Schedule 5 – Relevant Electronic Services Online Safety Code (Class 1C and Class 2 Material)

1 Structure

This Code is comprised of the terms of this Schedule together with the Online Safety Code (Class 1C and Class 2 Material) Head Terms (**Head Terms**).

2 Scope

This Code applies to a provider of a relevant electronic service (**RES**), so far as materials on that service are 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.

account holder, for an enterprise relevant electronic service, means the person who is the counterparty to the agreement with the provider of the service for the provision of the service.

closed communication relevant electronic service means a relevant electronic service the predominant purpose of which is to enable an end-user to communicate with another end-user other than the following:

a) an other communication relevant electronic service;

b) a dating service;

c) an enterprise relevant electronic service;

d) a telephony relevant electronic service;

e) a gaming service with communications functionality;

f) a gaming service with limited communications functionality.

dating service means a relevant electronic service the predominant purpose of which is:

a) to solicit, offer, promote or provide access to dating, relationship, compatibility, matrimonial, social or romantic referral services; and

b) to enable end-users to communicate with other end-users online,

but does not include such a service to the extent that its purpose is to connect end-users who offer their services for payment.

Note: Examples of services for payment are escort or sex work services.

enterprise relevant electronic service means a relevant electronic service:

a) the account holder for which is an organisation (and not an individual); and

b) the predominant purpose of which is to enable the account holder, in accordance with the terms of use for the service, to make the service available to a specified class of persons to facilitate communications between those persons; and

c) that is of a kind that is usually acquired by account holders for the purpose mentioned in paragraph b).

gaming service means:

(a) a gaming service with communications functionality; and

(b) a gaming service with limited communications functionality.

Note: There may be more than one 'provider' of a gaming service due to the supply chain used for different gaming services. For the purposes of this Code, the 'provider' of either type of gaming service is the provider that controls the version of the service made available to end-users and therefore controls the engineering and other decisions relating to the version of the features and settings made available to end-users by way of the service. For the avoidance of doubt, a person is not a provider of a gaming service of either type if the person merely resells the gaming service without alteration, and without having any control over the functionality, features, or content of the gaming service.

gaming service with communications functionality: a relevant electronic service is a **gaming service with communications functionality** if:

a) the predominant purpose of the service is to enable end-users in Australia to play online games with other end-users; and

b) the service enables sharing of user-generated URLs, hyper-linked text, images or videos between end-users;

but none of the following is a gaming service with communications functionality:

c) a gaming service with limited communications functionality;

d) a service that limits the sharing of user-generated material between end-users to any 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;

vi) ephemeral voice interactions.

gaming service with limited communications functionality means a relevant electronic service the predominant purpose of which is to enable Australian end-users to play online games with other end-users without enabling the sharing of user-generated URLs, hyper-linked text, images or videos between end-users (other than material of a kind referred to in paragraph (d) of the definition of gaming service with communications functionality).

other communication relevant electronic service means a relevant electronic service the predominant purpose of which is to:

a) enable end-users in Australia to view, search for or communicate with other end-users (target end-users) on the service without knowing the target end-user's phone numbers or email address; or

b) recommend target end-users to end-users in Australia, based on interests or connections common to the end-users,

other than the following:

c) a dating service;

d) an enterprise relevant electronic service;

e) a telephony relevant electronic service;

f) a gaming service with communications functionality;

g) a gaming service with limited communications functionality.

pre-assessed relevant electronic service means each of the following:

a) a closed communication relevant electronic service;

b) an other communication relevant electronic service;

c) a dating service;

d) a gaming service with communications functionality.

telephony relevant electronic service means a short messaging service (SMS) or a multimedia messaging service (MMS) provided over a public mobile telecommunications service as defined in subsection 32(1) of the *Telecommunications Act 1997*.

4 Risk profile

4.1 General requirement for risk assessment

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

i) is required to undertake a risk assessment and determine a risk profile; or

ii) is not required to undertake a risk assessment to determine a risk profile because it falls within a set category of relevant electronic service as set out in clause 4.4.

4.2 Risk assessment

a) Subject to clause 4.4 and except where the provider of a relevant electronic service 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, a provider of a relevant electronic service must undertake a risk assessment to assess the risk profile of the relevant electronic service (excluding any AI companion chatbot feature, if applicable) in relation to online pornography, self-harm material or high-impact violence in accordance with the following table:

If the risk that online pornography, self-harm material or high-impact violence material will be accessed or distributed on a service is …	**the risk profile of the service is …**
High	Tier 1
Medium	Tier 2
Low	Tier 3

b) Subject to clause 4.2(c), the provider of a:

i) relevant electronic service that is required to undertake a risk assessment under clause 4.2(a) (other than a telephony relevant electronic service);

ii) relevant electronic service that has chosen to automatically assign a Tier 1 risk profile as anticipated by clause 4.2(a) (other than a telephony relevant electronic service);

iii) a pre-assessed relevant electronic service; or

iv) a gaming service with limited communications functionality,

that includes an AI companion chatbot feature must undertake a risk assessment of that feature in respect of each generative AI restricted category of material in accordance with the following table (as applicable):

If the risk that online pornography will be generated using the AI companion chatbot feature is…	**the risk profile of the AI companion chatbot feature in relation to online pornography is …**
High	Tier 1
Moderate	Tier 2
Low	Tier 3

If the risk that high impact sexually explicit material will be generated using the AI companion chatbot feature is…	**the risk profile of the AI companion chatbot feature in relation to high impact sexually explicit material is …**
High	Tier 1
Moderate	Tier 2
Low	Tier 3

If the risk that self-harm material will be generated using the AI companion chatbot feature is…	**the risk profile of the AI companion chatbot feature in relation to self-harm material is …**
High	Tier 1
Moderate	Tier 2
Low	Tier 3

If the risk that high impact violence material will be generated using the AI companion chatbot feature is…	**the risk profile of the AI companion chatbot feature in relation to high impact violence material is …**
High	Tier 1
Moderate	Tier 2
Low	Tier 3

If the risk that violence instruction material will be generated using the AI companion chatbot feature is…	**the risk profile of the AI companion chatbot feature in relation to violence instruction material is …**

High	Tier 1
Moderate	Tier 2
Low	Tier 3

c) If:

i) the provider of a relevant electronic service is required to carry out a risk assessment under sub-clause b) in relation to an AI companion chatbot feature; and

ii) the sole or predominant purpose of the AI companion chatbot feature is to generate material in a particular generative AI restricted category,

then:

iii) the service provider is not required to undertake a risk assessment in relation to that category and will automatically have a Tier 1 risk profile in respect of that category; and

iv) is still required to undertake a risk assessment under clause 4.2(b) in relation to other categories.

Note: For example, if an AI companion chatbot feature has the sole or predominant purpose of enabling end-users to generate high impact violence material, the service provider will not be required to undertake a risk assessment in respect of that material. That feature will be required to comply with the measures for features with a Tier 1 risk profile, but only in respect of high impact violence material and not the other categories of material it does not have the sole or predominant purpose in respect of. The service provider will still need to conduct a risk assessment in respect of other relevant generative AI restricted categories of material to determine its risk profile in respect of those categories.

4.3 Methodology used for risk assessment and documentation

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

a) 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 (including the extent to which material posted on, distributed using or generated by the service will be available to end-users of the service in Australia and any generative artificial intelligence features of the service) or AI companion chatbot feature (as applicable), and, to the extent reasonably relevant, the additional requirements set out in clause 5 and any other criteria that are reasonably relevant for the purpose of determining the risk profile under this Code;

b) formulate in writing a plan and methodology for carrying out the risk assessment that ensures that each risk factor is accurately assessed;

c) carry out the risk assessment in accordance with the plan and methodology prepared under clause 4.3b), and by persons with the relevant skills, experience and expertise; and

d) as soon as practicable after determining the risk profile of a relevant electronic service or AI companion chatbot feature (as applicable), the provider of the service must record in writing:

i) details of the determination; and

ii) details of the conduct of any related risk assessment;

sufficient to demonstrate that they were made or carried out in accordance with this clause 4 and clause 5.

The record must include the reasons for the results of the assessment and the determination of the risk profile.

e) The provider of an AI companion chatbot feature that is required to do a risk assessment under clause 4.2(b) may:

i) if the AI companion chatbot feature is part of a relevant electronic service that is required to carry out a risk assessment under clause 4.1(a), carry out a single risk assessment for the relevant electronic service (including the AI companion chatbot feature) provided that separate risk profiles are assessed for the service as a whole, and for the AI companion chatbot feature; and

ii) cover all generative AI restricted categories of material at once, during the risk assessment for the AI companion chatbot feature, provided that a separate risk profile is assessed for each restricted category.

Note: Unlike some other Phase 2 codes, and with the exception of AI companion chatbot features, this Code requires a risk profile to be assigned to each service, not each category of relevant material on that service.

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

a) Clause 4.4b) sets out the categories of relevant electronic services that are not required to undertake a risk assessment under clause 4.2(a). However, the relevant provider must comply with the applicable compliance measures set out in this Code for services in the applicable category of relevant electronic service.

b) A provider of the following categories of relevant electronic services is not required to undertake a risk assessment under clause 4.2(a) to assess the risk profile of the relevant electronic service:

i) an enterprise relevant electronic service;

ii) a gaming service with limited communications functionality;

iii) a pre-assessed relevant electronic service.

c) Nothing in this clause 4.4 limits a provider's obligation to undertake a risk assessment of a AI companion chatbot feature where required by clause 4.2(b).

4.5 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 exempt from carrying out a risk assessment under clause 4.2(a) or (b) (as applicable); or

b) has previously carried out a risk assessment, but makes a change to its service that would result in the service falling within a higher risk tier,

it must carry out a risk assessment in accordance with clause 4.2(a) or (b) (as applicable) as soon as practicable and in any case no later than 6 months after the relevant change takes effect.

5 Risk assessment: requirements

a) This clause 5 applies where a provider of a relevant electronic service is required to undertake a risk assessment in accordance with clause 4.2(a) or (b) (as applicable).

b) A provider of a relevant electronic service must take into account the following additional matters when undertaking a risk assessment under clause 4.2(a) or (b), so far as they are relevant:

i) in the case of a service (excluding an AI companion chatbot feature):

(A) whether online pornography, self-harm material or high-impact violence material is permitted on the service;

(B) the terms or arrangements under which the provider acquires any content to be made available on the service;

(C) the likelihood that the service may be used to directly expose Australian children to online pornography, self-harm material or high-impact violence material;

(D) the likelihood that Australian children will use the service to access online pornography, self-harm material or high-impact violence material on the service;

(E) the functionality of the service (including generative artificial intelligence functionality or features) including the extent to which material posted on, distributed using or generated by the service will be available to end-users of the service in Australia;

ii) in the case of an AI companion chatbot feature:

(A) whether any generative AI restricted category of material is permitted on the feature and if so, the likely portion of that content as compared with other types of content;

(B) the likelihood that the feature may be used to directly expose Australian children to any generative AI restricted category of material;

(C) the likelihood that Australian children will use the feature to access any generative AI restricted category of material;

iii) in both cases:

(A) the terms of use for the service;

(B) the ages of end-users and likely end-users of the service;

(C) the likelihood that a significant number of Australian children will access the service;

(D) the number of Australian end-users that are monthly active account holders;

(E) the number of Australian children that are monthly active account holders;

Note: A service with a large number of Australian children that are monthly active account holders should be regarded as higher risk than a service with fewer such account holders.

