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

1 Structure

This Code is comprised of the terms of this Schedule together with the Online Safety Code (Class 1A and Class 1B Material) Head Terms (**Head Terms**).

2 Scope

(a) This Code only applies to a provider of a designated internet service (**DIS**) to the extent the service is provided to Australian end-users.

(b) For the purposes of this Code, **designated internet service** means an electronic service that:

(i) allows Australian end-users to access material using an internet carriage service; or

(ii) delivers material to persons having equipment appropriate for receiving that material, where the delivery of the service is by means of an internet carriage service,

but does not include:

(iii) a social media service; or

(iv) a relevant electronic service; or

(v) an on-demand program service.

(c) The definition of **designated internet service** includes a wide variety of unique services, and will include 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.

3 Definitions

Unless otherwise indicated, terms used in this Code have the meanings given in the Head Terms or as otherwise set out below:

Australian child means an Australian end-user under the age of 18 years.

general purpose DIS means a designated internet service that is either:

(a) a website or app that primarily provides information for business, commerce, charitable, professional, health, reporting news, scientific, educational, academic research, government, public service, emergency or counselling and support service purposes and/or enables related transactions; or

(b) a web browser.

classified DIS means a designated internet service that provides general entertainment, news or educational content being either:

(a) a film or computer game that has been classified R18+ or lower or is exempt from classification in accordance with the Classification Act;

(b) a film or computer game that has not been classified but, if classified would likely to be classified R18+ or lower;

(c) books, newspapers, and magazines, whether in digital or audio form, podcasts, or digital music that, if required to be classified, would not be classified Category 1 or Category 2 Restricted under the Classification Guidelines for Publications.

end-user-managed hosting service means a designated internet service provided directly to Australian end-users for the purpose of posting, storing, managing, and sharing material. Examples of end-user-managed hosting services include online file storage services, photo storage services or other online media hosting services.

Note: an end-user-managed hosting service differs from third-party hosting services (as defined in the Hosting Services Online Safety Code (Class 1A and Class 1B Material)) which have the primary purpose of supporting the delivery of another service online (e.g., web hosting services) and which do not directly interact with end-users.

enterprise customer means the organisation that a provider of an enterprise designated internet service is providing the service to.

enterprise designated internet service means a designated internet service (including an end-user-managed hosting service) that is being provided to an organisation for use by that organisation's end-users in the course of the organisations' activities but not by individual end-users for their own use.

Note: an enterprise designated internet service excludes Third-Party Hosting Services as (as defined in the Hosting Services Online Safety Code (Class 1A and Class 1B Material) and which are dealt with by that Code). The category of enterprise designated internet service would, for example, include sites designed for the ordering of commercial supplies by enterprises etc.

high impact DIS means a designated internet service

(a) has the sole or primary purpose of enabling Australian end-users to access high impact materials;

(b) makes available high impact material which has been posted by end-users; and

(c) where high impact material posted by end-users is accessible to Australian end-users of the services.

Note: This category would for example, include pornography sites that include end-user generated content that qualifies as high impact material.

high impact materials are materials which are:

(a) films or computer games which have been classified R18+ or X18+ in accordance with the Classification Act, or if classified would likely be classified as R18+ or X18+; or

(b) publications which have been classified Category 1 Restricted or Category 2 Restricted in accordance with the Classification Act, or if classified would likely be classified Category 1 Restricted or Category 2 Restricted.

professionally produced material is material produced by persons or entities who create such material:

(a) as a means of livelihood or for a commercial benefit; or

(b) on commission by the service provider (e.g., a musical album by a professional musician or graphic design firm/photographer showcasing their portfolio).

4 Risk profile

4.1 General requirement for risk assessment

(a) How this Code applies to a designated internet service depends on the risk posed to Australian end-users that class 1A and 1B material will be accessed, distributed, or stored on that service.

Note: Some categories of designated internet services will not have to undertake a risk assessment if they meet the requirements set out in clause 4.3.

(b) Subject to clause 4.3 and except where the designated internet service provider chooses to automatically assign a Tier 1 risk profile to the service in accordance with with section 5.2(a)(ii) of the Head Terms, a provider of a designated internet service must undertake a risk assessment to assess the risk posed to Australian end-users that class 1A and 1B material will be accessed, distributed, or stored on the service and must:

(i) determine the risk profile of the designated internet service as either Tier 1, Tier 2 or Tier 3. A Tier 1 service is one with a higher risk to Australian end-users that class 1A or 1B material will be accessed, distributed or stored on the service whereas Tier 2 represents a moderate risk of this occurring and Tier 3 services represent the lowest risk of this occurring; and

(ii) develop and apply a methodology and process for the risk assessment to determine the risk profile of the designated internet service (as either Tier 1, Tier 2 or Tier 3), using clause 5 below as a guide to assist with the development of appropriate methodology.

