

Schedule 8 – Equipment Online Safety Code (Class 1C and Class 2 Material)

1 Structure

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

2 Scope

This Code only applies to the following types of persons:

- (a) Manufacturers, to the extent that equipment is for use by Australian end-users;
- (b) Suppliers, to the extent that equipment is for use by Australian end-users; and
- (c) Maintenance and installation providers who provide maintenance or installation services to Australian end-users,

together known as **equipment providers**; and

- (d) OS providers, to the extent that equipment is for use by Australian end-users.

This Code only applies to equipment to the extent that it is hardware.

3 Definitions

Unless otherwise indicated, terms used in this Code have the meanings given in the Head Terms or as otherwise set out below.

child account or profile means an account, profile or similar that can be set up on a device for a young Australian child under the age of thirteen.

Note: A provider may have child accounts or profiles that also cover additional age groups, or different age options for child accounts or profiles, so long as they have a child account or profile that can be set up for Australian children under the designated age as a minimum and that the requirements of measure 2 below are met with respect to that child account or profile.

device in this Code has the same meaning as, and is used interchangeably with, equipment.

equipment means equipment that is for use by Australian end-users of:

- (a) a social media service;
- (b) a relevant electronic service;
- (c) a designated internet service; or
- (d) an internet carriage service,

in connection with that service.

equipment provider means a:

- (a) manufacturer;
- (b) supplier;
- (c) maintenance provider; or
- (d) installation provider.

gaming device means a device designed to enable Australian end-users to play online games with other end-users.

Note: A gaming device may be an interactive (Tier 1), secondary (Tier 2) or non-interactive (Tier 3) device.

installation provider means a person who installs equipment for Australian end-users.

interactive (Tier 1) device means equipment that satisfies all of the following:

- (a) is user-interactive;
- (b) is personal and portable (may be carried with the end-user);
- (c) is capable of operation without the use of any other interactive (Tier 1) device; and
- (d) general internet browsing through a screen or display capable of displaying video or images is an intended significant function of the device.

Note: Guidance on the application of this definition is set out in clause 6 below. The definition of an interactive (Tier 1) device includes any gaming devices with general internet browsing functionality, provided that the functionality is not attained through unauthorised third-party software, modifications, tools, 'hacks', or other methods that may breach any applicable terms of use.

maintenance provider means a person who maintains equipment for Australian end-users.

manufacturer means a person who:

- (a) manufactures equipment for the purposes of supply (whether by way of sale, lease, hire or hire purchase) to Australian end-users, including by:
 - (i) holding itself out to the public as the manufacturer of the equipment;
 - (ii) causing or permitting its name, a name by which it carries on business or a brand, or its mark to be applied to equipment supplied by the person as the manufacturer of the equipment;
 - (iii) causing or permitting another person, in connection with:
 - (A) the supply or possible supply of equipment by that other person; or
 - (B) the promotion by that other person by any means of the supply or use of equipment;to hold it out to the public as the manufacturer of the equipment; or
- (b) where there is no manufacturer falling within (a) above, imports equipment into Australia for the purposes of supply (whether by way of sale, lease, hire or hire purchase) to Australian end-users (provided that if a distributor imports on behalf of another entity, that other entity will be considered the manufacturer).

Note: This definition excludes offshore entities who are only involved in the physical manufacture of equipment (e.g. factories overseas). Further, in relation to (b) above, equipment can be imported into Australia outside of formal distribution channels such as by an unrelated third party (e. g. parallel import). In this situation, the person who imports the equipment (without authorisation from the manufacturer) is considered the manufacturer.

non-interactive (Tier 3) device means equipment that is not an interactive (Tier 1) device or a secondary (Tier 2) device.

operating system means a designated internet service that consists of an operating system for an interactive (Tier 1) device that is provided to Australian end-users.

Note: An operating system will only fall within the scope of this Code if it is a designated internet service, that is, where the operating system either allows end-users to access material using an internet carriage service, or delivers material to persons having equipment appropriate for receiving that material, where delivery is by means of an internet carriage service.

OS provider means a person who:

- (a) is the provider of an operating system; and
- (b) controls the final overall operating system for the device.

Note: The OS provider may also be the manufacturer of the interactive (Tier 1) device, or a third-party OS provider who provides the operating system to the manufacturer for use in the manufacturer's (Tier 1) interactive devices. This definition recognises that there may be more than one "provider" of an operating system due to the supply chain used for different devices. For example, a person may provide an operating system to a manufacturer and a manufacturer may provide that operating system to end-users. The OS provider for the purposes of this Code is the provider that controls the final overall operating system and therefore controls the engineering decisions related to the final version of the features and settings made available to end-users by way of the operating system on the device. As an example, a provider of an open-source operating system is not an OS provider of that operating system for the purposes of this Code as they do not control the final overall operating system of a device which incorporates that open-source operating system.

other interactive device means a device other than an interactive (Tier 1) device that:

- (a) has general internet browsing functionality as an intended significant function of the device; and
- (b) has functionality that:
 - (i) enables an end-user to use their device to share material with end-users of other devices; or
 - (ii) permits an end-user to view or search for other end-users for the purposes of communicating with them.

