

Consolidated Industry Codes of Practice for the Online Industry (Class 1C and 2 Material)

Head Terms

In force – latest version

Table of Contents

| | |
|---|-----------|
| Preamble | 3 |
| Head Terms | 6 |
| 1 Introduction | 6 |
| 1.1 Purpose | 6 |
| 1.2 Development | 6 |
| 1.3 Ongoing work on age assurance and other measures | 6 |
| 2 Definitions and interpretation | 7 |
| 2.1 Definitions | 7 |
| 2.2 Interpretation | 11 |
| 3 Coverage | 11 |
| 4 Online safety objectives | 12 |
| 5 Compliance | 12 |
| 5.1 Compliance measures | 12 |
| 5.2 Process to identify compliance measures | 15 |
| 5.3 Presence of class 1C and class 2 material will not necessarily establish non-compliance | 16 |
| 6 Industry participants not required to undertake certain steps or breach Australian laws or regulations | 16 |
| 6.1 Industry participants not required to undertake certain steps | 16 |
| 6.2 Effect of section 6.1 | 17 |
| 6.3 Lawful conduct | 17 |
| 6.4 No breach of Code where action required under another Australian law | 18 |
| 7 Code administration | 18 |
| 7.1 Commencement | 18 |
| 7.2 Enforceability | 18 |
| 7.3 Code reporting | 18 |
| 7.4 Complaints about Code compliance | 19 |
| 7.5 Ongoing role of industry representatives | 19 |
| 7.6 Code review | 19 |

Preamble

Background

Part 9 of the *Online Safety Act 2021* (Cth) anticipates that bodies and associations representing sections of the online industry should develop industry codes that are to apply to industry participants in the respective sections of the industry in relation to their online activities. Words used in this document have the meanings given in section 2.1 of the Head Terms below.

Part 9 also anticipates that industry standards may be determined by eSafety for participants in sections of the online industry in some circumstances.

The sections of the online industry to which codes or standards may apply pursuant to Part 9 (referred to in this Preamble as sections of the online industry) are as follows:

- providers of social media services, so far as those services are provided to end-users in Australia;
- providers of relevant electronic services, so far as those services are provided to end-users in Australia;
- providers of designated internet services, so far as those services are provided to end-users in Australia;
- providers of internet search engine services, so far as those services are provided to end-users in Australia;
- providers of app distribution services, so far as those services are provided to end-users in Australia;
- providers of hosting services, so far as those services host material in Australia;
- the group consisting of providers of internet carriage services, so far as those services are provided to customers in Australia; and
- the group consisting of persons who manufacture, supply, maintain or install equipment that is for use by end-users in Australia of a social media service, relevant electronic service, designated internet service or internet carriage service (in each case in connection with the service).

Structure

An existing set of industry codes and standards (also referred to as 'Phase 1' codes and standards) have been developed for class 1A and class 1B material (which includes amongst other things child sexual exploitation, pro-terror, crime and violence and drug-related material).

Note: All references to the Phase 1 codes and standards are intended to be to the most current version of those Phase 1 codes and standards.

These *Consolidated Industry Codes of Practice for the Online Industry (Class 1C and Class 2 Material)* (also referred to as 'Phase 2' codes) have been developed in relation to other material, not covered by the Phase 1 codes and standards, which is identified under the National Classification Scheme as being inappropriate for children, referred to as class 1C and class 2 material.

The Phase 1 codes and standards apply independently of the Phase 2 codes and are not addressed in this document. Each industry participant is responsible for ensuring that it complies with both the Phase 1

codes and standards and the Phase 2 codes, as applicable to the products and services provided by that industry participant.

As part of the Phase 2 codes, there are three separate industry codes that apply to different sections of the online industry. Each code has been developed by one or more industry bodies or associations that represent the relevant section of the online industry. Each code is comprised of a common set of Head Terms and a Schedule setting out terms applicable to the relevant section of the online industry covered by that code. These details are set out in the table below:

| Title | Code structure | Section of the online industry to which the code applies | Industry representative |
|--|-------------------------|---|--|
| Hosting Services Online Safety Code (Class 1C and Class 2 Material) | Head Terms + Schedule 1 | Providers of hosting services, so far as those services host material in Australia | <ul style="list-style-type: none"> • CA • DIGI |
| Internet Carriage Services Online Safety Code (Class 1C and Class 2 Material) | Head Terms + Schedule 2 | Providers of internet carriage services, so far as those services are provided to customers in Australia | <ul style="list-style-type: none"> • AMTA • CA |
| Internet Search Engine Services Online Safety Code (Class 1C and Class 2 Material) | Head Terms + Schedule 3 | Providers of internet search engine services, so far as those services are provided to end-users in Australia | <ul style="list-style-type: none"> • CA • DIGI |

Identifying the applicable code

For each online activity that they undertake, each participant in the online industry must identify and comply with the industry code that applies to that online activity.

Where a single electronic service could fall within the scope of more than one industry code, the relevant industry participant will only be required to comply with one code for that electronic service. The code that will apply in this situation is the code that is most closely aligned with the predominant purpose of the single electronic service.

No industry participant will have to comply with more than one industry code in relation to the same electronic service.