(c) The provider of a designated internet service must conduct any risk assessment required under this clause 4.1 as soon as is reasonably practical in accordance with section 5.2(a) of the Head Terms.

4.2 Methodology used for risk assessment and documentation

(a) If a risk assessment is required under this Code, the provider of the designated internet service must be able to reasonably demonstrate that the methodology used for the risk assessment is based on reasonable criteria. At a minimum, the provider of the designated internet service must consider:

(i) the primary purpose of the service; and

(ii) the functionality, the visibility/availability of posted material to Australian end-users of the service and any other criteria that are reasonably relevant for the purpose of determining the risk profile of the service under this Code,

with the primary purpose of the designated internet service being the principal and most significantly weighted criterion in undertaking the risk assessment.

Note: The majority of websites and apps accessible by Australian end users are designated internet services subject to this Code. Many designated internet services share common functionalities. For example, many designated internet services enable end-users to post content, post comments, and rate the products or services made available through the designated internet services. This functionality is not, by itself, indicative of a designated internet service being higher risk, and must be considered by the provider of the designated internet service in context. For example, a hairdressing salon that enables end users to upload hairstyles, should not accord that website a Tier 1 rating. For this reason, the purpose of a designated internet service is the primary consideration in determining the risk profile and measures that apply to designated internet services under this Code and must be given significant weight in undertaking a risk assessment.

(b) Where a provider of a designated internet service must undertake a risk assessment of a service under this Code, it must document its assessment of the risk profile of the service in a manner that clearly explains:

(i) the methodology used to determine the risk profile of that service (including the weighting given to each risk factor); and

(ii) the process by which the assessment was carried out.

4.3 Certain categories of designated internet services are not required to undertake a risk assessment

This clause 4.3 sets out the categories of designated internet services that are deemed to have a particular risk profile under the Code. A provider of a service that meets the requirements of this clause 4.3 is not required to undertake a risk assessment but must comply with any compliance measures listed for that category in clause 6 and specified in the table in clause 7.

(a) A high impact DIS is **deemed** to be a Tier 1 designated internet service and is not required to conduct a risk assessment for that service.

(b) A designated internet service is **deemed** to be a Tier 3 designated internet service where:

(i) the designated internet service is a general purpose DIS or a classified DIS; and

(ii) the designated internet service:

(A) does not enable end-users to post material to the service; or

(B) enables end-users to post material only for the purposes of enabling end-users to review or provide information on products, services or physical points of interest or locations made available on the designated internet service; or

(C) enables end-users to post material only for the purpose of sharing that material with other end-users for a business, informational or government service or support purpose; and

(iii) the designated internet service:

(A) does not offer a chat or messaging function; or

(B) offers a chat or messaging function but the chat or messaging function is limited to private messages or chat between the service and end-users for a business, informational or government service or support purpose.

(c) End-user-managed hosting services are deemed to have similar risk profiles and are not required to conduct a risk assessment under this Code. They are instead required to comply with the minimum compliance measures as set out in the table in clause 7.

(d) Enterprise designated internet services are **deemed** to have a similar risk profile and are not required to conduct a risk assessment under this Code. They are instead required to comply with the minimum compliance measures as set out in the table in clause 7.

4.4 Changes to risk profile of a designated internet service

If a provider of a designated internet service:

(a) makes a change to its service such that it would no longer have its risk deemed under clause 4.3; or

(b) makes a change to its service that would result in the service falling within a higher risk tier,

it must carry out a risk assessment in accordance with clause 4.1 and 4.2 above.

5 Guidance on risk assessment

(a) This clause 5(c) applies where a provider of a designated internet service is required to undertake a risk assessment under clause 4.

(b) When developing a methodology and process for identifying and assessing risks industry participants should take into account:

(i) the factors considered in the table below in clause 5(c),

(ii) the terms of any contract between the provider of the designated internet service and content providers;

(iii) the need to be objective in evaluating the risk of harm posed to Australian end-users should class 1A and 1B material be accessed, distributed or stored on the service;

(iv) the demographics of the intended user base;

(v) a forward-looking analysis of changes to the internal and external environment in which the designated internet service operates and their impact on the ability of a service to meet the objectives and outcomes of the Code including changes in the purpose, functionality and scale of the designated internet service;

(vi) the need to ensure responsible persons with the right level of skills, experience and expertise are involved in the risk assessment;

(vii) whether a different methodology and/or processes should be used to assess the risk for class 1A and class 1B material;

(viii) relevant local, regional and international guidance, (including guidance provided by eSafety) and best practices (for example, with reference to the Digital Trust & Safety Partnership ‘Safe Framework’) and

(ix) relevant international laws and regulations that address the assessment of online safety risks and harms, which seek to achieve objectives and outcomes similar to those contained in this Code.