(F) the predominant purpose of the service;

(G) a forward-looking analysis of:

(aa) likely changes to the operating environment for the service, including likely changes in the functionality or purpose of, or the scale of, the service; and

(ab) the impact of those changes on the ability of the service to meet the requirements of this Code;

(H) safety by design guidance and tools published or made available by a relevant government agency or a foreign or international body;

Note: Examples of relevant agencies and bodies are eSafety and the Digital Trust & Safety Partnership.

(I) relevant international laws and regulations applicable to the service that address online safety risks and harms similar to those addressed in this Code; and

(J) where applicable, design features and controls deployed to mitigate relevant risks.

Note: Without limiting this clause 5b), circumstances in which a matter will not be relevant to a service include where it is not relevant to the risk level of the service in the circumstances, relates to a topic that is irrelevant to the particular service due to its nature or requires consideration of information that is not available for the service.

6 Approach to measures and guidance for relevant electronic services

a) The tables in sections 7 to 15 below contain compliance measures for providers of relevant electronic services excluding any AI companion chatbot features, depending on the category of relevant electronic service being provided, or their risk profile.

b) The table in section 16 sets out compliance measures that apply to providers of AI companion chatbot features that are required to carry out a risk assessment under clause 4.2(b). These measures apply in addition to any compliance measures that otherwise apply to the relevant electronic service under a). To the extent there is any overlap in the measures in the table that applies to the relevant electronic service (excluding the AI companion chatbot feature), and the table in section 16, a single action by the provider may be sufficient to satisfy both measures.

c) Certain measures in this Code require a provider to take appropriate and proportionate action if it becomes aware of a breach of the terms and conditions it has in place with Australian end-users, including where contacted with information about such a breach by an end-user. For the avoidance of any doubt, some providers of relevant electronic services may not be capable of reviewing, assessing and/or removing material from their services in all circumstances (because such activity is not technically feasible or reasonably practicable) and a provider's awareness of a breach, and the appropriateness of any action taken in response, will be assessed in that context.

d) The table also includes 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.

e) Certain compliance measures will only apply to certain risk tiers or categories of RES (as specified at the top of each table, and in the column titled "Tier or category of RES") as set out in the tables in 7 to 16.

Note: A provider of an AI companion chatbot feature may have a different risk profile in respect of different categories of material. For example, an AI companion chatbot feature may have a Tier 1 risk profile for online pornography but a Tier 2 or Tier 3 risk profile for all other generative AI restricted categories. In that case, the Tier 1 compliance measures for the AI companion chatbot feature will only apply in relation to online pornography.

7 Compliance measures for all RES

The compliance measures in this table apply to all RES, but do not apply to any AI companion chatbot feature. These measures are additional to the other measures in the tables 8 to 15 below which each only apply to specific categories of RES (as specified) and table 16 which applies to certain AI companion chatbot features.

No.	Compliance measure
7.1	**Age assurance measures for online pornography and self-harm material** A provider who provides a relevant electronic service with the sole or predominant purpose of permitting end-users to share online pornography or self-harm material must, where technically feasible and reasonably practicable, implement: a) appropriate age assurance measures; and b) access control measures, before providing access to that service. A provider must also take appropriate steps to test and monitor the effectiveness of its age assurance and access control measures over time.
7.2	**Age assurance measures for gaming services** A provider who provides a gaming service that enables end-users to play a computer game that: a) is, or would likely be, classified as R18+ under the Classification Act because it constitutes simulated gambling material; or b) has otherwise been classified as R18+ in accordance with the Classification Act, must, where technically feasible and reasonably practicable, implement: c) appropriate age assurance measures; and d) access control measures, before providing access to that computer game. A provider must also take appropriate steps to test and monitor the effectiveness of its age assurance and access control measures over time. Note: Any computer game that has been classified by the Classification Board, or an approved classification tool, as R18+ under the Classification Act will fall within sub-measure b).

8 Compliance measures for closed communication relevant electronic services

The compliance measures in this table apply to closed communication relevant electronic services, but do not apply to any AI companion chatbot feature.

No.	Tier or category of RES	Compliance measure
8.1	closed communication relevant electronic service	**Terms and conditions prohibiting illegal activity** A provider of a service must: a) have terms and conditions in place with Australian end-users prohibiting the end-user from sharing material via the service in the course of engaging in any of the following categories of criminal activity: i. non-consensual sharing of intimate images; ii. grooming of children; or iii. sexual extortion (or sextortion); b) publish the terms and conditions by making them accessible on a website and/or application for the service (as relevant); c) ensure the prohibition described in sub-measure a) is set out in plain language in the terms and conditions; and d) if the provider becomes aware of a breach of the prohibition described in sub-measure a), take appropriate and proportionate action in a reasonably timely manner. It is not necessary that a particular form of words be used in the terms and conditions so long as the contractual effect of the terms and conditions is as required by sub-measure a). A provider must have systems and/or processes in place to support compliance with the obligation in sub-measure d). ***Guidance:*** *Providers should be aware that the material shared via the service in the course of engaging in the categories of criminal activity described in sub-measure a)i. to iii. could include class 1C and class 2 material.* *Providers have flexibility to design terms, systems, processes and policies to allow appropriate and proportionate responses to potential breaches on a case-by-case basis. Providers have the ability to exercise discretion to enforce terms and policies in accordance with the specific circumstances of each potential breach.* *Whilst appropriate and proportionate action in response to a breach will be dependent on the specific circumstances, and should take account of both the serious harm that may flow from relevant criminal activity and also the potential consequences of restricting access to core communications services relied on by end-users, it may include (for example):* • *warnings; or* • *account level actions such as suspensions, or ultimately account terminations, for extremely serious or repeated breaches.* *The contractual provisions required by sub-measure a), and the systems and/or processes required to support compliance with sub-measure d), may be drafted and/or implemented in a way that assists a provider to clearly establish whether there has, or has not, been a breach of the relevant prohibitions on sharing listed in sub-measure a). Whilst a provider should have reference to relevant criminal offences, this measure does not require a provider to contractually require an account holder not to share categories of material in the exact circumstances required by law, or to assess whether an end-user has breached the law (which can involve*

No.	Tier or category of RES	Compliance measure
		detailed fault elements and defences which may be extremely difficult for a provider to assess or identify), but can involve (for example): • *including a simply described prohibition in contractual terms (e.g. a prohibition on illegal conduct or on specific forms of sharing or conduct defined by the provider); or* • *setting a threshold test (in the systems and/or processes required to support compliance with sub-measure d)) which the provider can clearly apply, after which appropriate and proportionate action will be taken.* *A provider may become aware of a breach for the purposes of d) if information demonstrating a breach is provided to it via the reporting mechanism required by measure 8.2.* *Providers could provide educational information to support Australian end-users who are victims of, or otherwise impacted by, the categories of criminal activity described in sub-measure a).*
8.2	closed communication relevant electronic service	**Reporting mechanisms** A provider of a service must provide a tool or mechanism which enables Australian end-users to report breaches of the prohibitions described in measure 8.1 a) by end-users of the closed communication relevant electronic service. If an Australian end-user reports a breach via the tool or mechanism, the provider must: a) respond promptly to the end-user acknowledging receipt of the report; and b) consider any relevant information provided by the end-user pursuant to this tool or mechanism in a reasonably timely manner, and if appropriate take action pursuant to measure 8.1 d). The reporting tool or mechanism must: c) be easily accessible and easy to use; d) where the tool or mechanism does not involve use of a widely used communication mechanism – have clear instructions on how to use it; and e) ensure that the identity of the reporter is not disclosed to the reported 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, except as required by applicable law. The provider must develop and comply with internal policies and procedures for dealing with reports made through this tool or mechanism.
8.3	closed communication relevant electronic service	**Training for personnel responding to reports** A provider of a service must ensure that personnel responding to reports made by Australian end-users under measure 8.2 are trained in the communications relevant electronic service's policies and procedures for dealing with such reports.

No.	Tier or category of RES	Compliance measure
8.4	closed communication relevant electronic service	**Review of compliance of personnel with systems and processes** A provider of a service must review the effectiveness of its reporting mechanism (as required by measure 8.2) and processes to ensure information received via the reporting mechanism is considered and actioned (if necessary) as appropriate pursuant to measure 8.1 d). Such review must occur at least annually. ***Guidance:*** *This could include review and analysis of data collected for the year (e.g. responses and outcomes) as well as submitting test complaints via the reporting mechanism to review handling and response.*
8.5	closed communication relevant electronic service	**Tools, features and/or settings** A provider of a service must ensure that it has appropriate tools, features and/or settings available and accessible to assist Australian end-users to limit receipt of unsolicited material (including class 1C and class 2 material). Examples of such tools, features and/or settings include: a) tools, features and/or settings that allow Australian end-users to block messages from other end-users; and/or b) with respect to online pornography, tools, features and/or settings that automatically blur images detected as containing nudity on receipt.
8.6	closed communication relevant electronic service	**Updates to eSafety about relevant changes to technology** A provider of a service must share information with eSafety in writing about significant changes to the functionality of its service that are likely to have a material positive or negative effect on the access or exposure to, distribution of, or online storage of online pornography, self-harm material or high-impact violence material by Australian children. A provider may choose to provide this information in a Code report to eSafety under this Code. In implementing this measure, a provider is not required to disclose information to eSafety that is confidential. ***Guidance:*** *Changes that have a material negative effect should, ideally be communicated before a public announcement of the relevant changes.*
8.7	closed communication relevant electronic service	**Significant changes to the service** Before the provider of a service makes a material change to the service (including any significant new feature of the service enabled by generative artificial intelligence) that will significantly increase the risk of sharing of online pornography, self-harm material or high-impact violence material to Australian children, it must: a) carry out an assessment of the kinds of measures that could reasonably be incorporated into the service to minimise that risk; and

No.	Tier or category of RES	Compliance measure
		b) where appropriate, apply measures so identified to help to mitigate that risk.
8.8	closed communication relevant electronic service	**Improvement** Where technically feasible and reasonably practicable, a provider of a service must take appropriate steps to further develop and improve the tools, features and/or settings (as relevant) it has in place under measure 8.5 over time. Examples of activities that a provider may engage in to meet this measure include the following (to the extent directed towards, or relevant to, the matters covered by this Code): a) any activities designed to further develop the effectiveness of the tools, features and/or settings; b) tracking new and emerging risks or issues that may be causing harm to Australian children; c) investment in research and development and/or testing of novel technological solutions; d) investment in trust and safety teams dedicated to implementing regulatory requirements and policies which enhance online safety for users of online services; e) investment in review teams who conduct human review of reported material, and can consider material including factors like context; f) providing financial or technical support to non-governmental organisations with recognised online safety expertise to improve their infrastructure and/or technical capabilities; g) contributing to programs operated by non-governmental organisations; h) joining relevant industry organisations or other third party organisations intended to address online harm to children and sharing information on best practice approaches; i) contributing to industry initiatives (including initiatives lead by industry associations or other third party organisations); j) conducting or supporting research into and development of online safety tools, features and/or settings and approaches; k) providing support, either financial or in kind, to organisations the functions of which are or include protection of children online; l) extending the application of a feature or tool applied under another industry code or standard to operate in connection with its service; and m) activities that aim to refine algorithms or inputs into tools to improve their effectiveness. The provider must, at a minimum, engage in at least some of the example activities above in each calendar year.
8.9	closed communication relevant electronic service	**Information about tools and contact mechanisms** A provider of a service must provide clear and accessible information to Australian end-users regarding: a) the tools, features and/or settings required by measure 8.5; and

