Suggested code compliance report template and guidance for providers of equipment services

Phase 1 Codes for class 1A and class 1B material

# Introduction

Industry codes and standards are a key part of Australia’s online safety regulatory framework. Background information about the Phase 1 Codes which are in effect for six sections of the online industry, including equipment services, can be found on the [Background to the Phase 1 Codes](https://www.esafety.gov.au/industry/codes/background-to-the-phase-1-industry-codes) page on the eSafety website.

Equipment services are defined as:

* manufacturers of
* suppliers of
* those who maintain and install

equipment that is used to access online services.

An additional category of ‘operating system providers’ is also regulated by the Equipment Code.

Manufacturers and operating system providers are required to report to eSafety on their compliance with Phase 1 Codes either annually or on request by eSafety depending on their risk profile.

Manufacturers of interactive (Tier 1) devices and operating system providers must submit a code compliance report annually under minimum compliance measure (**MCM**) 13 in accordance with the reporting schedule set out in the [Phase 1 Codes Regulatory Guidance](https://www.esafety.gov.au/about-us/who-we-are/regulatory-schemes#phase-1-industry-codes). An interactive (Tier 1) device can also be categorised more specifically as a ‘children’s interactive device’ or ‘gaming device’.

Manufacturers of secondary (Tier 2) devices must submit a code compliance report on request by eSafety under MCM 14 and within two months of receiving a request.

A secondary (Tier 2) device can also be categorised more specifically as a ‘gaming device’.

No other equipment services are required to submit code compliance reports either annually or on request.

Information about risk tiers and device categorisation can be found in the Head Terms of the Phase 1 Codes and Schedule 5 – Equipment Online Safety Code (Class 1A and Class 1B Material). Further guidance can be found in the [Phase 1 Codes Regulatory Guidance](https://www.esafety.gov.au/about-us/who-we-are/regulatory-schemes#phase-1-industry-codes).

## Using this suggested code compliance report template and guidance

This code compliance report template provides an **optional** reporting format and additional guidance to assist service providers in completing their code compliance reports.

While service providers are not required to report to eSafety in a particular format, eSafety highly encourages using this code compliance report template. This will help ensure that service providers meet their reporting obligations under the Equipment Services Code and Head Terms. It will also best support service providers to provide the information eSafety requires to assess compliance and reduce the need for eSafety to seek clarifying information.

Where a service provider must submit a code compliance report to eSafety for multiple online activities, the service provider may choose to submit a consolidated code compliance report covering all applicable services. This optional code compliance report is designed to be used for reporting on one online service at a time.

The Equipment Services Code and Head Terms should be referred to while using this template for the full text of MCMs and guidance notes. These can be found on the [register of industry codes and standards](https://www.esafety.gov.au/industry/codes/register-online-industry-codes-standards). This template may also be used to report on any applicable Optional Compliance Measures (**OCM**). Only MCMs and OCMs applicable to manufacturers and/or operating system providers have been included in this optional code compliance report template.

This template and guidance do not override any of the requirements in the Phase 1 Codes and Standards, *Online Safety Act 2021* (Cth) (the **Act**), or other laws and regulations.

Further regulatory guidance from eSafety can be found in the [Phase 1 Codes Regulatory Guidance](https://www.esafety.gov.au/about-us/who-we-are/regulatory-schemes#phase-1-industry-codes).

## Requirements for Equipment Services Code compliance reports

At a minimum, a code compliance report for manufacturers of interactive (Tier 1) devices and/or operating system providers must contain the following information in accordance with MCM 13:

* The number of complaints from end-users in Australia received about compliance with the Equipment Services Code through the complaint mechanisms implemented under MCM 12.
* The steps taken to comply with the applicable MCMs.
* An explanation as to why the steps taken to comply with the measures are appropriate.

At a minimum, a code compliance report for manufacturers of secondary (Tier 2) devices must contain the following information in accordance with MCM 14:

* An explanation as to why the manufacturer considers the device to be a secondary (Tier 2) device.
* The steps taken to comply with the applicable MCMs.
* An explanation as to why the steps taken to comply with the measures are appropriate.

If a code compliance report is not provided to eSafety as required, or the report suggests non-compliance with the applicable Phase 1 Code or does not provide sufficient detail, eSafety may commence a compliance assessment and/or an investigation. Where the eSafety Commissioner is satisfied that a service provider has contravened, or is contravening, a code they may issue the service provider with a written direction to comply with that code. More information about eSafety’s approach to enforcement and investigative powers can be found on our website in our [Compliance and Enforcement Policy](https://www.esafety.gov.au/about-us/who-we-are/regulatory-schemes#compliance-and-enforcement-policy).