(c) Industry participants should use the following table as a guide for developing an appropriate methodology, noting that each service is different, and this guide should not be applied as strict criteria but rather as representing a sliding scale of potential risk indicators of Tier 1, Tier 2 and Tier 3 services:

Risk Factor	Indicators of Tier 3	Indicators of Tier 2	Indicators of Tier 1
Purpose	The provision of a general purpose DIS or a classified DIS.*	The purpose of the designated internet service is not to provide a general purpose DIS a classified DIS or a high impact DIS	The purpose of the designated internet service is to enable end-users to post or access high impact materials.**

Risk Factor	Indicators of Tier 3	Indicators of Tier 2	Indicators of Tier 1
Content contributors	The designated internet service primarily makes available professionally produced material to end-users.	The designated internet service makes available professionally produced material and end-user generated material.	The designated internet service primarily makes available to Australian end-users material which has been posted by any end-user.
Posting	Any uploaded material is visible only to the Australian end-user and service provider.	Any posted material is only visible to the service provider or a list of contacts created by the Australian end-user.	Any posted material is available to the service provider and may be made visible and accessible to Australian end-users of the service.

*Excluding a general purpose DIS or classified DIS that is deemed to have a risk profile pursuant to clause 4.3(c) above.
**Note that a designated internet service that is within the definition of a high impact DIS in clause 3 is deemed to have a Tier 1 risk profile pursuant to clause 4.3 above.

6 Approach to measures and guidance for designated internet services

(a) The table in clause 7 below contains mandatory minimum and optional compliance measures for providers of designated internet services, depending on their risk profile and type of designated internet service. The measures in the table in clause 7 below apply to providers of the following categories of relevant electronic services:

Category	Mandatory minimum compliance measures*	Optional compliance measures
Tier 1 designated internet service including high impact designated internet services	2-5, 7-12, 13, 17 ,19-25 and 29-31	15
Tier 2 designated internet service	3-6, 9, 10, 11, 19-21, 26-29 and 32	15
Tier 3 designated internet service including a general-purpose designated internet service, or a classified DIS that meets the requirements of clause 4.3	6 (if applicable, i.e., change in risk tier/profile)	All
End-user-managed hosting service	3-6, 10, 11, 13, 14, 18-21, 26-29, and 33	15
Enterprise designated internet service	1 and 34	

7 Compliance measures for class 1A and class 1B material

<table>
<tr><th colspan="2">Objective 1: Industry participants will take reasonable and proactive steps to create and maintain a safe online environment for Australian end-users.</th></tr>
<tr><th colspan="2">Outcome 1: Industry participants take reasonable and proactive steps to prevent access or exposure to, distribution of, and online storage of class 1A material.</th></tr>
<tr><td>Minimum compliance measures for:

enterprise designated internet services</td><td>1) Agreements with enterprise customers of enterprise designated internet services regarding distribution of illegal materials

A provider of an enterprise designated internet service must:

a) have an agreement in place with the enterprise customer requiring the enterprise customer to ensure the service is not used to distribute illegal materials; and

b) take appropriate action to enforce breaches of that agreement by the enterprise customer.

Guidance:

Providers of enterprise designated internet services provide their services to a wide array of organisations, including businesses, schools, interest-based user groups, clubs, charities and governments (i.e., enterprise customers). Providers of enterprise designated internet service 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

Enterprise customers are best placed to implement measures to manage the use of the designated internet service by their end-users. Such measures are outside the scope of this Code but could include requirements in agreements and/or policies as between the end-user and the enterprise customer (for example, employment agreements and workplace policies that prohibit the distribution of unlawful materials in the workplace) which reduce the risk of designated internet services being used to distribute unlawful materials in the enterprise setting.</td></tr>
<tr><td>Minimum compliance measure for:

Tier 1 designated internet services</td><td>2) Notifying appropriate entities about CSEM and pro-terror material on their services

If a provider of a Tier 1 designated internet service:

a) identifies CSEM and/or pro terror materials on its service; and

b) forms a good faith belief that the CSEM or pro terror materials is evidence of serious and immediate threat to the life or physical safety of an adult or child that is ordinarily resident in Australia

it must report such material to an appropriate entity within 24 hours or as soon as reasonably practicable.

An appropriate entity means foreign or local law enforcement (including, Australian federal or state police) or organisations acting in the public interest against child sexual abuse, such as the National Centre for Missing and Exploited Children (who may then facilitate reporting to law enforcement).

Guidance:

A provider should seek to make a report to an appropriate entity as soon as reasonably practicable in light of the circumstances surrounding that report. For example, in some circumstances, a provider acting in good faith, may need additional time to investigate the authenticity of a CSEM or pro-terror report.

