Schedule 3 – Designated Internet Services Online Safety Code (Class 1C and Class 2 Material) 28 February 202

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 designated internet service (**DIS**) 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.

(a) **classified DIS** means a DIS that has the sole or predominant purpose of providing general entertainment, news or educational content, being:

(i) films or computer games that:

(A) have been classified R18+ Restricted or lower; or

(B) are exempt from classification under the *Classification (Publications, Films and Computer Games) Act 1995* (Cth) (**Classification Act**); or

(ii) films or computer games that have not been classified but, if classified, would likely be classified R18+ Restricted or lower; or

(iii) books, newspapers and magazines, whether in digital or audio form, podcasts or digital music that, if required to be classified, would likely be classified Unrestricted or Category 1 restricted.

(b) **DIS Standard** means the *Online Safety (Designated Internet Services – Class 1A and Class 1B Material) Industry Standard 2024*.

(c) designated internet service or '**DIS'** has the meaning set out in section 14(1) of the *Online Safety Act* 2021 (Cth) (**OSA**).

(d) **deemed tier 1 high impact service** means a service that has an automatic Tier 1 risk profile in respect of a particular category of material pursuant to clause 4.4(a)(i).

(e) **deemed tier 1 high impact generative AI service** means a service that has an automatic Tier 1 risk profile in respect of a particular category of material pursuant to clause 4.4(b)(i).

(f) **end-user** of a DIS, means a natural person who uses the service.

Example: A DIS may be provided to a family, where a parent or carer has the agreement with the provider of the service. The parent or carer is the account holder. Family members (including the parent or carer who is the account holder) who use the service are end-users.

(g) **end-user managed hosting service** means:

(i) a DIS that is primarily designed or adapted to enable end-users to store or manage material; and

(ii) includes a service that is taken to be an end-user managed hosting service under clause 6(d)(iii)(B).

Note 1: Examples of end-user managed hosting services include online file storage services, photo storage services, and other online media hosting services, including such services that include functionality to allow end-users to post or share content.

Note 2: For the purposes of this Code, an enterprise DIS that meets this definition will be taken to be both an enterprise DIS and an end-user managed hosting service – see clause 6(d)(iii)(B).

Note 3: An end-user managed hosting service differs from third-party hosting services (as defined in the *Hosting Services Online Safety Code (Class 1A and Class 1B Material)* which has the sole or predominant purpose of supporting the delivery of another service online and which does not directly interact with end-users.

(h) **enterprise customer** means the account holder under the agreement for the provision of an enterprise DIS.

Note: The enterprise customer will often make the service available to a class of end-users, such as its staff.

(i) **enterprise DIS** means a DIS:

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

(ii) the predominant purpose of which is to enable the account holder, in accordance with the terms of use for the service, to use the service for the organisation's activities, including integrating the service into the organisation's own services that are or may be made available by the organisation to the organisation's end-users; and

(iii) that is of a kind that is usually acquired by account holders for the purpose mentioned in clause 3(i)(ii);

and includes a service that is taken to be an enterprise DIS under clause 6(d)(iii)(A).

Note 1: An enterprise DIS excludes third-party hosting services (as defined in the *Hosting Services Online Safety Code (Class 1A and Class 1B Materia*l) and which are dealt with by that Code).

Note 2: An enterprise DIS would, for example, include:

(iv) websites designed for the ordering of commercial supplies by enterprise customers; and

(v) services which provide pre-trained artificial intelligence or machine learning models for integration into a service deployed or to be deployed by an enterprise customer.

(j) **general purpose DIS** means a DIS that:

(i) is a website or application that:

(A) primarily provides information for business, commerce, charitable, professional, health, reporting news, scientific, educational, academic research, government, public service, emergency, or counselling and support service purposes; or

(B) enables transactions related to the matters in clause 3(j)(i)(A); or

(ii) is a web browser; and

(iii) cannot be characterised as a different category of designated internet service under this Code.

(k) **high impact classified material** means any of the following:

(i) films or the contents of a film that has:

(A) been classified X18+ by the Classification Board under the Classification Act;

(B) not been classified, but if classified, would likely be classified X18+

(collectively, **X18+ material**);

(ii) Films or the contents of a film that has been classified R18+ in accordance with the Classification Act (**R18+ Material**); and

(iii) publications and other material that is not a film or the contents of a film that is otherwise Class 2A material under the Code (**other 2A material)**;

Note: This may include, for example, books, newspapers and magazines, whether in digital or audio form, podcasts or digital music that if required to be classified, would likely be classified X18+ in a corresponding way in which a film would be classified under the Classification Act.

(iv) self-harm material; and

(v) simulated gambling material.

(l) **high impact class 2 DIS** means a DIS that:

(i) has the sole or predominant purpose of enabling end-users to access any or all of the following types of material:

(A) online pornography;

(B) self-harm material; and/or

(C) high impact violence material

and includes a service that is taken to be a high impact class 2 DIS because of clause 6(d)(i).

Note: High impact class 2 DIS would, for example, include websites or applications such as pornography websites, gore websites, and/or pro-suicide websites that contain sexually explicit, shocking violent and/or high impact self-harm end-user generated content, that qualifies as online pornography, high impact violence or self-harm material.

(m) **high impact class 2 generative AI DIS** means a DIS that:

(i) uses machine learning models to enable an end-user to produce material; and

(ii) has the sole or predominant purpose of being used to generate any or all of the following types of material:

(A) online pornography;

(B) self-harm material; and/or

(C) high impact violence material

and includes a service that is taken to be a high impact class 2 generative AI DIS because of clauses 6(d)(i) and 6(d)(ii).

Note 1: This category would, for example, include services with generative AI functionality to produce online pornography including completely new material and new material that has been created from

editing existing material (for example – deepfake online pornography), but only where the sole or predominant purpose of the service is to enable users to generate that material.