The Schedule for each industry code may provide further detail as to the intended scope of that code. If an industry participant is still unsure as to which industry code is applicable to a particular electronic service, the industry participant may seek guidance from eSafety.

Differentiating between services based on functionality

All industry codes collectively recognise that every online industry participant has a role to play in addressing risks associated with access or exposure to class 1C and class 2 material .

Electronic products and services provided across different sections of the online industry may include different functionalities, which in turn may be relevant to:

- the connection between a product or service and risks associated with access or exposure to class 1C and class 2 material;

- the relationship between a product or service and an end-user, including whether or not a service controls the end-user interface; and
- the visibility, control or administration of specific material accessible to an end-user.

The structure of the various industry codes, including the separate Head Terms and Schedules, is intended to ensure that differences such as these are appropriately accounted for.

Note: For example, social media services generally include a more direct interface between online material and end-users than exists for internet search engine services or app distribution services. Similarly, hosting services, internet carriage services and applicable equipment support access to material only in conjunction with another online service, and have different relationships with end-users and control over end-user interfaces.

First party hosting of materials by social media services, relevant electronic services, designated internet services, app distribution services and internet search engine services

For the purpose of the codes, if a provider of a social media service, relevant electronic service, designated internet service, app distribution service or internet search engine service hosts stored material for the purpose of providing such a service, the hosting of the stored material is not treated as a separate online activity that requires additional compliance measures, beyond those that apply to the social media service, relevant electronic service, designated internet service, app distribution service or internet search engine service (as applicable).

App distribution by social media services, relevant electronic services, designated internet services, hosting services and internet search engine services

For the purpose of the codes, if a provider of a social media service, relevant electronic service, designated internet service, hosting service or internet search engine service provides an app distribution service for first-party apps for the purpose of providing such a service, the provision of the app distribution service is not treated as a separate online activity that requires additional compliance measures, beyond those that apply to the social media service, relevant electronic service, designated internet service, hosting service or internet search engine service (as applicable).

Head Terms

1 Introduction

1.1 Purpose

- (a) The purpose of this Code is to establish appropriate safeguards for the community in relation to risks associated with access or exposure to certain types of material, referred to in this Code as 'class 1C' and 'class 2' material. Each participant in the online industry has a role to play in addressing these risks.
- (b) This Code sets out:
 - (i) online safety objectives used in this Code; and
 - (ii) a process for industry participants to follow in order to identify and implement compliance measures by reference to applicable online safety objectives.
- (c) In doing so, this Code recognises that:
 - (i) different services, products, and technologies may have different risk profiles;
 - (ii) compliance measures should be proportionate to the level of risk associated with a particular online activity or service and to the size and capacity of the industry participant responsible for that online activity or service; and
 - (iii) compliance measures should be flexible in order to enable effective implementation in practice, recognise the differences between unique services, and to adapt to changes in technology and in the risk environment.

1.2 Development

The industry representatives responsible for leading the development of this Code (as listed in the Preamble):

- (a) consulted widely with relevant industry participants in order to ensure that they adequately represented their section of the online industry and their views were adequately considered in the development of the codes;
- (b) consulted widely with the public, stakeholders and other interested parties to ensure that their views were adequately considered in the development of the codes; and
- (c) consulted with eSafety on the development of this Code.

1.3 Ongoing work on age assurance and other measures

Industry participants acknowledge the importance of age assurance, along with other complementary safety measures, as one way of protecting children from accessing or being exposed to class 1C and class 2 material. Different industry participants in different sections of the online industry will have different age assurance capabilities, which may change over time as technology develops. All industry participants will continue to look for ways to collaborate and contribute proactively to implement appropriate controls to protect children from accessing or being exposed to class 1C and class 2 material, whether through age assurance or through other complementary measures. This may include for example:

- (a) engaging with other industry participants, eSafety and other interested stakeholders on different age assurance options through government-led technology trials and consultation processes;

- (b) collaborating on the development of improved national and international approaches to age assurance and related issues such as the use of children's data, privacy preservation, data security, accessibility and respect for the best interests of children;
- (c) collaborating with domestic and international regulators, NGOs, industry associations and other peak bodies and stakeholders in activities of the kind referred to in paragraphs (a) and (b); and/or
- (d) actively engaging in the Code review process set out in section 7.6.

Where necessary and appropriate, developments in approaches to age assurance and other online safety measures will be considered for incorporation in future versions of this Code.

2 Definitions and interpretation

2.1 Definitions

Terms used in this Code have the meanings given in the OSA or otherwise as set out below:

access control measures means appropriate access controls designed to prevent an Australian end-user who has been identified as a child (via age assurance measures implemented for a relevant service) from proceeding to access the relevant service, the relevant material, or the relevant section of the service as specified in this Code.

age assurance is an umbrella term for a range of methods for assessing a user's age, including both age verification solutions (being solutions that aim to verify the exact age or age range of a given user) and age estimation solutions (being solutions that aim to estimate the exact age or age range of a given user).

Note: For these purposes an age range may, for example, include whether the user is over or under the age of 18.

app distribution service means a service that enables end-users to download apps, where the download of the apps is by means of a carriage service.

appropriate where used to qualify measures required under this Code means that when implemented by relevant industry participants the measures must be demonstrably reasonable, in accordance with section 5.1(b).

appropriate age assurance measures are age assurance measures determined to be appropriate in accordance with this Code by reference to section 5.1(c).