<u>Note</u>: Measure 1 is intended to supplement any existing laws requiring relevant electronic service providers to report CSEM and pro-terror materials under foreign</td></tr>
</table>

	laws e.g., to report materials to the National Centre for Missing and Exploited Children and/or under State and Territory laws e.g., that require reporting of child sexual abuse to law enforcement.
Minimum compliance measure for: **Tier 1 and Tier 2 designated internet services; and** **end-user-managed hosting services**	**3) Systems and processes for enforcement of policies prohibiting CSEM and pro-terror material and age restrictions set by the provider** A provider of a Tier 1 or a Tier 2 designated internet service and an end-user-managed hosting service must implement systems and processes that enable the provider to take appropriate enforcement action for breach of terms and conditions, community standards, and/or acceptable use policies, prohibiting CSEM and pro-terror material. At a minimum, a provider of a Tier 1 designated internet service must: a) remove instances of CSEM and pro-terror materials identified by the provider on the service as soon as reasonably practicable unless otherwise required to deal with unlawful CSEM and pro-terror materials by law enforcement b) terminate an end-user's account as soon as reasonably practicable in the event the Australian end-user is: i) distributing CSEM or pro-terror materials to Australian end-users with the intention to cause harm; ii) known to be an Australian child using the account; or iii) has repeatedly breached terms and conditions, community standards and/or acceptable use policies prohibiting CSEM and pro-terror materials on the service; and c) take reasonable steps to prevent end-users that repeatedly breach terms and conditions, community standards and/or acceptable use policies prohibiting CSEM and pro-terror material who have had their user account terminated from creating a new account. At a minimum an end-user-managed hosting services, must have standard operating procedures that either: i) refer Australian reporters of CSEM or pro-terror materials to eSafety resources; or ii) enable the provider to take appropriate action in response to breaches of terms and conditions, community standards, and/or acceptable use policies prohibiting class 1A materials. *Examples of appropriate action for a Tier 2 designated internet service include:* *a) removing instances of CSEM and pro-terror materials identified by the provider on the service as soon as reasonably practicable unless otherwise required to deal with unlawful CSEM and pro-terror materials by law enforcement;* *b) taking appropriate enforcement action against those who breach terms and conditions, community standards, and/or acceptable use policies prohibiting CSEM and pro-terror material that is reasonably proportionate to the level of harm associated with the relevant breach. Appropriate steps include:* *i) issuing warnings to end-users;* *ii) restricting the end-user's use of the service (e.g., where possible, blocking the Australian end-user from being able to post material using the service);* *iii) suspending the end-user's account for a defined period;* *iv) terminating the end-user's account; or* *v) taking reasonable steps to prevent end-users that repeatedly breach terms and conditions, community standards and/or acceptable use policies prohibiting CSEM and pro-terror material who have had their user account terminated from creating a new account.*

	Guidance: *Pursuant to measure 11 below, Tier 1 designated internet services must require the creation of an account to post material on their services. However, not all Tier 2 designated internet services will have account holders so some examples will not be appropriate for Tier 2 designated internet services that do not require end users to create an account (e.g., many websites). Where a designated internet service requires the creation of an account to use the service, in determining appropriate enforcement action, the provider should consider the potential harm that is related to the identified material, the efficacy of different types of intervention, the type of service, the severity of the policy violation and the frequency and scope of the violation.* *Reasonable steps under sub-measure 3 b) could include, for example, detecting the Australian end-user's device or identifier used for registration and blocking any material being uploaded from that device or identifier used for registration either indefinitely or for a period of time (depending on the severity of the policy violation) or, where the service requires end-users to hold an account and is subject to a pay wall, preventing use of a credit card known to be associated with the Australian end-user's account to create a new account.*
Minimum compliance measure for: **Tier 1 and Tier 2 designated internet services; and** **end-user-managed hosting services**	**4) Systems and processes for action of policies prohibiting class 1A materials (other than CSEM and pro-terror materials)** A provider of a Tier 1 or Tier 2 designated internet service or an end-user-managed hosting service must implement appropriate systems and processes that enable the provider to take appropriate action for breach of terms and conditions, community standards, and/or acceptable use policies, prohibiting class 1A materials (other than CSEM and pro-terror materials). Examples of appropriate systems and processes include: a) in the case of Tier 1 or Tier 2 designated internet services having processes that: i) include clearly specified internal channels for escalating and prioritising reports of class 1A material (other than CSEM and pro-terror materials) to the designated internet service; and ii) provide operational guidance to personnel as to steps that must be taken within specified time frames to deal with class 1A materials that breach the service provider's policies; b) in the case of end-user-managed hosting services, having standard operating procedures that either: i) refer Australian reporters of class 1A materials (other than CSEM and pro-terror materials) to eSafety resources; or ii) enable the provider to take appropriate action in response to breaches of terms and conditions, community standards, and/or acceptable use policies prohibiting class 1A materials (other than CSEM and pro-terror materials). ***Guidance:*** *The systems and processes required under measure 4 should be designed to enable providers of designated internet services to take appropriate action in a proportionate, scalable and effective manner based the scope and urgency of potential harm that is related to the reported material, the efficacy of different types of intervention on the service, the type and scale of service, and the source of reports. Providers should support processes with operational guidance that informs the personnel on the steps they need to take to confirm breaches of policies prohibiting class 1A materials and the actions they should take to enforce policies. See further measure 29 concerning policies for Class1A material.*
Minimum compliance measure for:	**5) Trust and safety function** A provider of a Tier 1 or Tier 2 designated internet service or an end-user-managed hosting service must ensure that they are resourced with reasonably adequate personnel to oversee the safety of the service. Such personnel must operationalise and evaluate the systems and processes required under this Code.