Note 2: See Note 3 to definition of model distribution platform for an example of an exclusion from this category.

Note 3: A high impact class 2 generative AI DIS may also be taken to be:
(a) a high impact class 2 DIS—see clause 6(d)(i); or
(b) a classified DIS—see clause 6(d)(ii).

(n) **high impact generative AI DIS** has the same meaning given to that term in the DIS Standard.

(o) **high impact material:**

(i) when used in relation to measures for a high impact generative AI DIS and a high impact class 2 generative AI DIS has the same meaning given to that term in the DIS Standard in relation to a high impact generative AI DIS; and

(ii) when used in relation to measures for a DIS other than a high impact generative AI DIS, has the same meaning given to that term in the DIS Standard in relation a DIS other than a high impact generative AI DIS.

(p) **high impact violence material** means class 2 material comprised of material that depicts shocking, gratuitous or exploitative real images, or images that are presented as if they are real, of violence against people or animals and/or gore.

(q) **model distribution platform** means a DIS which:

(i) has a purpose which includes making available machine learning models; and

(ii) allows end-users to upload machine learning models to the service.

Note 1: Models made available on the service (including models uploaded to the service) and their associated content and materials hosted on the service, are components of the service.

Note 2: Material that is generated by or using models made available on the service, but that is not stored on or accessible using the service, is not a component of the service.

Note 3: A model distribution platform which includes functionality to enable end-users to use a hosted model to generate synthetic high impact material is not considered a high impact class 2 generative AI DIS.

(r) **pre-assessed DIS** is a general purpose DIS that:

(i) in respect of posting or sharing of material—the relevant service:

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

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

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

(ii) in respect of chat or messaging functionality, the relevant service:

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

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

(s) **restricted category** means online pornography and self-harm material.

(t) **relevant high-risk material** means the material for which a designated internet service has a Tier 1 risk profile.

Note: A designated internet service may have a Tier 1 risk profile as a result of a risk assessment undertaken pursuant to clause 4.2 or because they have been deemed to have a Tier 1 risk profile in accordance with clause 4.4(a)(i) or (b)(i).

4 Risk profile

4.1 General requirement for a risk assessment

(a) How this Code applies to a DIS depends on whether the provider:

(i) is required to assess the risk that a restricted category of material will be accessed, distributed, generated or stored on that service by an Australian child 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 category of DIS as set out in clause 4.4.

4.2 Risk assessment

(a) Subject to clause 4.4, and except where the provider of a DIS:

(i) chooses to automatically assign a Tier 1 risk profile to the DIS in accordance with section 5.2(a)(ii) of the Head Terms, or;

(ii) is a high impact generative AI DIS

a provider of a DIS must undertake a risk assessment in respect of each restricted category to determine its risk profile for each restricted category in accordance with the following tables (as applicable):

If the risk that Australian children will access or be exposed to online pornography on a service is…	**the risk profile of the service in relation to online pornography is …**
High	Tier 1
Moderate	Tier 2
Low	Tier 3

If the risk Australian children will access or be exposed to self-harm material on a service is …	**the risk profile of the service in relation to self-harm material is …**
High	Tier 1

Moderate	Tier 2
Low	Tier 3

(b) Subject to clause 4.4, a high impact generative AI DIS must undertake a risk assessment in respect of online pornography in accordance with the following table:

If the risk that online pornography will be generated on a service by Australian children is…	**the risk profile of the service in relation to online pornography is …**
High	Tier 1
Moderate	Tier 2
Low	Tier 3

4.3 Methodology used for risk assessment and documentation

If a risk assessment is required under this Code, the provider of the DIS 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 DIS (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 AI features of the service) and, to the extent reasonably relevant, the additional requirements set out in clause 5, and any other criteria that are reasonably relevant for the purposes of determining the risk profile of the DIS under this Code;

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

(c) carry out the risk assessment in accordance with the plan and methodology prepared under clause 5, and by persons with the relevant skills, experience and expertise; and

(d) as soon as practicable after determining the risk profile of a designated internet service, 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 section.

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

The service provider may carry out a single risk assessment covering all relevant restricted categories of material at once, provided that a separate risk profile is assessed for each restricted category.

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

The following categories of DIS are not required to undertake a risk assessment in respect of certain categories of material under this Code.

(a) A high impact class 2 DIS:

(i) is not required to undertake a risk assessment for a category of material it has a sole or predominant purpose in respect of and will automatically have a Tier 1 risk profile in respect of that material;

(ii) is required to undertake a risk assessment in accordance with clause 4.2(a) in respect of the other categories of material it does not have a sole or predominant purpose in respect of.

Note: For example, a high impact class 2 DIS that has the sole or predominant purpose of providing access to online pornography (e.g. a porn site) will not be required to undertake a risk assessment in respect of online pornography and will be required to comply with measures for services with a Tier 1 risk profile for online pornography as set out in the table at clause 7. That same service will still be required to undertake a risk assessment in accordance with clause 5 to determine the applicable risk profile for the material it does not have the sole or predominant purpose in respect of and will need to comply with the measures for services with that risk profile set out in the table at clause 7.

(b) A high impact class 2 generative AI DIS:

(i) is not required to undertake a risk assessment in respect of the category of material the generation of which is its sole or predominant purpose and will automatically have a Tier 1 risk profile in respect of that material;

(ii) is required to undertake a risk assessment in accordance with clause 4.2(b) in respect of online pornography if that is not the material, the generation of which is its sole or predominant purpose.

Note: For example, a high impact class 2 generative AI DIS that has the sole or predominant purpose of enabling end-users to generate high impact violence material will not be required to undertake a risk assessment in respect of that material. That service will be required to comply with the measures for services 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. That service will also need to conduct a risk assessment in respect of online pornography to determine its risk profile in respect of that material and comply with the measures for services with that risk profile as set out in the table at clause 10.

