Schedule 2 – Relevant Electronic 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

This Code only applies to relevant electronic services to the extent provided to Australian end-users.

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.

carriage service provider has the meaning given in the *Telecommunications Act 1997* (Cth).

capable of reviewing and assessing materials means the provider of the relevant electronic service is able to access and view, or otherwise review, individual items of material communicated via the service and has sufficient visibility of content and end user activity to determine, in context, whether materials are class 1A or class 1B materials (as relevant and required by this Code) and whether a breach of terms and conditions, community standards, and/or acceptable use policies has occurred (as relevant and required by this Code);

and **not capable of reviewing and assessing materials** has an opposite corresponding meaning.

Note: Due to the nature of relevant electronic services, their functionality, and the manner in which they are otherwise regulated, providers of these services may not be capable of reviewing and assessing material communicated by end-users on their services. Further, as these services often provide an ability for end-users to communicate with end-users of other services, providers will not always have a contractual relationship with all end-users involved in a communication, or visibility surrounding any engagement between an end-user involved in a communication and another service provider. This can impact a provider's ability to review and assess all or some material.

A provider's ability to access and view individual items of material, and end-user activity, will therefore depend on whether the provider has both the legal and technical capacity to do so. If a provider is prohibited by law from undertaking such activity, or such activity is not technically feasible (e.g., due to the nature and functionality of the relevant electronic service), then the provider will not be capable of reviewing and assessing material A provider may be capable of accessing and viewing individual items of material in some circumstances but not others, for example, depending on whether sufficient information is given by the end-user about the context of material reported to the provider, in which case the provider will be deemed partially capable of reviewing and assessing material to the extent set out in clause 5.2.

capable of removing materials means the provider of the relevant electronic service is capable of removing individual items of material;

Note: If a provider is capable of removing individual items of material in some circumstances but not others, e.g., because the service is partially encrypted, the provider will be deemed partially capable of removing material to the extent set out in clause 5.2.

and **not capable of removing materials** has an opposite corresponding meaning.

Note: If removal, blocking or otherwise disabling access is not possible for either legal or technical reasons then the provider will not be capable of removing materials.

Note: See definition of "remove" below.

closed communication relevant electronic service means a relevant electronic service that enables an Australian end-user to access and communicate with a list of contacts created by the end-user but does not:

(a) enable Australian end-users to view, navigate or search for other end-users on the service without already having the recipient's contact details, such as phone number or email address, from another source in order to communicate with that recipient; or

(b) recommend other contacts to Australian end-users based on interests or shared connections.

***Guidance**: Closed communication relevant electronic services include a range of services including short messaging services (SMS), multimedia messaging services (MMS) and similar messaging services, as well as most email services. These are generally private communications services that enable end-users to communicate with end-users of other equivalent services (e.g., other end-users with a telephone number or email address, as relevant). Closed communication relevant electronic services will often not be capable of reviewing and assessing, or removing, materials.*

Note: A closed communication relevant electronic service includes messaging services where Australian end-users must already have a recipient's contact details (from a source other than the service) in order to contact them. This includes, for example, short messaging services (SMS), multimedia messaging services (MMS) and similar messaging services, as well as most email services.

Note: For the purposes of sub-clause (a) of this definition, knowing the recipient's name (without having any other details that would enable that recipient to be contacted such as a phone number or email address) does not constitute having the recipient's contact details.

dating service means a relevant electronic service or portion thereof that has the predominant purpose of offering, promoting, or providing access to dating, relationship, compatibility, matrimonial, or social/romantic referral services and that enables end-users to communicate with other end-users online, for example via an email, chat, or messaging function. For the avoidance of doubt, the term 'dating service' does not include services where one party is compensated for engaging in the social activity, such as escort services or sex work.

encrypted relevant electronic service means a relevant electronic service:

(a) which is entirely end-to-end encrypted; or

(b) where the communications between end-users are end-to-end encrypted,

but excludes a closed communication relevant electronic service.

***Guidance:** Encrypted relevant electronic services are relevant electronic services that have implemented encryption measures for private communications, often as a safety measure in response to the privacy and security concerns of legitimate users. Due to the nature of these services, providers of these services will often not be capable of reviewing and assessing or removing materials on the service.*

enterprise customer means the organisation that a provider of an enterprise relevant electronic service is providing the service to.

enterprise relevant electronic service means a relevant electronic service that is being provided to an organisation for the purpose of enabling communications (whether internal or external) by that organisation's end-users.

***Guidance**: Providers of enterprise relevant electronic 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 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.*

Enterprise customers are best placed to implement measures to manage the use of the relevant electronic 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 relevant electronic services being used to distribute unlawful materials in the enterprise setting.

gaming service with communications functionality means a relevant electronic service that:

(a) is not a closed communication relevant electronic service or gaming service with limited communications functionality;

(b) enables Australian end-users to play online games with other end-users; and

(c) enables the sharing of the following types of user-generated material between end-users:

(i) URLs or hyper-linked text;

(ii) images; and/or

(iii) videos,

but

(d) excludes a service that limits the sharing of user-generated material between end-users to any or all of the following:

(i) in-game images or footage;

(ii) user-generated designs (such as environments and artwork);

(iii) virtual objects or maps;

(iv) pre-selected messages;

(v) non-hyper-linked text that is subject to automated filtering technology; or

(vi) ephemeral voice interactions.

gaming service with limited communications functionality means a relevant electronic service that:

(a) is not a closed communication relevant electronic service;

(b) enables Australian end-users to play online games with other end-users; and

(c) does not enable the sharing of user-generated material between end-users referred to under (c) of the definition of **gaming service with communications functionality** above, other than the type of content listed under (d) of that definition.

open communication relevant electronic service means a relevant electronic service that:

(a) enables Australian end-users to view, navigate or search for other end-users on the service without already having the recipient's contact details, such as phone number or email address, from another source in order to communicate with that recipient; or

(b) recommends other contacts to Australian end-users based on interests or shared connections.

Note: An open communication relevant electronic service includes messaging services that enable Australian end-users to contact other end-users directly on the service without already having the recipient's contact details.

pre-assessed relevant electronic service means:

(a) a closed communication relevant electronic service;

(b) a dating service;

(c) an encrypted relevant electronic service;

(d) a gaming service with communications functionality; or

(e) an open communication relevant electronic service.

Note: Pre-assessed relevant electronic services are categories of relevant electronic services. The categories of services that may fall within the definition of relevant electronic services under the OSA are not fixed. Services that do not fall within the above categories, and are not otherwise enterprise relevant electronic services or gaming services with limited communications functionality, must do a risk assessment to determine their risk tier in accordance with clause 5.

remove means to remove, block or otherwise disable or prevent access to relevant material.

young Australian child means an Australian end-user under the age of 16 years.