Tier 1 and Tier 2 designated internet services; and **end-user-managed hosting services**	***Guidance:*** *The trust and safety function may be allocated to one or more employees or external third-party service providers. Some industry participants may rely on the risk management systems of a related entity to assist with complying with this obligation. Providers of Tier 1 and Tier 2 services can develop their own resources for this purpose or use resources provided by eSafety. The elements of the program will vary based on the organisation's size, maturity, capacity and capabilities.*
Minimum compliance measure for: **Tier 2 and Tier 3 designated internet services; and** **end-user-managed hosting services**	**6) Safety by design assessments for Tier 2 and Tier 3 designated internet services and end-user-managed hosting services** If a provider of a designated internet service or an end-user-managed hosting service: a) has previously done a risk assessment under this Code and implements a significant new feature that may result in the service falling within a higher risk Tier; or b) has not previously done a risk assessment under this Code (due to falling into a category of service that does not require a risk assessment) and implements a significant new feature that would take it outside that category and require the provider to undertake a risk assessment under this Code, then that provider must (re)assess its risk profile in accordance with clause 4.4 of this Code and take reasonable steps to mitigate any additional risks to Australian end-users concerning material covered by this Code that result from the new feature, subject to the limitations in section 6.1 of the Head Terms. In determining what steps are reasonable, providers may have reference to the factors listed in section 5.1(b) of the Head Terms. ***Guidance:*** *When conducting a safety by design assessment under this measure, providers of Tier 2 and Tier 3 designated internet services and end-user-managed hosting services should consider whether any of the systems, processes or procedures covered by this Code concerning Class 1A materials need to be updated in light of significant new feature.* *In implementing this measure, providers of Tier 2 and Tier 3 designated internet service and end-user-managed hosting services may, for example:* *i) use the safety by design tools published by eSafety to assess the safety risks associated with a new feature; and/or* *ii) consult additional guidance related to safety risks concerning Class 1A materials published by eSafety.*
Minimum compliance measure for: **Tier 1 designated internet services**	**7) Use of systems, processes, and technologies by Tier 1 designated internet services to detect and remove known CSAM** A provider of a Tier 1 designated internet service 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, providers of Tier 1 designated internet services must ensure their services use systems, processes and technologies that: a) automatically detect and flag known CSAM such as hash-matching technologies (for example, PhotoDNA, CSAI Match, and equivalent technology); b) prevent end-users from distributing known CSAM (for example, by 'black-holing' known URLs for such material or blocking or removing such material or preventing users from publicly posting detected material (prior to moderation); and c) identify phrases or words commonly linked to CSAM and linked activity to enable the provider to deter and reduce the incidence of such material and linked activity.

	Guidance: *In implementing this measure, providers of designated internet services should carefully consider the appropriateness of different detection options for their services. Providers should consider the availability of different options and the capability of the provider to use those options accurately, including the need for systems and processes that prioritise the materials detected for human review, the human resourcing required to review detected materials, and the need to provide adequate health and safety arrangements for personnel undertaking such review.* *When implementing the measure outlined in sub-measure 7(a) above, a provider should be alert to the fact that hash lists are not infallible, and an errant hash can have serious consequences for Australian end-users. A provider should therefore take care to safeguard against low quality hashes and hashes prone to collisions (e.g., compilation videos) by having a suitable confirmation and quality control process to independently confirm that the material depicted in the hash is CSAM. Where a hash is likely to lead to false results, a provider should not deploy it.*
Minimum compliance measure for: **Tier 1 designated internet services**	**8) Ongoing investment in systems and processes and/or technologies and personnel by Tier 1 designated internet services** A provider of a Tier 1 designated internet service 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 child sexual abuse material, proportionate to the incidence of such materials on the service and the extent such materials are accessible to Australian end-users.
Outcome 2: Industry participants take reasonable and proactive steps to prevent or limit access or exposure to, and distribution of class 1B material.	
Minimum compliance measure for: **Tier 1 and Tier 2 designated internet services**	**9) Safety by design assessments** See measure 6 above.
Minimum compliance measure for: **Tier 1 and Tier 2 designated internet services; and** **end-user-managed hosting services**	**10) Systems and processes for enforcement of policies** A provider of a Tier 1 or Tier 2 designated internet service or an end-user-managed hosting service must implement appropriate systems and processes that enable the provider to take appropriate action against end-users that breach terms and conditions, community standards, and/or acceptable use policies in relation to class 1B material. Examples of appropriate processes include: a) in the case of Tier 1 or Tier 2 designated internet services having: i) processes that include clearly specified internal channels for escalating and prioritising reports of breaches of the provider's terms and conditions, community standards, and/or acceptable use policies to the designated internet service; and ii) processes to provide operational guidance to personnel as to steps that must be taken within specified time frames to deal with the reports referred to in i) above. b) in the case of end-user-managed hosting services having: i) standard operating procedures that either refer reporters of class 1B materials to eSafety resources; or 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 1B materials. ***Guidance:*** *Systems and processes should be designed to enable providers of designated internet services to enforce policies in an appropriate, scalable and effective*