(c) An end-user managed hosting service is not required to undertake a risk assessment under this Code and must comply with the obligations for end-user managed hosting services set out in the table at clause 8.

(d) A classified DIS is not required to undertake a risk assessment under this Code and must comply with the obligations for classified DIS set out in the table at clause 9. A classified DIS that makes available high impact classified material must also comply with the measures set out in the table at clause 9 in respect of any high impact classified material it makes available.

(e) A model distribution platform is not required to undertake a risk assessment under this Code and must comply with the obligations for model distribution platforms set out in the table at clause 11.

(f) A pre-assessed DIS and an enterprise DIS are deemed to have a Tier 3 risk profile under this Code in respect of the restricted categories.

4.5 Changes to risk profile of a designated internet service

If a provider of a DIS:

(a) makes a change to its service such that it would no longer be exempt from carrying out a risk assessment under clause 4.4; 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 4.3 above.

5 Risk assessment: requirements

(a) This clause 5 applies where a provider of a DIS is required to undertake a risk assessment under clause 4.2.

(b) A provider of a DIS must take into account the following additional matters when undertaking a risk assessment of a service, so far as they are relevant to the service;

(i) whether online pornography is permitted on the service and if so, the likely portion of that content as compared with other types of content;

(ii) for a service that is not a high impact generative AI DIS service, whether self-harm material is permitted on the service and if so, the likely portion of that content as compared with other types of content;

(iii) the predominant purpose of the service, including the types of content available on the service;

(iv) the functionality of the service, including whether the service enables end-users in Australia to post or share material;

(v) the terms of use for the service;

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

(vii) the ages of end-users and likely end-users of the service in Australia;

(viii) the likelihood that the service may be used to directly expose an Australian child to a restricted category of material;

(ix) the likelihood that an Australian child will use the service to access a restricted category of material on the service;

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

(xi) For providers of a high impact generative AI service, the ages of end-users and likely end-users of the service in Australia, including the likelihood that:

(A) the service may be used by an Australian child to generate online pornography; and

(B) a significant number of Australian children will access the service;

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

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

(xiv) a forward-looking analysis of:

(A) 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

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

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.

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

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

Note: Without limiting this clause 5(b), 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 designated internet services

(a) The tables in clauses 7 to 11 below contain compliance measures for providers of designated internet services, depending on the category of DIS being provided, or their risk profile in respect of a particular restricted category of material. Specifically:

(i) the table in clause 7 applies to:

(A) providers of a DIS that are required to undertake a risk assessment pursuant to clause 4.1(a)(i)**;** and

(B) a deemed tier 1 high impact service;

(ii) the table in clause 8 applies to providers of end-user managed hosting services;

(iii) the table in clause 9 applies to classified DIS. The measures listed at 9.1 to 9.3 of the table apply to all providers of a classified DIS. The compliance measures listed at 9.4 to 9.6 apply to high impact classified material but only to the extent that such material is made available on the classified DIS;

(iv) the table in clause 10 applies to:

(A) providers of a high impact generative AI DIS that are required to undertake a risk assessment in respect of online pornography pursuant to cause 4.2(b) and/or 4.4(b)(ii); and

(B) a deemed tier 1 high impact generative AI service;

(v) the table in clause 11 apply to providers of a model distribution platform.

(b) The tables also include 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.

(c) Certain compliance measures only apply to certain categories of DIS (as specified at the top of each table and in the column titled “application”), to certain categories of material (as specified in each table in the column titled “application”) or to DIS providers who meet a certain risk profile in relation to a category of material (as specified in the column titled “risk tier”).

Note 1: A service provider may have a different risk profile in respect of each restricted category. For example, a DIS may be Tier 3 in respect of online pornography, but Tier 1 in respect of self-harm material. In that case, the DIS will need to comply with the requirements for services with a Tier 3 risk profile in respect of online pornography (as specified in the relevant table), and the requirements for services with a Tier 1 risk profile in respect of self-harm materials (as specified in the relevant table).

Note 2: In some cases, a measure will apply to a service that has a particular risk profile in respect of any restricted category of material it provides. For example, a DIS that is Tier 3 in respect of online pornography, but Tier 1 in respect of self-harm material, will need to comply with any measure that applies to a service that is Tier 1 in respect of any restricted category of material even though it is not Tier 1 in respect of both restricted categories.

(d) Where a DIS meets the definition of more than one kind of DIS under this industry standard, then, for the purposes of this Code:

(i) if the DIS meets the definition of a high impact class 2 DIS and a high impact class 2 generative AI DIS—the service is taken to be a service of each of those kinds; and

(ii) if the DIS meets the definition of a classified DIS and a high impact class 2 generative AI DIS—the service is taken to be a service of each of those kinds; and

(iii) if the DIS meets the definition of an enterprise DIS and an end-user managed hosting service—the service:

(A) when and to the extent made available to enterprise customers—is taken to be an enterprise DIS; and

(B) when and to the extent made available by the provider directly to end-users in Australia—is taken to be an end-user managed hosting service; and

(iv) if the DIS meets the definitions of 2 or more other kinds of DIS —the service will be taken to be the kind of DIS that is most closely aligned with the service's predominant purpose.

Note 1: For paragraphs (i) and (ii), this means the provider of the service must ensure the service meets the compliance measures that are applicable to each kind of service.

Note 2: For paragraph (iii), this means that the provider of the service must ensure the service meets the compliance measures applicable to:

(a) an enterprise DIS (when the service is being provided to enterprise customers); and

(b) an end-user managed hosting service (when the service is being provided directly to end-users).