Note: For the avoidance of doubt, a "companion app" that merely enables an end-user to interact with and/or control the device is not sufficient, without more, to meet any of the limbs in (a) or (b).

restricted account or profile means an account, profile or similar that can be set up on a device for an Australian end-user under the age of 18.

secondary (Tier 2) device means equipment that is not an interactive (Tier 1) device and satisfies all of the following:

- (a) is user-interactive;
- (b) may be personal or communal (intended for use by more than one end-user);
- (c) is capable of operation with or without the use of an interactive (Tier 1) device; and
- (d) general internet browsing is not an intended significant function of the device.

Note: Guidance on the application of this definition is set out in clause 6 below.

supplier means a person who supplies, by way of sale, lease, hire or hire purchase, equipment to Australian end-users (e.g., retailers of equipment), but does not include a person who supplies equipment in the course of:

- (a) performing services (such as maintenance services) on an existing device that has previously been supplied to the end-user by any supplier; or
- (b) replacing equipment that has previously been supplied to the end-user by the supplier, where such replacement does not involve a new sale, lease, hire or hire purchase of equipment in return for payment by the end-user.

Note: The exclusions in (a) and (b) above mean that, for example, a person will not be acting as a supplier when it replaces a device or component of a device in the course of servicing that device (e.g., when providing maintenance services), or where it replaces a device pursuant to warranty or statutory obligations. This includes where the replacement involves a refurbished device. In such circumstances, the "supplier" obligations under this Code will have already been complied with by the original supplier. While it will not be acting as a "supplier" for the purposes of this Code when replacing a device or component in the

course of maintenance services, a maintenance provider will have separate obligations as a maintenance provider under this Code.

user-interactive means a two-way flow of material between a device and an end-user.

4 Role of equipment providers and OS providers

Equipment providers play an important role in manufacturing (or importing), distributing, installing and maintaining equipment for Australian end-users, enabling them to access online services. OS providers provide the operating systems for devices that enable access to online services.

Equipment providers and OS providers are not providers of content services. The measures in this Code are designed to be proportionate to the role equipment and OS providers are able to play in creating and maintaining a safe online environment.

5 Risk profile

A number of different categories of equipment are covered by this Code – interactive (Tier 1) devices, secondary (Tier 2) devices and non-interactive (Tier 3) devices, as well as other interactive devices.

This categorisation reflects the fact that some factors common to each category (such as, for example, whether the device is user-interactive, personal or communal, standalone or only capable of operation with another device or whether the device has general internet browsing as a significant intended function on the device or not) may have an impact on the risks relevant to class 1C and class 2 material on services that can be accessed via the device.

Whilst there are a broad range of devices that may fall into each category, for the purposes of this Code and the compliance measures in this Code, each category is deemed to have a generally equivalent risk profile. However, given the breadth of different devices that could fall into each category some further differentiation is included in some compliance measures within this Code based on device-type where relevant. As such, compliance measures apply equally to all providers falling within each applicable category unless otherwise stated.

Additional guidance on these categories of equipment is included below in clause 6.

6 Guidance on categories of equipment

The definitions of interactive (Tier 1) devices, secondary (Tier 2) devices and non-interactive (Tier 3) devices under this Code are mutually exclusive. The definition of other interactive device is standalone and is intended to ensure that *all* devices other than interactive (Tier 1) devices that have general internet browsing functionality as an intended significant function and certain forms of communications functionality will be subject to relevant measures under this Code.

The table below provides further guidance on the terminology used in some of the definitions to assist with the application and understanding of those definitions. This guidance is not intended to modify or restrict the definitions.

Concept	Explanation	Example
User-interactive	There is a two-way flow of material between that device and the end-user.	<p>A smartphone or tablet is user-interactive as it allows an end-user to input text or speech and can generate material in various forms including text, sound, and visual images (including where material is generated by the device at the user's request using generative artificial intelligence functionality).</p> <p>A router or modem is not user-interactive as it does not generate material that an end-user can interact with.</p>

Concept	Explanation	Example
Personal	The equipment is portable and may be carried with the end-user.	Personal equipment such as smartphones, tablets or virtual reality headsets are portable and designed to be carried with the end-user, such that they are more likely to be used by an end-user privately rather than only in communal spaces. A communal smart home device such as a smart TV is not portable.
Communal	The equipment is not personal and generally intended for use by more than one end-user.	Smart TVs, smart screens or smart home devices are used by multiple household members.
Standalone	Is capable of being used without the use of another interactive (Tier 1) device.	A smart watch requires a connected smart phone to operate and would not be considered standalone. A personal computer can be operated without the use of any other interactive (Tier 1) device and would be considered standalone.
General internet browsing	General internet browsing is an intended significant function of the device. A device with general internet browsing as an intended significant function includes a device that: <ul style="list-style-type: none"> enables general internet browsing through an app or functionality created by the manufacturer or OS provider for that purpose, such as a web browser; and provides general access to the internet, with the ability to display text, images and videos. 	An e-book reader's intended significant function is to enable end-users to read e-books, rather than browse the internet. Additionally, e-book readers may have limited or no web-browsing apps or functionality, so general internet browsing is unlikely to be an intended significant function. One of a personal computer's intended significant function is to enable end-users to use web browsers and web-based applications, so general internet browsing is likely to be an intended significant function. Gaming devices that do not have general internet browsing functionality except through unauthorised third-party software, modifications, tools, 'hacks' or other methods that may breach any applicable terms of use do not have general internet browsing as an intended significant function of the device. A smart screen's intended significant function is to enable end-users to watch or stream content for general entertainment purposes via pre-loaded apps, rather than enabling users to interact with the device or services on the device, or browse the internet.

