Phase 1 Industry Codes (Class 1A and Class 1B Material)

Regulatory Guidance

December 2023

Australian Government | eSafetyCommissioner

eSafety.gov.au

Contents

Overview of this guidance

This guidance is for participants in industry sectors (**industry participants**) who are covered by the Consolidated Industry Codes of Practice for the Online Industry (Class 1A and Class 1B Material) (**Phase 1 Industry Codes**) as well as other stakeholders. It provides information about the Phase 1 Industry Codes and the functions of the eSafety Commissioner (**eSafety**) in monitoring and enforcing compliance with the Phase 1 Industry Codes.

The Phase 1 Industry Codes are a group of six codes developed by industry associations and registered by eSafety in 2023. Each Phase 1 Industry Code comprises a common set of Head Terms and a Schedule covering one of the following industry sections:

- Social Media Services
- App Distribution Services
- Hosting Services
- Internet Carriage Services
- Equipment Services (including manufacturers, suppliers, and those who maintain and install equipment that is used to access online services)
- Search Engine Services.

The Phase 1 Industry Codes commence on 16 December 2023, except for the Phase 1 Industry Code covering search engine services, which commences on 12 March 2024.

> Minimum Compliance Measures (MCMs) in each Phase 1 Industry Code are mandatory and enforceable from the commencement date for that code.

More information on the Phase 1 Industry Codes, including the development process, is available on eSafety's website.[1]

This guidance provides information on:

- the legal framework for industry codes and standards (Part 1)
- complying with the relevant Phase 1 Industry Code (Part 2)
- what eSafety can and cannot help industry participants with (Part 3)

[1] eSafety website, Industry Codes and Standards web page: https://www.esafety.gov.au/industry/codes

- communicating with eSafety (Part 4)
- how the industry codes interact with other regulatory requirements under the Online Safety Act 2021 (Cth) (the Act) (Part 5)
- eSafety's approach to compliance and enforcement (Part 6).

Part 1: Legal and regulatory framework for industry codes and standards

eSafety is Australia's independent online safety regulator. Its mandate is to promote and improve online safety for all Australians.

The Act provides eSafety with legislative powers to help prevent Australian residents and end-users in Australia from being exposed to harmful online content.

Part 9 of the Act set outs an Online Content Scheme which provides for:

- eSafety to investigate and require the removal of illegal and restricted online content
- the development of industry codes and industry standards that relate to illegal and restricted online content.

The removal powers in Part 9 relate to specific pieces of illegal or restricted online content and material, while the industry codes and standards are intended to address online material at a systemic level. Under industry codes, participants in specific sections of the online industry[2] are required to take steps to address the presence of this harmful online content on their services for people in Australia who are users of the service (**end-users in Australia**).

The Phase 1 Industry Codes are outcomes-based and set out the minimum steps and processes – known as 'minimum compliance measures' – that industry participants must take (**compliance measures**). The compliance measures are intended to be flexible to enable industry participants to take steps and meet their obligations in a way that is suited to their services.

[2] Sections of the online industry are specified in Section 135 of the *Online Safety Act 2021* (the Act). Section 136 provides that a person is a participant in a section of the online industry if the person is a member of a group that constitutes a section of the online industry.

eSafety can receive complaints and investigate potential breaches of the industry codes or standards.[3] Breaches will be enforceable by civil penalties and other enforcement options.[4]

Enforcement is discussed in more detail at Part 6 of this guidance.

a) What harmful online content is covered by industry codes and standards?

Industry codes and standards are to regulate online activities[5] related to class 1 and class 2 material. Class 1 and class 2 material include online content ranging from illegal and the most seriously harmful, such as videos showing the sexual abuse of children or acts of terrorism, through to content which is inappropriate for children, such as online pornography. eSafety refers broadly to such content as 'illegal and restricted online content.'

Online content involves a mix of written, video and image content. Class 1 and class 2 material are defined under the Act by reference to Australia's National Classification Scheme.[6] The definitions in the Act apply to films, publications, computer games and any other material.[7]

Additional information on the classification of material is available in the Online Content Scheme Regulatory Guidance on eSafety' s website.

eSafety developed sub-categories of class 1 and class 2 material to facilitate a two-phased approach to developing industry codes that prioritises the implementation of measures in preventing and reducing the most harmful online content.

Phase 1 Industry Codes deal with class 1A and class 1B material:

- Class 1A material is material that is seriously harmful and generally should not be accessible online.
- Class 1B material is also harmful but may be appropriate for adults to access provided suitable limitations are in place.

[3] Sections 40, 42 of the Act.
[4] Sections 143-144, 146-147 and Part 10 of the Act.
[5] Online activities are listed in Section 134 of the Act.
[6] A cooperative arrangement between the Australian Government and state and territory governments for the classification of films, computer games and certain publications. For further information visit the Australian Classification website at www.classification.gov.au.
[7] Other material is material that is not a film, publication or computer game: Sections 106-107 of the Act.

The remainder of the sub-categories – Class 1C, Class 2A, Class 2B – will be covered by Phase 2 of the Industry Codes.

Table 1: Sub-categories and eSafety's phased approach

Phase	Sub-category	Material	National Classification Scheme
Phase 1	Class 1A	• Child sexual exploitation material (CSEM) – material that promotes or provides instruction of paedophile activity. • Pro-terror material – material that advocates the doing of a terrorist act (including terrorist manifestos). • Extreme crime and violence material – material that describes, depicts, expresses or otherwise deals with matters of extreme crime, cruelty or violence (including sexual violence) *without justification*.[8] For example, murder, suicide, torture and rape. Material that promotes, incites or instructs in matters of extreme crime or violence.	• Class 1 • Refused Classification (RC)
Phase 1	Class 1B	• Crime and violence material – material that describes, depicts, expresses or otherwise deals with matters of crime, cruelty or violence *without justification*. Material that promotes, incites or instructs in matters of crime or violence. • Drug-related material – material that describes, depicts, expresses or otherwise deals with matters of drug misuse or addiction *without justification*. Material which includes detailed instruction or promotion of proscribed drug use.	• Class 1 • Refused Classification (RC)
Phase 2	Class 1C	• Online pornography – material that describes or depicts specific fetish practices or fantasies.	• Class 1 • Refused Classification (RC)
Phase 2	Class 2A	• Online pornography – other sexually explicit material that depicts actual (not simulated) sex between consenting adults.	• Class 2 • X18+ • Category 2 restricted

[8] Reference to 'without justification' highlights that the nature of the material must be considered, including its literary, artistic, or educational merit and whether it serves a medical, legal, social or scientific purpose. Section 11 of the *Classification (Publications, Films and Computer Games) Act 1995* outlines matters to be taken into account in making a decision on classification.

Phase	Sub-category	Material	National Classification Scheme
Phase 2	Class 2B	• Online pornography – material which includes realistically simulated sexual activity between adults. Material which includes high-impact[9] nudity. • Other high-impact material which includes high-impact sex, nudity, violence, drug use, language and themes. 'Themes' includes social Issues such as crime, suicide, drug and alcohol dependency, death, serious illness, family breakdown and racism.	• Class 2 • R18+ • Category 1 restricted

Guidance on how to classify material under the Phase 1 Industry Codes can also be found in Annexure A to the Head Terms – Consolidated Industry Codes of Practice for the Online Industry (Class 1A and Class 1B Material).

b) Which sections of the online industry are regulated by industry codes and standards?