7 Compliance measures for class 1C and class 2 material – DIS with a Tier 1-Tier 3 risk profile (excluding high impact generative AI DIS)

No	Risk Tier	Application	Compliance Measure
7.1	Tier 1	relevant high-risk materials	**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 designated internet service or the relevant high impact materials. A service provider must also take appropriate steps to test and monitor the effectiveness of its age assurance and access control measures over time.
7.2	Tier 1 and Tier 2	online pornography and/or self-harm material	**Continuous improvement for systems regarding online pornography and/or self-harm material** A provider of a service that: (a) is not a deemed tier 1 high impact service; and (b) does not allow online pornography and/or self-harm material on its service; must invest in and take appropriate steps to continuously improve systems which can detect online pornography and/or self-harm material and automatically action that material before it is encountered by end-users Note: A provider of a service will need to comply with this measure for online pornography where the service has a Tier 1 or Tier 2 risk profile for online pornography. A provider of a service will need to comply with this measure for self-harm material where the service has a Tier 1 or Tier 2 risk profile for self-harm material.
7.3	Tier 1 and Tier 2		**Reporting mechanisms** The provider of the service must provide tools which enable Australian end-users to report, flag and/or make a complaint about class 1C and/or class 2 materials which they consider may be contrary to a service's terms and conditions, and must, where appropriate ensure that these reports are evaluated and actioned. Such reporting mechanisms must:

			(a) be easily accessible and easy to use; and (b) be accompanied by clear instructions on how to use them. The provider must ensure that the identity of a complainant is not accessible, directly or indirectly, by any other end-user or account holder of the service without the express consent of the complainant, except as required by law. Note: A provider of a service will need to comply with this measure where the service: 1) has a Tier 1 or Tier 2 risk profile in respect of any restricted category of material; or 2) is a deemed tier 1 high impact service.
7.4	Tier 1		**On interface reporting tools** The provider of the service must ensure that the reporting tools referred to in measure 7.3 above are available and accessible to Australian end-users on-the interface of the designated internet service. ***Guidance:*** *In implementing these measures, providers of a designated internet service should ensure that reporting tools are integrated within the functionality of the designated internet service in a manner that is visible and accessible at the point the Australian end-user accesses materials.* Note: A provider of a service will need to comply with this measure where the service: 1) has a Tier 1 risk profile in respect of any restricted category of material; or 2) is a deemed tier 1 high impact service.
7.5	Tier 1 and Tier 2	online pornography and/or self-harm material	**Safety tools** The provider of a service that: (a) is not a deemed tier 1 high impact service; and (b) allows online pornography and/or self-harm material on the service must allow all end-users to opt-in at any time to appropriate safety tools which may limit their access or exposure to online pornography and/or self-harm material on the service. Appropriate safety tools may include solutions for: (a) filtering material; (b) removing material from marketing and/or recommender systems; (c) blocking material; (d) blurring material; (e) halting autoplay of material; and/or (f) placing interstitial notices on material so that users can click through to view if they wish.

			Information about the appropriate safety tools implemented by the provider must be readily accessible to Australian end-users. Note: A provider of a service will need to comply with this measure for online pornography where the service has a Tier 1 or Tier 2 risk profile for online pornography. A provider of a service will need to comply with this measure for self-harm material where the service has a Tier 1 or Tier 2 risk profile for self-harm material.
7.6	Tier 1	relevant high-risk material	**Terms and conditions** The provider of the service must have, and enforce, clear actions, policies or terms and conditions relating to the relevant high-risk material, which will include, to the extent applicable, terms and conditions dealing with the types of relevant high-risk material that are allowed or not allowed on the designated internet service. In implementing this measure, a provider of a DIS must: (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 must be implemented according to a graduated, risk-based approach. This approach may be different for different types of material. Note: A provider of a service will need to comply with this measure where the service: 1) has a Tier 1 risk profile in respect of any restricted category of material; or 2) is a deemed tier 1 high impact service.
7.7	Tier 2	online pornography and/or self-harm material	**Terms and conditions** The provider of the service must have, and enforce, clear actions, policies or terms and conditions relating to online pornography and/or self-harm material, which will include, to the extent applicable, terms and conditions dealing with the types of online pornography and/or self-harm material that are allowed or not allowed on the designated internet service. In implementing this measure, a provider of a DIS must: (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 must be implemented according to a graduated, risk-based approach. This approach may be different for different types of material. Note: A provider of a service will need to comply with this measure for online pornography where the service has a Tier 2 risk profile for online pornography. A provider of a service will need to comply with this measure for self-harm material where the service has a Tier 2 risk profile for self-harm material.

7.8	Tier 1 and Tier 2		**Trust and safety function** The provider of the 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. Note: A provider of a service will need to comply with this measure where the service: 1) has a Tier 1 or Tier 2 risk profile in respect of any restricted category of material; or 2) is a deemed tier 1 high impact service.
7.9	Tier 1		**Information about how services deal with relevant high-risk 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 distribution of relevant high-risk material on its service. Note: A provider of a service will need to comply with this measure where the service: 1) has a Tier 1 risk profile in respect of any restricted category of material; or 2) is a deemed tier 1 high impact service.
7.10	Tier 2	online pornography and/or self-harm material	**Information about how services deal with online pornography and/or self-harm 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 distribution of online pornography and/or self-harm material on its service. Note: A provider of a service will need to comply with this measure for online pornography where the service has a Tier 2 risk profile for online pornography. A provider of a service will need to comply with this measure for self-harm material where the service has a Tier 2 risk profile for self-harm material.
7.11	Tier 1		**Timely referral of unresolved complaints to eSafety** The provider of the 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. Note: A provider of a service will need to comply with this measure where the service: 1) has a Tier 1 risk profile in respect of any restricted category of material; or 2) is a deemed tier 1 high impact service.
7.12	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 the Commissioner about compliance with this Code. Note: A provider of a service will need to comply with this measure where the service: 1) has a Tier 1 risk profile in respect of any restricted category of material; or 2) is a deemed tier 1 high impact service.