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

Australian end-user means an end-user in Australia.

Category 1 restricted means the 'Category 1 restricted' classification under the National Classification Code,

Category 2 restricted means the 'Category 2 restricted' classification under the National Classification Code.

class 1 material has the meaning given to it under section 106 of the OSA.

Note: This can be summarised as:

- (i) material that is a film, the contents of a film, a computer game, a publication or the contents of a publication, and is:
 - (A) classified as RC under the Classification Act; or
 - (B) has not been classified, but if it were to be classified under the Classification Act, it would be likely to be classified as RC, or

- (ii) material that is not a film, the contents of a film, a computer game, a publication or the contents of a publication, but if it were to be classified in a corresponding way to the way in which a film would be classified under the Classification Act, the material would be likely to be classified as RC.

class 1A material is a subcategory of class 1 material considered by the *Consolidated Industry Codes of Practice for the Online Industry (Class 1A and Class 1B Material)* that is comprised of child sexual exploitation material, pro-terror material, and extreme crime and violence material.

class 1B material is a subcategory of class 1 material considered by the *Consolidated Industry Codes of Practice for the Online Industry (Class 1A and Class 1B Material)* that is comprised of crime and violence material and drug-related material.

class 1C material is a subcategory of class 1 material used for the purpose of this Code that:

- (a) is class 1 material because it describes or depicts specific fetish practices or fantasies; but
- (b) excludes class 1A material.

class 2 material has the meaning given to it under section 107 of the OSA.

Note: This can be summarised as:

- (i) material that is a film, the contents of a film, a computer game, a publication or the contents of a publication, and:
 - (A) is classified as X 18+, R 18+, Category 2 restricted or Category 1 restricted under the Classification Act; or
 - (B) has not been classified, but if it were to be classified under the Classification Act, it would be likely to be classified as X 18+, R 18+, Category 2 restricted or Category 1 restricted; or
- (ii) material that is not a film, the contents of a film, a computer game, a publication or the contents of a publication, but if it were to be classified in a corresponding way to the way in which a film would be classified under the Classification Act, the material would be likely to be classified as X 18+ or R 18+.

class 2A material is a subcategory of class 2 material defined for the purposes of this Code as being comprised of material that is a film, the contents of a film, or material that for the purposes of this Code is otherwise to be treated in a corresponding way to the way in which a film would be classified under the Classification Act that:

- (a) is classified X 18+ under the Classification Act; or
- (b) has not been classified, but if it were to be classified under the Classification Act, it would likely be classified X 18+,

because it depicts actual (not simulated) sexual activity between consenting adults.

Note 1: Certain online image-based material is to be treated in the same way as films under this Code. For example, material in the form of user-generated photographs (such as that which may be posted on a social media service) will be treated as if it was a film, and not as a publication. See the drafting note beneath the definition of 'publication' for further details.

Note 2: This subcategory will not be applicable to material that is a computer game, as there is no equivalent to the X 18+ classification rating for computer games.

Note 3: This subcategory may include 'deepfakes' and other synthetically generated materials to the extent that they depict actual (not simulated) sexual activity.

class 2B material is a subcategory of class 2 material defined for the purposes of this Code as being comprised of material that:

- (a) is class 2 material because it depicts high-impact sexually explicit images (including high-impact nudity); but

(b) excludes class 2A material.

Note 1: This subcategory may include 'deepfakes' and other synthetically generated materials to the extent that they depict high-impact sexually explicit material (including high-impact nudity) that is not class 2A material.

Note 2: In this definition, the reference to 'images' includes both still images and video images.

Classification Act means the *Classification (Publications, Films and Computer Games) Act 1995* (Cth).

Classification Guidelines means the Guidelines for the Classification of Computer Games, the Guidelines for the Classification of Films and the Guidelines for the Classification of Publications.

Classification Guidelines for Computer Games means the *Guidelines for the Classification of Computer Games 2023* as made under the Classification Act.

Classification Guidelines for Films means the *Guidelines for the Classification of Films 2012* as made under the Classification Act.

Classification Guidelines for Publications means the *Guidelines for the Classification of Publications 2005* as made under the Classification Act.

Classification Process means, in relation to a given item of material, the process that would be undertaken by the Classification Board under the Classification Act if required to classify that item of material.

classified means classified under the Classification Act.

Code means this Industry Code of Practice comprised of these Head Terms and the relevant Schedule identified in the Preamble.

Code report means a report described in section 7.3 of this Code.

electronic service has the meaning given in section 5 of the OSA.

end-user means a natural person who is an end-user of a product or online service covered by this Code.

eSafety means the eSafety Commissioner.

first-party app means an app that is provided by the same person who also provides an app distribution service in relation to that app.

high-impact online pornography means class 1C and class 2A material.

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.

Note: In this definition, the reference to 'images' includes both still images and video images.

high-priority restricted category of material means high-impact online pornography and self-harm material.

industry participant means, in relation to a section of the online industry, a member of a group that constitutes that section of the online industry.

material has the meaning given in section 5 of the OSA.