4 Role of relevant electronic services

(a) As outlined in section 5.1(b)(iii) of the Head Terms, it is the responsibility of each industry participant under this Code to demonstrate that the compliance measures it has adopted are reasonable, taking into account the importance of protecting and promoting human rights online, including associated statutory obligations. This clause provides additional guidance on the importance of these considerations, in designing and implementing the measures of this Code, having regard to the role of relevant electronic services in enabling private communications between Australian end-users.

(b) Relevant electronic services include a wide variety of unique services including short messaging services (SMS), multimedia messaging services (MMS), email, instant messaging services, dating services and services that enable Australian end-users to play online games with other end-users. Because the role of relevant electronic services is to facilitate private communication between end-users, the measures in this Code have been designed to be respectful of Australian end-users' legitimate expectations around the privacy and security of those communications and to ensure that measures do not contravene statutory obligations that are applicable to the providers of relevant electronic services. The statutory obligations that may be applicable to a provider of a relevant electronic service, depending on the type of service, include:

(i) the *Privacy Act 1988* (Cth);

(ii) Part 13 of the *Telecommunications Act 1997* (Cth);

(iii) the *Telecommunications (Interception and Access) Act 1979* (Cth);

(iv) various laws relating to unauthorised access to data/computers; and

(v) various laws relating to surveillance.

Many relevant electronic services are also subject to similar legislation in other jurisdictions. In particular, an industry participant should note section 6.1 of the Head Terms.

(c) The variety of relevant electronic services within the scope of this Code have varying capabilities to assess the materials contained in end-user communications. The types of measures that may be possible and/or appropriate for one type of relevant electronic service, will not be appropriate for others. For example, providers of an SMS or email service may not be able to (re)view and/or assess and, therefore, determine whether materials communicated by end-users are class 1A or class 1B materials or be capable of removing such materials from the service. Consequently,

the measures in this Code have been designed to take into account the differences between the purpose, functionality and user-base of each type of service, and the need for flexibility in the implementation.

5 How this code applies to relevant electronic services

5.1 General approach

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

(a) is required to determine the risk profile of the service in accordance with clause 5.3; or

(b) is not required to determine its risk profile under clause 5.5.

5.2 Relevance of providers' capability of reviewing, assessing and removing material, if requested

(a) The application of certain measures in this Code to a provider of a pre-assessed relevant electronic service or a Tier 1 or Tier 2 relevant electronic service depends on the provider's capability of reviewing, assessing, and/ or removing material. Some providers of a pre-assessed relevant electronic service or a Tier 1 or Tier 2 relevant electronic service may be capable of reviewing, assessing, and/or removing specific items of materials (as defined above) in some circumstances but not in others, in which case:

(i) the provider is deemed partially capable of reviewing, assessing and/or removing materials; and

(ii) will be subject to the measures in the Code that apply to a pre-assessed relevant electronic service or a Tier 1 or Tier 2 relevant electronic service capable or reviewing, assessing and/or removing materials to the extent compliance with the relevant minimum compliance measure(s) is reasonably practical.

Note: section 5.2 iii) refers to minimum compliance measures 3, 4, 8, 9, 11, 12, 19 and 21 to the extent those measures require a provider to be capable of reviewing, assessing and/or removing materials. Refer also to guidance in measures 26, 27 and 28.

(b) A provider of a pre-assessed relevant electronic service or a Tier 1 or Tier 2 relevant electronic service will, at eSafety's request, notify eSafety of the extent it is capable of reviewing and assessing material or capable of removing material, or not capable of doing so.

5.3 Requirement to assess risk and determine the risk profile

(a) Except where a relevant electronic service falls within one of the categories described in clause 5.5(a), a provider of a relevant electronic service must:

(i) 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;

(ii) determine the risk profile of the relevant electronic 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 and 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;

(iii) should a risk assessment in (ii) indicate that the service may be in-between risk tiers, assign the higher risk profile to that service; and

(iv) provide to eSafety, on request, a copy of its risk assessment as soon as reasonably practical in accordance with section 5.2(a) of the Head Terms.

Note: The obligation to determine the risk profile of a relevant electronic service does not apply to providers that notify that they are Tier 1 services in accordance with the requirements of section 5.2 (a) (ii) of the Heads Terms or to pre-assessed relevant electronic services, gaming services with limited communications functionality, or enterprise relevant electronic services.

(b) If a provider of a relevant electronic service is required to determine the risk profile of the service as either Tier 1, Tier 2 or Tier 3 under this Code, the provider must comply with the minimum compliance measures applicable to the risk profile of the service so determined as set out in clause 7(a) and specified in the table in clause 8.

5.4 Methodology used for risk assessment and documentation

(a) If a risk assessment is required under this Code, the provider of the relevant electronic service must:

(i) be able to reasonably demonstrate that the provider's risk assessment methodology is based on reasonable criteria which must at a minimum include criteria relating to the functionality, purpose and scale of the relevant electronic service, the requirements set out in 6(b) and 5.3(a)(iii) and any other criteria that are reasonably relevant for the purpose of determining the risk profile of the relevant electronic service under this Code; and

(ii) document its assessment of the risk profile of the service in a manner that clearly explains:

(A) the methodology used to determine the risk profile of the relevant electronic service (including the weighting given to each risk factor); and

(B) the process by which the assessment was carried out

5.5 Certain categories of relevant electronic services are not required to undertake a risk assessment

(a) A provider of:

(i) a closed communication relevant electronic service; or

(ii) a dating service; or

(iii) an encrypted relevant electronic service; or

(iv) an enterprise relevant electronic service; or

(v) a gaming service with communications functionality; or

(vi) a gaming service with limited communications functionality; or

(vii) an open communication relevant electronic service; or

(viii) a relevant electronic service that the provider chooses to automatically assign a Tier 1 risk profile to the relevant electronic service in accordance with section 5.2(a)(ii) of the Head Terms,

is not required to carry out a risk assessment under this Code.

(b) Providers of closed communication relevant electronic services must comply with the minimum compliance measures as listed for closed communication relevant electronic services in clause 7(a) and specified in the table in clause 8.

(c) Providers of dating services must comply with the minimum compliance measures as listed for dating services in clause 7(a) and specified in the table in clause 8.

(d) Providers of encrypted relevant electronic services must comply with the minimum compliance measures as listed for encrypted relevant electronic services in clause 7(a) and specified in the table in clause 8.

(e) Providers of enterprise relevant electronic services must comply with the minimum compliance measures as listed for enterprise relevant electronic services in clause 7(a) and specified in the table in clause 8.

(f) Providers of gaming service with communications functionality must comply with the minimum compliance measures as listed for gaming services with communications functionality in clause 7(a) and specified in the table in clause 8.

