australian Information Industry Association
- Australian Society of Authors
- Business Council of Australia
- Computer & Communications Industry Association (CCIA)
- Council of Small Business Organisations Australia (COSBOA)
- Information Technology Industry Council (ITIC)
- Internet Association of Australia
- IoT Alliance Australia
- Music Australia

- Screen Australia
- Standards Australia
- Tech Council of Australia
- Tech UK
- The Australian Digital Alliance
- Universities Australia

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

- Australian Community Managers
- Australian Council for Civil Liberties
- Australian Privacy Foundation
- IIS Partners
- Reset Australia

**Organisations working in the area of digital rights / policy:**

- AccessNow
- American Civil Liberties Union
- Australia's Internet Governance Forum
- Australian Seniors Computer Clubs Association (ASCCA)
- Brookings Institute
- Center for Democracy & Technology (CDT)
- Center for Information Policy Leadership
- Centre for Digital Wellbeing
- Centre for Responsible Technology
- Digital Rights Watch
- Electronic Frontier Foundation
- Electronic Frontiers Australia
- Future of Privacy Forum
- Global Network Initiative (GNI)
- Human Rights Watch
- Index on Censorship
- Internet Australia
- Internet Society
- Knight First Amendment Institute
- LGBT Tech
- Ranking Digital Rights

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

- Australian Communications and Media Authority
- Australian Human Rights Commission
- Australian Institute of Criminology
- Department of Home Affairs

- Department of Infrastructure, Transport, Regional Development, Communications and the Arts
- Office of the Australian Information Commissioner

### 4.5.3. Stakeholder Roundtable

Furthermore, during the 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:

- .auDA
- Access Now
- Alannah & Madeleine Foundation
- Assembly Four
- Australian Communications Consumer Action Network (ACCAN)
- Business Council of Australia (BCA)
- Consumer Action
- Council of Small Business Organisations Australia (COSBOA)
- Daniel Morcombe Foundation
- Digital Rights Watch
- Digital Trust & Safety Partnership
- Electronic Frontiers Australia
- Global Network Initiative (GNI)
- International Center for Missing & Exploited Children (ICMEC)
- Law Council of Asia & the Pacific
- Law Council of Australia
- Queensland University of Technology (QUT) Digital Media Research Centre
- Scarlett Alliance
- Swinburne University
- Tech Against Terrorism
- The Carly Ryan Foundation
- University of New South Wales (UNSW), School of Social Sciences
- Western Sydney University (UWS) Young & Resilient Centre

**As observers:**

- Department of Infrastructure, Transport, Regional Development, Communications and the Arts
- Office of the eSafety Commissioner

The Roundtable followed Chatham House Rules.

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

### 4.5.4. Research

To further strengthen insights from consultation and in line with the Position Paper's recommendations[15], 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 - 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/.

### 4.5.5. Response to 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).

## 4.6. 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 have been given due consideration 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.
- 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 submissions log and associated responses were published on https://onlinesafety.org.au/submissions/ along with the submissions and the research that was commissioned (refer to section 4.5.4 above).

Please refer to the enclosed document '*Submission log and associated responses*' for the complete submissions log and associated industry responses. Please note that this log 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.

[15] The Position Paper notes: "Appropriate forms of consultation may include working groups, focus groups, surveys or web forums. A combination of methods of consultation may be the best strategy to ensure effective consultation with interested parties." (p. 49, Office of the eSafety Commissioner, *Development of industry codes under the Online Safety Act, Position Paper,* September 2021)
[16] The survey took place immediately before the Optus data breach, and does not reflect any changes in attitudes or opinions, temporary or permanent, that may have resulted from that.

## 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]

### 4.7.1. Website / social media / general online communications

Please refer to section 4.5 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 section (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.
- 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.

### 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[17], the industry associations undertook the following measures to repeat or amplify the invitation to make a submission in response to the draft Codes:

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

- 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 to 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. The submissions and associated responses are recorded in the same log as for submission 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.

### 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:[18]

- 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

[18] 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.

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[19] (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 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.

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

- 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
- 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 30 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.[20]

**Position 6:** Industry associations will limit the number of codes developed.[21]

**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.

[20] 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.

[21] 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[22] 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 distribueSation 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**[23]: 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. |

[22] The Codes do not include blue language in Outcome 1.
[23] **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<br>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** | Refine draft codes, incorporate eSafety feedback | Industry |
| | **5 May 2022** | eSafety receives updated codes | |
| 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 | Consideration of, and response to, consultation input | Industry |
| | | Compilation of codes development methodology and consultation, registration document | |
| | | Association Board, etc. approvals | |
| | 9 September 2022 | eSafety receives codes for consideration | |
| 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 |