Note: The term 'material' is defined broadly under the OSA as material whether in the form of text, data, speech, music, other sounds, visual images, moving images, or any other form, or any combination of forms. For the avoidance of doubt, 'material' includes a film, the contents of a film, a computer game, a publication or the contents of a publication.

National Classification Code means the *National Classification Code (May 2005)* made under the Classification Act.

online activity has the meaning given in section 134 of the OSA.

Note: This term includes providing a social media service, so far as the service is provided to end-users in Australia; providing a relevant electronic service, so far as the service is provided to end-users in Australia; providing a designated internet service, so far as the service is provided to end-users in Australia; providing an internet search engine service, so far as the service is provided to end-users in Australia; providing an app distribution service, so far as the service is provided to end-users in Australia; providing a hosting service, so far as the service hosts material in Australia; providing an internet carriage service, so far as the service is provided to customers in Australia; and manufacturing, supplying, maintaining or installing equipment that is for use by end-users in Australia of a social media service, relevant electronic service, designated internet service or internet carriage service (in each case in connection with the service).

online pornography means class 1C, class 2A and class 2B material.

OSA means the *Online Safety Act 2021 (Cth)*.

parent means, in relation to an Australian child, a parent or guardian of that child.

Phase 2 Code means this Code and any other Industry Code of Practice made under the OSA in respect of class 1C and/or class 2 material.

Privacy Law means the *Privacy Act 1988 (Cth)*, any industry code made under that Act, and any other Australian law or regulation regulating the management of personal information.

publication has the meaning given in section 5 of the Classification Act, being any written or pictorial matter, but does not include a film, a computer game, or an advertisement for a publication, film or computer game.

Note: This is a statutory term used in the context of Australia's 'National Classification Scheme' and has a distinct meaning to how the same term is used under other legislative and regulatory schemes. Despite the definition of "any written or pictorial matter" appearing rather wide-ranging, it has a very specific treatment in a National Classification Scheme context and is generally limited to magazines, newspapers, serials, periodicals and books.

For the purpose of this Code, 'publication' has the same restricted interpretation. It does not extend to include any and all text-based or image-based material, or other forms of material that might appear to fall within the scope of a plain reading of the definition of publication. For example, material in the form of user-generated text and photographs (such as that which may be posted on a social media service) is not a publication and instead would fall into the wide category described in paragraph (ii) of the note under the definition of class 1 material (see above).

R 18+ means the 'R 18+' classification under the National Classification Code.

RC means the 'Refused Classification' classification under the National Classification Code.

self-harm material is a subcategory of class 2 material defined for the purposes of this Code as being comprised of material that is class 2 material because it encourages, promotes or provides instruction for:

- (a) suicide;
- (b) an act of deliberate self-injury; and/or
- (c) an eating disorder or behaviour associated with an eating disorder.

simulated gambling material is a subcategory of class 2 material defined for the purposes of this Code because it is a computer game that contains simulated gambling and is classified, or would be classified, R 18+ under the Classification Act.

Note: On how simulated gambling is defined, refer to the Guidelines for the Classification of Computer Games. Also visit www.classification.gov.au for more information.

X 18+ means the 'X 18+' classification under the National Classification Code.

2.2 Interpretation

- (a) In this Code, unless the contrary intention appears:
 - (i) where a term is defined in bold, it has that meaning;
 - (ii) headings are for convenience only and do not affect interpretation;
 - (iii) a reference to a statute, ordinance, code or other law includes regulations and other instruments under it and consolidations, amendments, re-enactments or replacements of any of them;
 - (iv) words in the singular include the plural and vice versa;
 - (v) where a word or phrase is defined, its other grammatical forms have a corresponding meaning; and
 - (vi) mentioning anything after the word 'include', 'includes' or 'including' does not limit what else might be included.
- (b) In this Code, where examples are provided of the manner in which a requirement of a particular provision of this Code may be satisfied, these examples should not be read as requiring or limiting the manner in which the relevant provision may be satisfied.

3 Coverage

- (a) This Code applies to class 1C material and class 2 material.
- (b) Unless otherwise stated, this Code applies to both classified and unclassified material.
- (c) This Code does not apply to class 1A or class 1B material.
- (d) The distinctions between the subcategories of class 1 and class 2 material under this Code have been drawn from descriptions of RC, X 18+, R 18+, Category 1 restricted and Category 2 restricted material under the National Classification Code and the Classification Guidelines, along with an understanding of the relative severity and potential for harm associated with different types of material.

Note: The subcategorisation of class 1 and class 2 material reflected in this Code is not currently reflected in the OSA, Classification Act, National Classification Code or Classification Guidelines. The subcategories were originally proposed by eSafety in guidance provided to industry participants in order to help distinguish between different types of class 1 and class 2 material. The purpose of using these subcategories is to recognise the different risk profile of these different types of material, and that industry participants may handle this material in different ways. For the avoidance of doubt, none of these subcategories referring to material classified or otherwise under the National Classification Code and the Classification Guidelines are intended to replace the associated definitions and their application under the National Classification Code and the Classification Guidelines. In the event of any conflict or inconsistency between the subcategories under this Code, and definitions and their application under the National Classification Code and the Classification Guidelines, the definitions and their application under the National Classification Code and the Classification Guidelines will take precedence.