	manner based on the urgency, and scope of potential harm that is related to the reported material, the efficacy of different types of intervention that are available on the service, the type of service, and the source of reports. Processes should be documented in a manner that clearly informs personnel on the steps they need to take to confirm breaches of policies and take action to enforce policies, within specified time frames including rapid response requirements where the physical safety of an Australian end-user is in immediate danger.
Minimum compliance measure for: **Tier 1 and Tier 2 designated internet services; and** **end-user-managed hosted services**	**11) Safety by design features and settings** A provider of a Tier 1 or a Tier 2 designated internet service or an end-user-managed hosted service must adopt appropriate features and settings that are designed to mitigate the risks to Australian end-users related to class 1A material. A provider of a Tier 1 designated internet service must at a minimum: a) implement measures that ensure that material can only be posted to or distributed on the service by a registered account holder; b) make clear in terms and conditions, community standards and/or acceptable use policies that an Australian child is not permitted to hold an account on the service; and c) take reasonable steps to prevent an Australian child from holding an account on the service, and to remove them from the service as set out in measure 3.
Minimum compliance measure for: **Tier 1 designated internet services**	**12) Ongoing investment in tools and personnel by Tier 1 designated internet services** A provider of a Tier 1 designated internet service 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.
Outcome 4: Industry participants take reasonable and proactive steps to limit hosting of class 1A and 1B material in Australia.	
Minimum compliance measure for: **end-user-managed hosting services**	**13) Limiting accessibility by Australian end-users (CSEM and pro-terror material) of end-user-managed hosting services** A provider of an end-user-managed hosting service must have practices and procedures to minimise the likelihood that CSEM and pro-terror material is accessible by Australian end-users on the end-user-managed 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. ***Guidance:*** *Examples of practices and procedures that may demonstrate compliance with this measure include the provider:* *a) developing and/or implementing technical tools or other practical measures aimed at enforcing those policies and procedures that aim to limit CSEM or pro-terror material; or* *b) configuring material reporting mechanisms in a way that places priority on reports of material claimed to be CSEM or pro-terror material (or where the report reasonably suggests that the material may be CSEM or pro-terror material).*
Minimum compliance measure for: **end-user-managed hosting services**	**14) Limiting accessibility by Australian end-users (Class 1B and non-CSEM/non-pro-terror Class 1A material) of end-user-managed hosting services** A provider of an end-user-managed hosting service 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. ***Guidance:*** *Examples of policies and procedures that may demonstrate compliance with this measure include the provider having policies, agreements, terms of use or other arrangements in place regarding class 1B and non-CSEM/non-pro-terror class 1A 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.	
Optional compliance measure for: **Tier 1 and Tier 2 designated internet services; and** **end-user-managed hosting services**	**15) Industry collaboration mechanisms for removing, disrupting and/or restricting class 1A and class 1B material** A provider of a Tier 1 or Tier 2 designated internet service and an end-user-managed hosting service may adopt measures to support Outcome 5 in relation to class 1A or class 1B material, including for example: a) joining industry organisations intended to address serious online harms, and/or share information on best practice approaches, that are relevant to the service; b) working with eSafety to share information, intelligence, and/or best practices relevant to addressing certain categories of class 1A or class 1B material, that are relevant to the service; c) collaborating with non-government or other organisations that facilitate the sharing of information, intelligence, and/or best practices relevant to addressing certain categories of class 1A or class 1B material; and/or d) joining and/or supporting global or local multi-stakeholder initiatives that bring together a range of subject matter experts to share information and best practices, collaborate on shared projects, and/or working to reduce online harms. Examples include the WePROTECT Global Alliance.
Outcome 6: Industry participants communicate and cooperate with eSafety in respect of matters relating to class 1A and class 1B material, including complaints.	
Minimum compliance measure for: **Tier 1 designated internet services**	**16) Timely referral of unresolved complaints to eSafety** A provider of a Tier 1 designated internet service 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. *Being 'unable to resolve the complaint' is intended to refer to situations where it becomes clear to the provider that their ultimate response to a given complaint is not to the satisfaction of the complainant and the complaint cannot reasonably be progressed any further between provider and complainant.* ***Guidance:*** *The time frames within which providers of a Tier 1 designated internet service should seek to resolve complaints of non-compliance with the code and refer issues to eSafety under this measure should be based on the scope and urgency of potential harm that is related to the complaint and the source of the complaint.*
Minimum compliance measure for: **Tier 1 designated internet services**	**17) Updates and consultation with eSafety about relevant changes to technology** A provider of a Tier 1 designated internet service 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.

