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:

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.

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.

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). Due to the nature of these services, and the manner in which they are otherwise regulated, providers of these services will often have no ability to view private communications shared 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. The measures applicable to closed communication relevant electronic services in this Code have been designed as a set of appropriate measures to address closed communication relevant electronic services given their nature.

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 have no ability to view private communications shared by end-users on their services. The measures applicable to encrypted relevant electronic services in this Code have been designed as a set of appropriate measures to address encrypted relevant electronic services given their nature.

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 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 at all, or 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) text that is subject to automated filtering technology; or

(vi) ephemeral voice interactions.

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 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. To the extent there is any conflict between the measures in this Code and the laws of any jurisdiction, an industry participant should note section 6 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 cannot assess whether materials communicated by end-users are class 1A or class 1B materials or remove 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 Risk profile

(a) Subject to clause 5(d), a provider of a relevant electronic 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

(b) Subject to clause 5(d) to 5(h), a provider of a relevant electronic service must 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.

(c) A provider of a relevant electronic service should use the table in clause 6(c) as a guide for developing an appropriate methodology for the risk assessment.

(d) A provider of:

(i) a closed communication relevant electronic service; or

(ii) an encrypted relevant electronic service; or

(iii) an enterprise relevant electronic service; or

(iv) a gaming service with limited communications functionality,

is not required to carry out a risk assessment under this Code. However, if such a provider makes a change to its service such that it would no longer be considered as a closed communication relevant electronic service, an encrypted relevant electronic service, an enterprise relevant electronic service or a gaming service with limited communications functionality, it must carry out a risk assessment in accordance with clause 5 (a) above.

(e) Providers of closed communication relevant electronic services are each treated as having an equivalent risk profile under this Code and must comply with the minimum

compliance measures as for closed communication relevant electronic services listed in clause 7(a) and specified in the table in clause 8.

(f) 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.

(g) 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.

(h) A gaming service with limited communications functionality is deemed to be a Tier 3 relevant electronic service. For the avoidance of doubt, a service that enables end-users to play online games with other end-users that is not a gaming service with limited communications functionality is required to undertake a risk assessment pursuant to clause 5(a).

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

(i) The provider must be able to reasonably demonstrate that the provider's risk assessment methodology is based on reasonable criteria which must, at a minimum, include functionality, purpose and scale of the relevant electronic service and any other criteria that are reasonably relevant for the purpose of determining the risk profile of the relevant electronic service under this Code.

(ii) A provider of a relevant electronic service must review the risk assessment following the implementation of any significant feature that may result in the service falling within a higher risk Tier.

(iii) A provider of a relevant electronic service must 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 each relevant electronic service the industry participant provides (including any weighting given to each risk factor); and

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

6 Guidance on risk assessment

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

(b) When adopting a methodology and process for identifying and assessing risks, industry participants should take into account the matters referred to in clause 5 and:

(i) the factors considered in the table below in clause 6(c), and the degree to which it has control of content;

(ii) expectations placed on users of that 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 relevant media services operations and the age of the user base;

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

(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 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:

<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).</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</td><td colspan="2">The relevant electronic service is primarily for general communication amongst the general population.</td></tr>
</table>

Risk Factor	Tier 3 Indicators	Tier 2 Indicators	Tier 1 Indicators
	service they have purchased; c) for communication within a gaming environment; d) to enable business communication outside of an enterprise environment.		
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 below 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 below apply to providers of the following categories of relevant electronic services:

Category	Description	Mandatory minumum compliance measures	Optional compliance measures
Relevant electronic service	all relevant electronic services covered by this Code	8 and 14	9
Tier 1 relevant electronic service	a relevant electronic service where the provider has determined the risk profile to be Tier 1 pursuant to clause 6(b) Note: A Tier 1 relevant electronic service does not include a closed communication relevant electronic service, encrypted relevant electronic service or enterprise relevant electronic service, as they are not required to designate a risk profile. These services are treated as a separate sub-category of relevant electronic service in the measures.	2 - 7, 11-13, 15, 17-22 and 26	16, and 23-25
Tier 2 relevant electronic service	a relevant electronic service where the provider has determined the risk profile to be Tier 2 pursuant to clause 6(b) Note: A Tier 2 relevant electronic service does not include a closed communication relevant electronic service, encrypted relevant electronic service or enterprise relevant electronic service, as they are not required to designate a risk profile. These services are treated as a separate sub-category of relevant electronic service in the measures.	2 - 7, 11-13, 18-22, and 27	16, and 23-25
Tier 3 relevant electronic service Note: See clause 7(i).	a relevant electronic service where the provider has determined the risk profile to be Tier 3 pursuant to clause 5(b) Note: A Tier 3 relevant electronic service does not	-	All

	include a closed communication relevant electronic service, encrypted relevant electronic service or enterprise relevant electronic service, as they are not required to designate a risk profile. These services are treated as a separate sub-category of relevant electronic service in the measures. Note: A gaming service with limited communications functionality is deemed to be a Tier 3 relevant electronic service.		
Closed communication relevant electronic service	closed communication relevant electronic services as defined in clause 2	2-4, 7, 11, 15, 18-20, 22, and 28	16, and 23-25
Encrypted relevant electronic service	encrypted relevant electronic services as defined in clause 3	2-4 ,6, 7, 11, 13,15, 17-20, 22, and 28	10, 16, and 23-25
Eenterprise relevant electronic service	enterprise relevant electronic services as defined in clause 3	1 and 29	-

(b) The table also sets out guidance on the implementation of some measures. This 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 customers of enterprise relevant electronic services 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.
Minimum compliance measures for: **Tier 1 relevant electronic services; and** **Tier 2 relevant electronic services;** **closed communication relevant electronic services; and** **encrypted relevant electronic services**	**2. Notifying appropriate entities about CSEM and pro-terror material on their services** If a provider of: a) a Tier 1 or Tier 2 relevant electronic service; b) a closed communication relevant electronic service; or c) an encrypted relevant electronic service, 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 Australian adult or child (i.e. an adult or child 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 report. A provider should ensure that such a report is compliant with other applicable laws such as privacy laws including the Privacy Act. Note a provider of a relevant electronic service may have additional legal obligations to report material under foreign laws e.g. to report materials to the National Center for Missing and Exploited Children.*
Minimum compliance measures for: **Tier 1 relevant electronic services; and** **Tier 2 relevant electronic services;** **closed communication**	**3. Systems and processes for responding to violation of policies prohibiting CSEM and pro-terror material** A provider of a Tier 1 or Tier 2 relevant electronic service must implement systems and processes that enable the provider to take appropriate action in response to violations of terms and conditions, community standards, and/or acceptable use policies prohibiting CSEM and pro-terror material, including at a minimum, systems and process that: a) enable the review by the provider of reports by Australian end-users of CSEM and pro-terror materials (more detail under "Trust and Safety function" below) and appropriate action to be taken in response; and