- (e) Industry participants may use different terminology to describe class 1C and class 2 material for different audiences.
- (f) Nothing under this Code requires the industry participant to arrange for any material to be classified or otherwise to replicate the classification functions of the Classification Board. However, where an industry participant applies a compliance measure under this Code that requires the industry participant to identify or distinguish between different subcategories of unclassified class 1 or class 2 material, the industry participant must develop a process for categorising that material in a way that is informed by the Classification Process. In each case, the process developed by the industry participant

will serve as a proxy for the Classification Process and may vary depending on the circumstances in which it is to be applied, including to take into account the nature and volume of material to be categorised. Where the compliance measure is to be applied in relation to a single known item of material, the process may involve a detailed review of that material and may follow the Classification Process more closely than where the compliance measure is to be applied at scale in relation to multiple unknown items of material.

Note: For example, when applying a compliance measure at scale, an industry participant may develop particular flags or triggers in order to identify material that is likely to be class 1C or class 2 material under this Code, where those flags or triggers are framed by reference to factors that would be taken into account pursuant to the Classification Process. Different industry participants may develop different flags or triggers, depending on the nature of the online activities they are undertaking, the nature of the material they are dealing with, and other relevant factors.

- (g) The nature of the Classification Process, and the variety of factors that will be relevant to take into account, along with the challenges of assessing material at scale, means that there is an inherent risk of different entities reaching different conclusions in relation to the categorisation of material under this Code. The fact that an industry participant:
 - (i) has categorised a given item of material in a different way to another industry participant, or in a different way to eSafety; or
 - (ii) has not identified every item of class 1C or class 2 material on a service provided by the industry participant,

will not of itself be an indicator that the industry participant has failed to comply with this Code.

4 Online safety objectives

The following online safety objectives are used in this Code:

- (a) **Objective 1:** Protect and prevent children in Australia from accessing or being exposed to class 1C and class 2 material.
- (b) **Objective 2:** Provide Australian end-users with effective information, tools and options to limit access and exposure to class 1C and class 2 material.

5 Compliance

5.1 Compliance measures

- (a) Each industry participant will follow the process set out in section 5.2 of this Code in order to identify and implement compliance measures that recognise the importance of the applicable online safety objectives specified in section 4 of this Code.
- (b) It is the responsibility of each industry participant to be able to demonstrate that the steps it has taken to implement the applicable compliance measures are reasonable, taking into account:
 - (i) the importance of the applicable online safety objectives specified in section 4 of this Code;
 - (ii) where relevant, the risk profile of the industry participant as set out in an applicable schedule;
 - (iii) the importance of protecting and promoting human rights online, including the right to freedom of expression, the right not to be subjected to arbitrary or unlawful interference with privacy, the right to protection from exploitation,

violence and abuse, and the rights and best interests of children, including associated statutory obligations;

Note: In this context, the rights of children include the rights recognised in the United Nations Convention on the Rights of the Child.

- (iv) the product or service in question, including its function, purpose, size/scale and maturity as well as the capacity and capabilities of the industry participant providing the product or service;
 - (v) in relation to a breach of applicable terms of use for an online service in relation to class 1C or class 2 material:
 - (A) the nature of the material and the extent to which the breach is inconsistent with online safety for end-users in Australia; and
 - (B) the extent to which the steps taken will or may reasonably be expected to achieve the online safety objectives specified in section 4 of this Code;
 - (vi) whether the steps taken are proportionate to the level of risk to online safety for end-users in Australia as a result of the material; and
 - (vii) other considerations set out in this Code.
- (c) In determining appropriate age assurance measures for the purpose of this Code:
- (i) service providers should take into account the technical accuracy, robustness, reliability and fairness of the solution for implementing the measure;

Note: While an industry participant should take reasonable steps to ensure that its age assurance measures cannot be circumvented, the fact that some end-users may have been able to circumvent the measures implemented will not of itself establish that those measures were not appropriate.

- (ii) appropriate age assurance measures must include reasonable steps to assess whether an Australian end-user is at least 18 years of age;
- (iii) service providers must consider whether age assurance measures have been designed to comply with Privacy Laws and whether the impact on user privacy of any such measures for a service is proportionate to the online safety objectives specified in section 4 of this Code;

Note: Privacy Laws may have a bearing on the design of any age assurance mechanisms implemented by a service provider. A service provider should consider conducting a privacy impact assessment of any age assurance measures they implement, to assist with the service provider's assessment of both positive and negative privacy impacts of those measures and ensure any relevant privacy notices are given, and other steps are taken, as required by Privacy Laws.