Under the Act, industry codes or industry standards are to apply to eight sections of the online industry.[10]

Table 2: Industry sections and example services covered by industry codes and standards

Industry section	Examples of services (non-exhaustive)
Social Media Services	• social networks • public media sharing networks • discussion forums • consumer review networks
Relevant Electronic Services	• instant messaging services • Short Message Services and Multimedia Message Services • chat services • online multi-player gaming services • email services • online dating services • enterprise messaging services
Designated Internet Services	• file storage services managed by end-users in Australia • websites and apps*

[9] Impact may be higher where content is detailed, accentuated, or uses special effects, prolonged, repeated frequently, realistic or encourages interactivity.
[10] Section 135 of the Act.

	*Note: Unless an online service is otherwise considered a Social Media Service or a Relevant Electronic Service.
Search Engine Services	• electronic services designed to collect, organise (index) and/or rank information on the World Wide Web (WWW) in response to end-user queries and return search results to end-user queries Note: Excludes search functionality within platforms where content or information can only be surfaced from that which has been generated/uploaded/created within the platform itself and not from the WWW more broadly.
App Distribution Services	• services distributing apps that can be accessed by end-users in Australia (for example, app stores/marketplace) Note: Excludes links to an app and download of apps from third party websites.
Hosting Services	• services which host-stored material in Australia (for example, a service with data centres located in Australia)
Internet Carriage Services	• retail Internet Service Providers that supply internet carriage services (including mobile and broadband) to end-users in Australia Note: Excludes providers of wholesale ISP services, including NBN Co.
Equipment Services	• Manufacturers, suppliers, maintainers and installers of equipment that is used to access online services[11] such as: o mobile phones o laptops o tablets o internet-enabled devices (such as smart TVs and gaming consoles) o immersive technologies (such as virtual reality headsets) o wi-fi routers Note: This section of the online industry includes manufacturers of these devices, as well as businesses and retail outlets that install, sell and/or repair/maintain such devices.

[11] 'Online services' is limited to social media services, relevant electronic services, designated internet services and internet carriage services: Section 135(2)(h) of the Act.

c) Which sections of the online industry must comply with the Phase 1 Industry Codes?

The Phase 1 Industry Codes apply to six sections of the online industry, summarised in the following table.

Table 3: Industry sections covered by Phase 1 Industry Codes

Industry section	Relevant code	Code structure
Social Media Services	Social Media Services Online Safety Code (**Social Media Services Code**)	Head Terms + Schedule 1
App Distribution Services	App Distribution Services Online Safety Code (**App Distribution Services Code**)	Head Terms + Schedule 2
Hosting Services	Hosting Services Online Safety Code (**Hosting Services Code**)	Head Terms + Schedule 3
Internet Carriage Services	Internet Carriage Services Online Safety Code (**Internet Service Provider Code**)	Head Terms + Schedule 4
Equipment Services	Equipment Online Safety Code (**Equipment Code**)	Head Terms + Schedule 5
Internet Search Engine Services	Internet Search Engine Services Online Safety Code (**Search Engine Services Code**)	Head Terms + Schedule 6

Relevant Electronic Services and Designated Internet Services are not covered by Phase 1 Industry Codes. These sections will be regulated under industry standards instead.

d) What is the difference between codes and standards?

Australian industry associations drafted industry codes for each of the sections of the online industry identified in Table 2 and submitted these to eSafety for registration. Each industry association represents one or more sections of the online industry. The relevant industry associations consulted with their members, other industry participants and the public more broadly in the preparation of the Phase 1 industry codes.

For an industry code to be registered, the eSafety Commissioner (**the Commissioner**) must be satisfied that it meets certain procedural and substantive requirements set out in the Act. In particular, the Commissioner must be satisfied that an industry

code submitted for registration provides appropriate community safeguards for matters of substantial relevance to the community before registering a code.[12]

Industry standards are different to industry codes because they are legislative instruments that are tabled before parliament. eSafety is responsible for developing industry standards, not industry associations.

The Commissioner registered six of the eight draft codes addressing class 1A and class 1B content but found that codes submitted by industry associations for Relevant Electronic Services and Designated Internet Services did not meet registration requirements. As a result, eSafety is developing industry standards to apply to these two sections of the online industry.[13]

Once an industry code is registered, it will apply unless it has been revised (and re-registered) or the Commissioner determines it is deficient.[14] An industry code may be deficient when:

- it is not operating as intended and fails to achieve the objectives of the Act
- it is no longer fit for purpose (for example, due to developments in technology or changes in the services described in the scope of the industry code)
- there is a serious unintended consequence from the implementation of an industry code.15

Such a determination may only be made after an industry code has been registered for at least 180 days.[16]

eSafety may use the information collected through compliance and enforcement action (see Part 6 of this guidance for more information) to inform a decision about whether an industry code is deficient.

If eSafety has concerns that an industry code may be deficient, eSafety will first give notice to the industry association responsible for the development of the relevant code and request that the deficiency (or deficiencies) identified be adequately addressed within a specified period.

---

[12] Section 140 of the Act.
[13] More information on the status of industry standards can be found at eSafety website, Industry Codes and Standards web page: https://www.esafety.gov.au/industry/codes
[14] Sections 142, 145(1)(c) of the Act.
[15] Section 145(1A)-(1B) of the Act.
[16] Section 145(1)(c) of the Act.

Part 2: Complying with the relevant industry code

Each Phase 1 Industry Code comprises a common set of Head Terms and a Schedule which sets out the compliance measures specific to the participants in the relevant sections of the online industry. Industry participants need to consider both the Head Terms and the Schedule to determine which Phase 1 Industry Code applies to them and to understand their obligations.

a) Identifying which code or standard applies

The Head Terms provide that each industry participant is required to comply with the Phase 1 Industry Code (or standard) that applies to each online activity they undertake.[17] If the industry participant has more than one online activity, it should determine the industry code or industry standard that is most clearly aligned with the predominant purpose of that single electronic service.[18]

Where the industry participant operates multiple online activities, (where separate online services are offered), the industry participant may be required to comply with different codes or standards for each service. Industry participants should consider clauses 2 and 3 of each Schedule, which outline the scope and definitions specific to each industry code, to help identify the Phase 1 Industry Code which applies to each online service offered. Some online services will fall within the Relevant Electronic Services and Designated Internet Services categories and will be covered by the industry standards for those services once they are determined.

Head Terms, Phase 1 Industry Codes

Identifying the applicable code or standard (page 4)

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

Where a single electronic service could fall within the scope of more than one industry code or industry standard, the relevant industry participant will only be

[17] Consolidated Industry Codes of Practice for the Online Industry (Class 1A and Class 1B Material) Head Terms, 4. Online activity is defined in Section 134 of the Act.
[18] Consolidated Industry Codes of Practice for the Online Industry (Class 1A and Class 1B Material) Head Terms, 4. Electronic service is defined in Section 5 of the Act.

required to comply with one code or industry standard, as the case may be, for that electronic service. The code or industry standard that will apply in this situation is the code or industry standard 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 or industry standard 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 or industry standard is applicable to a particular electronic service, the industry participant may seek guidance from eSafety.

A number of industry participants will provide multiple electronic services, in which case the service provider would be subject to the Phase 1 Industry Code or once registered, the Phase 1 Industry Standard, applicable to **each** electronic service or online activity.