7 Compliance measures

The table below contains compliance measures for equipment providers and OS providers for equipment that is for use by Australian end-users.

The table also sets out guidance on the implementation of some measures. The guidance notes are not intended to be binding, but are rather provided to provide further guidance on the way that a relevant industry participant may choose to implement a measure.

Compliance measures under this Code are applied to interactive (Tier 1) devices, secondary (Tier 2) devices, non-interactive (Tier 3) devices and other interactive devices. All providers should have regard to relevant guidance in this Code.

Certain compliance measures will only apply to certain categories of device (as specified in the column titled "Category of device") or to certain categories of provider (as specified in the column

titled "Category of provider"). If the measure is expressed to apply to 'equipment providers', then it applies to all equipment providers (but not OS providers).

8 Compliance measures for class 1C and class 2 material

No.	Category of device	Category of provider	Compliance measure
1.	interactive (Tier 1) devices	OS providers	<p>Account set-up</p> <p>An OS provider must enable Australian end-users to set up child accounts or profiles and restricted accounts or profiles for use on interactive (Tier 1) devices.</p> <p><u>Note:</u> The Phase 1 codes and standards require OS providers of children's interactive devices (as defined in the Phase 1 codes and standards) to set default safety settings for Australian end-users for children's interactive devices to the most restrictive privacy and location settings provided for on that device. Measures 1 to 4 of this Code supplement that existing requirement.</p> <p><u>Note:</u> Where an account or profile is set up for an end-user, the OS provider may apply defaults and settings as required by measures 2 and 3 below based on the age provided by, or on behalf of, the end-user as part of that set-up process. Default settings must remain in place whilst the end-user's submitted age remains less than the relevant threshold required by measure 2 or 3 (as applicable) noting, for the avoidance of doubt, that default settings may be altered by end-users, subject to sub-measure 2 b).</p>
2.	interactive (Tier 1) devices	OS providers	<p>Defaults and settings for child accounts or profiles</p> <p>An OS provider must:</p> <p>a) have:</p> <ol style="list-style-type: none"> i. appropriate default safety settings for child accounts or profiles set up under measure 1 that reduce the risk of such accounts or profiles being used to view online pornography; and ii. for interactive (Tier 1) devices that are mobile phones or tablets, tools, features and/or settings available to Australian end-users that can be used to reduce the risk of unsolicited contact (including unsolicited contact containing class 1C or class 2 material) via such child accounts or profiles; and <p>b) only permit the default safety settings, and tools, features and/or settings, referred to in sub-measure a) to be adjusted via an adult account or profile that is linked to the child account or profile.</p> <p>Default safety settings may reduce the risk of child accounts or profiles being used to view online pornography in a number of ways for the purposes of sub-measure a)i.. Examples of settings that could be applied (noting that not all will be possible for all services available on the device) could include, for example:</p> <ul style="list-style-type: none"> • automatic blocking of websites that are dedicated to online pornography; • detecting nudity and employing techniques such as blurring or warning messages; or • provision of other tools, features and/or settings that reduce the risk. <p>Tools, features and/or settings may reduce the risk of unsolicited contact (including unsolicited contact containing class 1C or class 2 material) to child accounts or profiles in a number of ways for the purposes of sub-measure a)ii.. Examples of tools, features and/or settings that could be applied (noting that not all will be possible for all services available on the device) could include, for example:</p>