relevant electronic services; and **encrypted relevant electronic services**	b) enable the prioritisation and, where necessary, escalation of reports of CSEM and pro-terror material by Australian end-users. A provider of: a) a closed communication relevant electronic service; or b) an encrypted relevant electronic service, must have standard operating procedures that either: i. refer Australian reporters of CSEM and pro-terror materials to eSafety resources; or ii. enable the review of reports by Australian end-users of CSEM and pro-terror materials (more detail under "Trust and Safety function" below and appropriate action in response). ***Guidance:*** *Closed communication relevant electronic services and encrypted relevant electronic services will often not have access to relevant messages so as to enable providers to review material being shared or any surrounding communications for context. 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 (eg 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 more fully investigate concerns. Referral of end-users to eSafety resources will help assist end-users in this regard. If a closed communication relevant electronic service is able to do so, it may instead choose option (ii).* *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 prohibiting CSEM and pro-terror materials and the actions they should take in response to violations 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.*
Minimum compliance measures for: **Tier 1 relevant electronic services; and** **Tier 2 relevant electronic services;** **closed communication relevant electronic services; and** **encrypted relevant electronic services**	**4. Systems and processes for responding to violation of policies (class 1A materials other than CSEM and pro-terror materials)** A provider of a Tier 1 or Tier 2 relevant electronic service must implement appropriate systems and processes that enable the provider to take appropriate action in response to violations of terms and conditions, community standards, and/or acceptable use policies prohibiting class 1A materials (other than CSEM and pro-terror materials). Examples of such systems and processes may include: a) having processes that include clearly specified internal channels for responding to and, where necessary, escalating reports of class 1A material by Australian end-users; and b) having processes to provide operational guidance to personnel as to steps that must be taken within specified time frames to deal with class 1A materials that violate the service provider's policies. A provider of: a) a closed communication relevant electronic service; or b) an encrypted relevant electronic service,

	must have 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 violations of terms and conditions, community standards, and/or acceptable use policies prohibiting class 1A materials (other than CSEM and pro-terror materials). ***Guidance:*** *Closed communication relevant electronic services and encrypted relevant electronic services will often not have access to relevant messages so as to enable providers to review material being shared or any surrounding communications for context. 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 (eg 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 more fully investigate concerns. Referral of end-users to eSafety resources will help assist end-users in this regard. If a closed communication relevant electronic service is able to do so, it may instead choose option (ii).* *Systems and processes for the review of, and response to, user reports should be designed to enable providers of relevant electronic services to take appropriate action 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 on the service, the type and scale of service, and the source of reports. Processes should be supported by 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.*
Minimum compliance measures for: **Tier 1 relevant electronic services; and** **Tier 2 relevant electronic services**	**5. Action in response to violations of policies** A provider of a Tier 1 or Tier 2 relevant electronic service must take appropriate action in response to violations of terms and conditions, community standards, and/or acceptable use policies prohibiting CSEM and pro-terror material that is reasonably proportionate to the level of harm associated with the relevant violation. The provider must: a) remove instances of CSEM or pro-terror materials identified by the provider on the service within 24 hours or as soon as reasonably practicable, unless otherwise required to deal with such material by law enforcement; b) take appropriate steps designed to deter an end-user who has violated the relevant terms and conditions, community standards and/or acceptable use policies regarding CSEM or pro-terror materials from additional violations of these specific policies and standards. Appropriate steps may include (depending on the service and material in question): i. issuing warnings to account holders; ii. restricting the end-user's use of their account (e.g. preventing the end-user from being able to send material using the service); iii. suspending the end-user's account for a defined period; iv. terminating the end-user's account; and/or v. taking reasonable steps to prevent end-users who repeatedly violate terms and conditions, community standards and/or acceptable use policies regarding CSEM or pro-terror materials who have had their user account terminated from creating a new account. ***Guidance:*** *In determining appropriate steps under sub-measure 5 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 violation and the frequency and scope of the violation. 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-meaure 5 b) v). could include, for example, detecting the end-user's device or IP address and blocking any new accounts created from that device or IP address 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; and** **Tier 2 relevant electronic services; and** **encrypted relevant electronic services**	**6. Trust and safety function** A provider of: a) a Tier 1 or Tier 2 relevant electronic service; or b) an encrypted relevant electronic service, 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: **Tier 1 relevant electronic services; and** **Tier 2 relevant electronic services;** **closed communication relevant electronic services; and** **encrypted relevant electronic services**	**7. Safety features and settings** 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. Providers of Tier 1 and Tier 2 relevant electronic service 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. At a minimum, a provider of Tier 1 relevant electronic service must: a) if the service allows the sending of messages, have settings that allow users to block messages from other users; b) if the service allows for the display of a user's online status, have tools and settings that enable end-users to be hidden or to appear offline; and c) if the relevant electronic service allows the creation of children's accounts: i. provide settings that are designed to prevent children from unwanted contact from strangers, including settings which: (A) make accounts of children under the age of 16 private by default; and (B) prevent the location of child accounts being shared with any accounts other than approved accounts by default.

