Phase 1 Codes (Class 1A and Class 1B Material) Regulatory Guidance

Updated December 2024

Australian Government | eSafetyCommissioner

eSafety.gov.au

Contents

Overview of this guidance

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

The Phase 1 Codes are a group of six codes developed by industry associations and registered by eSafety in 2023. Each Phase 1 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 Codes commenced on 16 December 2023, except for the Phase 1 Code covering search engine services which commenced on 12 March 2024.

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

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

This guidance provides information on:

- the legal and regulatory framework for industry codes and standards (Part 1)
- how to ensure compliance with the Phase 1 Codes obligations (Part 2)
- how eSafety can assist service providers (Part 3)
- communicating with eSafety (Part 4)

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

- how the Phase 1 Codes interact with other regulatory requirements under the *Online Safety Act 2021* (Cth) (the **Act**) (Part 5)
- eSafety's approach to compliance and enforcement with the Phase 1 Codes (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 and activity.

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**). These industry participants are referred to as 'service providers' in this guidance.

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

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.

---

[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.
[3] Sections 40, 42 of the Act.
[4] Sections 143-144, 146-147 and Part 10 of the Act.

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 ranges from the most seriously harmful illegal content, 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 can include written, video, audio and/or image-based material. Class 1 and class 2 material is 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 and Standards deal with class 1A and class 1B material:

- Class 1A material is material that is seriously harmful, including child sexual abuse material, pro-terror material, and extreme crime and violence.
- Class 1B material is also harmful but is more context dependent, and includes crime and violence and drug-related material.

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

[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.

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 is child sexual abuse material[8], that contains exploitative descriptions or depictions of a child, or 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**.[9] 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, or provides detailed instruction or promotion, **without justification**.	• 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] Child sexual abuse material, which shows a sexual assault against a child, is a narrower category and can be considered a sub-set of CSEM.

[9] 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 2	Class 2B	• Online pornography – material which includes realistically simulated sexual activity between adults. Material which includes high-impact[10] 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 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).

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

Under the Act, industry codes or standards apply to eight sections of the online industry.[11]

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

Industry section	Examples of services (non-exhaustive)
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* *Note: Unless an online service is otherwise considered a social media service or a relevant electronic service.

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

Social media services[12]	• social networks • public media sharing networks • discussion forums • consumer review networks
Search engine services	• electronic services designed to collect, organise (index) and/or rank information on the World Wide Web 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 World Wide Web more broadly.
App distribution services	• services distributing apps that can be accessed by end-users in Australia (for example app stores/marketplaces) Note: Excludes links to apps and download of apps from third party websites.
Hosting services	• services which host stored material in Australia (for example services with data centres located in Australia)
Internet carriage services	• retail internet service providers (ISPs) 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:
	  ○ mobile phones
	  ○ laptops
	  ○ tablets
	  ○ internet-enabled devices (such as smart TVs and gaming consoles)
	  ○ immersive technologies (such as virtual reality headsets)
	  ○ 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 or maintain such devices.

[12] As outlined on pages 14 to 15 of this guidance, where a service provider offers instant messaging, chat functionality, or any other functionality contained in the definition of relevant electronic services in section 13A of the Act, that service will likely be considered a relevant electronic service. This will affect providers of social media services, regardless of whether they predominantly provide social media functionality.

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

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

Table 3: Industry sections covered by Phase 1 Codes

Industry section	Applicable 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 Codes. These sections are regulated under the Phase 1 Standards instead:

- Relevant Electronic Services – Class 1A and Class 1B Material Industry Standard 2024 (**the Relevant Electronic Services Standard**)
- Designated Internet Services - Class 1A and Class 1B Material Industry Standard 2024 (**the Designated Internet Services Standard**).

More information can be found in our Phase 1 Standards Regulatory Guidance.

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 applicable industry associations consulted with their members, other service providers and the public more broadly in the preparation of the Phase 1 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.[13]

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 has registered industry standards to apply to these two sections of the online industry.[14]

Once an industry code is registered, it applies unless it has been revised (and re-registered) or the Commissioner determines it is deficient.[15] 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.[16]

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

Such a determination may only be made after an industry code has been registered for at least 180 days.[17]

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 applicable code and request that the deficiency (or deficiencies) identified be adequately addressed within a specified period.

[17] Section 145(1)(c) of the Act.