Minimum compliance measure for: **end-user-managed hosting services**	**18) Communication and cooperation with Commissioner concerning Code compliance** A provider of an end-user-managed hosting service 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.
Objective 2: Industry participants will empower people to manage access and exposure to class 1A and class 1B material.	
Outcome 7: Industry participants provide tools and/or information to limit access and exposure to class 1A and class 1B material.	
Minimum compliance measure for: **Tier 1 and Tier 2 designated internet services; and** **end-user-managed hosting services**	**19) Online Safety Resources** A provider of a Tier 1 or Tier 2 designated internet service or an end-user-managed hosting service must provide online safety resources that include clear and accessible information for Australian end-users regarding: a) the role and functions of eSafety, including how to make a complaint to eSafety; and b) information about the mechanisms in measure 20.
Outcome 8: Industry participants provide clear and effective reporting and complaints mechanisms for class 1A and class 1B material.	
Minimum compliance measure for: **Tier 1 and Tier 2 designated internet services; and** **end-user-managed hosting services**	**20) Reporting and complaints mechanisms** A provider of a Tier 1 or a Tier 2 designated internet service or end-user-managed hosting service 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. Such reporting mechanisms must: a) be easily accessible and easy to use; b) be accompanied by clear instructions on how to use them; and c) ensure that the identity of the reporter is not disclosed to the reported Australian end-user (i.e., the individual who has been reported should not be able to see the person who reported them), without the reporter's express consent.
Minimum compliance measure for: **Tier 1 and Tier 2 designated internet services; and** **end-user-managed hosting services**	**21) Complaints about compliance with Code** A provider of a Tier 1 or a Tier 2 designated internet service or end-user-managed hosting service 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.
Outcome 9: Industry participants effectively respond to reports and complaints about class 1A and class 1B material.	
Minimum Compliance measure for: **Tier 1 designated internet services**	**22) Appropriate steps for responding to Australian end-users' reports** A provider of a Tier 1 designated internet service must: a) take appropriate steps to promptly respond to reports made by Australian end-users of materials that violate the service's terms and conditions, community standards, and/or acceptable use policies; and b) ensure that an Australian end-user who reports class 1A or class 1B materials is:

	i) informed in a reasonably timely manner of the outcome of the report; ii) can seek a review of the response in sub-measure i) if the Australian end-user is dissatisfied with the providers' response under sub-measure i); and iii) notified of the outcome of a review under sub-measure ii). ***Guidance:*** *The manner in which a provider implements this measure and the timeliness of the actions required under this measure will depend on the type of material reported, the likelihood of harm that it poses to Australian end-users, the source of the report and the risk profile of the provider of the designated internet service. The provider should provide information to Australian end-users about indicative timeframes for responding to reports.* *In implementing this measure providers should consider if the minimum requirements of this measure should be supplemented, by additional actions for example by:* *i) a facility for Australian end-users to make a complaint if they are dissatisfied with the response to a report;* *ii) referring Australian end-users to relevant third-party support services;* *iii) directing Australian end-users to eSafety, where they are dissatisfied with the outcome of a report.*
Minimum Compliance measure for: **Tier 1 designated internet services**	**23) Policies and procedures for responding to Australian end-users' reports** A provider of a Tier 1 designated internet service must implement and document policies and procedures which detail how it gives effect to the requirements in measure 22.
Minimum Compliance measure for: **Tier 1 designated internet services**	**24) Training for personnel responding to reports** A provider of a Tier 1 designated internet service must ensure that personnel responding to reports are trained in the designated internet service's policies and procedures for dealing with reports.
Minimum Compliance measure for: **Tier 1 designated internet services**	**25) Reviews of effectiveness of systems and processes** A provider of a Tier 1 designated internet service 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.
Minimum compliance measures for: **Tier 2 designated internet services; and** **end-user-managed hosting services**	**26) Appropriate steps for responding to Australian end-users' reports** A provider of a Tier 2 designated internet service or an end-user-managed hosting service 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. ***Guidance:*** *The manner in which a provider implements this measure and the timeliness of the actions required under this measure will depend on the type of material reported, the likelihood of harm that it poses to Australian end-users, the source of the report and the risk profile of the provider of the designated internet service.*
Minimum compliance measure for: **Tier 2 designated internet services; and**	**27) Policies and procedures for responding to Australian end-users' reports** A provider of a Tier 2 designated internet service or an end-user-managed hosting service must implement and document policies and procedures which detail how it gives effect to the requirements in measure 26. ***Guidance:***