- (iv) service providers must consider the interaction between measures which require age assurance in this Code, and other applicable Australian laws which may require age assurance for the same product or service, including how to best achieve the online safety objectives specified in section 4 of this Code whilst minimising the collection of personal information;
- (v) examples of age assurance measures that will be considered appropriate for the purposes of this Code include:
 - (A) matching of photo identification;
 - (B) facial age estimation;
 - (C) credit card checks;

- (D) digital identity wallets or systems;
- (E) attestation by a parent of age or whether an Australian end-user is a child;
- (F) use of artificial intelligence technology to estimate age based on relevant data inputs;
- (G) other measures meeting the requirements of section 8 (Confirmation of age) of the Online Safety (Restricted Access Systems) Declaration 2022; and
- (H) relying upon appropriate age assurance measures implemented in respect of the relevant end-user by: (1) another party (whether another industry participant, government agency, a third party vendor or another third party) and confirmed by an age signal or other mechanism provided to the service provider by that other party; or (2) the service provider in respect of another service as contemplated in clause 5.1(c)(vi),

although this list is not comprehensive and additional age assurance measures may also be considered appropriate;

(vi) where:

- (A) a service provider provides a service that is subject to this Code;
- (B) the service provider also provides another service that is subject to this Code or another Phase 2 Code;
- (C) the service provider has appropriate age assurance measures in place for accessing material on at least one of the services; and
- (D) the relevant end-user has agreed for age assurance signals or settings to be shared between the services, such as by associating both services with a centralised account,

the provider may satisfy a requirement under this Code to implement appropriate age assurance measures for material on either service by sharing an age signal or other age-related settings generated by the age assurance measures in place for the other service, whether via a centralised account or otherwise.

Note: There may be technical or other reasons why it is not feasible or practicable to facilitate this sharing approach between services. Where a service provider does adopt this approach, the age assurance measures can be implemented at a point of the service provider's choosing, which could include when the end-user establishes a centralised account or at another point, provided that the measures are applied at a point that satisfies the relevant requirement under this Code.

(vii) examples of age assurance measures that will not be considered appropriate for the purposes of this Code include:

- (A) requiring a user to self-declare their own age or whether the user is a child (without more); and
- (B) contractual restrictions on the use of the relevant service by children (without more).

(d) In some cases, after taking all relevant considerations into account, it may be appropriate for an industry participant to take no steps to implement an applicable compliance measure.

- (e) Such steps taken by an industry participant to implement applicable compliance measures should be designed to be both effective and scalable and, as appropriate, should be supported by appropriate policies, procedures, systems and technologies.
- (f) No compliance measure specified in this Code will require an industry participant to take a step that the industry participant is already required to take under another industry code or industry standard made under the OSA.

Note: The intent is to avoid duplication between compliance measures that apply under the class 1A and class 1B codes and standards and those that apply under this Code. To the extent there is duplication, each industry participant should only be required to comply with the relevant measure under one instrument. This applies equally both to age assurance measures and to other compliance measures that may be required under this Code.

5.2 Process to identify compliance measures

In order to identify applicable compliance measures for class 1C and class 2 material in relation to an online activity, each industry participant will identify the code applicable to that activity (see Preamble) and take the following steps:

(a) **Step 1: Risk profile**

If the Schedule differentiates between online activities based on their risk profile and requires a risk assessment, the industry participant will either

- (i) assess the level of risk associated with the online activity and will assign a risk profile to that activity in accordance with the criteria set out in the Schedule; or
- (ii) prior to the date this Code comes into effect, and in lieu of carrying out a risk assessment, automatically assign the highest risk profile contemplated by the Schedule to that activity.

The Schedule may define different risk tiers for the purposes of assigning a risk profile. In this case, the tiers are intended to represent an overall level of risk relative to other online activities within the same section of the online industry (with 'Tier 3' representing lower level of relative risk, 'Tier 2' representing a moderate level of relative risk, and 'Tier 1' representing a higher level of relative risk). The tiers are not intended to represent a level of risk relative to other online activities within other sections of the online industry (that is, a Tier 1 activity under one Schedule will not necessarily carry the same level of absolute risk as a Tier 1 activity under another Schedule).

Where a risk assessment is required under a Schedule, the industry participant must conduct an initial risk assessment as soon as practicable and in any case no later than 6 months after the date this Code comes into effect in accordance with section 7.1. An industry participant must carry out subsequent risk assessments in accordance with the requirements set out on the applicable Schedule.

The industry participant will, at eSafety's request, notify eSafety of the risk profile it has assigned to the online activity or how its online activity, including its service or device type, is categorised under this Code, together with the participant's reasons for assigning that category.

Note: To inform eSafety as to how the Code applies to a participant's online activities, eSafety may seek an explanation from an industry participant as to how it has assessed risk or how it has assessed its online activities to fall into specific categories of services/devices. For example, a participant that is not required to undertake a risk assessment because a Schedule exempts particular categories of services from a risk assessment, will, upon request, notify eSafety that its service falls within the exempted category and the reasons for making this assessment. A participant may also be requested to provide details around its assessment where no risk tiering or exemptions apply.

Irrespective of the risk profile assigned by the industry participant, ultimately the risk profile for a given online activity will depend on the objective criteria specified in the Schedule. However, if the industry participant has automatically assigned the highest risk

profile to an activity in accordance with section 5.2(a)(ii), it must notify eSafety of that risk profile on or before the date this Code comes into effect.

If the Schedule does not differentiate between online activities based on their risk profile, then the industry participant may proceed directly to Step 2.