No.	Category of device	Category of provider	Compliance measure
			<ul style="list-style-type: none"> an ability for the end-user to block or filter certain features or functionality that present higher risks in relation to online pornography; enabling adult account or profile holders to pre-approve or block contacts on linked child accounts or profiles to help avoid unwanted contact or limit contact to trusted users; or provision of other tools, features and/or settings that reduce the risk. <p><i>Note:</i> It is acknowledged that default safety settings, and other tools, features and/or settings, on a device may not operate to reduce risk on all services that could be available on the relevant device. Some safety settings may relate to use of a particular service, or group of services, on the relevant device. Many safety settings may only operate across the OS provider's own services offering (not across all third-party services).</p> <p>Guidance:</p> <p><i>In addition to the default safety settings required by sub-measure a)i., an OS provider may have a range of additional safety tools, features and/or settings available to users on the device (noting sub-measure a)ii. as well as measures 3b), 8 and 9 below). It is not expected that an OS provider will have <u>all</u> of those on by default, acknowledging that to default all on may undermine the device's functionality or render it inoperable, and many may require user input to set-up. An OS provider will have complied with sub-measure a)i. if it has default safety settings as required by that sub-measure, even if it also has other safety settings that are not on by default for reasons such as those outlined in this Guidance.</i></p>
3.	interactive (Tier 1) devices that are mobile phones or tablets	OS providers	<p>Defaults and settings for restricted accounts or profiles</p> <p>For interactive (Tier 1) devices that are mobile phones or tablets, an OS provider must have:</p> <ol style="list-style-type: none"> default safety settings for restricted accounts or profiles set up under measure 1 that reduce the risk of such accounts or profiles being used to view online pornography; and tools, features and/or settings available to Australian end-users that can be used to reduce the risk of unsolicited contact (including unsolicited contact containing class 1C or class 2 material) via such restricted accounts or profiles. <p>Default safety settings may reduce the risk of restricted accounts or profiles being used to view online pornography in a number of ways for the purposes of sub-measure a). Examples of settings that could be applied (noting that not all will be possible for all services available on the device) could include, for example:</p> <ul style="list-style-type: none"> automatic blocking of websites that are dedicated to online pornography; detecting nudity and employing techniques such as blurring or warning messages; or provision of other tools, features and/or settings that reduce the risk. <p>Tools, features and/or settings may reduce the risk of unsolicited contact (including unsolicited contact containing class 1C or class 2 material) to restricted accounts or profiles in a number of ways for the purposes of sub-measure b). Examples of tools, features and/or settings that could be applied (noting that not all will be possible for all services available on the device) could include, for example:</p>

No.	Category of device	Category of provider	Compliance measure
			<ul style="list-style-type: none"> • an ability for the end-user to block or filter certain features or functionality that present higher risks in relation to online pornography; • enabling account holders to pre-approve or block contacts on restricted accounts or profiles to help avoid unwanted contact or limit contact to trusted users; or • provision of other tools, features and/or settings that reduce the risk. <p><u>Note:</u> It is acknowledged that default safety settings, and other tools, features and/or settings, on a device may not operate to reduce risk on all services that could be available on the relevant device. Some safety settings may relate to use of a particular service, or group of services, on the relevant device. Many safety settings may only operate across the OS provider's own services offering (not across all third-party services).</p> <p><u>Note:</u> If an OS provider has default safety settings meeting the requirements in sub-measure a) that assist more Australian end-users (i.e. not only Australian children) to reduce the risk of their accounts or profiles being used to view online pornography when using the device, such measures will be treated as default safety settings that meet sub-measure a). Similarly, if an OS provider has tools, features and/or settings available to more Australian end-users (i.e. not only Australian children) that reduce the risk of unsolicited contact, such measures will be treated as tools, features and/or settings that meet sub-measure b).</p> <p>Guidance:</p> <p><i>In addition to the default safety settings required by sub-measure a), an OS provider may have a range of additional safety tools, features and/or settings available to users on the device (noting sub-measure b) as well as measures 8 and 9 below). It is not expected that an OS provider will have <u>all</u> of those on by default, acknowledging that to default all on may undermine the device's functionality or render it inoperable, and many may require user input to set-up. An OS provider will have complied with sub-measure a) if it has default safety settings as required by that sub-measure, even if it also has other safety settings that are not on by default for reasons such as those outlined in this Guidance.</i></p>
4.	interactive (Tier 1) devices	OS providers	<p>Facilitating tools, features and/or settings on other OS provider services</p> <p>Where:</p> <ul style="list-style-type: none"> a) an OS provider provides the operating system for an interactive (Tier 1) device; b) the OS provider also offers any of the OS provider's own services on the interactive (Tier 1) device; and c) the OS provider has obligations under other Phase 2 codes to have tools, features and/or settings to mitigate risks to Australian children on such services, <p>that OS provider must share information about whether an account or profile is a child account or profile, or a restricted account or profile, with those services, or otherwise restrict a child account or profile, or a restricted account or profile, for those services, as necessary to facilitate such tools, features and/or settings.</p>
5.	interactive (Tier 1) devices	OS providers	<p>On-device measures for adult accounts or profiles</p> <p><u>Note:</u> The Phase 1 codes and standards require OS providers to make tools available to Australian end-users to assist in restricting the unauthorised access to and operation of an adult's interactive (Tier 1) device by a child. The following measure supplements that existing requirement.</p>