(g) Providers of gaming services with limited communications functionality must comply with the minimum compliance measures as listed for gaming services with limited communications functionality in clause 7(a) and specified in the table in clause 8.

(h) Providers of open communication relevant electronic services must comply with the minimum compliance measures listed for open communication relevant electronic services in clause 7(a) and specified in the table in clause 8.

5.6 Changes to risk profile of a relevant electronic service

If a provider of a relevant electronic service:

(a) makes a change to its service such that it would no longer be considered as a pre-assessed relevant electronic service or a gaming service with limited communications functionality or an enterprise relevant electronic service (as relevant); or

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

it must carry out a risk assessment in accordance with clause 5.3 above.

6 Risk assessment: requirements and guidance

(a) This clause 6 applies where a provider of a relevant electronic service is required to undertake a risk assessment under clause 5.

(b) A provider of a relevant electronic service that is required to undertake a risk assessment must take into account the following matters:

(i) the degree to which the provider has control of material on the service;

(ii) expectations placed on users of the service, including any contractual or other relevant arrangements;

(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 geographical spread of the service's operations and the age of the user base;

(v) a forward-looking analysis of changes to the internal and external environment in which the service operates and its impact on the ability of the service to meet the objectives and outcomes of this Code including changes in the functionality, purpose and scale of the 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 there are differences in the risk(s) related to class 1A and class 1B material on the service;

(viii) relevant local, regional and international guidance (for example, with reference to the Digital Trust & Safety Partnership 'Safe Framework'); and

(ix) relevant local, regional and international guidance or emerging best practices, such as written guidance provide by eSafety including relevant local laws and regulations that address the assessment of online safety risks and harms, that 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 that new or different risk factors may need to be considered.

<table>
<tr><th>Risk Factor</th><th>Tier 3 Indicators</th><th>Tier 2 Indicators</th><th>Tier 1 Indicators</th></tr>
<tr><td>Potential for virality (functionality)</td><td colspan="2">The relevant electronic service only enables sharing of:
a) material on a 1:1 basis between end-users, or within a defined group of end-users; or
b) ephemeral material (material that lasts or is displayed only for a short time) without a sharing function.</td><td>The relevant electronic service enables sharing and re-sharing of material to all end-users of the service / the general public and the material is permanent (i.e., not ephemeral).</td></tr>
<tr><td>Intended audience (purpose)</td><td>The relevant electronic service is primarily:
a) for communication within a known and specified end-user group (such as within a school, or neighbourhood or university community);
b) for communication for a limited commercial purpose such as to enable a potential customer to obtain, advise or give feedback to other end-users about a specific product or service they have purchased;
c) to enable business communication outside of an enterprise environment.</td><td colspan="2">The relevant electronic service is primarily for general communication amongst the general population or children under the age of 18.</td></tr>
</table>

Risk Factor	Tier 3 Indicators	Tier 2 Indicators	Tier 1 Indicators
Number of active Australian end-users of the service	1 - 500,000	500,001 - 3 million	Over 3 million
Discoverability of users	The relevant electronic service typically only enables end-users to access and communicate with a list of contacts created by the end-user and does not: a) enable end-users to view a list of other users' individual connections on the service; b) enable end-users to search for other end-users on the relevant electronic service using known identifiers (e.g., name, user name, email address); c) allow end-users to search for other end-users on the relevant electronic service based on interests or keywords; and d) recommend other contacts to end-users based on interests or shared connections.	The relevant electronic service enables end-users to do either of the following: a) view a list of other users' individual connections on the service; or b) search for other end-users on the relevant electronic service using known identifiers (e.g., name, user name, email address), but does not: c) allow end-users to search for other end-users on the relevant electronic service based on interests or keywords; or d) recommend other contacts to end-users based on interests or shared connections.	The relevant electronic service: a) enables end-users to search for other end-users on the relevant electronic service based on interests or keywords; or b) recommends other contacts to end-users based on interests or shared connections.

7 Approach to measures and guidance for relevant electronic services

(a) The table in clause 8 contains mandatory minimum and optional compliance measures for providers of relevant electronic services, depending on their risk profile and type of relevant electronic service. The measures in the table in clause 8 apply to providers of the following categories of relevant electronic services:

Category	Description	Mandatory minimum compliance measures	Optional compliance measures
Relevant electronic service	All relevant electronic services covered by this Code	7, 14	16, 23
Tier 1 relevant electronic service	A relevant electronic service that the provider has: (a) determined the risk profile to be Tier 1 pursuant to clause 5; or (b) automatically assigned a Tier 1 risk profile pursuant to section 5.2(a)(ii) of the Head Terms. Note: A Tier 1 relevant electronic service does not include a pre-assessed relevant electronic service, a gaming service with limited communications functionality, or an enterprise relevant electronic service, as they are not required to designate a risk profile. These services are treated as separate sub-categories of relevant electronic service in the measures.	2, 3, 4, 5, 6, 8, 9, 10, 11, 12, 13, 15, 17, 18, 19, 20, 21, 22, 24, 25, 26	
Tier 2 relevant electronic service,	A relevant electronic service where the provider has determined the risk profile to be Tier 2 pursuant to clause 5. Note: A Tier 2 relevant electronic service does not include a pre-assessed relevant electronic service, a gaming service with limited communications functionality, or an enterprise relevant electronic service, as they are not required to designate a risk profile. These services are treated as separate sub-categories of relevant electronic service in the measures.	2, 3, 4, 5, 6, 11, 12, 13, 18, 19, 20, 21, 22, 25, 27	
Tier 3 relevant electronic service	A relevant electronic service where the provider has determined the risk profile to be Tier 3 pursuant to clause 5. Note: A Tier 3 relevant electronic service does not include a pre-assessed relevant electronic service, a gaming service with limited communications functionality, or an enterprise relevant electronic service, as they are not required to designate a risk profile. These services are treated as separate sub-categories of relevant	--	

	electronic service in the measures.		
Open communication relevant electronic services	Open communication relevant electronic services as defined in clause 3	2, 3, 4, 5, 6, 8, 9, 10, 11, 12, 13, 15, 17, 18, 19, 20, 21, 22, 24, 25, 26	
Closed communication relevant electronic service	Closed communication relevant electronic services as defined in clause 3	2, 3, 4, 6, 10, 11, 12, 15, 18, 19, 20, 21, 22, 28	
Dating services	Dating services as defined in clause 3	2, 3, 4, 5, 6, 8, 10, 11, 12, 13, 15, 18, 19, 20, 21, 22, 24, 25, 28	
Encrypted relevant electronic service	Encrypted relevant electronic services as defined in clause 3	2, 3, 4, 5, 6, 10, 11, 12, 13, 15, 17, 18, 19, 20, 21, 22, 28	
Gaming services with communications functionality	Gaming services with communications functionality as defined in clause 3	2, 3, 4, 5, 6, 8, 11, 12, 13, 15, 18, 19, 20, 21, 22, 25, 28	
Gaming services with limited communications functionality	Gaming services with limited communications functionality as defined in clause 3	2	
Enterprise relevant electronic service	Enterprise relevant electronic services as defined in clause 3	1, 29	

(b) The table also sets out guidance on the implementation of some measures. This guidance is not intended to be binding on providers but to guide them on the way in which they may choose to implement a measure.