## Information already available or reported to eSafety

Service providers can refer to information provided under existing voluntary reporting, or another reporting requirement under the Act. This may include publicly available information. The purpose of this is to reduce the regulatory burden on service providers and potential duplication.

Where the information is already available or has been reported to eSafety, service providers should clearly refer eSafety to the information in code compliance reports and explain why further provision of information is not required.

## Confidentiality of information in code compliance reports

Generally, eSafety does not intend to publish code compliance reports provided by service providers. This does not however limit the eSafety Commissioner’s ability to exercise their functions under the Act. The Head Terms outline that if a service provider identifies material in a code compliance report as confidential information, eSafety must maintain such material in confidence.

eSafety considers that confidential information includes, but is not limited to:

* information that is commercial-in-confidence (including trade secrets)
* other business information that would be unreasonable to publish
* information that could affect law enforcement and public safety
* personal information.

However, there may be circumstances in which the Act, or another Australian law, requires or authorises eSafety to disclose this material.

The key purpose of the code compliance reports required under the Phase 1 Codes is to assist eSafety to determine compliance with the applicable Phase 1 Code and identify whether investigation and/or enforcement is appropriate and necessary. eSafety does not intend to publish code compliance reports as a matter of course. However, the information provided in a code compliance report may be relevant to the exercise of statutory powers and functions by eSafety. For example, eSafety may use the information in deciding whether to commence an investigation into a complaint about class 1 material, or to determine the subject matter or recipient of a notice given in connection to the Basic Online Safety Expectations. The Act also enables eSafety to disclose summaries of de-identified information and statistics derived from de-identified information. In these cases, information provided as part of a compliance report may be publicly communicated.

eSafety can also be required to produce material in certain circumstances including:

* in response to a request under the *Freedom of Information Act 1982* (Cth), although certain exceptions may apply
* at a court’s direction or in performance of its duties in court proceedings
* in response to a Minister, house of parliament or another government agency’s power to obtain information.

## Submitting code compliance reports to eSafety

Attachments necessary for understanding code compliance reports may be submitted alongside a code compliance report.

Code compliance reports together with any attachments should be submitted through eSafety’s industry codes and standards compliance portal. Service providers should request a link to the compliance portal by email to [codes@esafety.gov.au](mailto:codes@esafety.gov.au).

## What assistance eSafety can provide to service providers

eSafety can provide general guidance to service providers but cannot provide legal advice. Service providers are encouraged to seek their own legal advice. Further information about what eSafety can and cannot help service providers with can be found in the [Phase 1 Codes Regulatory Guidance](https://www.esafety.gov.au/about-us/who-we-are/regulatory-schemes#phase-1-industry-codes).

A service provider should contact eSafety if they have concerns about meeting any of the MCMs, including the relevant timeframe for a code compliance report or where it encounters difficulties of (dis)aggregation of data.

Questions or requests for guidance can be sent through eSafety’s industry codes and standards compliance portal. For a link to the portal, service providers should contact eSafety at [codes@eSafety.gov.au](mailto:codes@esafety.gov.au).

Service providers may also wish to contact the industry associations that developed the Phase 1 Industry Codes at [hello@onlinesafety.org.au](mailto:hello@onlinesafety.org.au).

# Suggested code compliance report template: Tier 1 and Tier 2 equipment services

Phase 1 Codes for class 1A and class 1B material

## General information

|  |  |
| --- | --- |
| Category of information | Provider response |
| Name of service providers | Click or tap here to enter text. |
| Name of device/operating system if different | Click or tap here to enter text. |
| Contact information – name, position, email | Click or tap here to enter text. |
| Reporting period\* | Click or tap here to enter text. |
| Date of code compliance report | Click or tap here to enter text. |

\*Information on reporting periods can be found in [Phase 1 Industry Codes Regulatory Guidance](https://www.esafety.gov.au/about-us/who-we-are/regulatory-schemes#phase-1-industry-codes).

## Type of equipment and risk categorisation

The Equipment Services Code defines different device types based on their risk and characteristics.