Example 1

An industry participant provides an internet carriage service that falls within the Internet Service Provider Code. That participant also manufactures and/or supplies equipment that falls within the Equipment Code.

As a result, the industry participant would need to comply with both Internet Service Provider and Equipment Codes.

Example 2

An industry participant manufactures and/or supplies equipment that is for use by end-users in Australia and makes available an online messaging service on those devices.

That industry participant would need to comply with the Equipment Code and once determined, the industry standard that applies to Relevant Electronic Services.

Industry standards for Relevant Electronic Services and Designated Internet Services are currently being developed by eSafety. Industry participants who offer multiple electronic services or a service which integrates multiple functions, will need to also review those industry standards, once determined, to ensure compliance.

Where the predominant purpose of an electronic service is unclear, eSafety will consider if the Relevant Electronic Services or Designated Internet Services standard

applies before considering the application of an industry code. For example, if an industry participant provides a service that has elements of a Social Media Service[19] but its predominant use is aligned with a Relevant Electronic Service[20], eSafety will likely consider that the industry standard for relevant electronic services will apply to that electronic service.

eSafety may seek information informally from an industry participant as to their risk profile or exercise the powers under a Code or the legislation to require the provision of this information.

b) Risk assessment

The Phase 1 Industry Codes are outcomes-based and take into account the level of risk that different kinds of services can pose to end-users in Australia in relation to class 1A and class 1B material.

The Social Media Services and Equipment Codes apply different compliance measures to industry participants depending on the risk that class 1A and class 1B material will be accessed, distributed, or stored on the service and made accessible to end-users in Australia. Services are categorised into three 'tiers' of risk. Tier 1 services are those that pose the highest level of relative risk and Tier 3 services pose the lowest.

Where required, industry participants must conduct their initial risk assessment as soon as practical following the commencement of the relevant industry code.[21] Given each Phase 1 Industry Code provided for a six-month transition period, it is expected that the risk assessment would be carried out prior to the date the code obligations come into effect or shortly thereafter.

In monitoring and assessing Phase 1 Industry Codes compliance, eSafety will consider whether an industry participant has accurately and objectively assessed its risk profile or categorised its service, as this may affect whether the industry participant has adopted the applicable compliance measures. eSafety may request information on risk categorisation informally or use its formal investigation powers.

The App Distribution Services, Hosting Services, Internet Service Providers and Search Engine Services Codes do not require risk assessments, as these services are treated under the codes to have a generally equivalent risk profile. As such, these

[19] As defined in Section 13 of the Act.
[20] As defined in Section 13A of the Act.
[21] Consolidated Industry Codes of Practice for the Online Industry (Class 1A and Class 1B Material) Head Terms, cl 5.2(a).

Phase 1 Industry Codes apply a uniform set of compliance measures for industry participants.

More information about risk profiles and risk assessments can be found in the Head Terms of relevant Schedule of the Phase 1 Industry Codes.

i. Assessing risk and categorisation in the Social Media Services and Equipment Codes

Social Media Services

The Social Media Services Code outlines that Social Media Services must undertake a risk assessment to determine whether they are a Tier 1, Tier 2 or Tier 3 Service, with two exceptions:

- The Social Media Service chooses to automatically assign a Tier 1 risk profile (Social Media Services Code, clause 4.1).
- The Social Media Service is deemed to have a Tier 3 risk profile (Social Media Services Code, clause 4.3).

The table in clause 5(d) of the Social Media Services Code is a useful guide for service providers to develop a risk assessment methodology. If a risk assessment indicates that the service may be in-between risk tiers, the provider **must** assign a higher risk profile to that service.[22]

If a service provider has chosen to automatically assign a Tier 1 risk profile to its Social Media Service, the service provider was meant to have notified eSafety on or before 16 December 2023.

If this has not been done prior to this date, a risk profile notification should be sent to codes@esafety.gov.au.

Equipment Services

The Equipment Code differentiates between three different kinds of equipment: interactive (Tier 1), secondary (Tier 2) and non-interactive (Tier 3) devices.

The guidance around the definitions of interactive (Tier 1) devices and secondary (Tier 2) devices in clause 5 of the Equipment Code assist participants categorise their devices and therefore understand their applicable compliance measures under the Equipment Code.

[22] Schedule 1 – Social Media Services Online Safety Code (Class 1A and Class 1B Material), cl 5(c).

The Equipment Code also creates the categories of 'OS provider' and 'gaming devices' to which additional compliance measures apply, irrespective of which risk tier the equipment falls under.

ii. eSafety may request information from industry participants about risk profiles or categories

If a risk assessment is required under an industry code, the industry participant must notify eSafety of the risk profile it has assigned to its online activities, services or device type upon eSafety's request.[23] The industry participant's response must include their reasons and justification for assigning a particular risk profile or category.

Where a provider is required to submit a code report under compliance measures 32 and 33 of the Social Media Services Code, that report must include details of any risk assessment and methodology adopted for the risk assessment. eSafety may also request preliminary information about risk profiles from industry participants prior to the due dates for these reports.

Where a service falls within a category which is exempt from risk assessment obligations, eSafety may request information from the industry participant about its reasons and justifications for the exemption.[24]

c) Implementing code requirements

Phase 1 Industry Codes are designed to provide industry participants with flexibility to implement compliance measures to meet the objectives and outcomes in a way that is suited to their services. This reflects a technology-neutral approach. The objectives and outcomes of the Phase 1 Industry Codes are listed in clause 4 of the Head Terms.

All compliance measures are mandatory unless they are specified as optional or if an industry participant is exempt based on their risk profile or category. More information about the process industry participants should take to identify and understand compliance measures can be found at clause 5 of the Head Terms.

---

[23] Consolidated Industry Codes of Practice for the Online Industry (Class 1A and Class 1B Material) Head Terms, cl 5.2(a)
[24] Consolidated Industry Codes of Practice for the Online Industry (Class 1A and Class 1B Material) Head Terms, cl 5.2(a), note.

To effectively implement the relevant compliance measures, industry participants should:

- use the process outlined at clause 5.2 of the Head Terms to identify the applicable industry code for each service, its risk profile (tier) and consequent compliance measures.
- use the guidance notes included in the Head Terms and each Schedule to assist in understanding compliance measures and how to meet them – these often include practical examples of steps industry participants could take, depending on the nature and functionality of their services
- be able to demonstrate that the compliance measures it has adopted are reasonable[25] – this will include demonstrating how compliance measures have been adopted, maintaining relevant documentation and providing that documentation to eSafety when required.

eSafety strongly encourages industry participants to take appropriate alternative action if compliance with a particular measure will result in breach of Australian laws or taking a step of the kind outlined in clause 6.1 of the Head Terms.

Participants should maintain detailed documentation about compliance with the relevant compliance measures and be prepared to report to eSafety about steps taken to comply when eSafety requires or requests this information.

i. Record keeping requirement

Industry participants should keep records of the compliance measures they have adopted for the previous two years.[26]

This information will help eSafety to assess whether industry participants are fulfilling their industry code obligations and whether an industry code is working as intended.

Information should be stored in a format that allows records to be retrieved and provided to eSafety (at eSafety's request, or as part of code compliance report requirements). Industry participants should retain an appropriate amount of detail in these records to assist eSafety to assess industry code compliance.