No.	Category of device	Category of provider	Compliance measure
			An OS provider for an interactive (Tier 1) device must permit an Australian end-user with an adult account or profile to adjust safety settings to a more restrictive level for a device which they intend to give to, or share with, a child.
6.	interactive (Tier 1) devices	manufacturers and OS providers	<p>Information regarding default measures</p> <p>A person who is a manufacturer of an interactive (Tier 1) device or an OS provider must ensure that easily accessible information in plain language is made available to Australian end-users about:</p> <ol style="list-style-type: none"> how to set up child accounts or profiles; how to set up restricted accounts or profiles; the default safety settings it has applied pursuant to measure 2a)i. and 3a) above; how to adjust those default safety settings; the tools, features and/or settings it has available pursuant to measure 2a)ii. and 3b) above; and how to adjust those tools, features and/or settings. <p>Guidance:</p> <p><i>Examples of how information can be made available include:</i></p> <ul style="list-style-type: none"> <i>use of a QR code on, or inside, packaging that leads to a website with information about the equipment's specific online safety features;</i> <i>provision of on-device information such as through the set-up process, or through other periodic or targeted pop-up alerts or notifications on-device about default measures; and/or</i> <i>inclusion of such information in online safety resources.</i>
7.	interactive (Tier 1) devices	manufacturers and OS providers	<p>Cost and application</p> <p>A person who is a manufacturer of an interactive (Tier 1) device or an OS provider must ensure that the person does not impose any additional charge to the end-user for the features and settings described in measures 2, 3 or 5.</p>
8.	interactive (Tier 1) devices	OS providers	<p>Tools, features and/or settings</p> <p><u>Note:</u> The Phase 1 codes and standards require OS providers to develop and implement relevant tools where appropriate within operating systems that allow Australian end-users to help reduce the risk of harm to children when using interactive (Tier 1) devices. The following measure supplements that existing requirement.</p> <p>In addition to the default safety settings and tools, features and/or settings required by measure 2 and 3, an OS provider must develop and implement appropriate tools, features and/or settings that assist Australian end-users to safely manage their experience when using the device including at a minimum managing the risk of exposure to online pornography.</p>

No.	Category of device	Category of provider	Compliance measure
			<p>Examples of how this could be done include:</p> <ul style="list-style-type: none"> • an ability for the end-user to block or permit certain websites (thus enabling end-users to decide whether certain websites should be accessible on the device); • an ability for the end-user to block or permit certain apps or services (thus enabling end-users to decide whether such apps or services should be available on the device); • enabling end-users to pre-approve or block contacts to help avoid unwanted contact or limit contact to trusted users; • to manage the risk of exposure to online pornography: <ul style="list-style-type: none"> ○ an ability for the end-user to block or filter certain features or functionality that present higher risks in relation to online pornography; ○ detecting nudity and employing techniques such as blurring or warning messages; ○ blocking website pop-ups, and advertisements, for online pornography; or • provision of other safety tools, features and/or settings, <p>as well as sharing clear and accessible guidance about the use and effect of such settings.</p> <p><u>Note:</u> It is acknowledged that tools, features and/or settings may not operate to reduce risk on <u>all</u> services that could be available on the relevant device. Some safety tools, features and/or settings may relate to use of a particular service, or group of services, on the relevant device. Many safety tools, features and/or settings may only operate across the OS provider's own services offering (not across all third-party services).</p> <p><u>Note:</u> Assisting end-users to safely manage their experience when using the device does not require assistance that is irrelevant to class 1C or class 2 material.</p> <p>Guidance:</p> <p><i>In implementing these measures, industry participants should also consider the needs and capabilities of children, for example with respect to complexity of language, ease of access etc..</i></p>
9.	other interactive devices	manufacturers	<p>Tools, features and/or settings</p> <p><u>Note:</u> The Phase 1 codes and standards require manufacturers of gaming devices to develop and implement appropriate tools that allow Australian end-users to help reduce the risk of harm to children when using gaming devices. The following measure supplements that existing requirement by adding requirements for all other interactive devices (including gaming devices that are other interactive devices).</p> <p>A manufacturer of an other interactive device must develop and implement appropriate tools, features and/or settings that assist Australian end-users to safely manage the experience of children when using the device including at a minimum managing the risk of exposure to online pornography.</p> <p>Examples of how this could be done include:</p>

No.	Category of device	Category of provider	Compliance measure
			<ul style="list-style-type: none"> • enabling end-users to implement password or PIN protection that restricts access to certain content, apps, or services; • enabling end-users to block certain websites (thus enabling end-users to decide whether certain websites should be accessible on the device) or disable internet browsing; • blocking the ability for other interactive devices to be used by users with accounts designed for children; • for other interactive devices that are also gaming devices: <ul style="list-style-type: none"> ○ enabling Australian end-users to set up an adult account or an account designed for a child within the gaming device; and ○ providing parental and carer controls so that Australian end-users with an adult account can disable or limit internet browsing functionality and disable or limit the playing of some or all games for Australian end-users with an account designed for a child; • for other interactive devices that are linked to, or otherwise used in conjunction with, interactive (Tier 1) devices: <ul style="list-style-type: none"> ○ extending relevant tools, features and/or settings applied to the interactive (Tier 1) device to the other interactive device; • for other interactive devices that are smart TVs: <ul style="list-style-type: none"> ○ parental controls that can be used to restrict use (e.g. viewing, downloading or playing) apps, channels or other programming; ○ use of pin numbers, pass codes or similar features to control access to categories of programming and/or material (e.g. programming and/or material with particular age ratings, or as selected by the user during set-up of the parental controls), <p>as well as sharing clear and accessible guidance about the use and effect of such settings.</p> <p><u>Note:</u> If a manufacturer of an other interactive device has tools, features and/or settings that assist more Australian end-users (i.e. not only Australian children) to safely manage their experience when using the device, such measures will be treated as tools, features and/or settings that meet this measure.</p> <p><u>Note:</u> It is acknowledged that tools, features and/or settings may not operate to reduce risk on <u>all</u> services that could be available on the relevant device. Some safety tools, features and/or settings may relate to use of a particular service, or group of services, on the relevant device. Many safety tools, features and/or settings may only operate across the manufacturer's own services offering (not across all third-party services).</p> <p><u>Note:</u> Tools, features and/or settings applied to accounts designed for children that assist with managing safety risks (including at a minimum the risk of exposure to online pornography) to children will be treated as tools, features and/or settings that meet this measure.</p> <p><u>Note:</u> Assisting Australian end-users to safely manage the experience of children when using the device does not require assistance that is irrelevant to class 1C or class 2 material.</p> <p>Guidance:</p>