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

Objective 1: Industry participants will take reasonable and proactive steps to create and maintain a safe online environment for Australian end-users	
Outcome 1: Industry participants take reasonable and proactive steps to prevent access or exposure to, distribution of, and online storage of class 1A material.	
Minimum compliance measures for: **enterprise relevant electronic services**	**1) Agreements with enterprise customers regarding distribution of materials** A provider of an enterprise relevant electronic 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 relevant electronic 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 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.* *Enterprise customers are best placed to implement measures to manage the use of the enterprise relevant electronic services 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 enterprise relevant electronic services being used to distribute unlawful materials in the enterprise setting.*
Minimum compliance measures for: **pre-assessed relevant electronic services;** **Tier 1 relevant electronic services;** **Tier 2 relevant electronic services;** **and** **gaming services with limited communications functionality**	**2) Notifying appropriate entities about CSEM and pro-terror material on their services** If a provider of: a) a pre-assessed relevant electronic service; b) a Tier 1 or Tier 2 relevant electronic service; or c) a gaming service with limited communications functionality, both: i) identifies CSEM and/or pro-terror materials on its service; and ii) forms a good faith belief that the CSEM or pro-terror material is evidence of a serious and immediate threat to the life or physical safety of an adult or child 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). Note: Measure 2 is intended to supplement any existing laws requiring relevant electronic service providers to report CSEM and pro-terror materials under foreign 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. ***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 noting that the referral of materials under this measure to appropriate authorities is time critical. For example, in some circumstances, a provider acting in good faith, may need additional time to investigate the authenticity of a report but when a report has been authenticated, an appropriate authority should be informed without delay. A provider should ensure that such a report is compliant with other applicable laws, such as privacy laws.*
Minimum compliance measures for: **pre-assessed relevant electronic services;** **Tier 1 relevant electronic services;** **and** **Tier 2 relevant electronic services**	**3) Systems and processes for responding to breaches of policies relating to class 1A materials** A provider of: a) a pre-assessed relevant electronic service; or b) a Tier 1 or Tier 2 relevant electronic service, that is capable of reviewing and assessing materials and removing materials must implement systems and processes that enable the provider to take appropriate action in response to breaches of terms and conditions, community standards, and/or acceptable use policies relating to class 1A material including at a minimum, systems and process that: i) enable the review by the provider of reports by Australian end-users of class 1A materials (more detail under "Trust and Safety function" below) and appropriate action to be taken in response; and ii) enable the prioritisation by the provider and, where necessary, escalation of reports of class 1A materials by Australian end-users. **Systems and processes for responding to breaches of policies relating to class 1A materials for pre-assessed relevant electronic services and Tier 1 and Tier 2 relevant electronic services that are not capable of reviewing and assessing or removing class 1A materials.** A provider of: a) a pre-assessed relevant electronic service; or b) a Tier 1 or Tier 2 relevant electronic service, that is not capable of reviewing and assessing materials and removing materials must have standard operating procedures that either: i) where the provider is not capable of reviewing and assessing materials, refer Australian end-users who are reporters of class 1A materials to eSafety resources; or ii) where the provider is capable of reviewing and assessing materials enable the provider to take appropriate action in response to breaches of terms and conditions, community standards, and/or acceptable use policies relating to class 1A material. ***Guidance:*** *Where this measure requires systems and processes for the review, and response to, user reports, such systems and processes should be designed to enable providers of relevant electronic services to enforce policies in a proportionate, scalable and effective manner based on 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 of service and the source of reports. Processes should be documented in a manner that clearly informs personnel of the steps they need to take to confirm breaches of policies relating to class 1A materials and the actions they should take in response to breaches of policies, including rapid response requirements for reports of CSEM or pro-terror materials, or where the physical safety of an end-user is in immediate danger.*

	Certain relevant electronic services such as closed communication relevant electronic services and encrypted relevant electronic services will often not be capable of reviewing and assessing materials or capable of removing materials because they are legally not permitted to detect the relevant material and/or do not have access to relevant messages to enable providers to review material being shared or any surrounding communications to assess context in accordance with the National Classification Scheme. For example, providers of SMS, MMS services, and encrypted relevant electronic services often do not have access to the content of any communications, and closed communication relevant electronic services often enable end-users to communicate with end-users of other equivalent services (e.g., other end-users with a telephone number or email address) which can also act as a barrier to relevant investigations. Where this is the case, providers of closed communication relevant electronic services are best able to assist end-users by explaining how they can engage with relevant authorities who are able to investigate concerns more fully. Referral of end-users to eSafety resources will help assist end-users in this regard. For example, eSafety has power to take direct action against end-users that share class 1A materials under the OSA. If a closed communication relevant electronic service is able to do so, it may instead choose to take appropriate action in response to breaches of terms and conditions, community standards, and/or acceptable use policies relating to class 1A material.
Minimum compliance measures for: **pre-assessed relevant electronic services;** **Tier 1 relevant electronic services;** **and** **Tier 2 relevant electronic services**	**4) Action in response to breaches of policies relating to class 1A material** A provider of a pre-assessed relevant electronic service or a Tier 1 or Tier 2 relevant electronic service that is capable of reviewing and assessing materials must take appropriate action in response to violations of terms and conditions, community standards, and/or acceptable use policies for class 1A material that is reasonably proportionate to the level of harm associated with the relevant breach in accordance with the systems, processes and standard operating procedures required by measure 3. A provider that is subject to this measure must: a) where capable of removing materials, 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; and 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 class 1A materials from additional breaches of these terms and conditions, policies, and/or standards. Appropriate steps include (depending on the service and material in question): i) issuing warnings to account holders; ii) restricting the end-user's use of their account (e.g., preventing the end-user from being able to send material using the service); iii) suspending the end-user's account for a defined period; iv) terminating the end-user's account; and/or v) taking reasonable steps to prevent end-users who repeatedly breach terms and conditions, community standards, and/or acceptable use policies regarding class 1A material who have had their user account terminated from creating a new account. ***Guidance:*** *In determining appropriate steps under sub-measure 4 b), 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 breach and the frequency and scope of the breach. A provider of a Tier 1 or Tier 2 relevant electronic service should have a clear, documented policy outlining the criterion that will be used if applying any of the above measures.* *The kinds of reasonable steps that could be considered under sub-measure 4 b) v) could include, for example, detecting the end-user's device or identifier used for registration and blocking any new accounts created from that device or identifier used for registration either indefinitely or for a period of time*