No.	Tier or category of RES	Compliance measure
		b) the contact tools and/or mechanisms required by measure 8.2 and 8.16. Information must be provided in a manner that is reasonably capable of being easily understood by most users of all ages permitted on the service.
8.10	closed communication relevant electronic service	**Information for Australian end-users about the role and functions of eSafety, including how to make a complaint to eSafety** A provider of a service must publish clear information that is accessible to Australian end-users which explains the role and functions of eSafety, including how to make a complaint to eSafety.
8.11	closed communication relevant electronic service	**Information to assist end-users with managing risks relating to class 1C and class 2 material** A provider of a service must provide clear information that is accessible to Australian end-users about steps that end-users can take to manage and mitigate risks relating to class 1C and class 2 material. ***Guidance:*** *This might include support or help articles for users of the service. Such articles might provide information on safe behaviour on services.*
8.12	closed communication relevant electronic service	**Location on or via service that is dedicated to providing online safety information** A provider of a service must establish a location on or via the service that is dedicated to providing online safety information, that: a) contains information required under this Code; b) includes information about how Australian end-users can contact third party services that may provide counselling and support; and c) is accessible to Australian end-users. ***Guidance:*** *A provider could raise Australian end-users' awareness about the availability of safety information on its services, through interstitial mechanisms such as account notifications, on-service advertising campaigns or pop-up notices when material is being posted or viewed by Australian end-users. Providers could contribute to off-service campaigns targeted at the general public, Australian end-users or specific sections of the community such as teachers, parents and carers, older users or vulnerable groups. A provider could contribute to an off-service campaign by providing financial assistance, advertising collateral, expert advisers, or other support services.*
8.13	closed communication relevant electronic service	**Reporting to eSafety on Code compliance** Where eSafety issues a written request to a provider of a service to submit a Code report, the provider named in such request must submit to eSafety a Code report which includes the following information:

No.	Tier or category of RES	Compliance measure
		a) the steps that the provider has taken to comply with the compliance measures under this Code; and b) an explanation as to why those measures are appropriate. A provider that 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 will not be required to submit a Code report to eSafety more than once in any 12-month period.
8.14	closed communication relevant electronic service	**Trust and safety function** A provider of a service must have, or have access to, sufficient personnel to oversee the safety of the service. Such personnel must have the skills, experience and qualifications needed to ensure that the provider complies with the requirements of this Code at all times.
8.15	closed communication relevant electronic service	**Engagement** A provider of a service must either: a) appropriately engage with safety and community organisations (such as civil society groups, public interest groups and representatives of marginalised communities), academics and government to gather information to help inform the measures taken for the purposes of protecting or preventing children from accessing or being exposed to class 1C and class 2 material; or b) enter into arrangements for cooperating and collaborating with other organisations (such as industry associations) in activities of the kind referred to in paragraph a) to enhance online safety for Australians. A provider of a service must consider information obtained through such engagement. ***Guidance:*** *Engagement may occur within and/or outside Australia as relevant to the issue under consideration.* *Engagement may occur regularly in the course of ongoing relationships with organisations, academics or government, during development of new service features or in other appropriate circumstances.*
8.16	closed communication relevant electronic service	**Complaints tools** A provider of a service must provide a tool or mechanism which enables Australian end-users to make a complaint about a breach of this Code by the provider. If an Australian end-user makes a complaint of the kind referred to in this measure, the provider must consider any relevant information provided by the Australian end-user pursuant to their complaint in a reasonably timely manner. The complaints tool or mechanism must: a) be easily accessible and simple to use; and

No.	Tier or category of RES	Compliance measure
		b) where the tool or mechanism does not involve use of a widely used communication mechanism – have clear instructions on how to use it. The provider must develop and comply with internal policies and procedures for dealing with complaints made through this tool or mechanism.
8.17	closed communication relevant electronic service	**Timely referral of unresolved complaints to eSafety** A provider of a service must promptly refer to eSafety complaints from Australian end-users concerning a material non-compliance with this Code by the provider, where the provider is unable to resolve the complaint within a reasonable timeframe.
8.18	closed communication relevant electronic services	**Timely response to communications from eSafety** The provider of a service must implement policies and procedures that ensure that it responds in a timely and appropriate manner to communications from eSafety about compliance with this Code.

9 Compliance measures for other communication relevant electronic services

The compliance measures in this table apply to other communication relevant electronic services, but do not apply to any AI companion chatbot feature.

No.	Tier or category of RES	Compliance measure
9.1	other communication relevant electronic service	**Terms and conditions prohibiting illegal activity** A provider of a service must: a) have terms and conditions in place with end-users prohibiting the sharing of online pornography by an end-user to an end-user who is an Australian child; b) publish the terms and conditions by making them accessible on a website and/or application for the service (as relevant); c) ensure the prohibition described in sub-measure a) is set out in plain language in the terms and conditions; and d) if the provider becomes aware of a breach of the prohibition described in sub-measure a), take appropriate and proportionate action in a reasonably timely manner.

No.	Tier or category of RES	Compliance measure
		It is not necessary that a particular form of words be used in the terms and conditions so long as the contractual effect of the terms and conditions is as required by sub-measure a). A provider must have systems and/or processes in place to support compliance with the obligation in sub-measure d). ***Guidance:*** *Providers have flexibility to design terms, systems, processes and policies to allow appropriate and proportionate responses to potential breaches on a case-by-case basis. Providers have the ability to exercise discretion to enforce terms and policies in accordance with the specific circumstances of each potential breach.* *Whether an action taken in response to a breach is appropriate will depend on the specific circumstances of the breach. A provider should consider the context in which the breach occurred, the severity of the harm that may flow from the breach and the potential consequences of restricting access to a service relied on by an end-user in determining whether action is appropriate and proportionate in any given circumstance. Such action may include warnings, strikes, suspensions or, for serious or repeated breaches, account removal.* *A provider may become aware of a breach for the purposes of sub-measure d) if information demonstrating a breach is provided to it via the reporting mechanism required by measure 9.2.*
9.2	other communication relevant electronic service	**Reporting mechanisms** A provider of a service must provide a tool or mechanism which enables Australian end-users to report breaches of the prohibition described in measure 9.1 a). If an Australian end-user reports a breach via the tool or mechanism, the provider must: a) respond promptly to the end-user acknowledging receipt of the report; and b) if appropriate, take action pursuant to measure 9.1 d). The reporting tool or mechanism must: c) be available in-service, that is, not solely on a website separate to the website for the service, unless it is not technically feasible or reasonably practicable for the provider to do this; d) be easily accessible and easy to use; and e) ensure that the identity of the reporter is not disclosed to the reported 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, except as required by applicable law. The provider must develop and comply with internal policies and procedures for dealing with reports made through this tool or mechanism.
9.3	other communication	**Training for personnel responding to reports**

No.	Tier or category of RES	Compliance measure
	relevant electronic service	A provider of a service must ensure that personnel responding to reports made by Australian end-users under measure 9.2 are trained in the communications relevant electronic service's policies and procedures for dealing with such reports.
9.4	other communication relevant electronic service	**Review of compliance of personnel with systems and processes** A provider of a service must review the effectiveness of its reporting mechanism (as required by measure 9.2) and processes to ensure information received via the reporting mechanism is considered and actioned (if necessary) as appropriate pursuant to measure 9.1 d). Such review must occur at least annually. ***Guidance:*** *This could include review and analysis of data collected for the year (e.g. responses and outcomes) as well as submitting test complaints via the reporting mechanism to review handling and response.*
9.5	other communication relevant electronic service	**Safety features and settings** A provider of a service must ensure that it has appropriate tools, features and/or settings available and accessible to assist Australian end-users to limit receipt of unsolicited material (including class 1C and class 2 material). At a minimum, such tools, features and/or settings must include: a) if the service allows the sending of messages between end-users: i) tools that allow Australian end-users to block direct messages from other end-users; and ii) settings for Australian end-users that allow them to prevent the receipt of unwanted messages from other end-users; and b) if the service allows the sending of messages in a group chat between three or more end-users – tools that allow Australian end-users to leave that group chat. If the provider allows Australian children to become end-users of the service, the provider must ensure that the settings referred to in paragraph a)ii. above are defaulted to the most restrictive setting for an Australian child at the time of account registration. Other examples of such tools, features and/or settings include: c) with respect to online pornography, tools, features and/or settings that automatically blur images detected as containing nudity on receipt; d) if the service uses recommender systems to present material to end-users – tools, features and/or settings that prevent or reduce the occurrence of online pornography, self-harm material and high-impact violence material from being promoted to Australian children; and e) if the provider allows Australian children to become end-users of services – have default settings for Australian children that prevent an end-user who is over the age of 18 years and is not connected to an Australian child from being able to use the service to send a direct message to that Australian child.

No.	Tier or category of RES	Compliance measure
		Guidance: *For these purposes, the circumstances in which an end-user will be considered to be "connected" to an Australian child include if: (1) they are friends on the service; (2) the Australian child follows the end-user; or (3) the Australian child has the end-user saved as a phone contact.* *For the avoidance of doubt, the reference to defaulting settings to "the most restrictive settings" refers to the most restrictive settings that are available and possible on the service.*
9.6	other communication relevant electronic service	**Updates to eSafety about relevant changes to technology** A provider of a service must share information with eSafety in writing about significant changes to the functionality of its service that are likely to have a material positive or negative effect on the access or exposure to, distribution of, or online storage of class 1C or class 2 material by Australian children. A provider may choose to provide this information in a Code report to eSafety under this Code. In implementing this measure, a provider is not required to disclose information to eSafety that is confidential. ***Guidance:*** *Changes that have a material negative effect should, ideally be communicated before a public announcement of the relevant changes.*
9.7	other communication relevant electronic service	**Significant changes to the service** Before the provider of a service makes a material change to the service (including any significant new feature of the service enabled by generative artificial intelligence) that will significantly increase the risk of sharing of online pornography, self-harm material or high-impact violence material to Australian children, it must: a) carry out an assessment of the kinds of measures that could reasonably be incorporated into the service to minimise that risk; and b) where appropriate, apply measures so identified to help to mitigate that risk.
9.8	other communication relevant electronic service	**Improvement** Where technically feasible and reasonably practicable, a provider of a service must take appropriate steps to further develop and improve the tools, features and/or settings (as relevant) it has in place under measure 9.5 over time. Examples of activities that a provider may engage in to meet this measure include the following (to the extent directed towards, or relevant to, the matters covered by this Code): a) any activities designed to further develop the effectiveness of the tools, features and/or settings; b) tracking new and emerging risks or issues that may be causing harm to Australian children;

No.	Tier or category of RES	Compliance measure
		c) investment in research and development and/or testing of novel technological solutions; d) investment in trust and safety teams dedicated to implementing regulatory requirements and policies which enhance online safety for users of online services; e) investment in review teams who conduct human review of reported material, and can consider material including factors like context; f) providing financial or technical support to non-governmental organisations with recognised online safety expertise to improve their infrastructure and/or technical capabilities; g) contributing to programs operated by non-governmental organisations; h) joining relevant industry organisations or other third party organisations intended to address online harm to children and sharing information on best practice approaches; i) contributing to industry initiatives (including initiatives lead by industry associations or other third party organisations); j) conducting or supporting research into and development of online safety tools, features and/or settings and approaches; k) providing support, either financial or in kind, to organisations the functions of which are or include protection of children online; l) extending the application of a feature or tool applied under another industry code or standard to operate in connection with its service; and m) activities that aim to refine algorithms or inputs into tools to improve their effectiveness. The provider must, at a minimum, engage in at least some of the example activities above in each calendar year.
9.9	other communication relevant electronic service	**Information about tools and contact mechanisms** A provider of a service must provide clear and accessible information to Australian end-users regarding: a) the tools, features and/or settings required by measure 9.5; and b) the contact tools and/or mechanisms required by measure 9.2 and 9.16. Information must be provided in a manner that is reasonably capable of being easily understood by most users of all ages permitted on the service.
9.10	other communication relevant electronic service	**Information for Australian end-users about the role and functions of eSafety, including how to make a complaint to eSafety** A provider of a service must publish clear information that is accessible to Australian end-users which explains the role and functions of eSafety, including how to make a complaint to eSafety.
9.11	other communication	**Information to assist end-users with managing risks relating to class 1C and class 2 material**