No.	Category of device	Category of provider	Compliance measure
			<p><i>In implementing these measures, industry participants should also consider the needs and capabilities of children, for example with respect to complexity of language, ease of access etc..</i></p>
10.	interactive (Tier 1) devices	manufacturers	<p>Provision of information about safe use of equipment online</p> <p><u>Note:</u> The Phase 1 codes and standards require manufacturers of interactive (Tier 1) devices to ensure that certain information is available in the form of online safety resources. The following measure supplements that existing requirement.</p> <p>A manufacturer of interactive (Tier 1) devices must ensure that easily accessible information in plain language with respect to:</p> <ol style="list-style-type: none"> a) the tools, features and/or settings described in measure 8; and b) the role of eSafety, including a link to eSafety’s complaints form, <p>is available in the form of online safety resources.</p> <p>This information must include information about how Australian end-users can limit access to online pornography through use of those tools when using that equipment.</p> <p>Guidance:</p> <p><i>In implementing these measures, industry participants should also consider the needs and capabilities of children, for example with respect to complexity of language, ease of access etc..</i></p> <p><i>A manufacturer of interactive (Tier 1) devices may also choose to provide additional information about the safe use of that device.</i></p> <p><i>Examples of the types of information that could be provided include:</i></p> <ul style="list-style-type: none"> • <i>the risks presented by interactive (Tier 1) devices in respect of online material that is unsuitable for children;</i> • <i>the availability and use of online content filtering or other software; or</i> • <i>how to support a child's safe use of social media services, relevant electronic services and designated internet services where accessible through the equipment.</i>
11.	other interactive devices	manufacturers	<p>Provision of information about safe use of equipment online</p> <p><u>Note:</u> The Phase 1 codes and standards require manufacturers of gaming devices to provide information to Australian end-users about how to support online safety in a child’s use of such devices as well as information where the gaming device has functionality that enables Australian end-users to freely browse the internet (regarding the existence of that functionality). The following measure supplements that existing requirement by adding requirements for all other interactive devices (including gaming devices that are other interactive devices).</p> <p>A manufacturer of an other interactive device must ensure that easily accessible information in plain language is made available to Australian end-users with respect to:</p> <ol style="list-style-type: none"> a) the role of eSafety, including a link to eSafety’s complaints form; and

No.	Category of device	Category of provider	Compliance measure
			<p>b) the tools, features and/or settings described in measure 9.</p> <p>Note: Gaming devices that do not have internet browsing functionality except through unauthorised third-party software, modifications, tools, 'hacks' or other methods that may breach any applicable terms of use do not have functionality that enable Australian end-users to freely browse the internet.</p> <p>Guidance:</p> <p><i>In implementing these measures, industry participants should also consider the needs and capabilities of children, for example with respect to complexity of language, ease of access etc..</i></p>
12.	interactive (Tier 1) devices	suppliers	<p>Provision of information about safe use of equipment online</p> <p>Note: The Phase 1 codes and standards require suppliers of interactive (Tier 1) devices to provide certain information at or around the time of a sale. The following measure supplements that existing requirement.</p> <p>A supplier of interactive (Tier 1) devices must provide easily accessible information in plain language about:</p> <p>a) the fact that such devices have some default safety settings that will be applied if a child account or profile or restricted account or profile is set up; and</p> <p>b) the fact that other tools, features and/or settings are available that will help Australian end-users manage access to forms of inappropriate material and to otherwise safely manage their experience when using the device, at or around the time of a sale.</p> <p>It is not necessary that a particular form of words be used so long as the effect of the information is as required by sub-measure a) and b).</p> <p>A supplier is not expected to provide device-specific information for every type of interactive (Tier 1) device but must ensure that general information regarding the availability of default safety settings for child accounts or profiles and restricted accounts or profiles (as required by measure 2 or 3) and tools, features and/or settings (as required by measure 2, 3 and 8) is provided at or around the time of sale.</p> <p>Note: Information about safely managing a user's experience when using the device does not require the inclusion of information that is irrelevant to class 1C or class 2 material or the tools, features and/or settings required by this Code.</p> <p>Guidance:</p> <p><i>In implementing these measures, industry participants should also consider the needs and capabilities of children, for example with respect to complexity of language, ease of access etc.</i></p> <p><i>Examples of how this could be done include:</i></p> <ul style="list-style-type: none"> • <i>providing information on customer receipts;</i> • <i>having in-store signage or demonstrations, which may direct users to online information resources;</i> • <i>in the case of online supply, providing information or links to information (for example, in an online user guide) or linking to manufacturer provided information; or</i>