	(depending on the severity of the policy breach) or, where the service is subject to a pay wall, preventing use of a credit card known to be associated with the end-user's account to create a new account.
Minimum compliance measures for: **Tier 1 relevant electronic services;** **Tier 2 relevant electronic services;** **dating services;** **open communication relevant electronic services;** **encrypted relevant electronic services;** **and** **gaming services with communications functionality**	**5) Trust and safety function** A provider of: a) a Tier 1 or Tier 2 relevant electronic service; b) a dating service; c) an open communication relevant electronic service; d) an encrypted relevant electronic service; or e) a gaming service with communications functionality, must ensure that it is 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. ***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.* *The trust and safety function should regularly report to the industry participant's senior management on safety issues related to the service. The trust and safety function should be subject to an adequate level of oversight and accountability by senior management and there should be clear protocols for escalating safety issues within the organisation.*
Minimum compliance measures for: **pre-assessed relevant electronic services;** **Tier 1 relevant electronic services;** **and** **Tier 2 relevant electronic services**	**6) Safety features and settings** A provider of: a) a Tier 1 or Tier 2 relevant electronic service; b) a dating service; c) an open communication relevant electronic service; d) an encrypted relevant electronic service; or e) a gaming service with communications functionality, must evaluate the types of features and settings they could adopt to minimise risks to Australian end-users related to class 1A material and adopt the most appropriate features and/or settings for the type of service offered. **Safety features and settings for Tier 1 relevant electronic services, open communication relevant electronic services, and gaming services with communications functionality:** At a minimum, a provider of: a) a Tier 1 relevant electronic service; b) an open communication relevant electronic service; or c) a gaming service with communications functionality, must: i) if the service allows the sending of messages, have settings that allow users to block messages from other users; ii) 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;

	iii) if the service allows the creation of accounts by a young Australian child, provide settings that are designed to prevent children from unwanted contact from strangers, including settings which: (A) make accounts of a young Australian child private by default; and (B) prevent the location of a young Australian child using the service being shared with any accounts other than accounts approved by the young Australian child or their parent or guardian. **Safety features and settings for dating services** At a minimum, a provider of a dating service must: a) have settings that allow users to block messages from another user from interacting with the user; b) require an end-user to register for the service before uploading content or using the communication features, and during the registration process, collect and retain a phone number, email address, social media account, or other identifier; and c) take reasonable steps to prevent the creation of accounts by individuals under the age of 18 years. ***Guidance:*** *The reasonable steps that must be taken by dating services under sub measure c) could include:* *i) requiring a user to declare their date of birth during the account registration process;* *ii) implementing age estimation technology to determine a user's age;* *iii) using artificial intelligence tools that help to understand someone's real age; and/or* *iv) blocking the identifier used for registration from re-registering for the service.* **Safety features and settings for closed communication relevant electronic services and encrypted relevant electronic services** A provider of: a) a closed communication relevant electronic service; or b) an encrypted relevant electronic service, must require a user to register for the service using a phone number, email address, or other identifier.
Minimum compliance measures for: **all relevant electronic services**	**7) Safety by design assessments** If a provider of a relevant electronic 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 subsequently implements a significant new feature that would take it outside that category, then that provider must take reasonable steps to (re)assess the application of the Code to the service, in accordance with clause 5, and if applicable conduct a risk assessment in accordance with clauses 5.3 and 5.6. 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 an assessment under this measure, the provider of a relevant electronic service should consider whether any of the systems, processes or procedures that it must implement under this Code need to be updated in light of such new product or feature. *In implementing this measure, the provider of the relevant electronic service may, for example:* *i) use the safety by design tools published by eSafety to assess the safety risks associated with a new product or feature; and* *ii) consult additional guidance related to safety risks published by eSafety.*
Minimum Compliance measure for: **Tier 1 relevant electronic services;** **open communication relevant electronic services;** **dating services;** **and** **gaming services with communications functionality**	**8) Use of systems, processes, and technologies to detect and remove known child sexual abuse material** A provider of: a) a Tier 1 relevant electronic service; b) an open communication relevant electronic service that is not a carriage service provider; c) a dating service; or d) a gaming service with communications functionality, that is capable of reviewing and assessing material on the service and removing material from the service will implement systems, processes, and/or technologies designed to detect, flag, and/or remove instances of known CSAM from the service. Examples of systems processes and/or technologies designed that may be used by providers to detect, flag, and/or remove instances of known CSAM in accordance with this measure include, but are not limited to: i) hashing technologies, machine learning, or artificial intelligence that scan for known CSAM; and/or ii) the implementation of systems and/or processes designed to detect key words, behavioural signals, and/or patterns associated with the distribution of CSAM. Note: This measure does not require the implementation of technologies such as client-side scanning that would enable access to material on encrypted relevant electronic services by a third party other than the senders and intended recipients of that material, or prevent services from adopting encryption. ***Guidance:*** *In implementing this measure, providers of the relevant categories of relevant electronic service 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 human resourcing required to review detected materials, and the need to provide adequate health and safety arrangements for personnel undertaking such review. The rights and expectations of legitimate users of relevant electronic services, above) are also important factors for providers to consider when considering the detection option that is appropriate for a particular service. In addition, the use of certain technology, such as hashing, may not be technically possible on some surfaces, such as a 3D game environment. If a service is not able to use such technology (e.g., due to encryption), it may instead deploy systems and processes designed to detect behavioural signals where the provider holds sufficient data that can be used, reasonably accurately, for the purpose of such an analysis.*
Minimum Compliance measure for: **Tier 1 relevant electronic services;** **and**	**9) Use of systems, processes and technologies to detect and remove known pro-terror material** A provider of: a) a Tier 1 relevant electronic service; or b) an open communication relevant electronic service, that is capable of reviewing and assessing material on the service and removing material from the service will implement systems, processes, and/or technologies