Interactive (Tier 1) devices, secondary (Tier 2) devices and non-interactive (Tier 3) devices are mutually exclusive. Additional specific categories of devices are defined as follows:

* **Children’s interactive device:** equipment that is an interactive (Tier 1) device targeted at children. These devices are subject to additional heightened requirements recognising the need for increased protections.
* **Gaming device:** a device designed to enable end-users in Australia to play online games with other end-users. These devices may be an interactive (Tier 1), secondary (Tier 2) or non-interactive (Tier 3) device.
* **Operating system provider**: a provider that has control over the final overall operating system for an interactive (Tier 1) device. An operating system provider may also be the manufacturer of the interactive (Tier 1) device, or a third-party operating system provider that provides the operating system for use in the manufacturer’s interactive (Tier 1) device.

The Equipment Services Code should be referred to for the full and complete definitions of device categorisations (clause 3) and table (clause 5). See also clause 5.2 of the Head Terms.

Where required, service providers must conduct their initial risk assessment as soon as practical following the commencement of the applicable industry code. eSafety may request further information about the risk assessment carried out by a service and its risk categorisation during the course of monitoring and assessing compliance as the need arises. eSafety may request information on risk categorisation informally or use its formal investigation powers.

Manufacturers of secondary (Tier 2) devices are required to provide an explanation in their code compliance reports about why Tier 2 applies instead of Tier 1.

#### What type of equipment service does the service provider provide? (tick all that apply)

Response

Manufacturer

Supplier

Maintenance and installation

Operating system

#### What is the service’s risk and device categorisation according to the most recently conducted risk assessment (tick all that apply)?

Response

Interactive (Tier 1) device

Secondary (Tier 2) device

Children’s interactive device

Gaming device

#### Was the risk and device categorisation carried out as soon as reasonably practical from the time the provider was required to do so?

Response

YES

If yes, please specify the date of the completed risk and device categorisation and why the assessment was considered to be carried out as soon as reasonably practical:

Click or tap here to enter text.

NO

If no, please provide reasons for delay:

Click or tap here to enter text.

#### Did the service’s risk and device categorisation change during the reporting period?

Response

YES

NO

Please provide reasons and dates for any change(s) to risk and device categorisation during the reporting period. For example, because of a change in functionality or a new feature.

Click or tap here to enter text.

#### Provide the service’s risk and device categorisation in the following table.

**Guidance:**

* Manufacturers of secondary (Tier 2) devices are required to provide an explanation in their code compliance reports about why Tier 2 applies instead of Tier 1. This can be achieved by completing the table below and providing details in the appropriate field.
* When completing this table, refer to the definitions of device categorisations (clause 3) and table (clause 5) of the Equipment Services Code. See also clause 5.2 of the Head Terms.
* This question is optional for manufacturers of interactive (Tier 1) devices. eSafety may issue a risk assessment request if the information is not provided.
* This question does not apply to operating system providers.

|  |  |  |
| --- | --- | --- |
| Concept | Provide the following information | |
| User-interactive | * Is there a two-way flow of material between the device and the end-user? | YES  NO |
| * Which categorisation applies? | Interactive (Tier 1) devices  Secondary (Tier 2) devices  Non-interactive (Tier 3) devices |
| * Provide details | Click or tap here to enter text. |
| Personal | * Is the equipment portable and may be carried with the end-user? | YES  NO |
| * Which categorisation applies? | Interactive (Tier 1) devices  Secondary (Tier 2) devices  Non-interactive (Tier 3) devices |
| * Provide details | Click or tap here to enter text. |
| Communal | * Is the equipment not personal and generally intended for use by more than one end-user? | YES  NO |
| * Which categorisation applies? | Interactive (Tier 1) devices  Secondary (Tier 2) devices  Non-interactive (Tier 3) devices |
| * Provide details | Click or tap here to enter text. |
| Standalone | * Is the equipment capable of being used without the use of another interactive (Tier 1) device? | YES  NO |
| * Which categorisation applies? | Interactive (Tier 1) devices  Secondary (Tier 2) devices  Non-interactive (Tier 3) devices |
| * Provide details | Click or tap here to enter text. |
| General internet browsing | * Is a significant function of the device general internet browsing such as a device that:  1. 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 2. provides general access to the internet, with the ability to display text, images and videos. | YES  NO |
| * Which categorisation applies? | Interactive (Tier 1) devices  Secondary (Tier 2) devices  Non-interactive (Tier 3) devices |
| * Provide details | Click or tap here to enter text. |
| Summary/any other information | * Please provide a summary of the service’s risk/device categorisation and any other information | Click or tap here to enter text. |

## Minimum Compliance Measures

Please provide your report against applicable minimum compliance measures.