[25] Consolidated Industry Codes of Practice for the Online Industry (Class 1A and Class 1B Material) Head Terms, cl 5.1(b).
[26] Consolidated Industry Codes of Practice for the Online Industry (Class 1A and Class 1B Material) Head Terms, cl 7.2(b).

Examples of records eSafety would expect to be available under the Phase 1 Industry Codes include, but are not limited to:

- policies regarding class 1A and class 1B material
- standard operating procedures, or other systems, processes or policies for enforcing policies regarding class 1A and class 1B material
- data on reports received regarding class 1A and class 1B material, and complaints about code compliance
- data on actions taken in response to complaints made by end-users in Australia
- information about tools, systems and processes the industry participant deploys to detect and remove, or otherwise prevent the availability of class 1A and class 1B material, and in particular child sexual abuse material and pro-terror material
- information about investments the industry participant is making in tools, safety technologies or research to enhance the safety of the service.

Part 3: What eSafety can and cannot help industry participants with

a) Legal advice

eSafety can provide general guidance to industry participants but cannot provide legal advice.

Examples of advice that may, depending on the guidance sought, be legal in character include:

- interpretation of a provision in industry codes (or standard) or the Act
- appropriate classification of material
- whether the risk assessment undertaken is appropriate
- whether certain actions or particular tools will satisfy compliance measures.

Where industry participants are concerned about their code compliance, they should seek their own legal advice.

b) Seeking general information and guidance

The Head Terms state that industry participants may seek guidance and information from eSafety if they are unsure which Phase 1 Industry Code (or standard) applies to them and what steps they should take to meet compliance measures.[27]

The guidance or information that eSafety will be able to provide in response to such requests will be general in nature. eSafety is unable to provide legal advice.

eSafety will seek to work cooperatively with industry participants and will place significant weight on good faith and reasonable efforts by an industry participant to comply with the applicable industry code, particularly in the early stages.

Industry participants can contact eSafety at codes@esafety.gov.au.

Industry participants may also wish to contact industry associations that developed the Phase 1 Industry Codes at hello@onlinesafety.org.au.

[27] Consolidated Industry Codes of Practice for the Online Industry (Class 1A and Class 1B Material) Head Terms, 4.

eSafety will also engage – both informally and in the course of compliance assurance activities – with industry participants and also industry associations to understand industry participants' experiences during implementation of Phase 1 Industry Codes. This will assist eSafety to identify any challenges and unintended consequences that may be contrary to the objectives of the Act.

eSafety will look to publish updated guidance on how to comply with Phase 1 Industry Codes as particular compliance and enforcement issues are identified.

Part 4: Communicating with eSafety

Certain measures in the Phase 1 Industry Codes require industry participants to communicate with eSafety.

The key communication obligations for industry participants are:

- notifying eSafety of risk profiles (Social Media Services and Equipment Codes)
- updating eSafety about relevant changes to the functionality of their services (Social Media Services, App Distribution Services, Equipment and Search Engine Services Codes)
- referring complaints to eSafety (Social Media Services, Internet Carriage Services and Search Engine Services Codes)
- notifying eSafety of app removals (App Distribution Services Code)
- submitting code compliance reports (applies to industry participants under all industry codes, except Tier 3 Social Media Services; and Equipment Services that are **not** manufacturers of Tier 1 devices, operating system providers, or manufacturers of Tier 2 devices).

eSafety's systems will securely store information provided as part of these communications.

eSafety expects industry participants covered by Phase 1 Industry Codes to communicate with eSafety in a timely, appropriate and collaborative manner. Phase 1 Industry Codes contain compliance measures that require some industry participants to implement specific policies and procedures that ensure they respond to eSafety about particular industry code matters.[28]

Even if there is no express compliance measure to communicate with eSafety on particular matters, eSafety considers that productive communication is consistent with the objectives and outcomes of industry codes, and therefore essential to enable the co-regulatory scheme to succeed.[29]

Industry participants can contact eSafety at codes@esafety.gov.au.

[28] See for example, Hosting Services Code, compliance measure 5; Equipment Code, compliance measure 3.
[29] Outcome 6 across the Phase 1 Industry Codes is that Industry participants communicate and cooperate with eSafety in respect of matters relating to class 1A and class 1B material, including complaints.

a) Risk profile notifications

Unless an industry participant has automatically assigned the highest risk tier to its service, it does not need to proactively notify eSafety of its risk profile or category. eSafety can, however, seek this information from an industry participant. Further information on the notification requirements is at Part 2(b) of this guidance.

b) Relevant changes to service functionality

The Social Media Services, App Distribution Services, Equipment Services and Search Engine Services Codes each require industry participants to provide updates to eSafety on significant new features or changes to service functionality that may have a material effect on end-users in Australia. These requirements support outcome 6 of the Phase 1 Industry Codes – to communicate and cooperate with eSafety in respect of matters relating to class 1A and class 1B material.

Phase 1 Industry Codes do not require industry participants to provide these updates prior to the launch of a new feature or functionality, nor do they require the industry participant to disclose confidential information to eSafety.

Compliance measures across the Phase 1 Industry Codes vary in terms of when an industry participant is required to notify eSafety of a change to service functionality, and in what format.

Table 4: Notification requirements for changes to service functionality under the Phase 1 Industry Codes

Code and compliance measure	Format and timeframe
Social Media Services Compliance measure 19	Timeframe not specified. Format not specified: A Tier 1 service provider may choose to provide the information in a code compliance report to eSafety.
App Distribution Services Compliance measure 6	Format and timeframe not specified.
Equipment Services Compliance measure 4	Format and timeframe not specified, except for clarifying that information will be shared after any public announcement.
Search Engine Services Compliance measure 8	Updates eSafety on any significant changes to the service: • within 42 days of a written request by eSafety, if the new features or functionality has a material negative effect on risk, and • in the Search Engine Service's code compliance report.

This is a proactive obligation that sits alongside eSafety's investigatory powers[30] as well as eSafety's powers in connection with the Basic Online Safety Expectations (outlined in Part 5 of this guidance). Confidentiality concerns are not grounds for refusing to provide a particular document or piece of information when required to under the Act.

eSafety recommends that industry participants provide updates to eSafety as soon as practicable following the launch of a relevant new feature or functionality change.

In some circumstances, it may be appropriate for an industry participant to provide an update through a code compliance report given to eSafety rather than through a separate notification. However, if there is a reasonable period of time between the implementation of the feature and the provision of the code compliance report, we expect that eSafety will be notified of the new feature separately to the code compliance report.

Generally, eSafety considers that it would be good practice for industry participants to notify eSafety within two weeks of a new feature or functionality change.

c) Referring complaints to eSafety

i. Referring complaints to eSafety about non-compliance: Tier 1 Social Media Services and Search Engine Services

Industry participants that provide a Tier 1 Social Media Service or a Search Engine Service must refer to eSafety any complaints made about their non-compliance with the relevant industry code that they have not been able to resolve.[31]

eSafety expects industry participants to set up dedicated mechanisms enabling end-users in Australia to make complaints about non-compliance with the relevant industry code and internal pathways which also enable the industry participant to identify which user complaints relate to their obligations under a Phase 1 Industry Code.

eSafety considers this requirement will be met if the industry participant directs an individual user to eSafety's industry codes' complaint form, which is available at esafety.gov.au/report and esafety.gov.au/industry/codes.

---

[30] See generally Part 14 of the Act. The Act enables the Commissioner to require a person to provide documents or information or attend before the Commissioner in relation to an investigation under Section 42, which includes an investigation into whether an industry participant has breached a relevant industry code or standard: Section 199.