open communication relevant electronic services	designed to detect, flag, and/or remove instances of known pro-terror materials from the service. Examples of systems, processes, and/or technologies that may be used by providers to detect, flag, and/or remove instances of known pro-terror materials in accordance with this measure include, but are not limited to: i) hashing technologies, machine learning, or artificial intelligence that scans for known pro-terror materials; and/or ii) the implementation of systems and/or processes designed to detect key words, behavioural signals, and/ or patterns associated with the distribution of known pro-terror materials. This minimum compliance measure does not apply to carriage service providers to the extent that they provide relevant electronic services via carriage services. Note: This measure does not require the implementation of technologies such as client-side scanning that would enable access to material on encrypted relevant electronic services by a third party other than the senders and intended recipients of that material, or prevent services from adopting encryption. ***Guidance:*** *In implementing this measure, providers of the relevant categories of relevant electronic 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. The rights and expectations of legitimate users of relevant electronic services are also important factors for providers to consider when considering the detection option that is appropriate for a particular service.*
Minimum compliance measure for: **Tier 1 relevant electronic services;** **dating services;** **open communication relevant electronic services;** **closed communication relevant electronic services BUT EXCLUDING carriage service providers;** **and** **encrypted relevant electronic services**	**10) Actions to be taken to disrupt or deter CSAM and pro-terror materials** A provider of: a) a Tier 1 relevant electronic service; b) a dating service; c) an open communication relevant electronic service; d) closed communication relevant electronic service; or e) an encrypted relevant electronic service, must take actions and must invest in systems, processes, and/or technologies that aim to disrupt and/or deter end-users from using the service to create, post or disseminate CSAM and pro-terror material. This minimum measure does not apply to carriage service providers to the extent that they provide relevant electronic services via carriage services. Note: this measure applies to both known pro-terror material and known CSAM and first generation CSAM and pro-terror materials (previously unknown material). Note: This measure does not require the implementation of technologies such as client-side scanning that would enable access to material on encrypted relevant electronic services by a third party other than the senders and intended recipients of that material, or prevent services from adopting encryption. ***Guidance:*** *In implementing this measure, providers must consider that the threat to online safety posed by first generation CSAM and pro-terror material (previously unknown material) is often different to the threat posed by known material. First generation material is more likely to indicate current and ongoing safety risks such as against a child being groomed and coerced into producing new abusive images.* *Providers should monitor and assess the appropriateness of different disruption and deterrence options for taking action against the risk of pro-terror materials*

	and CSAM on their services. Important factors in considering the practicality of implementing different options include: *i) the extent to which the provider is capable of accessing, viewing and/or removing material on the service; and* *ii) the rights and expectations of legitimate users of relevant electronic services.* *Examples of actions providers may take to disrupt and deter end-users from using the service to create, post, or disseminate CSAM and pro-terror material include, but are not limited to:* *i) using AI or machine learning techniques (such as behavioural signals) to detect and remove CSAM and pro-terror materials;* *ii) interventions that are targeted at preventing end-users from posting this material on the service, for example, by acquiring and utilising off-platform information can help identify and block the registration of potential users that have distributed CSAM and /or pro-terror material in other environments; and* *iii) deploying safety tools that disrupt or deter the distribution of CSAM and/or pro-terror materials.* *The type of investments that can be made under this clause include, but are not limited to:* *i) investment in research and development and/or testing of novel technological solutions to address CSAM and/or pro-terror material, for example nudging techniques targeted at deterring end-users from engaging with such materials and/or prompting users to file reports about such material;* *ii) providing financial or technical support to non-governmental organisations that have recognised expertise in tackling CSAM or pro-terror material to improve their infrastructure and/or technical capabilities;* *iii) contributing to programs operated by non-governmental organisations such as Tech Against Terrorism that are designed to improve the capability of services to detect CSAM and/or pro-terror materials; and* *iv) making technological solutions available to other service without charge or on an open-source basis.*
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 measures for: **pre-assessed relevant electronic services;** **Tier 1 relevant electronic services;** **and** **Tier 2 relevant electronic services**	**11) Systems and processes for enforcement of policies by Tier 1 and Tier 2 relevant electronic services and pre-assessed relevant electronic services** A provider of: a) a Tier 1 or Tier 2 relevant electronic service; or b) a pre-assessed relevant electronic service, that is capable of reviewing and assessing materials, must implement appropriate systems and processes that enable the provider to take action for breaches of terms and conditions, community standards, and/or acceptable use policies in relation to class 1B material. Appropriate systems and processes include: ii) having processes that include clearly specified internal channels for the provider to respond to and, where necessary, escalate reports by Australian end-users of breaches of the provider's terms and conditions, community standards, and/or acceptable use policies; and ii) having processes for the provider to provide operational guidance to personnel as to steps that must be taken within specified timeframes to deal with class 1B materials that breach the service provider's policies.

	Systems and processes for enforcement of policies by Tier 1 and Tier 2 relevant electronic services and pre-assessed relevant electronic services that are not capable of reviewing and assessing class 1B materials from the service A provider of: a) a Tier 1 or Tier 2 relevant electronic service; or b) a pre-assessed relevant electronic service, must have standard operating procedures that either: i) if the provider is not capable of reviewing and assessing materials reported by Australian end-users of the service, refer Australian reporters of class 1B materials to eSafety resources; or ii) if the provider is capable of reviewing and assessing materials reported by Australian end-users of the service, enable the provider to determine and take appropriate action for breaches of terms and conditions, community standards, and/or acceptable use policies in relation to class 1B material. ***Guidance:*** *Certain relevant electronic services such as closed communication relevant electronic services and encrypted relevant electronic services will often not be capable of reviewing and assessing materials or capable of removing materials because they are legally not permitted to detect the relevant material and/or do not have access to relevant messages to enable providers to review material being shared or any surrounding communications to assess context in accordance with the National Classification Scheme. For example, providers of SMS, MMS services and encrypted relevant electronic services often do not have access to the content of any communications, and closed communication relevant electronic services often enable end-users to communicate with end-users of other equivalent services (e.g., other end-users with a telephone number or email address) which can also act as a barrier to relevant investigations. As such, providers of closed communication relevant electronic services are best able to assist end-users by explaining how they can engage with relevant authorities who are able to investigate concerns more fully. Referral of end-users to eSafety resources will help assist end-users in this regard. For example, eSafety has power to take action against end-users that share class 1A materials under the OSA. If a closed communication relevant electronic service is able to do so, it may instead choose option (ii).* *Systems and processes to provide operational guidance to personnel as to steps that must be taken to deal with reports should be designed to enable providers of relevant electronic 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.*
Minimum compliance measures for: **pre-assessed relevant electronic services;** **Tier 1 relevant electronic services;** **and** **Tier 2 relevant electronic services**	**12) Action in response to breaches of policies** A provider of: a) a Tier 1 or Tier 2 relevant electronic service; or b) a pre-assessed relevant electronic service, that is capable of reviewing and assessing materials must take appropriate action in response to breaches of terms and conditions, community standards, and/or acceptable use policies for class 1B materials that is reasonably proportionate to the level of harm associated with the relevant breach in accordance with the systems, processes, and/or standard operating procedures required by measure 11. Examples of appropriate steps include (depending on the service and material in question): i) where the provider is capable of removal of material, removal of the relevant material;