7.13	Tier 1		**Updates to eSafety about relevant changes to technology** A service provider must share information with eSafety in writing about significant changes to the functionality of their services that are likely to have a material positive or negative effect on the access or exposure to, distribution of, or online storage of relevant high-risk materials 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 of a service will need to comply with this measure where the service: 1) has a Tier 1 risk profile in respect of any restricted category of material; or 2) is a deemed tier 1 high impact service.
7.14	Tier 2	online pornography and/or self-harm material	**Updates to eSafety about relevant changes to technology** A service provider must share information with eSafety in writing about significant changes to the functionality of their services that are likely to have a material positive or negative effect on the access or exposure to, distribution of, or online storage of online pornography and/or self-harm 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 of a service will need to comply with this measure for online pornography where the service has a Tier 2 risk profile for online pornography. A provider of a service will need to comply with this measure for self-harm material where the service has a Tier 2 risk profile for self-harm material.
7.15	Tier 1		**Information for Australian end-users about the role and functions of eSafety, including how to make a complaint to eSafety** The provider of the 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. Note: A provider of a service will need to comply with this measure where the service: 1) has a Tier 1 risk profile in respect of any restricted category of material; or 2) is a deemed tier 1 high impact service.
7.16	Tier 2		**Information for Australian end-users about the role and functions of eSafety, including how to make a complaint to eSafety**

			The provider of the 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. Note: A provider of a service will need to comply with this measure where the service has a Tier 2 risk profile in respect of any restricted category of material.
7.17	Tier 1		**Location on or via service that is dedicated to providing online safety information** The provider of the service must establish a location accessible 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:*** *The provider of the service could raise Australian end-users' awareness about the availability of safety information on its service, 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 also 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 may also contribute to an off-service campaign by providing financial assistance, advertising collateral, expert advisers, or other support services.* Note: A provider of a service will need to comply with this measure where the service: 1) has a Tier 1 risk profile in respect of any restricted category of material; or 2) is a deemed tier 1 high impact service.
7.18	Tier 1	online pornography and/or self-harm material	**Complaints tools** The provider of the service, other than a deemed tier 1 high impact service, must provide tools which enable Australian end-users to make a complaint about: (a) the provider's handling of reports about online pornography and/or self- harm material that is accessible on the service; or (b) any other aspect of the provider's compliance with this Code. Such complaints tools must: (a) be easily accessible on or through the service and easy to use; (b) be accompanied by plain language instructions on how to use them; and

			(c) enable the complainant to specify the non-compliance to which the report or complaint relates. The provider must ensure that the identity of a complainant is not accessible, directly or indirectly, by any other end-user or account holder of the service without the express consent of the complainant, except as required by law. Note: A provider of a service will need to comply with this measure where the service has a Tier 1 risk profile in respect of any restricted category of material.
7.19	Tier 1	relevant high-risk material	**Complaints tools** The provider of the deemed tier 1 high risk service must provide tools which enable Australian end-users to make a complaint about the providers compliance with this Code. Such reporting mechanisms must: (a) be easily accessible on or through the service and easy to use; (b) be accompanied by plain language instructions on how to use them; and (c) enable the complainant to specify the non-compliance to which the complaint relates. The provider must ensure that the identity of a complainant is not accessible, directly or indirectly, by any other end-user or account holder of the service without the express consent of the complainant, except as required by law. Note: A provider of a service will need to comply with this measure where the service is a deemed tier 1 high impact service.
7.20	Tier 1 and Tier 2		**Training for personnel responding to reports and complaints** The provider of the service must ensure that personnel responding to reports referred to in compliance measures 7.3, 7.18 and 7.19 are trained in the designated internet service's policies and procedures for dealing with reports and complaints. Note: A provider of a service will need to comply with this measure where the service: 1) has a Tier 1 or Tier 2 risk profile in respect of any restricted category of material; or 2) is a deemed tier 1 high impact service.
7.21	Tier 1		**Review of compliance personnel with systems and processes** The provider of the service must review the effectiveness of its reporting systems and processes to ensure reports are assessed and actioned (if necessary) within reasonably expeditious timeframes, based on the level of harm the material poses to Australian children. Such review must occur at least annually.

			Note: A provider of a service will need to comply with this measure where the service: 1) has a Tier 1 risk profile in respect of any restricted category of material; or 2) is a deemed tier 1 high impact service.
7.22	Tier 1	relevant high-risk material	**Significant changes to services** The provider of the service must ensure that before it makes a material change to the service that will significantly increase the risk of sharing relevant high-risk material to an Australian child, it must: (a) carry out an assessment of the kinds of features and settings that could reasonably be incorporated into the service to minimise that risk; and (b) where appropriate, apply features and settings so identified to help to mitigate that risk. Note: A provider of a service will need to comply with this measure where the service: 1) has a Tier 1 risk profile in respect of any restricted category of material; or 2) is a deemed tier 1 high impact service.
7.23	Tier 1		**Engagement** The provider of the service must appropriately engage with safety and community organisations (such as civil society groups, public interest groups and representatives of marginalised communities) academics and governments to gather information to help inform measures taken for the purposes of protecting or preventing children from accessing or being exposed to class 1C and class 2 material. The provider of the service must consider information obtained through such engagement. ***Guidance:*** *Engagement and knowledge sharing 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.* Note: A provider of a service will need to comply with this measure where the service: 1) has a Tier 1 risk profile in respect of any restricted category of material; or 2) is a deemed tier 1 high impact service.
7.24	Tier 1, Tier 2 and Tier 3	online pornography and/or self-harm material	**Notifying changes to features and functions – generating high impact material** A service provider must share information with eSafety in writing about significant changes to the functionality of their services that are likely to significantly increase or decrease the risk of generation of online pornography and/or self-harm material by Australian children using generative artificial intelligence. Where applicable, 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 of a service will need to comply with this measure where the service: 1) has a Tier 1, 2 or 3 risk profile in respect of any restricted category of material; or 2) is a deemed tier 1 high impact service.
7.25	Tier 1 and 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) the steps that the provider has taken to comply with the compliance measures under this Code; (b) details of any risk assessment it is required to undertake pursuant to this Code; and (c) an explanation as to why these steps are appropriate. A provider of a service 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 of a service will not be required to submit a Code report to eSafety more than once in any 12-month period. Note: A provider of a service will need to comply with this measure where the service: 1) has a Tier 1 or Tier 2 risk profile in respect of any restricted category of material; or 2) is a deemed tier 1 high impact service.