[31] Social Media Services Code, compliance measure 18; Search Engine Services Code, compliance measure 7.

This form requires a user to identify whether they have already made a complaint to the industry participant about its non-compliance with the code.

eSafety recommends that industry participants give users who make a complaint a reference number to provide to eSafety so the complaint can be tracked by eSafety and the industry participant.

eSafety also recommends that industry participants provide data on the number of complaints they have referred to eSafety as part of code compliance reports (see Part 3(e) of this guidance).

ii. Referring complaints to eSafety: Internet Service Providers

The Internet Service Provider Code requires Internet Service Providers to either respond to any complaint it receives from an end-user in Australia about class 1A and class 1B material, or refer the user to eSafety.[32] eSafety considers that this obligation could be met if the industry participant's complaints handling process directs the end-user making the complaint to eSafety's illegal and restricted content reporting form, which is available at esafety.gov.au/report.

This requirement to refer users is separate and in addition to compliance measure 7 of the Internet Service Providers Code, and similar compliance measures under the other Phase 1 Industry Codes, that require industry participants to provide links or information to end-users in Australia about how to make a complaint to eSafety.

d) Notifying eSafety of app removals

The App Distribution Services Code requires App Distribution Services to notify eSafety if they remove a third-party app from their service, where the removal relates to the availability of class 1A material.[33] This notification must be made in writing and as soon as reasonably practical.

What is reasonably practical will depend on the circumstances of the particular case. eSafety considers that 24 hours will usually be an appropriate period to notify eSafety. This supports the purpose of the compliance measure and provides consistency with App Distribution Services' broader obligations under the Act.

Timely notification enables eSafety to determine whether other app distribution services should be informally asked or formally required (via an app removal notice,

[32] Internet Service Provider Code, compliance measure 8.
[33] App Distribution Services Code, compliance measure 5.

if the conditions are met) to remove an app which provides access to class 1 material.

An app removal notice is a written notice issued by eSafety under the Act. If certain requirements under the Act are met, the notice can be given to require the App Distribution Service to remove an app, including a computer program, that provides access to class 1 material from a service, within 24 hours or a longer timeframe specified by eSafety.[34]

eSafety will directly contact App Distribution Services to establish and implement a notification process.

e) Reporting on compliance with industry codes

Industry participants may be required to report to eSafety on their compliance with an applicable Phase 1 Industry Code (**code compliance report**) either annually or on request by eSafety.[35]

If a code compliance report is not provided to eSafety as required, or the report suggests non-compliance with the applicable Phase 1 Industry Code or does not provide sufficient detail, eSafety may commence an investigation and/or issue an industry participant with a written direction to comply with the industry code.[36]

Table 5: Reporting requirements under each Phase 1 Industry Code

Code	Reporting compliance measures
Social Media Services	Compliance measure 32 – Code compliance reports • Applies to: Tier 1 Social Media Services Compliance measure 33 – On request by eSafety • Applies to: Tier 2 Social Media Services
App Distribution Services	Compliance measure 9 – On request by eSafety • Applies to all App Distribution Services
Hosting Services	Compliance measure 8 – On request by eSafety • Applies to all Hosting Services
Internet Service Providers	Compliance measure 10 – On request by eSafety • Applies to all Internet Service Providers
Equipment Services	Compliance measure 13 – Code compliance reports

[34] Section 128 of the Act.
[35] Consolidated Industry Codes of Practice for the Online Industry (Class 1A and Class 1B Material) Head Terms, cl 7.3. See also each applicable Schedule for the information required under code compliance reports.
[36] Section 143 of the Act.

Code	Reporting compliance measures
	• Applies to: Manufacturers of interactive (Tier 1) devices and operating system providers Compliance measure 14 – On request by eSafety • Applies to: Manufacturers of secondary (Tier 2) devices
Search Engine Services	Compliance measure 17 – On request by eSafety • Applies to all Search Engine Services

i. eSafety's preferred approach to code compliance reporting timeframes

Annual Code Compliance Reports

Certain industry participants covered by the Social Media Services Code and Equipment Code are required to submit code compliance reports annually.

Even though the first code compliance reports are required to be submitted within 12 months after the commencement of Phase 1 Industry Codes (which would be 16 December 2024),[37] eSafety will consider industry participants that submit their first code compliance report by **15 February 2025** to be compliant with their code compliance reporting requirement.

The reason for this approach is to ensure the reporting period can cover a full 12-month period from the commencement of the Phase 1 Industry Codes and to allow the industry participants sufficient time to collate the data and prepare the code compliance report.

eSafety's preference is for all code compliance reports to cover:

- a reporting period of 12 months
- consistent reporting periods (every 12 months)
- the same reporting periods for industry participants.

eSafety's preferred timeframe for code compliance reports is outlined in **Table 6**.

[37] Social Media Services Code, compliance measure 32; Equipment Services Code, compliance measure 13.

Table 6: eSafety's preferred code compliance reporting timeframes

	Year 1		Year 2	
	First report due	**Reporting period**	**Second report due**	**Reporting period**
Social Media Services Code and Equipment Code	15 February 2025	16 December 2023 – 15 December 2024 (12 months)	15 February 2026	16 December 2024 – 15 December 2025 (12 months)

This approach will ensure consistency in reporting periods between years 1 and 2 and will support eSafety to understand an industry participant's progress in meeting compliance measures each year. It is also expected to be easier to administer for industry participants given other regulatory or voluntary reporting schemes industry participants are involved in, compared to a shorter reporting period.

Having comparable data between industry participants in an industry section will assist eSafety understand whether a Phase 1 Industry Code is working as intended or if there are deficiencies that need to be addressed.[38] This will also assist eSafety to contribute to any review of industry codes coordinated by industry associations.[39]

Code compliance reports will also help eSafety identify whether investigation and/or enforcement action is required. However, where other information is available, eSafety will not wait until code compliance reports are provided before taking investigatory or enforcement steps.

Code compliance reports on request

Where a code compliance report is required to be submitted on eSafety's request, the industry participant must submit their code compliance report **within 2 months** of receiving eSafety's request.

eSafety will not require an industry participant to provide a code compliance report earlier than 12 months after the relevant Phase 1 Industry Code comes into effect.

This does not preclude eSafety from asking industry participants for other information under different provisions in the relevant Phase 1 Industry Codes (for example, a risk profile notification).

[38] Section 145(1)(c) of the Act.
[39] Consolidated Industry Codes of Practice for the Online Industry (Class 1A and Class 1B Material) Head Terms, cl 7.6.

ii. Code compliance report format

eSafety will develop templates that industry participants can use to submit code compliance reports. While industry participants are not required to report to eSafety in a particular format, eSafety highly encourages using a code compliance report template developed by eSafety. This will best support industry participants to provide the information eSafety requires to assess compliance and reduce the likelihood that eSafety will need to seek clarifying information.

eSafety's industry codes webpage will contain practical guidance on how to access relevant forms or templates as they become available.

iii. Confidentiality of information in code compliance reports

Generally, eSafety does not intend to publish code compliance reports or confidential information provided by industry participants. This does not however limit the eSafety Commissioner's ability to exercise her functions under the Act.