Minimum compliance measures for: **relevant electronic services**	**8. 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 and subsequently implements a significant new feature that would require the provider to undertake a risk assessment under this Code, then that provider must (re)assess its risk profile in accordance with 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, the provider of a Tier 1 or Tier 2 relevant electronic service 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 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.*
Optional Compliance measure for: **relevant electronic services**	**9. Use of technological tools to detect and remove known CSAM** A provider of a relevant electronic service may consider the availability and appropriateness of technological tools designed to detect, flag and/or remove instances of known CSAM the particular relevant electronic service, for example, through the use of hashing, machine learning, artificial intelligence or other safety technologies, and may implement such tools where available and appropriate for the relevant service. ***Guidance:*** *For many relevant electronic services, intercepting, accessing or monitoring private communications could result in breach of applicable statutory obligations and/or be contrary to the interests and/or expectations of legitimate users of the service and/or may not be technically possible, and as such any use should be considered carefully. The rights and expectations of legitimate users of relevant electronic services, and the statutory obligations of the provider (as outlined in clause 3 above) are important factors to consider when considering whether the use of such technology 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 technological tools (e.g. due to encryption or statutory obligations), it may consider the availability and appropriateness of technological tools designed to detect behavioural signals as set out in measure 10 below.*
Optional Compliance measure for: **encrypted relevant electronic services**	**10. Use of technological tools to detect behavioural signals associated with CSEM and pro-terror material** Where it holds data that can be used for such an analysis, a provider of an encrypted relevant electronic service may deploy technological tools designed to detect behavioural signals associated with the distribution of CSEM or pro-terror material, and may implement such tools where available and appropriate for the relevant service.
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: **Tier 1 relevant electronic services; and** **Tier 2 relevant electronic services;** **closed communication relevant electronic services; and** **encrypted relevant electronic services**	**11. Systems and processes for enforcement of policies** A provider of a Tier 1 or Tier 2 relevant electronic service must implement appropriate systems and processes that enable the provider to take appropriate action for violations of terms and conditions, community standards, and/or acceptable use policies in relation to class 1B material. Examples of appropriate systems and processes may include: a) having processes that include clearly specified internal channels for responding to and, where necessary, escalating reports of violations of the provider's terms and conditions, community standards and/or acceptable use policies by Australian end-users; and b) having processes to provide operational guidance to personnel as to steps that must be taken within specified timeframes to deal with class 1B materials that violate the service provider's policies. A provider of: a) a closed communication relevant electronic service; or b) an encrypted relevant electronic service, must have standard operating procedures that either: i) refer Australian reporters of class 1B materials to eSafety resources; or ii) enable the provider to take appropriate action for violations of terms and conditions, community standards, and/or acceptable use policies in relation to class 1B material. ***Guidance:*** *Closed communication relevant electronic services and encrypted relevant electronic services will often not have access to relevant messages so as to enable providers to review material being shared or any surrounding communications for context. 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 (eg 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 more fully investigate concerns. Referral of end-users to eSafety resources will help assist end-users in this regard. 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: **Tier 1 relevant electronic services; and** **Tier 2 relevant electronic services**	**12. Action in response to violation of policies** A provider of a Tier 1 or Tier 2 relevant electronic service must take appropriate action in response to violations of terms and conditions, community standards, and/or acceptable use policies that is reasonably proportionate to the level of harm associated with the relevant violation. Appropriate steps may include (depending on the service and material in question): a) removal of the relevant material; b) issuing warnings to account holders; c) restricting the end-user's use of their account (e.g. preventing the end-user from being able to send material using the service); d) suspending the user's account for a defined period;