8 Compliance measures for class 1C and class 2 material – end-user managed hosting services

No.	Compliance measure
8.1	**Terms and conditions prohibiting illegal activity** The provider of the 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.	Compliance measure
	(c) ensure the prohibition described in sub-measure 8.1(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 8.1(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 8.1(a). The provider of the service must have systems and/or processes in place to support compliance with the obligation in sub-measure 8.1(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 8.1(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 8.1(a), and the systems and/or processes required to support compliance with sub-measure 8.1(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 8.1(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):* *(a) 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* *(b) 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 8.1(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 8.1(a).*
8.2	**Reporting mechanisms**

No.	Compliance measure
	The provider of the service must provide a tool or mechanism which enables Australian end-users to report breaches of the prohibitions described in measure 8.1 above by end-users of the end-user managed hosting 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 the tool or mechanism in a reasonably timely manner, and if appropriate take action pursuant to measure 8.1. The reporting tool or mechanism must: (a) be easily accessible and easy to use; (b) where the tool or mechanism does not involve use of a widely used communication mechanism, include or be accompanied by clear instructions on how to use it; and (c) 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 of the service must develop and comply with internal policies and procedures for dealing with reports made through this tool or mechanism.
8.3	**On interface reporting tools** The provider of the service must ensure that the reporting tools referred to in measure 8.2 above are available and accessible to Australian end-users on-the interface of the designated internet service.
8.4	**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.
8.5	**Training for personnel responding to contact** The provider of the service must ensure that personnel responding to reports made by Australian end-users under measure 8.2 are trained in the end-user managed hosting service's policies and procedures for dealing with such reports.
8.6	**Review of compliance personnel with systems and processes** The provider of the service must review the effectiveness of its reports and complaints mechanism (as required by measure 8.2 and processes to ensure information received via the reports and complaints mechanism is considered and actioned (if necessary) as appropriate pursuant to measure 8.1. Such review must occur at least annually.
8.7	**Information to assist end-users with managing risks relating to class 1C and class 2 material**

No.	Compliance measure
	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.
8.8	**Information for Australian end-users about the role and functions of eSafety, including how to make a complaint to eSafety** The provider of the 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.
8.9	**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. The complaints tool or mechanism must: (a) be easily accessible and easy 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.
8.10	**Timely referral of unresolved complaints to eSafety** The provider of the 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 appropriately resolve the complaint within a reasonable timeframe.
8.11	**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 the Commissioner about compliance with this Code.
8.12	**Reporting to eSafety on Code compliance** Where eSafety issues a written request to a provider of the 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 these steps are appropriate. A provider of a service 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 of a service will not be required to submit a Code report to eSafety more than once in any 12-month period.

9 Compliance measures for class 1C and class 2 material-classified DIS

No.	Compliance measure
Measures for all classified DIS	
9.1	**Reporting mechanisms** A provider of a classified DIS that only makes available content that has been classified in accordance with the Classification Act must ensure end-users are provided a mechanism to report content which they consider may have been incorrectly classified. All other providers of classified DIS, must provide tools which enable Australian end-users to report, flag and/or make a complaint about content which they consider may be contrary to a service's terms and conditions, and ensure that these reports are considered and actioned appropriately. Such reporting mechanisms must: (a) be easily accessible and easy to use; and (b) be accompanied by clear instructions on how to use them. The provider must ensure that the identity of a complainant is not accessible, directly or indirectly, by any other end-user or account holder of the service without the express consent of the complainant.
9.2	**Trust and safety function** The provider of the 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.
9.3	**Reporting to eSafety on Code compliance** Where eSafety issues a written request to the provider of the 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 these steps are appropriate. A provider of a service 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 of a service will not be required to submit a Code report to eSafety more than once in any 12-month period.
Measures for high impact classified material	
9.4	**Appropriate measures to limit the risk of child end-users accessing or being exposed to other 2A and/or self-harm material**

	A provider of a classified DIS must, to the extent technically feasible and reasonably practicable implement appropriate measures that limit the risk of Australian children accessing or being exposed to other 2A material, R18+ and/or self- harm material. Examples of how a classified DIS could comply with this measure include: (a) enabling the creation of child profiles on the service to limit children's access to other 2A material, R18+ and/or self-harm material; or (b) implementing notices or functions e.g. warning labels, blurring, halting autoplay, and notice screens on other class 2A material, R18+ and self-harm material; or (c) filtering other 2A material, R18+ and self- harm material out of discovery feeds by downlisting, deprioritising or quarantining such material to Australian children; or (d) ensuring that recommender systems, algorithms, and other choice architecture, do not promote other 2A material, R18+ or self- harm material to Australian children; or (e) enabling users to opt in at any time to appropriate safety tools which may limit their access or exposure to other 2A material, R18+ or self-harm materials.
9.5	**Age assurance measures** A provider of a classified DIS must, where technically feasible and reasonably practicable, implement: (a) appropriate age assurance measures; and (b) access control measures, before providing access to X18+ material and/or simulated gambling material. A service provider must also take appropriate steps to test and monitor the effectiveness of its age assurance and access control measures over time.
9.6	**Information about tools and settings** To the extent a provider of a classified DIS implements features, functionalities or settings to comply with measures 9.4 and 9.5, the provider must provide clear and accessible information to explain those features, functionalities or settings in a manner that is easily understood by users of all ages permitted on the service. ***Guidance:*** *A provider may take steps to deprioritize, downlist, quarantine or remove material from recommender systems to limit the risk of Australian children being exposed to it. As no user action is required for these processes to take effect, providers do not have to provide information about these actions.*