	ii) issuing warnings to account holders; iii) restricting the end-user's use of their account (e.g., preventing the end-user from being able to send material using the service); iv) suspending the user's account for a defined period; v) terminating the user's account; and/or vi) taking reasonable steps to prevent end-users that repeatedly breach terms and conditions, community standards and/or acceptable use policies who have had their user account terminated from creating a new account. ***Guidance:*** *In determining appropriate steps under measure 12, 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. A provider subject to this requirement should have a clear, documented policy outlining the criterion that will be used if applying any of the above measures.* *The kinds of appropriate steps that could be considered in relation to sub-measure 12* v) *include, for example, detecting the end-user's device or identifier used for registration and blocking any new accounts created 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 is subject to a pay wall, preventing use of a credit card known to be associated with the end-user's account to create a new account.*
Minimum compliance measures for: **Tier 1 relevant electronic services;** **Tier 2 relevant electronic services;** **encrypted relevant electronic services;** **dating services;** **open-communications relevant electronic services;** **and** **gaming services with communications functionality**	**13) Trust and safety function** See measure 5 above.
Minimum compliance measures for: **all relevant electronic services**	**14) Safety by design assessments** See measure 7 above.
Outcome 4: Industry participants take reasonable and proactive steps to limit hosting of class 1A and 1B material in Australia.	
	This outcome does not require additional measures for relevant electronic services (see preamble to Head Terms).

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 materials.	
Minimum compliance measures for: **pre-assessed relevant electronic services;** **and** **Tier 1 relevant electronic services**	**15) Forum** A provider of: a) a Tier 1 relevant electronic service; or b) a pre-assessed relevant electronic service with more than 1 million monthly active account holders (or more than 1 million active services in operation (SIO) for providers of closed communication relevant electronic services that provide those services via carriage services) in Australia, must take part in an annual forum organised or facilitated by any industry association referred to in the Head Terms to discuss and evaluate the effectiveness of measures implemented under this Code and share best practice in implementing the Code and online safety in general with other industry participants. Note: the industry association responsible for the organisation and facilitation of the forum will ensure that the annual forum will allow online participation.
Optional compliance measures for: **all relevant electronic services**	**16) Working with researchers and academics** A provider of a relevant electronic service 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.
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 measures for: **Tier 1 relevant electronic services;** **encrypted relevant electronic services;** **and** **open communication relevant electronic services**	**17) Updates and consultation with eSafety about relevant changes to technology** A provider of: a) a Tier 1 relevant electronic service; b) an encrypted relevant electronic service; c) an open communication relevant electronic service; d) a closed communication relevant electronic service that is capable of reviewing and assessing materials; or e) a gaming service with communications functionality, must share information with eSafety about significant new features or functions released by the provider of the service that the provider reasonably considers are likely to have a significant effect on the access or exposure to, distribution of, and online storage of class 1A or class 1B materials in the reports it provides in accordance with measure 26 or measure 28.
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 measures for: **pre-assessed relevant electronic services;**	**18) Information for Australian end-users about the role and functions of eSafety, including how to make a complaint to eSafety** A provider of: a) a pre-assessed relevant electronic service; or b) a Tier 1 or Tier 2 relevant electronic service,

Tier 1 relevant electronic services; **and** **Tier 2 relevant electronic services**	must publish clear information that is accessible to Australian end-users regarding: i) the role and functions of eSafety, including how to make a complaint to eSafety; and ii) information about the mechanisms described in measure 19.
Outcome 8: Industry participants provide clear and effective reporting and complaints mechanisms for class 1A and class 1B material.	
Minimum compliance measures for: **pre-assessed relevant electronic services;** **Tier 1 relevant electronic services;** **and** **Tier 2 relevant electronic services**	**19) Reporting and complaints mechanisms for class 1A and class 1B material for providers of a Tier 1 or Tier 2 relevant electronic service or a pre-assessed relevant electronic service that is capable of reviewing and assessing materials** A provider of: a) a Tier 1 or Tier 2 relevant electronic service; or b) a pre-assessed relevant electronic service, that is capable of reviewing and assessing materials, must provide a tool, mechanism, or other process which enables Australian end-users to report, flag, and/or make a complaint about material accessible on the service that breaches the provider's terms and conditions, community standards, and/or acceptable use policies. Such reporting mechanisms must: i) be easily accessible and easy to use; ii) be accompanied clear instructions on how to use them, as well as an overview of the reporting process; and iii) 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. **Reporting and complaints mechanisms for class 1A and class 1B material for providers of Tier 1 or Tier 2 relevant electronic services or pre-assessed relevant electronic services that are not capable of reviewing and assessing materials** A provider of: a) a Tier 1 or Tier 2 relevant electronic service; or b) a pre-assessed relevant electronic service that is not capable of reviewing and assessing materials must: i) provide a tool, mechanism, or other process that assists Australian end-users to report, flag, or make complaints about materials that breach a service's terms and conditions, community standards, and/or acceptable use policies; ii) make available, via its website, a link to eSafety's online content reporting form; and iii) respond promptly, in accordance with measures 3 and 11, to complaints about class 1A or class 1B material made by Australian end-users. ***Guidance:*** *Certain relevant electronic services such as closed communication relevant electronic services and encrypted relevant electronic services will often not be capable of reviewing and assessing material or capable of removing materials*

	because they are legally not permitted to detect the relevant material and/or do not have access to relevant messages to enable providers to review material being shared or any surrounding communications to assess context in accordance with the National Classification Scheme. For example, providers of SMS, MMS services, and encrypted relevant electronic services often do not have access to the content of any communications, and closed communication relevant electronic services often enable end-users to communicate with end-users of other equivalent services (e.g., other end-users with a telephone number or email address) which can also act as a barrier to relevant investigations. As such, providers are best able to assist end-users by making it easy for complainants to refer complaints to eSafety, who can investigate concerns more fully. A provider may choose to respond to a complaint directly if it believes it has all relevant material available to it to do so, but otherwise may refer the complainant to eSafety.
Minimum compliance measures for: **pre-assessed relevant electronic services;** **Tier 1 relevant electronic services;** **and** **Tier 2 relevant electronic services**	**20) Complaints about handling of reports and/or compliance with Code** A provider of: a) a pre-assessed relevant electronic service; or b) a Tier 1 or Tier 2 relevant electronic service, must provide a tool, mechanism, or other process which enables Australian end-users to make a complaint about the provider's compliance with this Code.
Outcome 9: Industry participants effectively respond to reports and complaints about class 1A and class 1B material.	
Minimum compliance measures for: **pre-assessed relevant electronic services;** **Tier 1 relevant electronic services;** **and** **Tier 2 relevant electronic services**	**21) Appropriate steps for responding to Australian end-users regarding actions taken on reports:** A provider of a: a) Tier 1 or Tier 2 relevant electronic service; or b) a pre-assessed relevant electronic service, that is capable of reviewing and assessing material must: i) take appropriate steps, as required by measures 4 and 12, to promptly respond to reports made by Australian end-users of material that breaches the provider's terms and conditions, community standards, and/or acceptable use policies; ii) implement and document policies and procedures which detail how it gives effect to the requirement in a); and iii) ensure that personnel responding to reports are trained in the relevant electronic service's policies and procedures for dealing with reports. ***Guidance:*** *The manner in which a provider implements sub-measure 21 i), 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 relevant electronic service.* *A provider of a service that is not capable of reviewing and assessing material should instead note measure 19.* *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.*