No.	Tier or category of RES	Compliance measure
	relevant electronic service	A provider of a service must provide clear information that is accessible to Australian end-users about steps that end-users can take to manage and mitigate risks relating to class 1C and class 2 material. ***Guidance:*** *This might include support or help articles for users of the service. Such articles might provide information on safe behaviour on services.*
9.12	other communication relevant electronic service	**Location on or via service that is dedicated to providing online safety information** A provider of a service must establish a location on or via the service that is dedicated to providing online safety information, that: a) contains information required under this Code; b) includes information about how Australian end-users can contact third party services that may provide counselling and support; and c) is accessible to Australian end-users. ***Guidance:*** *A provider could raise Australian end-users' awareness about the availability of safety information on its services, through interstitial mechanisms such as account notifications, on-service advertising campaigns or pop-up notices when material is being posted or viewed by Australian end-users. Providers could contribute to off-service campaigns targeted at the general public, Australian end-users or specific sections of the community such as teachers, parents and carers, older users or vulnerable groups. A provider could contribute to an off-service campaign by providing financial assistance, advertising collateral, expert advisers, or other support services.*
9.13	other communication relevant electronic service	**Reporting to eSafety on Code compliance** Where eSafety issues a written request to a provider of a 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 the compliance measures under this Code; and b) an explanation as to why those measures are appropriate. A provider that 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 will not be required to submit a Code report to eSafety more than once in any 12-month period.
9.14	other communication relevant electronic service	**Trust and safety function**

No.	Tier or category of RES	Compliance measure
		A provider of a service must have, or have access to, sufficient personnel to oversee the safety of the service. Such personnel must have the skills, experience and qualifications needed to ensure that the provider complies with the requirements of this Code at all times.
9.15	other communication relevant electronic service	**Engagement** A provider of a service must either: a) appropriately engage with safety and community organisations (such as civil society groups, public interest groups and representatives of marginalised communities), academics and government to gather information to help inform the measures taken for the purposes of protecting or preventing children from accessing or being exposed to class 1C and class 2 material; or b) enter into arrangements for cooperating and collaborating with other organisations (such as industry associations) in activities of the kind referred to in paragraph a) to enhance online safety for Australians. A provider of a service must consider information obtained through such engagement. ***Guidance:*** *Engagement may occur within and/or outside Australia as relevant to the issue under consideration.* *Engagement may occur regularly in the course of ongoing relationships with organisations, academics or government, during development of new service features or in other appropriate circumstances.*
9.16	other communication relevant electronic service	**Complaints tools** A provider of a service must provide a tool or mechanism which enables Australian end-users to make a complaint about a breach of this Code by the provider. If an Australian end-user makes a complaint of the kind referred to in this measure, the provider must consider any relevant information provided by the Australian end-user pursuant to their complaint in a reasonably timely manner. The complaints tool or mechanism must: a) be easily accessible and simple to use; and b) where the tool or mechanism does not involve use of a widely used communication mechanism – have clear instructions on how to use it. The provider must develop and comply with internal policies and procedures for dealing with complaints made through this tool or mechanism.
9.17	other communication	**Timely referral of unresolved complaints to eSafety** A provider of a service must promptly refer to eSafety complaints from Australian end-users concerning a material non-compliance with this Code by the provider, where the provider is unable to resolve the complaint within a reasonable timeframe.

No.	Tier or category of RES	Compliance measure
	relevant electronic service	
9.18	other communication relevant electronic services	**Timely response to communications from eSafety** The provider of a service must implement policies and procedures that ensure that it responds in a timely and appropriate manner to communications from eSafety about compliance with this Code.

10 Compliance measures for dating services

The compliance measures in this table apply to dating services, but do not apply to any AI companion chatbot feature.

No.	Tier or category of RES	Compliance measure
10.1	dating service	**Terms and conditions prohibiting illegal activity** A provider of a service must: a) have terms and conditions in place with Australian end-users that include any restrictions that they impose in relation to the sharing of class 1C and class 2 material on their service including at a minimum prohibiting the end-user from sharing material via the service in the course of engaging in any of the following categories of criminal activity: i. non-consensual sharing of intimate images; ii. grooming of children; or iii. sexual extortion (or sextortion); b) publish the terms and conditions by making them accessible on a website and/or application for the service (as relevant); c) ensure the prohibition described in sub-measure a) is set out in plain language in the terms and conditions; and d) if the provider becomes aware of a breach of the prohibition described in sub-measure a), take appropriate and proportionate action in a reasonably timely manner including the moderation of content to comply with the terms and conditions. It is not necessary that a particular form of words be used in the terms and conditions so long as the contractual effect of the terms and conditions is as required by sub-measure a). A provider must have systems and/or processes in place to support compliance with the obligation in sub-measure d).

No.	Tier or category of RES	Compliance measure
		Guidance: *Providers have flexibility to design terms, systems, processes and policies to allow appropriate and proportionate responses to potential breaches on a case-by-case basis. Providers have the ability to exercise discretion to enforce terms and policies in accordance with the specific circumstances of each potential breach.* *Whilst appropriate and proportionate action in response to a breach will be dependent on the specific circumstances, and should take account of the serious harm that may flow from relevant criminal activity, it may include (for example):* • *warnings; or* • *account level actions such as suspensions, or ultimately account terminations, for extremely serious or repeated breaches.* *The contractual provisions required by sub-measure a), and the systems and/or processes required to support compliance with sub-measure d), may be drafted and/or implemented in a way that assists a provider to clearly establish whether there has, or has not, been a breach of the relevant prohibitions on sharing listed in sub-measure a). Whilst a provider should have reference to relevant criminal offences, this measure does not require a provider to contractually require an account holder not to share categories of material in the exact circumstances required by law, or to assess whether an end-user has breached the law (which can involve detailed fault elements and defences which may be extremely difficult for a provider to assess or identify), but can involve (for example):* • *including a simply described prohibition in contractual terms (e.g. a prohibition on illegal conduct or on specific forms of sharing or conduct defined by the provider); or* • *setting a threshold test (in the systems and/or processes required to support compliance with sub-measure d)) which the provider can clearly apply, after which appropriate and proportionate action will be taken.* *A provider may become aware of a breach for the purposes of sub-measure d) if information demonstrating a breach is provided to it via the reporting mechanism required by measure 10.3.* *Providers could provide educational information to support Australian end-users who are victims of, or otherwise impacted by, the categories of criminal activity described in sub-measure a).*
10.2	dating service	**Detection** A provider of a dating service must implement appropriate systems, processes and policies: a) which allow, where technically feasible and reasonably practicable, for the detection of class 1C or class 2 material sent in a communication involving an Australian end-user where that incident violates the provider's terms and conditions; and b) to review any such detected incidents that violate the provider's terms and conditions and take action as required by measure 10.1 d).
10.3	dating service	**Reporting mechanisms**

No.	Tier or category of RES	Compliance measure
		A provider of a service must provide a tool or mechanism which enables Australian end-users to report breaches of the prohibitions described in measure 10.1 a) by end-users of the dating service. If an Australian end-user reports a breach via the tool or mechanism, the provider must: a) respond promptly to the end-user acknowledging receipt of the report; and b) consider any relevant information provided by the end-user pursuant to this tool or mechanism in a reasonably timely manner and if appropriate take action pursuant to measure 10.1 d). The reporting tool or mechanism must: c) be easily accessible and easy to use; d) where the tool or mechanism does not involve use of a widely used communication mechanism – have clear instructions on how to use it; and e) ensure that the identity of the reporter is not disclosed to the reported 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, except as required by applicable law. The provider must develop and comply with internal policies and procedures for dealing with reports made through this tool or mechanism.
10.4	dating service	**Training for personnel responding to reports** A provider of a service must ensure that personnel responding to reports made by Australian end-users under measure 10.3 are trained in the service's policies and procedures for dealing with such reports.
10.5	dating service	**Review of compliance of personnel with systems and processes** A provider of a service must review the effectiveness of its reporting mechanism (as required by measure 10.3) and processes to ensure information received via the reporting mechanism is considered and actioned (if necessary) as appropriate pursuant to measure 10.1 d). Such review must occur at least annually. ***Guidance:*** *This could include review and analysis of data collected for the year (e.g. responses and outcomes) as well as submitting test complaints via the reporting mechanism to review handling and response.*
10.6	dating services	**Tools, features and/or settings** A provider of a service must ensure that it has appropriate tools, features and/or settings available and accessible to assist Australian end-users to limit receipt of unsolicited material (including class 1C and class 2 material). Examples of such tools, features and/or settings include:

No.	Tier or category of RES	Compliance measure
		a) tools and settings that allow Australian end-users to block messages from other end-users; and/or b) with respect to online pornography, tools, features and/or settings that automatically blur images detected as containing nudity on receipt.
10.7	dating services	**Updates to eSafety about relevant changes to technology** Unless it has implemented: a) appropriate age assurance measures; and b) access control measures, before providing access to its service, the provider of a service must share information with eSafety in writing about significant changes to the functionality of its service that are likely to have a material positive or negative effect on the access or exposure to, distribution of, or online storage of class 1C or class 2 material by Australian children. A provider may choose to provide this information in a Code report to eSafety under this Code. In implementing this measure, a provider is not required to disclose information to eSafety that is confidential. ***Guidance:*** *A provider of a dating service may, at its option, choose either to implement appropriate age assurance measures and access control measures on its service or to provide updates as required by this measure.* *Changes that have a material negative effect should, ideally, be communicated before a public announcement of the relevant changes.*
10.8	dating services	**Significant changes to the service** Unless it has implemented: a) appropriate age assurance measures; and b) access control measures, before providing access to its dating service, before the provider of a service makes a material change to the service (including any significant new feature of the service enabled by generative artificial intelligence) that will significantly increase the risk of sharing of online pornography, self-harm material or high-impact violence material to Australian children, it must: c) carry out an assessment of the kinds of measures that could reasonably be incorporated into the service to minimise that risk; and d) where appropriate, apply measures so identified to help to mitigate that risk. ***Guidance:***

No.	Tier or category of RES	Compliance measure
		A provider of a dating service may, at its option, choose either to implement appropriate age assurance measures and access control measures on its service or to comply with this measure with respect to significant new features.
10.9	dating services	**Improvement** Where technically feasible and reasonably practicable, a provider of a service must take appropriate steps to further develop and improve the tools, features and/or settings (as relevant) it has in place under measure 10.6 over time. Examples of activities that a provider may engage in to meet this measure include the following (to the extent directed towards, or relevant to, that matters covered by this Code): a) any activities designed to further develop the effectiveness of the tools, features and/or settings; b) tracking new and emerging risks or issues that may be causing harm to Australian children; c) investment in research and development and/or testing of novel technological solutions; d) investment in trust and safety teams dedicated to implementing regulatory requirements and policies which enhance online safety for users of online services; e) investment in review teams who conduct human review of reported material, and can consider material including factors like context; f) providing financial or technical support to non-governmental organisations with recognised online safety expertise to improve their infrastructure and/or technical capabilities; g) contributing to programs operated by non-governmental organisations; h) joining relevant industry organisations or other third party organisations intended to address online harm to children and sharing information on best practice approaches; i) contributing to industry initiatives (including initiatives lead by industry associations or other third party organisations); j) conducting or supporting research into and development of online safety tools, features and/or settings and approaches; k) providing support, either financial or in kind, to organisations the functions of which are or include protection of children online; l) extending the application of a feature or tool applied under another industry code or standard to operate in connection with its service; and m) activities that aim to refine algorithms or inputs into tools to improve their effectiveness. The provider must, at a minimum, engage in at least some of the example activities above in each calendar year.
10.10	dating services	**Information about tools and contact mechanisms** A provider of a service must provide clear and accessible information to Australian end-users regarding:

No.	Tier or category of RES	Compliance measure
		a) the tools, features and/or settings required by measure 10.6; and b) as the contact tools and/or mechanisms required by measure 10.3 and 10.17. Information must be provided in a manner that is reasonably capable of being easily understood by most users of all ages permitted on the service.
10.11	dating services	**Information for Australian end-users about the role and functions of eSafety, including how to make a complaint to eSafety** A provider of a service must publish clear information that is accessible to Australian end-users which explains the role and functions of eSafety, including how to make a complaint to eSafety.
10.12	dating services	**Information to assist end-users with managing risks relating to class 1C and class 2 material** A provider of a service must provide clear information that is accessible to Australian end-users about steps that end-users can take to manage and mitigate risks relating to class 1C and class 2 material. ***Guidance:*** *This might include support or help articles for users of the service. Such articles might provide information on safe behaviour on services.*
10.13	dating services	**Location on or via service that is dedicated to providing online safety information** A provider of a service must establish a location on or via the service that is dedicated to providing online safety information, that: a) contains information required under this Code; b) includes information about how Australian end-users can contact third party services that may provide counselling and support; and c) is accessible to Australian end-users. ***Guidance:*** *A provider could raise Australian end-users' awareness about the availability of safety information on its services, through interstitial mechanisms such as account notifications, on-service advertising campaigns or pop-up notices when material is being posted or viewed by Australian end-users. Providers could contribute to off-service campaigns targeted at the general public, Australian end-users or specific sections of the community such as teachers, parents and carers, older users or vulnerable groups. A provider could contribute to an off-service campaign by providing financial assistance, advertising collateral, expert advisers, or other support services.*
10.14	dating services	**Reporting to eSafety on Code compliance**

No.	Tier or category of RES	Compliance measure
		Where eSafety issues a written request to a provider of a 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 the compliance measures under this Code; and b) an explanation as to why those measures are appropriate. A provider that 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 will not be required to submit a Code report to eSafety more than once in any 12-month period.
10.15	dating service	**Trust and safety function** A provider of a service must have, or have access to, sufficient personnel to oversee the safety of the service. Such personnel must have the skills, experience and qualifications needed to ensure that the provider complies with the requirements of this Code at all times.
10.16	dating service	**Engagement** A provider of a service must either: a) appropriately engage with safety and community organisations (such as civil society groups, public interest groups and representatives of marginalised communities), academics and government to gather information to help inform the measures taken for the purposes of protecting or preventing children from accessing or being exposed to class 1C and class 2 material; or b) enter into arrangements for cooperating and collaborating with other organisations (such as industry associations) in activities of the kind referred to in paragraph a) to enhance online safety for Australians. A provider of a service must consider information obtained through such engagement. ***Guidance:*** *Engagement may occur within and/or outside Australia as relevant to the issue under consideration.* *Engagement may occur regularly in the course of ongoing relationships with organisations, academics or government, during development of new service features or in other appropriate circumstances.*
10.17	dating service	**Complaints tools** A provider of a service must provide a tool or mechanism which enables Australian end-users to make a complaint about a breach of this Code by the provider. If an Australian end-user makes a complaint of the kind referred to in this measure, the provider must consider any relevant information provided by the Australian end-user pursuant to their complaint in a reasonably timely manner. The complaints tool or mechanism must:

No.	Tier or category of RES	Compliance measure
		a) be easily accessible and simple to use; and b) where the tool or mechanism does not involve use of a widely used communication mechanism – have clear instructions on how to use it. The provider must develop and comply with internal policies and procedures for dealing with complaints made through this tool or mechanism.
10.18	dating service	**Timely referral of unresolved complaints to eSafety** A provider of a service must promptly refer to eSafety complaints from Australian end-users concerning material non-compliance with this Code by the provider, where the provider is unable to resolve the complaint within a reasonable timeframe.
10.19	dating service	**Timely response to communications from eSafety** The provider of a service must implement policies and procedures that ensure that it responds in a timely and appropriate manner to communications from eSafety about compliance with this Code.

11 Compliance measures for gaming services with communications functionality

The compliance measures in this table apply to gaming services with communications functionality, but do not apply to any AI companion chatbot feature.

No.	Tier or category of RES	Compliance measure
11.1	gaming service with communications functionality	**Terms and conditions prohibiting illegal activity** A provider of a service must: a) have terms and conditions in place with Australian end-users prohibiting the end-user from sharing material via the service in the course of engaging in any of the following categories of criminal activity: i. non-consensual sharing of intimate images; ii. grooming of children; or iii. sexual extortion (or sextortion); b) publish the terms and conditions by making them accessible on a website and/or application for the service (as relevant);

No.	Tier or category of RES	Compliance measure
		c) ensure the prohibition described in sub-measure a) is set out in plain language in the terms and conditions; and d) if the provider becomes aware of a breach of the prohibition described in sub-measure a), take appropriate and proportionate action in a reasonably timely manner. It is not necessary that a particular form of words be used in the terms and conditions so long as the contractual effect of the terms and conditions is as required by sub-measure a). A provider must have systems and/or processes in place to support compliance with the obligation in sub-measure d). ***Guidance:*** *Providers should be aware that the material shared via the service in the course of engaging in the categories of criminal activity described in sub-measure a)i. to iii. could include class 1C and class 2 material.* *Providers have flexibility to design terms, systems, processes and policies to allow appropriate and proportionate responses to potential breaches on a case-by-case basis. Providers have the ability to exercise discretion to enforce terms and policies in accordance with the specific circumstances of each potential breach.* *Whilst appropriate and proportionate action in response to a breach will be dependent on the specific circumstances, and should take account of the serious harm that may flow from relevant criminal activity, it may include (for example):* • *warnings; or* • *account level actions such as suspensions, or ultimately account terminations, for extremely serious or repeated breaches.* *The contractual provisions required by sub-measure a), and the systems and/or processes required to support compliance with sub-measure d), may be drafted and/or implemented in a way that assists a provider to clearly establish whether there has, or has not, been a breach of the relevant prohibitions on sharing listed in sub-measure a). Whilst a provider should have reference to relevant criminal offences, this measure does not require a provider to contractually require an account holder not to share categories of material in the exact circumstances required by law, or to assess whether an end-user has breached the law (which can involve detailed fault elements and defences which may be extremely difficult for a provider to assess or identify), but can involve (for example):* • *including a simply described prohibition in contractual terms (e.g. a prohibition on illegal conduct or on specific forms of sharing or conduct defined by the provider); or* • *setting a threshold test (in the systems and/or processes required to support compliance with d)) which the provider can clearly apply, after which appropriate and proportionate action will be taken.* *A provider may become aware of a breach for the purposes of sub-measure d) if information demonstrating a breach is provided to it via the reporting mechanism required by measure 11.2.* *Providers could provide educational information to support Australian end-users who are victims of, or otherwise impacted by, the categories of criminal activity described in sub-measure a).*

No.	Tier or category of RES	Compliance measure
11.2	gaming service with communications functionality	**Reporting mechanisms** A provider of a service must provide a tool or mechanism which enables Australian end-users to report breaches of the prohibitions described in measure 11.1 a) by end-users of the gaming service with communications functionality. If an Australian end-user reports a breach via the tool or mechanism, the provider must: a) respond promptly to the end-user acknowledging receipt of the report; and b) consider any relevant information provided by Australian end-users pursuant to this tool or mechanism in a reasonably timely manner, and if appropriate take action pursuant to measure 11.1 d). The reporting tool or mechanism must: c) be easily accessible and easy to use; d) where the tool or mechanism does not involve use of a widely used communication mechanism – have clear instructions on how to use it; and e) ensure that the identity of the reporter is not disclosed to the reported 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, except as required by applicable law. The provider must develop and comply with internal policies and procedures for dealing with reports made through this tool or mechanism.
11.3	gaming service with communications functionality	**Training for personnel responding to reports** A provider of a service must ensure that personnel responding to reports made by Australian end-users under measure 11.2 are trained in the gaming service with communications functionality's policies and procedures for dealing with such reports.
11.4	gaming service with communications functionality	**Review of compliance of personnel with systems and processes** A provider of a service must review the effectiveness of its reporting mechanism (as required by measure 11.2) and processes to ensure information received via the reporting mechanism is considered and actioned (if necessary) as appropriate pursuant to measure 11.1 d). Such review must occur at least annually. ***Guidance:*** *This could include review and analysis of data collected for the year (e.g. regarding compliance of personnel with relevant systems and processes) as well as submitting test complaints via the reporting mechanism to review handling and response.*
11.5	gaming services with	**Safety features and settings** A provider of a service must ensure that it has appropriate tools, features and/or and settings available and accessible to assist Australian end-users to limit receipt of unsolicited material (including class 1C and class 2 material).

No.	Tier or category of RES	Compliance measure
	communications functionality	At a minimum, such tools, features and/or settings must include: (a) if the service allows the sending of messages between end-users – tools, features and/or settings that allow Australian end-users to block, mute or otherwise prevent receipt of messages (including messages containing class 1C and class 2 material) from other end-users; and (b) if the service allows the sending of messages in a group chat between three or more end-users – tools, features and/or settings that allow Australian end-users to leave that group chat. An example of other such tools, features and/or settings includes: (c) if the service uses recommender systems to present material to end-users – it has tools, features and/or settings that prevent or reduce the occurrence of class 1C and class 2 material from being promoted to Australian children.
11.6	gaming services with communications functionality	**Updates to eSafety about relevant changes to technology** A provider of a service must share information with eSafety in writing about significant changes to the functionality of its service that are likely to have a material positive or negative effect on the access or exposure to, distribution of, or online storage of class 1C or class 2 material by Australian children. A provider may choose to provide this information in a Code report to eSafety under this Code. In implementing this measure, a provider is not required to disclose information to eSafety that is confidential. ***Guidance:*** *Changes that have a material negative effect should, ideally, be communicated before a public announcement of the relevant changes.*
11.7	gaming services with communications functionality	**Significant changes to the service** Before the provider of a service makes a material change to the service (including any significant new feature of the service enabled by generative artificial intelligence) that will significantly increase the risk of sharing of online pornography, self-harm material or high-impact violence material to Australian children, it must: a) carry out an assessment of the kinds of measures that could reasonably be incorporated into the service to minimise that risk; and b) where appropriate, apply measures so identified to help to mitigate that risk.
11.8	gaming services with communications functionality	**Improvement** Where technically feasible and reasonably practicable, a provider of a service must take appropriate steps to further develop and improve the tools, features and/or settings (as relevant) it has in place under measure 11.5 over time.