10 Compliance measures for class 1C and class 2 material-high impact generative AI DIS

No.	Risk Tier	Application	Compliance measure
10.1	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 service or being able to generate relevant high-risk material. A service provider must also take appropriate steps to test and monitor the effectiveness of its age assurance and access control measures over time.
10.2	Tier 2	online pornography	**Safety by design defaults – online pornography** The provider of the service must either: (a) implement the age assurance and access controls measures outlined in measure 10.1 above before providing access to the service, or being able to generate online pornography; or (b) implement systems, processes and/or technologies that prevent the service from being used to generate outputs that contain online pornography; and (c) regularly review and test models on the potential risk that model is used to generate online pornography; and (d) 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 online pornography. ***Guidance:*** *A requirement to put in place systems, processes, and/or technologies to prevent the service from being used to generate outputs that contain online pornography should take account of the fact that not all high impact generative AI DIS providers 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.*

No.	Risk Tier	Application	Compliance measure
10.3	Tier 1	relevant high-risk material	**Terms and conditions – relevant high-risk material** The provider of the service must have, and enforce, clear actions, policies or terms and conditions relating to the relevant high-risk material. In implementing this measure, a provider of a DIS 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.
10.4	Tier 2	online pornography	**Terms and conditions – online pornography** The provider of the service must have, and enforce, clear actions, policies or terms and conditions relating to online pornography, which will include, to the extent applicable, terms and conditions dealing with whether any type of online pornography is permitted to be generated using the service. In implementing this measure, a provider of a DIS 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.
10.5	Tier 1	relevant high-risk materials	**Reporting mechanisms – relevant high-risk material** The provider of the service must provide tools which enable Australian end-users to report, flag and/or make a complaint about relevant high-risk material generated on the service which they consider may be contrary to a service's terms and conditions, and must where appropriate, ensure that these reports are evaluated and actioned. Such reporting mechanisms must: (a) be easily accessible and easy to use; and (b) be accompanied by clear instructions on how to use them.

No.	Risk Tier	Application	Compliance measure
			The provider must ensure that the identity of a complainant is not accessible, directly or indirectly, by any other end-user or account holder of the service without the express consent of the complainant, except as required by law.
10.6	Tier 2	online pornography	**Reporting mechanisms – online pornography** The provider of the service must provide tools which enable Australian end-users to report, flag and/or make a complaint about online pornography generated on the service which they consider may be contrary to a service's terms and conditions, and must, where appropriate ensure that these reports are evaluated and actioned. Such reporting mechanisms must: (a) be easily accessible and easy to use; and (b) be accompanied by clear instructions on how to use them. The provider must ensure that the identity of a complainant is not accessible, directly or indirectly, by any other end-user or account holder of the service without the express consent of the complainant, except as required by law.
10.7	Tier 1	relevant high-risk materials	**On interface reporting tools** The provider of the service must ensure that the reporting tools referred to in measure 10.5 above are available and accessible to Australian end-users on-the interface of the designated internet service. ***Guidance:*** *In implementing these measures, the provider should ensure that reporting tools are integrated within the functionality of the designated internet service in a manner that is visible and accessible at the point the Australian end-user accesses materials.*
10.8	Tier 1	relevant high-risk materials	**Information about how services deal with relevant high-risk 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 relevant high-risk material on its service.
10.9	Tier 2	online pornography	**Information about how services deal with online pornography** 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 online pornography on its service.

No.	Risk Tier	Application	Compliance measure
10.10	Tier 1 and Tier 2		**Trust and safety function** The provider of the 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. Note: A provider of a service will need to comply with this measure where the service: 1) has a Tier 1 or Tier 2 risk profile in respect of online pornography; or 2) is a deemed tier 1 high impact generative AI service.
10.11	Tier 1		**Timely referral of unresolved complaints to eSafety** The provider of the 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.
10.12	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 the Commissioner about compliance with this Code.
10.13	Tier 1		**Engagement** The provider of the service must appropriately engage with safety and community organisations (such as civil society groups, public interest groups and representatives of marginalised communities), academics and governments to gather information to help inform measures taken for the purposes of protecting or preventing children from generating the relevant high-risk material. The provider of the service must consider information obtained through such engagement. ***Guidance:*** *Engagement and knowledge sharing may occur within and/or outside Australia as relevant to the issue under consideration. This may be by way of an annual event or through ongoing relationships. 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.*
10.14	Tier 1	relevant high-risk material	**Updates to eSafety about relevant changes to technology** A service provider must share information with eSafety in writing about significant changes to the functionality of their services that are likely to have a material positive or negative effect on the risk of generation of relevant high-risk materials by Australian children using generative artificial intelligence. A service provider may choose to provide this information in an annual report to eSafety under this Code.