No.	Category of device	Category of provider	Compliance measure
13.	interactive (Tier 1) devices	maintenance and installation providers	<ul style="list-style-type: none"> • <i>in the case of online supply, providing information or links to information in online articles such as help pages.</i> <p>Provision of information about safe use of equipment online</p> <p><u>Note:</u> The Phase 1 codes and standards require a person who is a maintenance provider or an installation provider of interactive (Tier 1) devices to provide certain information upon request. The following measure supplements that existing requirement.</p> <p>If a person is a maintenance provider or an installation provider of interactive (Tier 1) devices, that person must provide information with respect to:</p> <ol style="list-style-type: none"> a) the availability of default safety settings for interactive (Tier 1) devices; and b) that these will be applied to child accounts or profiles and restricted accounts or profiles, upon request. <p>Guidance:</p> <p><i>A maintenance provider or an installation provider is not expected to provide device-specific information for every type of interactive (Tier 1) device but must ensure that they are prepared to provide general information regarding the availability of default safety settings for child accounts or profiles and restricted accounts or profiles (as required by measures 2 and 3) on request.</i></p> <p><i>A maintenance provider or an installation provider may choose to also provide additional assistance in the following ways:</i></p> <ul style="list-style-type: none"> • <i>an installation provider or a maintenance provider may refer end-users who have questions to information available online (e.g., on the manufacturer's website, or eSafety's website);</i> • <i>an installation provider or a maintenance provider can assist Australian end-users in setting up any online safety tools or features and respond to queries from end-users regarding those online safety tools or features.</i> <p><i>In implementing these measures, industry participants should also consider the needs and capabilities of children, for example with respect to complexity of language, ease of access etc..</i></p>
14.	interactive (Tier 1) devices	OS providers	<p>Improvement</p> <p>Where technically feasible and reasonably practicable, an OS provider for an interactive (Tier 1) device must take appropriate steps to further develop and improve the safety tools, features and/or settings it has in place under measures 2, 3 and 8 over time.</p> <p>Examples of activities that a provider may engage in to meet this measure include the following (to the extent directed towards, or relevant to, the matters covered by this Code):</p> <ol style="list-style-type: none"> a) any activities designed to further develop the effectiveness of the tools, features and/or settings; b) tracking new and emerging risks or issues that may be causing harm to Australian children; c) investment in research and development and/or testing of novel technological solutions;

No.	Category of device	Category of provider	Compliance measure
			<ul style="list-style-type: none"> d) investment in trust and safety teams dedicated to implementing regulatory requirements and policies which enhance online safety for users of online services; e) providing financial or technical support to non-governmental organisations with recognised online safety expertise to improve their infrastructure and/or technical capabilities; f) contributing to programs operated by non-governmental organisations; g) joining relevant industry organisations or other third party organisations intended to address online harm to children and sharing information on best practice approaches; h) contributing to industry initiatives (including initiatives lead by industry associations or other third party organisations); i) conducting or supporting research into and development of online safety tools, features and/or settings and approaches; j) providing support, either financial or in kind, to organisations the functions of which are or include protection of children online; k) extending the application of a tool, feature and/or setting applied to a service that is subject to a different industry code or standard under the OSA to operate in connection with its interactive (Tier 1) device; and l) activities that aim to refine algorithms or inputs into tools to improve their effectiveness. <p>The OS provider must, at a minimum, engage in at least some of the example activities above in each calendar year.</p>
15.	interactive (Tier 1) devices secondary (Tier 2) devices other interactive device	manufacturers and OS providers	<p>Trust and safety function</p> <p>A person who is a manufacturer of an interactive (Tier 1) device, a secondary (Tier 2) device or an other interactive device, or an OS provider for an interactive (Tier 1) device, must have, or have access to, sufficient personnel to oversee the safety of the device. 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.</p>
16.	interactive (Tier 1) devices	manufacturers and suppliers	<p>Right to complain</p> <p>If a person is a manufacturer or supplier of interactive (Tier 1) devices, that person must make available information to Australian end-users on their right to complain to a content provider under the Phase 2 codes and/or eSafety (including where a complaint to a content provider remains unresolved).</p>
17.	interactive (Tier 1) devices	manufacturers and OS providers	<p>Complaints mechanism</p> <p>If a person is a manufacturer of interactive (Tier 1) devices, or an OS provider, that person must have a complaints mechanism which enables Australian end-users to make a complaint about a breach of this Code by the provider.</p> <p>Such complaints mechanism must:</p>