No.	Tier or category of RES	Compliance measure
		Examples of activities that a provider may engage in to meet this measure include the following (to the extent directed towards, or relevant to, the matters covered by this Code): a) any activities designed to further develop the effectiveness of the tools, features and/or settings; b) tracking new and emerging risks or issues that may be causing harm to Australian children; c) investment in research and development and/or testing of novel technological solutions; d) investment in trust and safety teams dedicated to implementing regulatory requirements and policies which enhance online safety for users of online services; e) investment in review teams who conduct human review of reported material, and can consider material including factors like context; f) providing financial or technical support to non-government organisations with recognised online safety expertise to improve their infrastructure and/or technical capabilities; g) contributing to programs operated by non-governmental organisations; h) joining relevant industry organisations or other third party organisations intended to address online harm to children and sharing information on best practice approaches; i) contributing to industry initiatives (including initiatives lead by industry associations or other third party organisations); j) conducting or supporting research into and development of online safety tools, features and/or settings and approaches; k) providing support, either financial or in kind, to organisations the functions of which are or include protection of children online; l) extending the application of a feature or tool applied under another industry code or standard to operate in connection with its service; and m) activities that aim to refine algorithms or inputs into tools to improve their effectiveness. The provider must, at a minimum, engage in at least some of the example activities above in each calendar year.
11.9	gaming services with communications functionality	**Information about tools and contact mechanisms** A provider of a service must provide clear and accessible information to Australian end-users regarding: a) the tools, features and/or settings required by measure 11.5; and b) the contact tools and/or mechanisms required by measure 11.2 and 11.16. Information must be provided in a manner that is reasonably capable of being easily understood by most users of all ages permitted on the service.

No.	Tier or category of RES	Compliance measure
11.10	gaming services with communications functionality	**Information for Australian end-users about the role and functions of eSafety, including how to make a complaint to eSafety** A provider of a service must publish clear information that is accessible to Australian end-users which explains the role and functions of eSafety, including how to make a complaint to eSafety.
11.11	gaming services with communications functionality	**Information to assist end-users with managing risks relating to class 1C and class 2 material** A provider of a service must provide clear information that is accessible to Australian end-users about steps that end-users can take to manage and mitigate risks relating to class 1C and class 2 material. ***Guidance:*** *This might include support or help articles for users of the service. Such articles might provide information on safe behaviour on services.*
11.12	gaming services with communications functionality	**Location on or via service that is dedicated to providing online safety information** A provider of a service must establish a location on or via the service that is dedicated to providing online safety information, that: a) contains information required under this Code; b) includes information about how Australian end-users can contact third party services that may provide counselling and support; and c) is accessible to Australian end-users. ***Guidance:*** *A provider could raise Australian end-users' awareness about the availability of safety information on its services, through interstitial mechanisms such as account notifications, on-service advertising campaigns or pop-up notices when material is being posted or viewed by Australian end-users. Providers could contribute to off-service campaigns targeted at the general public, Australian end-users or specific sections of the community such as teachers, parents and carers, older users or vulnerable groups. A provider could contribute to an off-service campaign by providing financial assistance, advertising collateral, expert advisers, or other support services.*
11.13	gaming services with communications functionality	**Reporting to eSafety on Code compliance** Where eSafety issues a written request to a provider of a 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 the compliance measures under this Code; and b) an explanation as to why those measures are appropriate.

No.	Tier or category of RES	Compliance measure
		A provider that 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 will not be required to submit a Code report to eSafety more than once in any 12-month period.
11.14	gaming service with communications functionality	**Trust and safety function** A provider of a service must have, or have access to, sufficient personnel to oversee the safety of the service. Such personnel must have the skills, experience and qualifications needed to ensure that the provider complies with the requirements of this Code at all times.
11.15	gaming service with communications functionality	**Engagement** A provider of a service must either: a) appropriately engage with safety and community organisations (such as civil society groups, public interest groups and representatives of marginalised communities), academics and government to gather information to help inform the measures taken for the purposes of protecting or preventing children from accessing or being exposed to class 1C and class 2 material; or b) enter into arrangements for cooperating and collaborating with other organisations (such as industry associations) in activities of the kind referred to in paragraph a) to enhance online safety for Australians. A provider of a service must consider information obtained through such engagement. ***Guidance:*** *Engagement may occur within and/or outside Australia as relevant to the issue under consideration.* *Engagement may occur regularly in the course of ongoing relationships with organisations, academics or government, during development of new service features or in other appropriate circumstances.*
11.16	gaming service with communications functionality	**Complaints tool** A provider of a service must provide a tool or mechanism which enables Australian end-users to make a complaint about a breach of this Code by the provider. If an Australian end-user makes a complaint of the kind referred to in this measure, the provider must consider any relevant information provided by the Australian end-user pursuant to their complaint in a reasonably timely manner. The complaints tools or mechanism must: a) be easily accessible and simple to use; and b) where the tool or mechanism does not involve use of a widely used communication mechanism – have clear instructions on how to use it.

No.	Tier or category of RES	Compliance measure
		The provider must develop and comply with internal policies and procedures for dealing with complaints made through this tool or mechanism.
11.17	gaming service with communications functionality	**Timely referral of unresolved complaints to eSafety** A provider of a service must promptly refer to eSafety complaints from Australian end-users concerning material non-compliance with this Code by the provider, where the provider is unable to resolve the complaint within a reasonable timeframe.
11.18	gaming service with communications functionality	**Timely response to communications from eSafety** The provider of a service must implement policies and procedures that ensure that it responds in a timely and appropriate manner to communications from eSafety about compliance with this Code.

12 Gaming services with limited communications functionality (R18+)

The compliance measures in the table apply to gaming services with limited communications functionality that:

a) are, or would likely be, classified as R18+ under the Classification Act because they constitutes simulated gambling material; or

b) have otherwise been classified as R18+ in accordance with the Classification Act,

but do not apply to any AI companion chatbot feature.

Note: Any computer game that has been classified by the Classification Board, or an approved classification tool, as R18+ under the Classification Act falls within b) and must comply with this table.

No.	Tier or category of RES	Compliance measure
12.1	gaming services with limited communications functionality within the scope of this table 12	**Information for Australian end-users** A provider of a service must publish clear online safety information that is accessible to Australian end-users which:

No.	Tier or category of RES	Compliance measure
		a) explains the role and functions of eSafety, including how to make a complaint to eSafety; b) includes information about the complaints tool or mechanism required by measure 12.3; and c) includes information about how Australian end-users can contact third party services that may provide counselling and support.
12.2	gaming services with limited communications functionality within the scope of this table 12	**Reporting to eSafety on Code compliance** Where eSafety issues a written request to a provider of a 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 the compliance measures under this Code; and b) an explanation as to why those measures are appropriate. A provider that 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 will not be required to submit a Code report to eSafety more than once in any 12-month period.
12.3	gaming services with limited communications functionality within the scope of this table 12	**Complaints tool** A provider of a service must provide a tool or mechanism which enables Australian end-users to make a complaint about a breach of this Code by the provider. If an Australian end-user makes a complaint of the kind referred to in this measure, the provider must consider any relevant information provided by Australian end-users pursuant to their complaint in a reasonably timely manner. The complaints tool or mechanism must: a) be easily accessible and simple to use; and b) where the tool or mechanism does not involve use of a widely used communication mechanism – have clear instructions on how to use it. The provider must develop and comply with internal policies and procedures for dealing with complaints made through this tool or mechanism.

13 Compliance measures for enterprise relevant electronic service

There are no additional compliance measures for enterprise RES.

14 Compliance measures for telephony RES

The compliance measures in this table apply to telephony RES.

No.	Tier or category of RES	Compliance measure
14.1	telephony relevant electronic service	**Terms and conditions prohibiting illegal activity** A provider of a service must: a) have terms and conditions in place with Australian end-users prohibiting the end-user from sharing material via the service in the course of engaging in any of the following categories of criminal activity: i. non-consensual sharing of intimate images; ii. grooming of children; or iii. sexual extortion (or sextortion); b) publish the terms and conditions by making them accessible on a website and/or application for the service (as relevant); c) ensure the prohibition described in sub-measure a) is set out in plain language in the terms and conditions; and d) if the provider becomes aware of a breach of the prohibition described in sub-measure a), take appropriate and proportionate action in a reasonably timely manner. It is not necessary that a particular form of words be used in the terms and conditions so long as the contractual effect of the terms and conditions is as required by sub-measure a). A provider must have systems and/or processes in place to support compliance with the obligation in sub-measure d). ***Guidance:*** *Providers should be aware that the material shared via the service in the course of engaging in the categories of criminal activity described in sub-measure a)i. to iii. could include class 1C and class 2 material.* *Providers have flexibility to design terms, systems, processes and policies to allow appropriate and proportionate responses to potential breaches on a case-by-case basis. Providers have the ability to exercise discretion to enforce terms and policies in accordance with the specific circumstances of each potential breach.* *Whilst appropriate and proportionate action in response to a breach will be dependent on the specific circumstances, and should take account of both the serious harm that may flow from relevant criminal activity and also the potential consequences of restricting access to core communications services relied on by end-users, it may include (for example):* • *warnings; or* • *account level actions such as suspensions, or ultimately account terminations, for extremely serious or repeated breaches.*

No.	Tier or category of RES	Compliance measure
		The contractual provisions required by sub-measure a), and the systems and/or processes required to support compliance with sub-measure d), may be drafted and/or implemented in a way that assists a provider to clearly establish whether there has, or has not, been a breach of the relevant prohibitions on sharing listed in sub-measure a). Whilst a provider should have reference to relevant criminal offences, this measure does not require a provider to contractually require an account holder not to share categories of material in the exact circumstances required by law, or to assess whether an end-user has breached the law (which can involve detailed fault elements and defences which may be extremely difficult for a provider to assess or identify), but can involve (for example): • *including a simply described prohibition in contractual terms (e.g. a prohibition on illegal conduct or on specific forms of sharing or conduct defined by the provider); or* • *setting a threshold test (in the systems and/or processes required to support compliance with sub-measure d)) which the provider can clearly apply, after which appropriate and proportionate action will be taken.* *A provider may become aware of a breach for the purposes of sub-measure d) if information demonstrating a breach is provided to it via the reporting mechanism required by measure 14.2.* *Providers could provide educational information to support Australian end-users who are victims of, or otherwise impacted by, the categories of criminal activity described in sub-measure a).*
14.2	telephony relevant electronic service	**Reporting mechanisms** A provider of a service must provide a tool or mechanism which enables Australian end-users to report breaches of the prohibitions described in measure 14.1 a) by end-users of the telephony relevant electronic service. If an Australian end-user reports a breach via the tool or mechanism, the provider must: a) respond promptly to the end-user acknowledging receipt of the report; and b) consider any relevant information provided by Australian end-users pursuant to this tool or mechanism in a reasonably timely manner and if appropriate take action pursuant to measure 14.1 d). The reporting tool or mechanism must: c) be easily accessible and easy to use; d) where the tool or mechanism does not involve use of a widely used communication mechanism – have clear instructions on how to use it; and e) ensure that the identity of the reporter is not disclosed to the reported 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, except as required by applicable law. The provider must develop and comply with internal policies and procedures for dealing with reports made through this tool or mechanism.