No.	Risk Tier	Application	Compliance measure
			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.*
10.15	Tier 2	online pornography	**Updates to eSafety about relevant changes to technology** A service provider must share information with eSafety in writing about significant changes to the functionality of their services that are likely to have a material positive or negative effect on the risk of generation of online pornography by Australian children using generative artificial intelligence. 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.*
10.16	Tier 1		**Information for Australian end-users about the role and functions of eSafety, including how to make a complaint to eSafety** The provider of the 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.
10.17	Tier 2		**Information for Australian end-users about the role and functions of eSafety, including how to make a complaint to eSafety** The provider of the 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. Note: A provider of a service will need to comply with this measure where the service has a Tier 2 risk profile in respect of online pornography.
10.18	Tier 1		**Location on or via service that is dedicated to providing online safety information** The provider of the service must establish a location accessible on or via the service that is dedicated to providing online safety information, that:

No.	Risk Tier	Application	Compliance measure
			(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 also 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 may also contribute to an off-service campaign by providing financial assistance, advertising collateral, expert advisers, or other support services.*
10.19	Tier 1	online pornography	**Complaints tools** The provider of the service, other than a deemed tier 1 high impact generative AI service must provide tools which enable Australian end-users to make a complaint about: (a) the provider's handling of reports about online pornography that is accessible on the service; and (b) the providers compliance with this Code. Such reporting mechanisms must: (a) be easily accessible on or through the service and easy to use; (b) be accompanied by plain language instructions on how to use them; and (c) enable the complainant to specify the non-compliance to which the complaint relates. The provider must ensure that the identity of a complainant is not accessible, directly or indirectly, by any other end-user or account holder of the service without the express consent of the complainant, except as required by law.
10.20	Tier 1	relevant high-risk material	**Complaints tools** The provider of the deemed tier 1 high risk generative AI service must provide tools which enable Australian end-users to make a complaint about the providers compliance with this Code. Such reporting mechanisms must: (a) be easily accessible on or through the service and easy to use;

No.	Risk Tier	Application	Compliance measure
			(b) be accompanied by plain language instructions on how to use them; and (c) enable the complainant to specify the non-compliance to which the complaint relates. The provider must ensure that the identity of a complainant is not accessible, directly or indirectly, by any other end-user or account holder of the service without the express consent of the complainant, except as required by law.
10.21	Tier 1 and Tier 2		**Training for personnel responding to reports and complaints** The provider of the service must ensure that personnel responding to reports referred to in compliance measures 10.5, 10.6, 10.19 and 10.20 are trained in the designated internet service's policies and procedures for dealing with reports and complaints. Note: A provider of a service will need to comply with this measure where the service: 1) has a Tier 1 or Tier 2 risk profile in respect of online pornography; or 2) is a deemed tier 1 high impact generative AI service.
10.22	Tier 1		**Review of compliance personnel with systems and processes** The provider of the service must review the effectiveness of its reporting systems and processes to ensure reports are assessed and actioned (if necessary) within reasonably expeditious timeframes, based on the level of harm the material poses to Australian children. Such review must occur at least annually.
10.23	Tier 1		**Significant changes to services** The provider of the service must ensure that before it makes a material change to the service that is likely to significantly increase the risk of enabling an Australian child to generate the relevant high-risk material it must: (a) carry out an assessment of the kinds of features and settings that could reasonably be incorporated into the service to minimise that risk; and (b) where appropriate, apply features and settings so identified to help to mitigate that risk.
10.24	Tier 1 and Tier 2		**Reporting to eSafety on Code compliance** Where eSafety issues a written request to a provider of the 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; (b) details of any risk assessment it is required to undertake pursuant to this Code; and (c) an explanation as to why these steps are appropriate.

No.	Risk Tier	Application	Compliance measure
			A provider of a service 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 of a service will not be required to submit a Code report to eSafety more than once in any 12-month period. Note: A provider of a service will need to comply with this measure where the service: 1) has a Tier 1 or Tier 2 risk profile in respect of online pornography; or 2) is a deemed tier 1 high impact generative AI service.

11 Compliance measures for model distribution platforms

No.	Compliance Measure
11.1	**Polices and contractual terms relating to applicable Australian content laws** A provider of a model distribution platform must have in place policies and/or contractual terms that make clear to customers of the service that customers must, when using the service, comply with applicable Australian content laws and regulations, including industry codes or standards made pursuant to the OSA, that create legal obligations for customers relating to class 1C and class 2 material. ***Guidance:*** *For the purpose of this measure, providers of a model distribution platform may satisfy this measure in different ways and by making use of different language. Providers may consider that existing language in polices and/or contractual terms satisfies this requirement.*

11.2	**Enforcement action relating to customer breaches of polices and contractual terms** A provider of a model distribution platform service must: a) take appropriate and proportionate enforcement action with respect to customers of the service that breach its policies and/or contractual terms relating to complying with applicable Australian content laws and regulations, including industry codes or standards made pursuant to the OSA that create legal obligations for customers relating to class 1C and class 2 material; b) Have systems and processes, including standard operating procedures to: i. enforce their policies when they become aware of non-compliance with the policies and/or contractual terms outlined in measure 11.1; and ii. escalate reports of non-compliance with measure 11.1 above. ***Guidance:*** *Providers have flexibility to design and enforce terms and policies to allow appropriate and proportionate responses to potential breaches on a case-by-case basis. Examples of appropriate and proportionate enforcement action may include notifying, warning, or suspending the account(s) of the customer in question.*
11.3	**Contact mechanisms** A provider of a model distribution platform must: a) ensure that end-users can contact the provider in relation to breaches of applicable Australian content laws and regulations by customers of the model distribution platform service; b) provide information or links to information about: i. applicable Australian content laws and regulations; and ii. the role and function of eSafety and how to make a complaint to eSafety under the Online Safety Act. ***Guidance:*** *Examples of how a provider of a model distribution platform can comply with this measure include:* *(a) by making available online an email address;* *(b) by providing a web form (Contact Us or similar).*
11.4	**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 the Commissioner about compliance with this Code.

11.5	**Reporting to eSafety on Code compliance** Where eSafety issues a written request to a provider of a model distribution platform, the provider named in such request must submit to eSafety a Code report which includes the following information: (a) the steps that the provider has taken to comply with their applicable compliance measures; and (b) an explanation as to why these steps are appropriate. A provider of a model distribution platform who has received such a request from eSafety is required to submit a Code report within 2 months of receiving the request, but for the first request no earlier than 12 months after this Code comes into effect. A provider of a model distribution platform will not be required to submit a Code report to eSafety more than once in any 12-month period.