### Outcomes 1-2

By complying with the minimum compliance measures under Outcome 7, equipment services will also meet the requirements under Outcomes 1-2.

### Outcome 4[[1]](#footnote-2)

Not applicable.

### Outcome 5: Service providers consult, cooperate and collaborate with other service providers in respect of the removal, disruption and/or restriction of class 1A and class 1B materials

#### MCM 1: Industry forums (manufacturers of interactive (Tier 1) devices, gaming devices, operating system providers)

**Guidance on information to include:**

* Specify the name, date, location (in person or online), duration and organiser of the annual forum that the provider took part in during the reporting period.
* List and describe sessions attended or chaired in the forum programme that covered sharing relevant issues, advances and best practice in online safety with other service providers. A copy of the programme, agenda or other item describing sessions or topics may be marked and provided as an attachment.
* Describe any practical outcomes following forum attendance, if any (for example, implementation of a tool or process)
* Explain why the steps taken to comply with this MCM are appropriate.

Response

Click or tap here to enter text, or attach response as a separate document.

#### OCM 2: Industry forums (manufacturers of secondary (Tier 2) devices)

**Guidance on information to include:**

* Specify the name, date, location (in person or online), duration and organiser of any annual forum referred to in MCM 1 that the provider took part in during the reporting period.

Response

Click or tap here to enter text, or attach response as a separate document.

### Outcome 6: Service providers communicate and cooperate with eSafety in respect of matters relating to class 1A and class 1B material, including complaints

#### MCM 3: Communication with eSafety concerning complaints (manufacturers of interactive (Tier 1) devices)

**Guidance on information to include:**

* Specify the policies and processes in place that ensure the service responds to communications from eSafety in a timely and appropriate manner concerning complaints about potential breaches of the Equipment Services Code.
* Describe the documented steps and procedures personnel are required to follow.
* Explain why the steps taken to comply with this MCM are appropriate.

Response

Click or tap here to enter text, or attach response as a separate document.

#### MCM 4: Transparency (manufacturers of Tier 1 and Tier 2 devices, operating system providers)

**Guidance on information to include:**

* eSafety considers that it would be good practice for service providers to notify eSafety within two weeks of a new feature or functionality change.
* Specify the dates and notifications made to eSafety regarding significant changes to the functionality of the service that were likely to have a material positive or negative effect on the access or exposure to, distribution of, and online storage of class 1A or class 1B materials by Australian end-users.
* If information was not shared during the year, provide details of changes made during the year to the functionality of the service that were likely to have a material positive or negative effect on the access or exposure to, distribution of, and online storage of class 1A or class 1B materials by Australian end-users.
* Specify if there were no notifications made to eSafety because there were no significant changes to the functionality of the service.

Response

Click or tap here to enter text, or attach response as a separate document.

### Outcome 7: Service providers provide tools and/or information to limit access and exposure to class 1A and class 1B material

By complying with MCMs under Outcome 7, equipment providers will also meet the requirements of Outcomes 1-2.

#### MCM 5: Provision of information about safe use of equipment online (manufacturers of interactive (Tier 1) devices, children’s interactive devices, gaming devices)

**Guidance on information to include:**

* If the service is a manufacturer of an interactive (Tier 1) device or a gaming device, specify, describe and provide an active link (or screenshot with location details) to information about:
  + eSafety’s role
  + eSafety’s user complaints form for non-compliance with Phase 1 Industry Codes
  + how end-users in Australia can limit access to class 1A material and class 1B material when using the equipment.
* If the service is a manufacturer of children’s interactive devices or gaming devices, specify, describe and provide an active link (or screenshot with location details) to information about how to support online safety in a child’s use of those devices.
* If the service is a manufacturer of a gaming device with functionality that enables end-users in Australia to freely browse the internet, specify, describe and provide an active link (or screenshot with location details) to information that such functionality exists on the device.
* Specify and describe any steps taken to ensure the information is accessible, easy to understand and considers the needs and capabilities of children in understanding the information.
* Explain why the steps taken to comply with this MCM are appropriate.

Response

Click or tap here to enter text, or attach response as a separate document.