No.	Tier or category of RES	Compliance measure
14.3	telephony relevant electronic service	**Information about contact mechanisms** A provider of a service must provide clear and accessible information to Australian end-users regarding the contact tools and/or mechanisms required by measure 14.2 and 14.7. Information must be provided in a manner that can be easily understood by users of all ages permitted on the service.
14.4	telephony relevant electronic service	**Information for Australian end-users about the role and functions of eSafety, including how to make a complaint to eSafety** A provider of a service must publish clear information that is accessible to Australian end-users which explains the role and functions of eSafety, including how to make a complaint to eSafety.
14.5	telephony relevant electronic service	**Information to assist end-users with managing risks relating to class 1C and class 2 material** A provider of a service must provide clear information that is accessible to Australian end-users about steps that end-users can take to manage and mitigate risks relating to class 1C and class 2 material. ***Guidance:*** *This might include support or help articles for users of the service. Such articles might provide information on safe behaviour on services.*
14.6	telephony relevant electronic service	**Reporting to eSafety on Code compliance** Where eSafety issues a written request to a provider of a 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) a description of the service's functionalities and features during the reporting period and an explanation of why the service is properly characterised as a telephony relevant electronic service (noting providers may refer eSafety to information previously provided in this regard); b) details of any risk assessment it is required to undertake pursuant to this Code together with information about the risk assessment methodology adopted; c) the steps that the provider has taken to comply with the compliance measures under this Code; and d) an explanation as to why those measures are appropriate. A provider that 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 will not be required to submit a Code report to eSafety more than once in any 12-month period.
14.7	telephony relevant	**Complaint tools**

No.	Tier or category of RES	Compliance measure
	electronic service	A provider of a service must provide a tool or mechanism which enables Australian end-users to make a complaint about a breach of this Code by the provider. If an Australian end-user makes a complaint of the kind referred to in this measure, the provider must consider any relevant information provided by Australian end-users pursuant to their complaint in a reasonably timely manner. Such complaints tool or mechanism must: a) be easily accessible and simple to use; and b) where the tool or mechanism does not involve use of a widely used communication mechanism – have clear instructions on how to use it. The provider must develop and comply with internal policies and procedures for dealing with complaints made through this tool or mechanism.
14.8	telephony relevant electronic service	**Timely response to communications from eSafety** The provider of a service must implement policies and procedures that ensure that it responds in a timely and appropriate manner to communications from eSafety about compliance with this Code.

15 Compliance measures for Tier 1 – Tier 3

The compliance measures in this table apply to RES with a risk profile of Tier 1, Tier 2 or Tier 3 (as specified) as assessed under clause 4.2(a), but do not apply to any AI companion chatbot feature.

No.	Tier or category of RES	Compliance measure
15.1	Tier 1 Tier 2	**Terms and conditions prohibiting illegal activity** A provider of a service must: a) have terms and conditions in place with Australian end-users prohibiting the end-user from sharing material via the service in the course of engaging in any of the following categories of criminal activity: i. non-consensual sharing of intimate images; ii. grooming of children; or

No.	Tier or category of RES	Compliance measure
		iii. sexual extortion (or sextortion); b) publish the terms and conditions by making them accessible on a website and/or application for the service (as relevant); c) ensure the prohibition described in sub-measure a) is set out in plain language in the terms and conditions; and d) if the provider becomes aware of a breach of the prohibition described in sub-measure a), take appropriate and proportionate action in a reasonably timely manner. It is not necessary that a particular form of words be used in the terms and conditions so long as the contractual effect of the terms and conditions is as required by sub-measure a). A provider must have systems and/or processes in place to support compliance with the obligation in sub-measure d). ***Guidance:*** *Providers should be aware that the material shared via the service in the course of engaging in the categories of criminal activity described in sub-measure a)i. to iii. could include class 1C and class 2 material.* *Providers have flexibility to design terms, systems, processes and policies to allow appropriate and proportionate responses to potential breaches on a case-by-case basis. Providers have the ability to exercise discretion to enforce terms and policies in accordance with the specific circumstances of each potential breach.* *Whilst appropriate and proportionate action in response to a breach will be dependent on the specific circumstances, and should take account of both the serious harm that may flow from relevant criminal activity and also the potential consequences of restricting access to core communications services relied on by end-users, it may include (for example):* • *warnings; or* • *account level actions such as suspensions, or ultimately account terminations, for extremely serious or repeated breaches.* *The contractual provisions required by sub-measure a), and the systems and/or processes required to support compliance with sub-measure d), may be drafted and/or implemented in a way that assists a provider to clearly establish whether there has, or has not, been a breach of the relevant prohibitions on sharing listed in sub-measure a). Whilst a provider should have reference to relevant criminal offences, this measure does not require a provider to contractually require an account holder not to share categories of material in the exact circumstances required by law, or to assess whether an end-user has breached the law (which can involve detailed fault elements and defences which may be extremely difficult for a provider to assess or identify), but can involve (for example):* • *including a simply described prohibition in contractual terms (e.g. a prohibition on illegal conduct or on specific forms of sharing or conduct defined by the provider); or* • *setting a threshold test (in the systems and/or processes required to support compliance with sub-measure d)) which the provider can clearly apply, after which appropriate and proportionate action will be taken.* *A provider may become aware of a breach for the purposes of sub-measure d) if information demonstrating a breach is provided to it via the reporting mechanism required by measure 15.2.*

No.	Tier or category of RES	Compliance measure
		Providers could provide educational information to support Australian end-users who are victims of, or otherwise impacted by, the categories of criminal activity described in sub-measure a).
15.2	Tier 1 Tier 2	**Reporting mechanisms** A provider of a service must provide a tool or mechanism which enables Australian end-users to report breaches of the prohibitions described in measure 15.1 a) by end-users of the service. If an Australian end-user reports a breach via the tool or mechanism, the provider must: a) respond promptly to the end-user acknowledging receipt of the report; and b) consider any relevant information provided by the end-user pursuant to this tool or mechanism in a reasonably timely manner and if appropriate take action pursuant to measure 15.1 d). The reporting tool or mechanism must: c) be easily accessible and easy to use; d) where the tool or mechanism does not involve use of a widely used communication mechanism, have clear instructions on how to use it; and e) ensure that the identity of the reporter is not disclosed to the reported 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, except as required by applicable law. The provider must develop and comply with internal policies and procedures for dealing with reports made through this tool or mechanism.
15.3	Tier 1 Tier 2	**Training for personnel responding to reports** A provider of a service must ensure that personnel responding to reports made by Australian end-users under measure 15.2 are trained in the service's policies and procedures for dealing with such reports.
15.4	Tier 1 Tier 2	**Review of compliance of personnel with systems and processes** A provider of a service must review the effectiveness of its reporting mechanism (as required by measure 15.2) and processes to ensure information received via the reporting mechanism is considered and actioned (if necessary) as appropriate pursuant to measure 15.1 d). Such review must occur at least annually. ***Guidance:*** *This could include review and analysis of data collected for the year (e.g. responses and outcomes) as well as submitting test complaints via the reporting mechanism to review handling and response.*
15.5	Tier 1	**Safety features and settings**

No.	Tier or category of RES	Compliance measure
		A provider of a service must ensure that it has appropriate tools, features and/or settings available and accessible to assist Australian end-users to limit receipt of unsolicited material (including class 1C and class 2 material). At a minimum, such tools, features and/or settings must include: a) if the service allows the sending of messages between end-users: i. tools that allow Australian end-users to block direct messages from other end-users; and ii. settings for Australian end-users that allow them to mute or otherwise prevent receipt of unwanted messages (including messages containing class 1C and class 2 material) from other end-users; and b) if the service allows the sending of messages in a group chat between three or more end-users – tools that allow Australian end-users to leave that group chat. If the provider allows Australian children to become end-users of the service, the provider must ensure that the settings referred to in paragraph a)ii. above are defaulted to the most restrictive setting for an Australian child at the time of account registration. Other examples of such tools, features and/or settings include: c) with respect to online pornography, tools, features and/or settings that automatically blur images detected as containing nudity on receipt; d) if the service uses recommender systems to present material to end-users – tools, features and/or settings that prevent or reduce the occurrence of online pornography, self-harm material and high-impact violence material from being promoted to Australian children; and e) if the provider allows Australian children to become end-users of services – have default settings for Australian children that prevent an end-user who is over the age of 18 years and is not connected to an Australian child from being able to use the service to send a direct message to that Australian child. ***Guidance:*** *For these purposes, the circumstances in which an end-user will be considered to be "connected" to an Australian child include if: (1) they are friends on the service; (2) the Australian child follows the end-user; or (3) the Australian child has the end-user saved as a phone contact.* *For the avoidance of doubt, the reference to defaulting settings to "the most restrictive settings" refers to the most restrictive settings that are available and possible on the service.*
15.6	Tier 1	**Significant changes to the service** Before the provider of a service makes a material change to the service (including any significant new feature of the service enabled by artificial intelligence) that will significantly increase the risk of sharing of online pornography, self-harm material or high-impact violence material to Australian children, it must:

No.	Tier or category of RES	Compliance measure
		a) carry out an assessment of the kinds of measures that could reasonably be incorporated into the service to minimise the risk; and b) where appropriate, apply measures so identified to help to mitigate that risk.
15.7	Tier 1	**Improvement** Where technically feasible and reasonably practicable, a provider of a service must take appropriate steps to further develop and improve the tools, features and/or settings (as relevant) it has in place under measure 15.5 over time. Examples of activities that a provider may engage in to meet this measure include the following (to the extent directed towards, or relevant to, the matters covered by this Code): a) any activities designed to further develop the effectiveness of the tools, features and/or settings; b) tracking new and emerging risks or issues that may be causing harm to Australian children; c) investment in research and development and/or testing of novel technological solutions; d) investment in trust and safety teams dedicated to implementing regulatory requirements and policies which enhance online safety for users of online services; e) investment in review teams who conduct human review of reported material, and can consider material including factors like context; f) providing financial or technical support to non-government organisations with recognised online safety expertise to improve their infrastructure and/or technical capabilities; g) contributing to programs operated by non-governmental organisations; h) joining relevant industry organisations or other third party organisations intended to address online harm to children and sharing information on best practice approaches; i) contributing to industry initiatives (including initiatives lead by industry associations or other third party organisations); j) conducting or supporting research into and development of online safety tools, features and/or settings and approaches; k) providing support, either financial or in kind, to organisations the functions of which are or include protection of children online; l) extending the application of a feature or tool applied under another industry code or standard to operate in connection with its service; and m) activities that aim to refine algorithms or inputs into tools to improve their effectiveness. The provider must, at a minimum, engage in at least some of the example activities above in each calendar year.
15.8	Tier 1 Tier 2	**Information about tools and contact mechanisms** A provider of a service must provide clear and accessible information to Australian end-users regarding:

No.	Tier or category of RES	Compliance measure
		a) the tools, features and/or settings required by measure 15.5; and b) the contact tools and/or mechanisms required by measure 15.2 and 15.16. Information must be provided in a manner that is reasonably capable of being easily understood by most users of all ages permitted on the service.
15.9	Tier 1 Tier 2	**Information for Australian end-users about the role and functions of eSafety, including how to make a complaint to eSafety** A provider of a service must publish clear information that is accessible to Australian end-users which explains the role and functions of eSafety, including how to make a complaint to eSafety.
15.10	Tier 1 Tier 2	**Information to assist end-users with managing risks relating to class 1C and class 2 material** A provider of a service must provide clear information that is accessible to Australian end-users about steps that end-users can take to manage and mitigate risks relating to class 1C and class 2 material. ***Guidance:*** *This might include support or help articles for users of the service. Such articles might provide information on safe behaviour on services.*
15.11	Tier 1	**Location on or via service that is dedicated to providing online safety information** A provider of a service must establish a location on or via the service that is dedicated to providing online safety information, that: a) contains information required under this Code; b) includes information about how Australian end-users can contact third party services that may provide counselling and support; and c) is accessible to Australian end-users. ***Guidance:*** *A provider could raise Australian end-users' awareness about the availability of safety information on its services, through interstitial mechanisms such as account notifications, on-service advertising campaigns or pop-up notices when material is being posted or viewed by Australian end-users. Providers could contribute to off-service campaigns targeted at the general public, Australian end-users or specific sections of the community such as teachers, parents and carers, older users or vulnerable groups. A provider could contribute to an off-service campaign by providing financial assistance, advertising collateral, expert advisers, or other support services.*
15.12	Tier 1	**Updates to eSafety about relevant changes to technology** A provider of a service must share information with eSafety in writing about significant changes to the functionality of its service that are likely to have a material positive or negative effect on the access or exposure to, distribution of, or online storage of class 1C and