The Head Terms outline that if an industry participant identifies material in a code compliance report as confidential information, eSafety must maintain such material in confidence.[40]

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 Industry Codes is to assist eSafety to determine compliance with the relevant Phase 1 Industry 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

[40] Consolidated Industry Codes of Practice for the Online Industry (Class 1A and Class 1B Material) Head Terms, cl 7.3(b).

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. 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)
- 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.

The Phase 1 Industry Codes also allow for industry participants to refer to information provided under existing voluntary reporting, or another reporting requirement under the Act.[41] This may include publicly available information or information provided in response to a notice in connection with the Basic Online Safety Expectations (discussed in Part 5(a) of this guidance). The purpose of this is to reduce the regulatory burden on industry participants and potential duplication.

[41] Consolidated Industry Codes of Practice for the Online Industry (Class 1A and Class 1B Material) Head Terms, cl 7.3(d)-(e).

Part 5: How do Phase 1 Industry Codes interact with other regulatory requirements under the Act?

eSafety has a range of legislative functions and powers to regulate harmful online content, including powers to issue removal notices and investigate breaches of industry participants' regulatory requirements. Some of these functions and powers interact with regulatory requirements under the Phase 1 Industry Codes.

This section outlines how Phase 1 Industry Codes may interact with other regulatory requirements in the Act.

a) Basic Online Safety Expectations

The Basic Online Safety Expectations (**Expectations**) set out the steps the Australian Government expects should be taken by providers of Designated Internet Services, Relevant Electronic Services and Social Media Services to keep end-users in Australia safe online.

Compliance with the Expectations is not mandatory. However, eSafety has powers under the Act to obtain information from the applicable providers on a periodic or non-periodic basis, about the steps they are taking to comply with the Expectations. eSafety can also publish statements about whether providers have or have not complied with the Expectations and summaries of the information received in response to notices. The aim is to increase the transparency and accountability of providers, thereby helping to incentivise and improve safety standards.[42]

The Expectations are set out in a determination from the Minister for Communications, Urban Infrastructure, Cities and the Arts.[43] The Determination is a regulatory instrument. In addition to the Expectations, it also includes non-exhaustive examples of reasonable steps that can be taken to meet the Expectations.

---

[42] See generally Part 4 of the Act. A failure to comply with a reporting notice to the extent that a person is able can attract a civil penalty (up to 500 penalty units) in addition to other enforcement action: Section 50 of the Act.

[43] For the complete Expectations, see *Online Safety (Basic Online Safety Expectations) Determination 2022* (23 January 2022) and associated Explanatory Statement. Both can be found on the Federal Register of Legislation's website at https://www.legislation.gov.au/.

The Expectations cover a broader range of online material and activity than the Phase 1 Industry Codes. While some Expectations relate to material that can be required to be removed under the Act, other Expectations require steps in relation to all unlawful or harmful material and activity. Examples of unlawful material and activity covered by the Expectations include material that is illegal or refused classification[44], grooming of children, and the sharing non-consensual intimate images. Other harmful online material and activity covered by the Expectations include:

- all material or activity prohibited by law
- all harmful online material and activity under the Act
- other harmful activity that is prohibited or otherwise addressed in a provider's terms of use, policies and procedures, or standards of conduct for end-users.

Accordingly, the compliance measures in the Phase 1 Industry Codes are narrower in scope than the Expectations as they focus on class 1A and class 1B material, rather than the broader unlawful and harmful material and activity covered by the Expectations.

Interaction with Phase 1 Industry Codes

Compliance measures in the Phase 1 Industry Codes (and forthcoming industry standards) will be more specific and prescriptive than those in the Expectations.

Steps taken to meet Expectations that relate to class 1 material will be relevant for many compliance measures under the Phase 1 Industry Codes. However, compliance with each compliance measure in the Phase 1 Industry Codes will be assessed on its own merit.

Similarly, given the breadth of the Expectations, additional steps beyond those set out in the Phase 1 Industry Codes (and forthcoming industry standards) may be required to meet the applicable Expectations.

In certain circumstances, eSafety may use information about a provider's compliance with the Expectations or information published in a transparency report to determine whether to commence an investigation about non-compliance with a code or standard.

[44] Under the National Classification Scheme.

eSafety's Regulatory Guidance – Basic Online Safety Expectations contains additional information about the Expectations and highlights where the Expectations may overlap with compliance measures under industry codes and standards.

More information about providing code compliance reports under both the Phase 1 Industry Codes scheme and Expectations is in Part 4(e) of this guidance.

b) Online Content Scheme

The Online Content Scheme under the Act gives eSafety a range of powers to deal with class 1 and class 2 material.

The framework for the development of industry codes and standards is one of the key features of this Part of the Act and focuses on improving, at a systemic level, the risk that class 1 and class 2 material is provided on the online services.

Other parts of the Online Content Scheme are focussed on removing specific pieces of highly harmful content and material. Key features include the following:

1. A complaints scheme for online material that may be illegal or for which access should be restricted.
2. Investigation and information gathering powers which allow eSafety to receive complaints about class 1 and class 2 material and investigate the provision of class 1 and class 2 material, whether in relation to a complaint or on eSafety's own initiative.
3. Removal and restriction powers which allow eSafety to, in certain circumstances, give notices that require providers of Social Media Services, Relevant Electronic Services, Designated Internet Services and Hosting Services to remove class 1 material and certain class 2 material (or restrict access to certain class 2 material) from their services or ensure that access to certain types of material is age restricted.
4. Powers related to compliance and enforcement of removal notices or notices requiring the restriction of material. This includes formal warnings, civil penalties, injunctions and seeking Federal Court orders to require a person to cease providing social media service, relevant electronic service, designated internet service or internet carriage service.

Key interaction with the Phase 1 Industry Codes

The Phase 1 Industry Codes deal with class 1A and class 1B material on online services at a **systemic level** while the other powers under the Online Content Scheme relate to **specific identified examples** of class 1 and class 2 material or content.

Under the Online Content Scheme, eSafety may give a notice to providers of Social Media Services, Relevant Electronic Services, Designated Internet Services or Hosting Services to take all reasonable steps to remove class 1 material within 24 hours or a longer timeframe specified by eSafety.[45]

In addition, eSafety may give a written notice to an App Distribution Service to require it to cease enabling the download of a particular app when certain requirements under the Act are met.[46]

eSafety can also give a link deletion notice to Search Engine Services requiring the service to stop providing a link that enables access to class 1 material within 24 hours or a longer timeframe specified by eSafety when certain requirements under the Act are met.[47]

These powers under the Online Content Scheme complement the compliance measures that industry participants are required to comply with under the Phase 1 Industry Codes.

Social Media Services, Hosting Service Providers, App Distribution Services and Search Engine Services must comply with any relevant notices issued by eSafety in relation to specific content and must also comply with the relevant Phase 1 Industry Code.

More information about the Online Content Scheme can be found in our Regulatory Guidance – Online Content Scheme.

c) Abhorrent Violent Conduct Powers

The Act includes powers which allow eSafety to request or require an Internet Service Provider to block material that promotes, incites, instructs in or depicts

[45] Sections 109-110 of the Act.
[46] Section 128 of the Act
[47] Section 124 of the Act.