(b) **Step 2: Implementation of compliance measures**

In accordance with the terms of the relevant Schedule, the industry participant must implement any applicable compliance measures, in accordance with section 5, as set out in the Schedule. In some cases, no compliance measures will apply to the industry participant under the Schedule. The industry participant may also define and implement additional compliance measures not set out in the Schedule.

(c) **Step 3: Reports relating to technical feasibility and practicability**

If requested in writing to do so by eSafety, the industry participant must give to eSafety, within a reasonable period, a report:

(i) that describes:

(A) the cases in which it was not, or would not, be technically feasible; or

(B) the cases in which it was not, or would not, be reasonably practicable,

for the industry participant to take steps to implement a compliance measure identified in the Schedule involving systems or technologies of a particular kind; and

(ii) to the extent that there are alternative actions that are technically feasible and reasonably practicable for the industry participant, that describes the alternative actions taken by the industry participant.

The report must provide justification for the actions described, and the conclusions, in the report.

5.3 Presence of class 1C and class 2 material will not necessarily establish non-compliance

The presence of class 1C or class 2 material on a product or service, or the fact that a particular end-user may have been exposed to or accessed class 1C or class 2 material on or via a product or service, does not of itself establish a failure by the industry participant responsible for that product or service to have the processes in place required by this Code or that the industry participant has otherwise failed to comply with its obligations under this Code. In particular, this Code acknowledges that compliance measures designed to proactively detect or control exposure or access to class 1C or class 2 material on or via a product or service may not be successful in all cases.

6 Industry participants not required to undertake certain steps or breach Australian laws or regulations

6.1 Industry participants not required to undertake certain steps

This Code does not require any industry participant to undertake steps that do the following:

(a) implement or build a systematic weakness, or a systematic vulnerability, into a form of encrypted service or other information security measure;

Note: Examples of 'other information security measures' include private firewall configurations, VPN tunnels and private networking links, which work directly or complement encryption to protect legitimate cybersecurity and data integrity interests.

- (b) implement or build a new decryption capability in relation to encrypted services;
- (c) render methods of encryption less effective;
- (d) undertake monitoring of private communications between end-users;

Note: In considering whether an industry participant has taken reasonable steps to implement a particular compliance measure under this Code, it will be relevant for the industry participant to take into account the desirability of not intruding upon, and otherwise maintaining the privacy and integrity of, private communications between end-users. However, where indicated in the Schedule, it may be appropriate for an industry participant to take steps that involve analysis of behavioural signals and other data or trends.

- (e) share, either directly or through an intermediary such as a relevant industry association, with another industry participant any information:
 - (i) that comprises any trade secret or other commercially-sensitive information about its business, organisation or other undertaking;
 - (ii) that may raise concerns about the potential anti-competitive effects of sharing that information; or
 - (iii) that the industry participant is prohibited from disclosing pursuant to a duty of confidence or under another law or regulation by which the industry participant is bound;
- (f) verify or publish the real identity of any end-user (though an industry participant may be required to implement compliance measures that are intended to prevent end-users from exploiting anonymity or other identity shielding techniques to share class 1C or class 2 material);
- (g) use or disclose personal information of an Australian end-user (or do anything else) in a way that would put the industry participant in breach of any applicable Privacy Law;
- (h) use or disclose personal information of a foreign end-user (or do anything else) in a way that would put the industry participant in breach of any law or regulation relating to the management of personal information of that foreign end-user; or
- (i) take any action within Australia that is prohibited under another Australian law or regulation by which the industry participant is bound.

6.2 Effect of section 6.1

- (a) An industry participant cannot use section 6.1 to excuse it from otherwise complying with an applicable Code requirement.
- (b) Where an industry participant is concerned that compliance with a Code requirement is reasonably likely to result in the industry participant taking steps that would do anything described in section 6.1(a) to 6.1(i), the industry participant must either:
 - (i) communicate to eSafety the industry participant's specific concerns about complying with the Code requirement; or
 - (ii) take an alternative approach to meeting the Code requirement that does not require the industry participant to take steps described in section 6.1(a) to 6.1(i).

6.3 Lawful conduct

Nothing in this Code prohibits any industry participant from engaging in conduct for which, while ordinarily unlawful, a lawful exception, exclusion or protection from liability exists under Australian law and applies to that participant's conduct. For example, see section 474.24 of the *Criminal Code Act 1995* (Cth).

6.4 No breach of Code where action required under another Australian law

An industry participant will not be in breach of this Code merely where it takes an action in Australia that is required by another Australian law or regulation by which the industry participant is bound.

7 Code administration

7.1 Commencement

- (a) This Code comes into effect six months from the date of registration by eSafety.
- (b) If after the effective date in section 7.1(a) eSafety notifies an industry participant that it is non-compliant with a measure required under this Code and the participant has reasonable grounds for not being fully compliant, the participant will not be in breach provided that it can demonstrate to eSafety's reasonable satisfaction that it is working towards achieving compliance on or before the first anniversary of the date of registration.

Note: Examples of reasonable grounds for not being fully compliant by the date specified in section 7.1(a) may include circumstances where significant engineering or system changes are required in order to implement a measure.

7.2 Enforceability

- (a) If an industry participant fails to comply with this Code, then eSafety may make use of their enforcement powers pursuant to Part 9, Division 7, of the OSA.
- (b) Industry participants are expected to keep records of the compliance measures they have implemented to comply with this Code for a period of two years.