No.	Category of device	Category of provider	Compliance measure
			<p>a) be easily accessible and simple to use; and</p> <p>b) be accompanied by plain language instructions on how to use it.</p> <p>If an Australian end-user makes a complaint of the kind referred to in this measure, the provider must consider any relevant information provided by the Australian end-user pursuant to their complaint in a reasonably timely manner.</p>
18.	interactive (Tier 1) devices	manufacturers and OS providers	<p>Timely referral of unresolved complaints to eSafety</p> <p>A person who is a manufacturer of interactive (Tier 1) devices, or an OS provider, 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.</p>
19.	interactive (Tier 1) devices	manufacturers and suppliers	<p>Communication with eSafety concerning complaints</p> <p>If a person is a manufacturer or supplier of interactive (Tier 1) devices, that person must implement policies and processes that ensure it responds in a timely and appropriate manner to communications from eSafety about complaints of breach of this Code.</p>
20.	interactive (Tier 1) devices	manufacturers and OS providers	<p>Engagement</p> <p>A person who is a manufacturer of interactive (Tier 1) devices or an OS provider must appropriately engage with safety and community organisations (such as civil society groups, public interest groups and representatives of marginalised communities), academics and government to gather information to help inform the measures it takes to protect or prevent Australian children from accessing or being exposed to class 1C and class 2 material.</p> <p>A provider must consider information obtained through such engagement.</p> <p>Guidance:</p> <p><i>Engagement may occur within and/or outside Australia as relevant to the issue under consideration.</i></p> <p><i>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.</i></p>
21.	interactive (Tier 1) devices	suppliers	<p>Staff</p> <p><u>Note:</u> The Phase 1 codes and standards require suppliers of interactive (Tier 1) devices to provide tools or training to staff to enable staff to appropriately respond to questions from Australian end-users regarding online safety, including available complaints mechanisms. This measure builds on that existing requirement.</p> <p>A supplier of interactive (Tier 1) devices must provide tools or training to staff to:</p> <p>a) enable staff to appropriately comply with measure 12 (to the extent those staff are involved in meeting measure 12); and</p> <p>b) enable staff to appropriately respond to questions from Australian end-users regarding available complaints mechanisms in place under measure 17 (to the extent those staff are involved in responding to such questions).</p>

No.	Category of device	Category of provider	Compliance measure
			<p>Guidance:</p> <p><i>Examples of how this can be done include making online safety resources available to staff, directing staff to other online safety resources (e.g., manufacturer online safety information or eSafety's website) or through staff training.</i></p>
22.	interactive (Tier 1) devices secondary (Tier 2) devices other interactive device	manufacturers and OS providers	<p>Updates to eSafety about relevant changes in technology</p> <p>If a person is a manufacturer of an interactive (Tier 1) device, a secondary (Tier 2) device or an other interactive device, or an OS provider, that person must share information with eSafety in writing about significant changes to the functionality for such devices (or operating systems) released by the manufacturer or OS provider (as applicable) that are likely to have a material positive or negative effect on the access or exposure to, distribution to, and online storage of online pornography by Australian children. The person may choose to provide this information in a Code report to eSafety under this Code.</p> <p>In implementing this measure, a provider is not required to disclose information to eSafety that is confidential.</p> <p>Guidance:</p> <p><i>Changes that have a material negative effect should, ideally, be communicated before a public announcement of the relevant changes.</i></p>
23.	interactive (Tier 1) devices	OS providers	<p>Significant changes to an operating system</p> <p>Before an OS provider makes a material change to the operating system for an interactive (Tier 1) device (including any new feature of the operating system enabled by generative artificial intelligence) that will significantly increase the risk of sharing of online pornography to an Australian child, it must:</p> <ol style="list-style-type: none"> a) carry out an assessment of the kinds of measures that could reasonably be incorporated into the operating system to minimise that risk; and b) where appropriate, apply measures so identified to help to mitigate that risk.
24.	interactive (Tier 1) devices	manufacturers and OS providers	<p>Reporting to eSafety on Code compliance (manufacturers of interactive (Tier 1) devices and OS providers)</p> <p>If a person is a manufacturer of an interactive (Tier 1) device or an OS provider, then where eSafety issues a written request to that person to submit a Code report, the person named in such request must submit to eSafety a Code report which includes the following information:</p> <ol style="list-style-type: none"> 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 measures are appropriate. <p>A person 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 person will not be required to submit a Code report to eSafety more than once in any 12 month period.</p>

No.	Category of device	Category of provider	Compliance measure
25.	secondary (Tier 2) devices other interactive devices	manufacturers	<p>Reporting to eSafety on Code compliance (manufacturers of secondary (Tier 2) devices and other interactive devices)</p> <p>If a person is a manufacturer of a secondary (Tier 2) device or an other interactive device, then where eSafety issues a written request to that person to submit a Code report, the person named in such request must submit to eSafety a Code report which includes the following information:</p> <ul style="list-style-type: none"> a) an explanation as to why the manufacturer considers the device to be a secondary (Tier 2) device or an other interactive device (as relevant); b) if the manufacturer considers a secondary (Tier 2) device not to be an other interactive device, an explanation as to why this is the case; c) the steps that the provider has taken to comply with the compliance measures under this Code; and d) an explanation as to why these measures are appropriate. <p>A person 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 person will not be required to submit a Code report to eSafety more than once in any 12 month period.</p>