'abhorrent violent conduct.'[48] These blocking requests and blocking notices can be issued in certain circumstances as defined by the Act.[49] They are only used where an online crisis event has been declared by eSafety under the Online Crisis Protocol.[50]

The Internet Service Providers Code operates alongside and complements the Abhorrent Violent Conduct scheme and related Online Crisis Protocol. The Internet Service Providers Code requires an Internet Service Provider to become a signatory to the Online Crisis Protocol on eSafety's request.[51]

More information about eSafety's Abhorrent Violent Conduct Powers can be found in the online publication Abhorrent Violent Conduct Powers - Regulatory Guidance.

d) Safety by Design

One of eSafety's functions under the Act is to formulate written guidelines or statements recommending best practices for promoting and maintaining online safety for Australians.[52]

Safety by Design is an eSafety initiative consisting of a set of principles and assessment tools that position user safety as a fundamental design consideration for online platforms and services. The initiative also includes resources for investors and financial entities and engagement with the tertiary education sector.

Safety by Design principles

At the heart of Safety by Design are three principles that provide platforms and services with guidance as they incorporate, assess and enhance user safety:

- **Service provider responsibility** - the burden of safety should never fall solely upon the user. Every attempt must be made to ensure that online harms are understood, assessed and addressed in the design and provision of online platforms and services.
- **User empowerment and autonomy** - the dignity of users is of central importance. Products and services should align with the best interests of users.
- **Transparency and accountability** - transparency and accountability are hallmarks of a robust approach to safety. They not only provide assurances that platforms

[48] Part 8 of the Act.
[49] Sections 95, 99 of the Act.
[50] A protocol developed by eSafety, Australian Internet Service Providers and the Communications Alliance (the industry body responsible for drafting the Internet Service Provider Code) setting out the administrative procedures required to notify Internet Service Providers of a potential online crisis event.
[51] Internet Service Providers Code, compliance measure 3.
[52] Section 27(1)(p)-(q) of the Act.

and services are operating according to their published safety objectives, but also assist in educating and empowering users about steps they can take to address safety concerns.

Example of the Service Provider Responsibility Principle in the Social Media Services Code

- The Social Media Services Code requires Tier 1 and Tier 2 Social Media Services to have reasonably adequate personnel to oversee the safety of the service.[53] While trust and safety functions may be allocated to external third-party service providers, the Social Media Service remains responsible for any outsourced functions and having appropriate processes in place to ensure compliance with the relevant compliance measure.
- In practice, Social Media Services must integrate their trust and safety function into the culture of their business. eSafety expects that trust and safety functions and implementation of the codes' compliance measures are subject to an adequate level of oversight and accountability by senior management.

Safety by Design assessment tools

The Safety by Design assessment tools are intended to provide both a safety health check and a learning resource that helps companies continually improve online safety. The Safety by Design assessment tools take industry participants through sets of targeted multiple-choice questions, as well as information that is relevant to the overarching stream they select.[54] The multiple-choice questions ask industry participants about the systems, processes and practices that are in place at their company. The responses generate a tailored report that identifies opportunities to improve user safety.

Interaction with Social Media Services and Search Engine Services Codes

Safety by Design principles and tools, although voluntary, can be used by industry participants as a way to support compliance with the Phase 1 Industry Codes. In particular, Safety by Design tools are referred to in the Social Media Services Code as a way to comply with compliance measures 5 and 13, and in the Search Engine Services Code as a way to comply with compliance measure 4.[55]

---

[53] Social Media Services Code, compliance measure 4.
[54] Streams include (1) Founder CEO/Director/Founder or (2) Product/Policy/Project Owner or Manager.
[55] Under Outcomes 1 and 2 to take reasonable and proactive steps to prevent or limit access or exposure to, and distribution of class 1A and 1B material.

These voluntary tools and their foundational principles provide industry participants with realistic, actionable and achievable measures to help safeguard users from online risks and harms. Industry participants can use these principles and tools to guide them as they incorporate, assess and enhance user safety for their platforms and products.

More information on the Safety by Design initiative and tools can be found on eSafety's website.

Part 6: eSafety's approach to compliance and enforcement

a) Monitoring and assessing code compliance

eSafety will monitor compliance with Phase 1 Industry Codes from the commencement of the Phase 1 Industry Codes. This will inform any decision eSafety makes to commence an investigation and/or issue a direction to comply with a Phase 1 Industry Code under the Act.[56]

eSafety may investigate, on its own initiative or in response to complaints, whether an industry participant has complied with the relevant Phase 1 Industry Code.[57]

eSafety can require the provision of relevant information through examination or the production of documents from any person for the purpose of an investigation under the Act.[58] A refusal or failure to provide the required information or documents may be subject to criminal or civil penalties where an appropriate exemption to the requirement cannot be made out.[59]

i. Information eSafety will take into account

eSafety may take a range of information into account when monitoring and considering industry participants' compliance with Phase 1 Industry codes, such as:

- complaints made directly to eSafety about potential non-compliance[60]
- information from unresolved user complaints about potential non-compliance referred to eSafety by Tier 1 Social Media Services[61]
- code compliance reports provided to eSafety
- information obtained through other eSafety regulatory mechanisms (such as the Expectations and complaints data about illegal and restricted online material)
- information that industry participants already publish voluntarily or as part of international transparency initiatives

[56] Section 143 of the Act.
[57] Section 42(1)(f) of the Act
[58] See generally Part 14 of the Act.
[59] Section 205 of the Act. Exemptions specified at subsections (3), (4) and (5).
[60] eSafety can receive complaints about potential code breaches under Section 40 of the Act.
[61] Social Media Services Code, compliance measure 18.

- information from stakeholders such as researchers, non-governmental organisations, law enforcement and/or other governments
- information obtained through any routine monitoring initiated by eSafety (for example, eSafety may check whether Tier 1 and Tier 2 Social Media Services have in place reporting and complaints mechanisms for class 1A and class 1B material).

ii. eSafety's approach to assessing compliance

In assessing an industry participant's compliance with a Phase 1 Industry Code, eSafety will consider whether the actions an industry participant has taken to fulfil the applicable compliance measures are reasonable in the relevant circumstances.

Industry participants are responsible for demonstrating that the compliance measures they have adopted are reasonable. Clause 5.1(b) of the Head Terms details the factors that they must take into account.

Head Terms, Phase 1 Industry Codes, clause 5.1(b)

It is the responsibility of each industry participant to be able to demonstrate that the compliance measures it has adopted are reasonable, taking into account:

(i) the importance of the applicable online safety objectives and outcomes 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;

(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; and

(v) other considerations set out in this Code.

In assessing compliance with the applicable code, eSafety will consider the factors just listed and will also consider the following:

- The risks related to the service and the proportionality of the steps taken by an industry participant in meeting a compliance measure, relative to the risks.
- Whether an industry participant can demonstrate that it is, or is effectively working towards, meeting the objective or outcome of a compliance measure. While industry participants will not be required to prove that the compliance measures they have adopted are achieving all objectives and outcomes, they should be able to demonstrate how the steps taken are working towards those objectives and outcomes. Substantiated information establishing that an industry participant has plans to take further action or other steps in the short to medium term will also be relevant.
- Whether a significant amount of class 1A and class 1B material is available on the service. eSafety recognises that the presence of class 1A and class 1B material on a service does not necessarily establish non-compliance with a Phase 1 Industry Code.[62] But where the steps taken by the industry participant to prevent or limit this material (particularly class 1A material) are having very little to no impact, this could indicate that the compliance measures adopted by the industry participant are not reasonable for its service.
- Whether an industry participant can demonstrate the effectiveness of a step taken to systemically address the availability or accessibility of class 1A or class 1B material.
- Whether the industry participant has engaged constructively with eSafety and is acting in good faith to meet their compliance measures.