end-user-managed hosting services	*Providers should set and monitor internal targets for response times in their policies and procedures that prioritise responses and reviews of material that evidences an immediate risk to the physical safety to an Australian end-user.*
Minimum compliance measure for: **Tier 2 designated internet services; and** **end-user-managed hosting services**	**28) Training for personnel responding to reports** A provider of a Tier 2 designated internet service or an end-user-managed hosting service must ensure that personnel responding to reports are trained in the designated internet service's policies and procedures for dealing with reports.
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.	
Minimum compliance measure for: **Tier 1 and Tier 2 designated internet services; and** **end-user-managed hosting services**	**29) Publication of policies** A provider of a Tier 1 or Tier 2 designated internet service or an end-user-managed hosting service 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. ***Guidance:*** *In implementing this measure, a provider of a designated internet service or an end-user-managed hosting service should:* *i) use simple, plain, and straightforward language;* *ii) to the extent practicable, be clear about the type of material that is prohibited; and* *iii) communicate such terms and conditions, standards and/or policies to all personnel that are directly involved in actioning them.*
Minimum Compliance measure for: **Tier 1 designated internet services**	**30) Information explaining how designated internet services deal with class 1A and class 1B material** A provider of a Tier 1 designated internet service 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.
Outcome 11: Industry participants publish annual reports about class 1A and 1B material and their compliance with this Code.	
Minimum compliance measure for: **Tier 1 designated internet services**	**31) Annual reporting by providers of a Tier 1 designated internet service** A provider of a Tier 1 designated internet service must submit a Code report which as a minimum contains the following information: a) details of any risk assessment it is required to undertake pursuant to the Code, together with information about the risk assessment methodology adopted; b) the steps that the provider has taken to comply with the applicable minimum compliance measures; c) the volume of CSEM or pro terror material removed by the provider of the designated internet service; and d) an explanation as to why these measures are appropriate.

	The first Code report must be submitted to eSafety 12 months after this Code comes into effect. Subsequent Code reports must be submitted annually. Note: 'appropriate' has the meaning given in the Head Terms
Minimum compliance measure for: **Tier 2 designated internet services**	**32) Reporting by providers of a Tier 2 designated internet service** Where eSafety issues a written request to a provider of a Tier 2 designated internet service to submit a Code report, the provider named in such request must submit to eSafety a Code report which includes the following information: a) details of any risk assessment it is required to undertake pursuant to the Code, together with information about the risk assessment methodology adopted; b) the steps that the provider has taken to comply with their applicable minimum compliance measures; and c) an explanation as to why these measures are appropriate. A provider of a Tier 2 designated internet service who has received such a request from eSafety is required to submit a Code report within 6 months of receiving the request, but for the first request no earlier than 12 months after this Code comes into effect. A provider of a Tier 2 designated internet service will not be required to submit a Code report to eSafety more than once in any 12-month period. Note: 'appropriate' has the meaning given in the Head Terms.
Minimum compliance measure for: **end-user-managed hosting services**	**33) Reporting by providers of an end-user-managed hosting service** Where eSafety issues a written request to a provider of an end-user-managed hosting service to submit a Code report, the provider named in such request must submit to eSafety a Code report which includes the following information: a) the steps that the provider has taken to comply with their applicable minimum compliance measures; and b) an explanation as to why these measures are appropriate. A provider of an end-user-managed hosting service who has received such a request from eSafety is required to submit a Code report within 6 months of receiving the request, but for the first request no earlier than 12 months after this Code comes into effect. A provider of an end-user-managed hosting service will not be required to submit a Code report to eSafety more than once in any 12-month period. Note: 'appropriate' has the meaning given in the Head Terms.
Minimum compliance measure for: **enterprise designated internet services**	**34) Reporting by providers of an enterprise designated internet service** Where eSafety issues a written request to a provider of an enterprise designated internet service, the provider named in such request must confirm in writing to eSafety that the provider is compliant with minimum compliance measure 1. A provider of an enterprise designated internet service who has received such a request from eSafety must provide written confirmation to eSafety within 2 months of receiving the request. A provider of an enterprise designated internet service will not be required to submit a Code report to eSafety more than once in any 12-month period.