No.	Tier or category of RES	Compliance measure
		class 2 material by Australian children. A provider may choose to provide this information in a Code report to eSafety under this Code. In implementing this measure, a provider is not required to disclose information to eSafety that is confidential. ***Guidance:*** *Changes that have a material negative effect should, ideally, be communicated before a public announcement of the relevant changes.*
15.13	Tier 1 Tier 2	**Reporting to eSafety on Code compliance** Where eSafety issues a written request to a provider of a service to submit a Code report, the provider named in such request must submit to eSafety a Code report which includes the following information: a) details of any risk assessment it is required to undertake pursuant to this Code together with information about the risk assessment methodology adopted; b) the steps that the provider has taken to comply with the compliance measures under this Code; and c) an explanation as to why those measures are appropriate. A provider that 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 will not be required to submit a Code report to eSafety more than once in any 12-month period.
15.14	Tier 1 Tier 2	**Trust and safety function** A provider of a service must have, or have access to, sufficient personnel to oversee the safety of the service. Such personnel must have the skills, experience and qualifications needed to ensure that the provider complies with the requirements of this Code at all times.
15.15	Tier 1	**Engagement** A provider of a service must either: a) appropriately engage with safety and community organisations (such as civil society groups, public interest groups and representatives of marginalised communities), academics and government to gather information to help inform the measures taken for the purposes of protecting or preventing children from accessing or being exposed to class 1C and class 2 material; or b) enter into arrangements for cooperating and collaborating with other organisations (such as industry associations) in activities of the kind referred to in paragraph a) to enhance online safety for Australians. A provider of a service must consider information obtained through such engagement. ***Guidance:***

No.	Tier or category of RES	Compliance measure
		Engagement may occur within and/or outside Australia as relevant to the issue under consideration. *Engagement may occur regularly in the course of ongoing relationships with organisations, academics or government, during development of new service features or in other appropriate circumstances.*
15.16	Tier 1 Tier 2	**Complaints tools** A provider of a service must provide a tool or mechanism which enables Australian end-users to make a complaint about a breach of this Code by the provider. If an Australian end-user makes a complaint of the kind referred to in this measure, the provider must consider any relevant information provided by the Australian end-user pursuant to their complaint in a reasonably timely manner. Such complaints tool or mechanism must: a) be easily accessible and simple to use; and b) where the tool or mechanism does not involve use of a widely used communication mechanism, have clear instructions on how to use it. The provider must develop and comply with internal policies and procedures for dealing with complaints made through this tool or mechanism.
15.17	Tier 1 Tier 2	**Timely referral of unresolved complaints to eSafety** A provider of a service must promptly refer to eSafety complaints from Australian end-users concerning material non-compliance with this Code by the provider, where the provider is unable to resolve the complaint within a reasonable timeframe.
15.18	Tier 1	**Timely response to communications from eSafety** The provider of a service must implement policies and procedures that ensure that it responds in a timely and appropriate manner to communications from eSafety about compliance with this Code.

16 Compliance measures for AI companion chatbot features

The compliance measures in this table apply to AI companion chatbot features included as part of a:

i) relevant electronic service that is required to undertake a risk assessment under clause 4.2(a) (other than a telephony relevant electronic service);

ii) relevant electronic service that has chosen to automatically assign a Tier 1 risk profile as anticipated by clause 4.2(a) (other than a telephony relevant electronic service);

iii) pre-assessed relevant electronic service; or

iv) gaming service with limited communications functionality.

An AI companion chatbot feature that meets the risk tier specified in the "Risk Tier" column in respect of a generative AI restricted category of material, must comply with that measure for the relevant generative AI restricted category of material. An AI companion chatbot feature may have a different risk profile for each generative AI restricted category of material. For example, an AI companion chatbot feature may have a Tier 1 risk profile for online pornography but a Tier 2 or Tier 3 risk profile for all other generative AI restricted categories. In that case, the Tier 1 compliance measures for the AI companion chatbot feature will only apply in relation to online pornography.

No.	Risk Tier	Compliance measure
16.1	Tier 1	**Age assurance measures** The provider of the service must, where technically feasible and reasonably practicable, implement: (a) appropriate age assurance measures; and (b) access control measures, before providing access to the feature or being able to generate the generative AI restricted category of material. The provider must also take appropriate steps to test and monitor the effectiveness of its age assurance and access control measures over time. Note: A provider will need to comply with this measure for the generative AI restricted category of material for which it has a Tier 1 risk profile.
16.2	Tier 2	**Safety by design defaults – generative AI restricted categories of material** The provider of the service must either: (a) implement the age assurance and access controls measures outlined in measure 16.1 above before providing access to the feature, or being able to generate a generative AI restricted category of material; or (b) comply with the following: (i) implement systems, processes and/or technologies that prevent the feature from being used to generate outputs that contain a generative AI restricted category of material; (ii) regularly review and test models on the potential risk that model is used to generate a generative AI restricted category of material; and (iii) promptly following review and/or testing, adjust models and deploy mitigations with the aim of reducing the misuse and unintentional use of models to generate a generative AI restricted category of material. ***Guidance:*** *A requirement to put in place systems, processes, and/or technologies to prevent the feature from being used to generate outputs that contain a generative AI restricted category of material should take account of the fact that not all AI companion chatbot feature providers*

No.	Risk Tier	Compliance measure
		will always have sufficient visibility and control of their models—if a provider lacks that visibility or control of certain aspects so that it cannot deploy all mitigations, it will have to rely on other systems, processes and technologies that are available. Note: A provider will need to comply with this measure for the generative AI restricted category of material for which it has a Tier 2 risk profile.
16.3	Tier 1 Tier 2	**Terms and conditions** The provider of the service must have, and enforce, clear actions, policies or terms and conditions relating to the generation of the generative AI restricted categories of material, which will include, to the extent applicable, terms and conditions dealing with whether any type of generative AI restricted category of material is permitted to be generated using the feature. In implementing this measure, the service provider should: (a) use simple, plain, and straightforward language; (b) to the extent practicable, be clear about the type of any material that is prohibited; and (c) communicate such terms and conditions, standards and/or policies to all personnel that are directly involved in their enforcement. Relevant policies and actions should be implemented according to a graduated, risk-based approach. This approach may be different for different types of material. Note: A provider will need to comply with this measure for the generative AI restricted category of material for which it has a Tier 1 or Tier 2 risk profile.
16.4	Tier 1 Tier 2	**Reporting mechanisms** Note: Relevant electronic services on which AI companion chatbot features appear are generally required by this Code to provide a tool or mechanism which enables Australian end-users to report breaches of certain prohibitions in terms and conditions. See for example, measure 15.2. This measure 16.4 contains additional requirements for those tools or mechanisms. As Tier 3 relevant electronic services and gaming service with limited communications functionality are not required by this Code to have such tools or mechanisms, they are subject to specific requirements under this measure in the event they include an AI companion chatbot feature. The provider of the service must ensure that any tool or mechanism it has in place for reporting breaches of relevant prohibitions in terms and conditions as required by this Code, also enables Australian end-users to report a generative AI restricted category of material generated using the AI companion chatbot feature which they consider may be contrary to the service's terms and conditions, and the provider must handle that report in the same way as it is required to handle other reports of breach via the tool or mechanism under this Code. The provider of the service must ensure that: (a) information required by this Code to be given about the tool or mechanism includes, where relevant, information about reporting under this measure; and (b) training required by this Code to be given to personnel responding to reports via the tool or mechanism covers reports of the kind provided for in this measure.

No.	Risk Tier	Compliance measure
		If the service on which the AI companion chatbot feature appears is a Tier 3 relevant electronic service or a gaming service with limited communications functionality that is not otherwise required by this Code to have a tool or mechanism in place for reporting breaches, then the provider of that service must: (c) comply with measure 15.2 of this Code as if the service was a Tier 2 relevant electronic service, except that references in measure 15.2 to an end-user reporting a breach will be read as references to reports of the kind described in this measure; and (d) comply with measure 15.3 of this Code as if the service was a Tier 2 relevant electronic service, except that references in measure 15.3 to reports will be read as references to reports of the kind described in this measure; and (e) provide clear and accessible information to Australian end-users regarding the tools and/or mechanisms required by this measure. Information must be provided in a manner that is reasonably capable of being easily understood by most users of all ages permitted on the service. Note: A provider will need to comply with this measure for the generative AI restricted category of material for which it has a Tier 1 or Tier 2 risk profile.
16.5	Tier 1 Tier 2	**Information about how services deal with generative AI restricted categories of material** The provider of the service must publish clear and accessible information that explains the actions they take to reduce the risk of harm to Australian children caused by the generation of a generative AI restricted category of material using the feature. Note: A provider will need to comply with this measure for the generative AI restricted category of material for which it has a Tier 1 or Tier 2 risk profile.
16.6	Tier 1 Tier 2	**Updates to eSafety about relevant changes to technology** The provider of the service must share information with eSafety in writing about significant changes to the functionality of their AI companion chatbot feature that are likely to have a material positive or negative effect on the risk of generation of a generative AI restricted category of material by Australian children. A service provider may choose to provide this information in an annual report to eSafety under this Code. In implementing this measure, a provider is not required to disclose information to eSafety that is confidential. ***Guidance:*** *Changes that have a material negative effect should, ideally be communicated before a public announcement of the relevant changes.* Note: A provider will need to comply with this measure for the generative AI restricted category of material for which it has a Tier 1 or Tier 2 risk profile.
16.7	Tier 1	**Complaints tools** Note: Relevant electronic services on which AI companion chatbot features appear are generally required by this Code to provide a tool or mechanism which enables Australian end-users to make a complaint of breach of this Code by the provider. See for example, measure 15.16. This measure contains additional requirements for those tools or mechanisms. As Tier 3 relevant electronic services and some gaming services with limited communications functionality are not required by this Code to have such tools or mechanisms, they are subject to specific requirements under this measure in the event they include an AI companion chatbot feature. The provider of the service must ensure that any tool or mechanism it has in place to enable Australian end-users to make a complaint about a breach of this Code by the provider, enables Australian end-users to make a complaint about a breach of the measures in this

No.	Risk Tier	Compliance measure
		table 16 and the provider must handle that complaint in the same way as it is required to handle other complaints via the tool or mechanism under this Code. The provider of the service must ensure that information required by this Code to be given about the tool or mechanism includes, where relevant, information about making complaints under this measure. If the service on which the AI companion chatbot feature appears is a Tier 3 relevant electronic service or a gaming service with limited communications functionality that is not otherwise required by this Code to have a tool or mechanism in place for making complaints about a breach of this Code by the provider, then the provider of that service must: (a) comply with measure 15.16 of this Code as if the service was a Tier 2 relevant electronic service, except that references in measure 15.16 to complaints about a breach of this Code will be read as reference to complaints about a breach of the measures in this table 16; and (b) provide clear and accessible information to Australian end-users regarding the tools and/or mechanisms required by this measure. Information must be provided in a manner that is reasonably capable of being easily understood by most users of all ages permitted on the service. Note: A provider will need to comply with this measure for the generative AI restricted category of material for which it has a Tier 1 risk profile.
16.8	Tier 1	**Significant changes to services** Before the provider of a service makes a material change to the AI companion chatbot feature that is likely to significantly increase the risk of enabling an Australian child to generate the generative AI restricted category of material it must: (a) carry out an assessment of the kinds of measures that could reasonably be incorporated into the feature to minimise that risk; and (b) where appropriate, apply measures so identified to help to mitigate that risk. Note: A provider will need to comply with this measure for the generative AI restricted category of material for which it has a Tier 1 risk profile.