In assessing compliance, eSafety:

- will take a fair and evidence-based approach
- will focus on the impact compliance measures are having on the accessibility of class 1A and class 1B material to end-users in Australia where that information is available – this is consistent with the scope of Phase 1 Industry Codes
- will not assess compliance with optional compliance measures[63]
- will, to the extent that compliance with particular compliance measures is targeted, focus on compliance measures related to addressing and mitigating the most seriously harmful material – predominantly child sexual exploitation material and pro-terror material (class 1A)

[62] Consolidated Industry Codes of Practice for the Online Industry (Class 1A and Class 1B Material) Head Terms, cl 5.3.
[63] Compliance with optional enforcement measures may be taken into account by eSafety when considering whether or not a Phase 1 Industry Code is deficient.

- may use information gathered from monitoring, assessment and enforcement action to identify specific priority areas for compliance during subsequent years
- will communicate any priority areas publicly to encourage proactive compliance.

eSafety recognises the importance of industry participants being given sufficient time to prepare for the required compliance measures. This is reflected in the 6-month transition period from registration to commencement in the Phase 1 Industry Codes.

Further, eSafety will, in the 6-12 months following commencement, principally focus on monitoring and compliance rather than enforcement for this initial period. However, enforcement options will be considered during this period in instances of serious or deliberate non-compliance.

iii. What happens if an industry participant is not complying with an industry code?

eSafety will ordinarily take the following steps to help identify whether an industry participant is not complying with a Phase 1 Industry Code:

Step 1: Actively monitor compliance with the Phase 1 Industry Code. This could include assessing the number of complaints about potential non-compliance that eSafety has received and compiling complaints about class 1A and class 1B material that have been received by eSafety about illegal and restricted online material on the relevant service(s).

Step 2: Commence an investigation. This could include informally approaching an industry participant to obtain further information or the use of information-gathering powers under the Act.[64] The investigatory steps taken by eSafety will depend on the nature of the potential breach, the information already available to eSafety and other factors.

Step 3: The eSafety Commissioner or relevant delegate determines whether they are satisfied that the industry participant has contravened or is contravening a Phase 1 Industry Code that applies to them.

Step 4: The eSafety Commissioner or relevant delegate gives a written direction to comply with an industry code under the Act.[65]

Step 5: If an industry participant does not comply with the written direction, eSafety will determine whether to take additional compliance and enforcement steps. Non-

[64] Sections 199, 203 of the Act.
[65] Section 143 of the Act.

compliance may lead to enforcement action, including a civil penalty of up to 500 penalty units.[66]

The steps taken in each case will depend on the circumstances. In some cases, eSafety may decide education and/or an informal request to seek rectification of a compliance issue is appropriate and likely to achieve compliance quickly.

Under the Head Terms of the Phase 1 Industry Codes, if eSafety has notified an industry participant that they are non-compliant but the industry participant has reasonable grounds for not being fully compliant, the industry participant will not be in breach provided they can demonstrate to eSafety's reasonable satisfaction that they are working towards compliance before the first anniversary of the registration date of the relevant Phase 1 Industry Code.[67]

Industry participants may seek guidance and information from eSafety, noting the limitations around the advice eSafety can provide outlined at Part 3.

iv. Review rights

An industry participant may seek either internal review or external review by the Administrative Appeals Tribunal of certain actions taken by eSafety relating to industry codes and standards.[68]

The purpose of these review rights is to ensure that eSafety has made the correct and preferable decision on a case-by-case basis.

Table 7: Reviewable directions for Phase 1 Industry Codes

Reviewable directions under the Act[69]	Who can seek review
Giving a direction to comply with a code Varying a direction to comply with a code Refusal to revoke a direction to comply with a code	The industry participant named in the direction

[66] Section 143(2) of the Act. The monetary value of 1 penalty unit is $313 (at the date of this regulatory guidance). In addition, the maximum penalty ordered by a Court against a corporation (which can include online service providers) can be 5 times more than the maximum penalty ordered against an individual.
[67] Consolidated Industry Codes of Practice for the Online Industry (Class 1A and Class 1B Material) Head Terms, cl 7.1 (b).
[68] Sections 220, 220A of the Act.
[69] Section 220(19) of the Act, referring to decisions under Section 143.

An internal review may not always be appropriate, particularly if the direction has been given by the eSafety Commissioner. Additional information about seeking a review can be found on eSafety's website.

b) Enforcement options

eSafety takes a graduated approach, where appropriate, to compliance and enforcement that strives to balance the protection of Australians while ensuring no undue burden is imposed on service providers and individuals.

eSafety has a range of enforcement options under the Act for addressing non-compliance with industry codes.

Enforcement options include the following:

- **Formal warnings:** A formal warning can be issued to advise an industry participant that they have failed to comply with the requirements of a Phase 1 Industry Code. This may be appropriate where there are no aggravating features or circumstances. A formal warning can be given on its own or at the same time as a written direction to comply with a Phase 1 Industry Code.[70]
- **Written direction to comply:** A participant can be given a written direction to comply if eSafety is satisfied that the participant has contravened or is contravening the requirements of a Phase 1 Industry Code that applies to them.[71] Failure to comply with a written direction may result in additional compliance action.
- **Enforceable undertakings:** An enforceable undertaking is available where an industry participant has failed to comply with a direction to comply with a Phase 1 Industry Code. An industry participant may enter into an agreement with eSafety to ensure compliance with a Phase 1 Industry Code. Once accepted by eSafety, the undertakings that an industry participant has agreed to can be enforced by a Court.[72]
- **Injunctions:** An injunction is an order granted by the Federal Court of Australia or the Federal Circuit Court of Australia to compel an industry participant to take certain actions, or to refrain from taking certain actions. An injunction is available where an industry participant has not complied with a direction to comply with a Phase 1 Industry Code.[73]

[70] Section 144 of the Act.
[71] Section 143 of the Act.
[72] Section 164 of the Act.
[73] Section 165 of the Act.

- **Infringement notices and civil penalty orders:** These require payment of a financial penalty and can be directed towards industry participants who do not comply with a direction to comply with a Phase 1 Industry Code.[74] A civil penalty order can only be made by a Court following civil penalty proceedings. An infringement notice can be given by an infringement officer within eSafety.
- **Seeking Federal Court orders to require a person to cease providing a social media service or internet carriage service:** eSafety may apply to the Federal Court of Australia to seek an order that a particular provider of Social Media Services, Relevant Electronic Services or Designated Internet Services stop providing that service in Australia, or for an Internet Service Provider to stop supplying that service in Australia. To apply for the order, eSafety must be satisfied that a service failed to comply with a civil penalty provision under the Online Content Scheme (such as a written direction to comply with a Phase 1 Industry Code) on two or more occasions over the past 12 months, and continued operation of the service poses a significant community safety risk. To grant the order, the Federal Court of Australia must also be satisfied of those factors.[75] eSafety will usually only pursue this option in relation to non-compliance with the industry codes or standards in the most extreme circumstances, such as where there is continuous and wilful non-compliance.

More information about eSafety's approach to enforcement and investigative powers can be found on our website in our Compliance and Enforcement Policy.

[74] Sections 162-163 of the Act.
[75] Sections 156-159 of the Act.

eSafety.gov.au