	e) terminating the user's account; and/or f) taking reasonable steps to prevent end-users that repeatedly violate 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 sub-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 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 appropriate steps that could be considered in relation to sub-measure 12* f) *include, for example, detecting the end-user's device or IP address and blocking any new accounts created from that device or IP address 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; and** **Tier 2 relevant electronic services; and** **encrypted relevant electronic services**	**13. Trust and safety function** See measure 6 above.
Minimum compliance measures for: **relevant electronic services**	**14. Safety by design assessments** See measure 8 above.
Outcome 4: Industry participants take reasonable and proactive steps to prevent or limit hosting of class 1A and 1B material in Australia.	
	This outcome does not require additional measures for relevant electronic services (see preamble to Heads of Terms).
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: **Tier 1 relevant electronic services;** **closed communication relevant electronic services; and** **encrypted relevant electronic services**	**15. Forum** A provider of: a) a Tier 1 relevant electronic service; b) a closed communication relevant electronic service; or c) an encrypted relevant electronic service, must take part in an annual forum organised or facilitated by any industry association referred to in the Heads of Terms to discuss and evaluate the effectiveness of measures implemented under this Code and share best practice in implementing the Code and online safety in general with other industry participants.

Optional compliance measures for: **Tier 1 relevant electronic services; and** **Tier 2 relevant electronic services;** **closed communication relevant electronic services; and** **encrypted relevant electronic services**	**16. Working with researchers and academics** A provider of: a) a Tier 1 or Tier 2 relevant electronic service; b) a closed communication relevant electronic service; or c) an encrypted 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; and** **encrypted relevant electronic services**	**17. Updates and consultation with eSafety about relevant changes to technology** A provider of: a) a Tier 1 relevant electronic service; or b) an encrypted relevant electronic service, must share information with eSafety about significant new features or functions released by the provider of the relevant electronic service that the provider reasonably considers are likely to have a significant effect on the access or exposure to, distribution of, and online storage of class 1A or class 1B materials in the reports it provides in accordance with measure 26. In implementing this measure industry participants are not required to disclose information to the eSafety that is confidential.
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: **Tier 1 relevant electronic services; and** **Tier 2 relevant electronic services;** **closed communication relevant electronic services; and** **encrypted 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 Tier 1 or Tier 2 relevant electronic service; b) a closed communication relevant electronic service; or c) an encrypted relevant electronic service, must publish clear information that is accessible to 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 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:	**19. Reporting and complaints mechanisms for class 1A and class 1B material** A provider of a Tier 1 and Tier 2 relevant electronic service must provide a tool, mechanism or other process which enables Australian end-users to report, flag

Tier 1 relevant electronic services; and **Tier 2 relevant electronic services;** **closed communication relevant electronic services; and** **encrypted relevant electronic services**	and/or make a complaint about material accessible on the service that violates 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 clear instructions on how to use them, as well as an overview of the reporting process; 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. A provider of: a) a closed communication relevant electronic service; or b) an encrypted relevant electronic service, must: i) provide tools, mechanisms or other processes that assist Australian end-users to report, flag or make complaints about materials that breach a service's terms and conditions, community standards, and/or acceptable use policies; ii) make available clear and accessible information to Australian end-users about the use of reporting tools, mechanisms or other processes; iii) make available, via its website, a link to eSafety's online content reporting form; and iv) respond promptly to complaints about class 1A or class 1B material made by Australian end-users by either (A) responding to the complaint, or (B) referring the complainant to eSafety. ***Guidance:*** *Closed communication relevant electronic services and encrypted relevant electronic services will often not have access to relevant messages so as to enable providers to review material being shared or any surrounding communications for context. 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 (eg 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 more fully investigate concerns. 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: **Tier 1 relevant electronic services; and** **Tier 2 relevant electronic services;** **closed communication relevant electronic services; and**	**20. Complaints about handling of reports and/or compliance with Code** A provider of: a) a Tier 1 or Tier 2 relevant electronic service; b) a closed communication relevant electronic service; or c) an encrypted relevant electronic service, must provide a tool, mechanism or other process which enable Australian end-users to make a complaint about the provider's compliance with this Code.