7.3 Code reporting

- (a) Where required by this Code, an industry participant will submit a report to eSafety on its compliance with this Code (a **Code report**) containing the information set in the applicable Schedule.
- (b) If an industry participant identifies any material in a Code report as the industry participant's confidential information, eSafety must maintain such material in confidence.
- (c) Where an industry participant must submit a Code report to eSafety for multiple online activities, the industry participant may submit a consolidated Code report that covers all those activities.
- (d) An industry participant may satisfy an obligation to submit a Code report by referring eSafety to material provided through other existing voluntary transparency reporting that the industry participant makes available, provided that such reporting adequately addresses the reporting requirements set out in this section 7.3.
- (e) To avoid duplication in reporting to eSafety, an industry participant will not be required to provide a Code report about a matter under this Code where that matter has already been reported to eSafety pursuant to another requirement under the OSA, provided that the industry participant has drawn eSafety's attention to the previous report and explained why a further report under this Code is not required as a consequence.

Note: The requirements for submitting Code reports are set out in the applicable Schedule. An industry participant should contact eSafety if it has concerns about meeting any of the requirements, including the relevant timeframe for a report or where it encounters difficulties of (dis)aggregation of data.

7.4 Complaints about Code compliance

- (a) This section applies where the Schedule specifies that the industry participant must enable an Australian end-user to make a complaint to an industry participant about the industry participant's compliance with this Code.
- (b) Except where the Schedule specifies that an industry participant may refer a complaint in section 7.4(a) to eSafety or another participant that is better placed to deal with the complaint, an industry participant must:
 - (i) investigate every complaint that is made to that industry participant, other than where the complaint appears frivolous or vexatious or otherwise not made in good faith; and
 - (ii) complete the investigation, and notify the complainant of the outcome, within a reasonable time (taking into account the subject matter of the complaint and the online safety objectives specified in section 4 of this Code).

7.5 Ongoing role of industry representatives

The industry representatives responsible for leading the development of this Code (as listed in the Preamble) will:

- (a) play a role in the proactive promotion of this Code to both industry participants and Australian end-users;
- (b) to provide guidance to relevant industry participants;
- (c) engage with industry bodies and associations that represent other sections of the online industry on matters relating to online safety;
- (d) engage with eSafety's relevant advisory committee or other relevant stakeholder forum on the general operation of this Code;
- (e) raise concerns with eSafety about this Code on behalf of industry participants; and
- (f) participate in ongoing review and revision of this Code as contemplated in section 7.6 of this Code.

Over time, additional industry representatives may emerge and/or choose to participate in the administration of this Code.

7.6 Code review

- (a) This Code will be reviewed after it has been in operation for two years, and thereafter at three yearly intervals.
- (b) Each review will be coordinated by the industry representatives responsible for leading the development of this Code (as listed in the Preamble) and will be based on the input of industry participants, eSafety, and other interested stakeholders.
- (c) The industry representatives responsible for each review will seek input on the terms of reference from industry participants, eSafety and other interested stakeholders (including young people).
- (d) Each review will at a minimum consider:
 - (i) the continued relevance of the risk assessment methodology and compliance measures (including Code reports) set out in this Code;

- (ii) any developments that have created gaps in this Code that should be filled or rendered compliance measures set out in this Code unnecessary;
 - (iii) any potential changes in risk vectors for industry sections or industry sub-sections;
 - (iv) any developments, including technological, that may impact on the compliance measures that apply under this Code, including as a result of investment and research activities undertaken by industry participants;
 - (v) areas that have caused confusion for industry participants;
 - (vi) how industry participants have complied with this Code, including results of any compliance monitoring, insights from complaints handling (including areas of systemic non-compliances) and insights in relation to the handling of appeals by Australian end-users against decisions taken to comply with Code and industry participant's policies or terms and conditions;
 - (vii) how successful or unsuccessful this Code has been in achieving the online safety objectives specified in section 4 of this Code;
 - (viii) the public's and other stakeholders' awareness, understanding and response to this Code;
 - (ix) any changes to the National Classification Scheme as agreed between the Australian, State and Territory governments, including any changes to the Classification Act, the National Classification Code, the Classification Guidelines or the Classification Process; and
 - (x) other matters raised by eSafety or other government bodies in relation to this Code.
- (e) The industry representatives responsible for each review will consult with eSafety on a confidential basis prior to releasing a draft revised code for public comment.
 - (f) The industry representatives responsible for each review will ensure that a draft of the revised code will be published and members of the public, relevant sections of the industry and other relevant stakeholders are invited to make a submission about the draft within a public consultation period that runs for at least 30 days.
 - (g) The industry representatives responsible for each review will consider submissions that were received from the public, participants in the relevant sections of the industry and other relevant stakeholders within the public consultation period.
 - (h) Once the review has been completed and where, as a result of a review, the code(s) have been revised, the industry representatives responsible for each revision will submit the revised code(s) for registration to eSafety.
 - (i) Notwithstanding any of the above, any proposed changes to this Code will be implemented in accordance with the applicable process in Part 9, Division 7, Subdivision C of the OSA.