#### MCM 6: Tools (operating system providers, manufacturers of gaming devices)

**Guidance on information to include:**

* If the service is an operating system provider, specify and describe:
  + tools developed and implemented to help reduce the risk of harm to children when using interactive (Tier 1) devices. For example, enabling child accounts and profiles, parent/guardian controls, clear and accessible guidance.
  + the default safety settings that implement the most restrictive privacy and location settings for children’s interactive devices provided by the operating system provider to end-users in Australia (if applicable).
  + tools available to end-users in Australia to assist in restricting the unauthorised access to and operation of an adult's interactive (Tier 1) device by a child. For example, making available security measures that prevent unauthorised access where the device does not have parent/guardian controls enabled.
* If the service is a manufacturer of gaming devices, specify and describe tools implemented that allow end-users in Australia to reduce the risk of harm to children when using these devices. For example, enabling child accounts and profiles, parental/guardian controls that limit internet browsing functionality on adult accounts, or limit available games on child accounts.
* Specify and describe any steps taken to ensure the information is accessible, easy to understand and considers the needs and capabilities of children in understanding the information.
* Explain why the steps taken to comply with this MCM are appropriate.

Response

Click or tap here to enter text, or attach response as a separate document.

#### MCM 7: Staff

Not applicable.

#### OCM 8: Provision of information about the safe use of equipment online (manufacturers of interactive (Tier 1) devices)

**Guidance on information to include:**

* Specify, describe and provide an active link (or screenshot with location details) to any additional only safety information provided to end-users in Australia and its form. For example, safety warnings, QR codes or packaging with information about the risks of harmful online material; using content filtering or other software; or supporting a child's safe use of social media services, relevant electronic services and designated internet services accessible through the equipment.

Response

Click or tap here to enter text, or attach response as a separate document.

#### OCM 9: Safety features and settings (manufacturers of secondary (Tier 2) devices)

**Guidance on information to include:**

* If the service is a manufacturer of secondary (Tier 2) devices, specify and describe any reasonable steps taken to:
  + consider features and/or settings that are designed to mitigate the risks to children when accessing material via the device.
  + develop and implement tools for content filtering technologies and other safety features to help reduce the risk of harm to children.

Response

Click or tap here to enter text, or attach response as a separate document.

### Outcome 8: Service providers provide clear and effective reporting and complaints mechanisms for class 1A and class 1B material

#### MCM 10: Right to complain (manufacturers of interactive (Tier 1) devices)

**Guidance on information to include:**

* Specify, describe and provide an active link (or screenshot with location details) to information for end-users in Australia about their right to complain to a content provider and/or eSafety (including where a complaint to a content provider remains unresolved) about class 1A and 1B material, or unsolicited electronic messages that promote such material.
* Explain why the steps taken to comply with this MCM are appropriate.

Response

Click or tap here to enter text, or attach response as a separate document.

#### MCM 11: Link to eSafety form (manufacturers of interactive (Tier 1) devices)

**Guidance on information to include:**

* Specify, describe and provide an active link (or screenshot) to the service’s online safety resources including a link to eSafety’s online content complaints reporting form.

Response

Click or tap here to enter text, or attach response as a separate document.

### Outcome 9: Service providers effectively respond to reports and complaints about class 1A and class 1B material

#### MCM 12: Handling code complaints (manufacturers of interactive (Tier 1) devices, operating system providers)

**Guidance on information to include:**

* Specify and describe, and provide an active link (or screenshot with location details) to the complaints mechanism in place to deal with complaints from end-users in Australia concerning potential non-compliance and breach of the Phase 1 Industry Codes.
* Explain why the steps taken to comply are appropriate.

Response

Click or tap here to enter text, or attach response as a separate document.

### Outcome 10: Service providers provide clear and accessible information about class 1A and class 1B material

By complying with the minimum compliance measures under Outcome 7, equipment service providers will also meet the requirements of Outcome 10.

### Outcome 11: Service providers publish annual reports about class 1A and 1B material and their compliance with this code

#### MCM 13: Annual reporting (manufacturers of interactive (Tier 1) devices, operating system providers)

* Provide the total number of complaints received during the reporting period from end-users in Australia about potential non-compliance and breach of the Phase 1 Industry Codes in accordance the complaints handling mechanism required under MCM 12.
* Identify and describe any trends or categories of complaints.

Response

Click or tap here to enter text, or attach response as a separate document.

## List of attachments referred to in responses

Click or tap here to enter text.

1. There is no Outcome 3. [↑](#footnote-ref-2)