encrypted relevant electronic services	
Outcome 9: Industry participants effectively respond to reports and complaints about class 1A and class 1B material.	
Minimum compliance measures for: **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 Tier 1 or Tier 2 relevant electronic service must: a) take appropriate steps to promptly respond to reports of material that violates the provider's terms and conditions, community standards, and/or acceptable use policies made by Australian end-users; b) implement and document policies and procedures which detail how it gives effect to the requirement in (a); and c) ensure that personnel responding to reports are trained in the relevant electronic service's policies and procedures for dealing with reports. ***Guidance:*** *The manner in which a provider implements sub-measure 21 (a), 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 closed communication relevant electronic service or encrypted relevant electronic service 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: **Tier 1 relevant electronic services; and** **Tier 2 relevant electronic services;** **closed communication relevant electronic services; and** **encrypted relevant electronic services**	**22. Publication of policies relating to the OSA** A provider of: a) a Tier 1 or Tier 2 relevant electronic service; b) a closed communication relevant electronic service; or c) an encrypted relevant electronic service, must publish appropriate terms and conditions, community standards, and/or acceptable use policies, regarding content which is not acceptable on the service, having regard to the nature of the service. Such terms and conditions, community standards and/or acceptable use policies must make clear that the broad categories of material within class 1A material are prohibited on the service. ***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;* *iii) communicate such terms and conditions, standards and/or policies to all personnel that are directly involved in their enforcement.*
Optional compliance measures for:	**23. Safety awareness campaigns** A provider of: a) a Tier 1 or Tier 2 relevant electronic service;

Tier 1 relevant electronic services; and **Tier 2 relevant electronic services;** **closed communication relevant electronic services; and** **encrypted relevant electronic services**	b) a closed communication relevant electronic service; or c) an encrypted 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.
Optional compliance measures for: **Tier 1 relevant electronic services; and** **Tier 2 relevant electronic services;** **closed communication relevant electronic services; and** **encrypted relevant electronic services**	**24. Dedicated section of website** A provider of: a) a Tier 1 or Tier 2 relevant electronic service; b) a closed communication relevant electronic service; or c) an encrypted relevant electronic service, may establish a dedicated section of the service to house online safety information, such as a safety centre.
Optional compliance measures for: **Tier 1 relevant electronic services; and** **Tier 2 relevant electronic services;** **closed communication relevant electronic services; and** **encrypted relevant electronic services**	**25. Information explaining how relevant electronic service providers protect the safety of children using their services.** A provider of: a) a Tier 1 or Tier 2 relevant electronic service; b) a closed communication relevant electronic service; or c) an encrypted relevant electronic service, may publish easily accessible and understandable information that explains the actions it takes to minimise the risk of harm to children on the service.
Outcome 11: Industry participants publish annual reports about Code compliance.	
Minimum compliance measures for: **Tier 1 relevant electronic services**	**26. Annual reporting by providers of a Tier 1 relevant electronic service** A provider of a Tier 1 relevant electronic service must submit a Code report which as a minimum contains the following information: a) details of the risk assessment it has carried out pursuant to clause 3, 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; and c) 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 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 the risk assessment it has carried out pursuant to clause 3, 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 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 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.
Minimum compliance measures for: **closed communications relevant electronic services; and** **encrypted relevant electronic services**	**28) Reporting by providers of a closed communications relevant electronic service or an encrypted relevant electronic service** Where eSafety issues a written request to a provider of an closed communications relevant electronic service or 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: a) the steps that the provider has taken to comply with their applicable minimum compliance measures; and b) an explanation as to why these measures are appropriate. A provider of a closed communications relevant electronic service or an encrypted relevant electronic 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 closed communications 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.
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.