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 measures for: **pre-assessed relevant electronic services;** **Tier 1 relevant electronic services;** **and** **Tier 2 relevant electronic services**	**22) Publication of policies** A provider of: a) a pre-assessed relevant electronic service; or b) a Tier 1 or Tier 2 relevant electronic service; must publish appropriate terms and conditions, community standards, and/or acceptable use policies, regarding material that 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. ***Guidance:*** *In implementing this measure, a provider of a relevant electronic 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 their enforcement.*
Optional compliance measures for all relevant electronic services	**23) Safety awareness campaigns** A provider of a relevant electronic service 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.
Minimum compliance measures for: **Tier 1 relevant electronic services;** **dating services;** **and** **open communication relevant electronic services**	**24) Dedicated section of website for Tier 1 relevant electronic services** A provider of: a) a Tier 1 relevant electronic service; b) an open communication relevant electronic service; or c) a dating service, 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, and that as a minimum contains the information in measures 18, 19, 20, and 25.
Minimum compliance measures for: **Tier 1 relevant electronic services;** **Tier 2 relevant electronic services;** **dating services;** **open communication**	**25) Information explaining the use of tools and settings.** A provider of: a) a Tier 1 or Tier 2 relevant electronic service; b) a dating service; c) an open communication relevant electronic service; or d) a gaming service with communications functionality, must provide easily accessible and understandable information that explains the tools and settings they make available under measure 6.

relevant electronic service; **and** **gaming services with communications functionality**	
Outcome 11: Industry participants publish annual reports about class 1A and 1B material and their compliance with this Code.	
Minimum compliance measures for: **Tier 1 relevant electronic services;** **and** **open communication relevant electronic services**	**26) Annual reporting by providers of a Tier 1 relevant electronic service and open communication relevant electronic services** A provider of a a) Tier 1 relevant electronic service; or b) an open communication relevant electronic service, must submit a Code report which as a minimum contains the following information: i) details of any risk assessment the provider is required to undertake pursuant to clause 5, together with information about the risk assessment methodology adopted; ii) the steps that the provider has taken to comply with the applicable minimum compliance measures; iii) an explanation as to why these measures are appropriate; and iv) the volume of CSEM or pro terror material removed by the provider of the relevant electronic service. The first Code report must be submitted by a provider of a Tier 1 relevant electronic service or an open communication relevant electronic service to eSafety 12 months after this Code comes into effect. A provider of a Tier 1 relevant electronic service or an open communication relevant electronic service must submit subsequent Code reports to eSafety annually. Note: 'appropriate' has the meaning given in the Head Terms. ***Guidance:*** *As part of explaining what steps the provider has taken and why they are appropriate, in c) and d) above, the provider should also explain any limitations on the capability of reviewing and assessing material and/or the removal of material. For instance, some providers may be capable of reviewing and assessing whether a breach of policies relating to class1 A or class1B materials has occurred in some circumstances (depending on what information has been provided by the end-user etc.) but not in others where it does not have sufficient surrounding context/visibility*
Minimum compliance measures for: **Tier 2 relevant electronic services**	**27) Reporting by providers of a Tier 2 relevant electronic service** Where eSafety issues a written request to a provider of a Tier 2 relevant electronic service to submit a Code report, the provider named in such request must submit to eSafety a Code report which includes the following information: a) details of any risk assessment the provider is required to undertake pursuant to clause 5, 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 relevant electronic service who has received such a request from eSafety is required to submit a Code report within 2 months of receiving the request, but for the first request no earlier than 12 months after this

	Code comes into effect. A provider of a Tier 2 relevant electronic 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. ***Guidance:*** *As part of explaining what steps the provider has taken and why they are appropriate, in b) and c) above, the provider should also explain any limitations on the capability of reviewing and assessing material and/or the removal of material. For instance, some providers may be capable of reviewing and assessing whether a breach of policies relating to class1 A or class1B materials has occurred in some circumstances (depending on what information has been provided by the end-user etc.) but not in others where it does not have sufficient surrounding context/visibility*
Minimum compliance measures for: **dating services;** **closed communication relevant electronic services;** **gaming services with communications functionality;** **and** **encrypted relevant electronic services**	**28) Reporting by providers of a closed communication relevant electronic service, encrypted relevant electronic service, dating service or a gaming service with communications functionality** Where eSafety issues a written request to a provider of: a) a closed communication relevant electronic service; b) a dating service; c) a gaming service with communications functionality; or d) an encrypted relevant electronic service, to submit a Code report, the provider named in such request must submit to eSafety a Code report which includes the following information: e) the steps that the provider has taken to comply with their applicable minimum compliance measures; and f) an explanation as to why these measures are appropriate. A provider of a closed communication relevant electronic service, a dating service, a gaming service with communications functionality, or an encrypted relevant electronic service who has received such a request from eSafety is required to submit a Code report within 2 months of receiving the request, but for the first request no earlier than 12 months after this Code comes into effect. A provider of a closed communication relevant electronic service or an encrypted relevant electronic 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. ***Guidance:*** *As part of explaining what steps the provider has taken and why they are appropriate, in b) and c) above, the provider should also explain any limitations on the capability of reviewing and assessing material and/or the removal of material. For instance, some providers may be capable of reviewing and assessing whether a breach of policies relating to class1A or class 1B materials has occurred in some circumstances (depending on what information has been provided by the end-user etc.) but not in others where it does not have sufficient surrounding context/visibility*.
Minimum compliance measures for: **enterprise relevant electronic services**	**29) Reporting by providers of an enterprise relevant electronic service** Where eSafety issues a written request to a provider of an enterprise relevant electronic 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 relevant electronic service who has received such a request from eSafety is required to provide written confirmation to eSafety within 2 months of receiving the request. A provider of an enterprise relevant electronic service will not be required to comply with such a request more than once in any 12-month period.