Part 2: Complying with the Phase 1 Codes

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

Identifying which code or standard applies

The Head Terms specify that service providers are required to comply with the Phase 1 Code or Standard applicable to each service which they operate.[18]

Where the service provider operates multiple online activities (where separate online services are offered), they may be required to comply with different codes or standards for each service. Service providers should consider clauses 2 and 3 of each Schedule, which outline the scope and definitions specific to each industry code, to help identify which applies to each online service it offers.

Example 1

A service provider operates an internet carriage service that falls within the Internet Service Provider Code. That provider also manufactures and/or supplies equipment that falls within the Equipment Code.

As a result, the provider would need to comply with both Internet Service Provider Code and the Equipment Code.

Example 2

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

The provider would need to comply with the Equipment Code and, once it commences, the Relevant Electronic Services Standard.

[18] 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.

Phase 1 Standards for relevant electronic services and designated internet services have been registered by eSafety and commence on 22 December 2024. Service providers that offer multiple electronic services, or a service which integrates multiple functions, will need to also review those industry standards to ensure compliance.

eSafety may seek information informally from a service provider about its risk profile, or exercise the powers under the applicable code or standard of the Act to require the provision of this information.

Providers that align with both a social media service and relevant electronic service

Services are increasingly fulfilling multiple purposes and offering several features for users. In particular, some social media services are also relevant electronic services. For example, a social media service may offer a range of features that enable social interaction and allow users to post content as outlined in the Act's definition for a social media service. If that service also includes, for example, instant messaging or chat functionality, then that service is likely to meet the definition of 'relevant electronic service' in the Act and therefore be subject to the Relevant Electronic Services Standard. The presence of other features relating to social media does not affect this categorisation.

The relevant electronic services definition provides for any service which enables communication with other end-users by means of email, instant messaging services, SMS services, MMS services, or online chat services, as well as services that enable end-users to play online games together. **A service which meets the definition is considered a relevant electronic service and the provider will be required to comply with the Relevant Electronic Services Standard, regardless of whether the service also meets the definition of another industry section.**

This is because section 5.2 of the Relevant Electronic Services Standard provides that it applies 'to the exclusion of any industry code'. The Act also provides that industry standards prevail over inconsistent industry codes.[19]

This creates a more uniform regulatory framework, which recognises the specific risks that messaging, chat and similar communications features provide, and which provides for greater certainty in the face of converging and evolving technologies.

[19] Section 150 of the Act.

Impacts on social media services with messaging, chat, or other 'Relevant Electronic Service' functionalities

Services which fit this scenario were subject to the Social Media Services Code, which came into effect on 16 December 2023. Actions taken by service providers in order to comply with the Social Media Services Code will assist in ensuring compliance with the Relevant Electronic Services Standard because the minimum compliance measures in the Social Media Services Code are largely applicable to the Relevant Electronic Services Standard (see Annexure A to this guidance). Providers can adapt any compliance processes established in response to the Social Media Services Code to the Relevant Electronic Services Standard.

However, once the Relevant Electronic Services Standard commences, services that fall into the definitions of both social media services and relevant electronic services will no longer have to comply with the Social Media Services Code. Instead, they will have to comply with the Relevant Electronic Services Standard.

To reduce the compliance burden for that subset of services, **eSafety will not enforce requirements on Tier 1 social media services which also constitute relevant electronic services to submit annual code compliance reports for the first year of industry codes operation (ending 16 December 2024),** as would have been required under MCM 32 of the Social Media Services Code.[20] Providers of a Tier 1 social media service which also constitutes a relevant electronic service may nonetheless choose to submit a Social Media Services Code compliance report, which eSafety will take into consideration in the future when determining whether to request or require information from relevant electronic services, including reports.

Risk assessment

The Phase 1 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 App Distribution Services Code, Hosting Services Code, Internet Service Providers Code and Search Engine Services Code do not require risk assessments, as these services are treated under the Phase 1 Codes to have a generally equivalent risk profile. As such, these Phase 1 Codes apply a uniform set of compliance measures.

However, the Social Media Services Code and the Equipment Code apply different compliance measures to providers depending on the risk that class 1A and class 1B

[20] For reporting periods see pages 27-28 of this guidance.

material will be accessed, distributed or stored on the service and made accessible to end-users in Australia. These 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, providers of these services must conduct their initial risk assessment as soon as practical.[21] Given each Phase 1 Code provided for a six-month transition period, it is expected that the risk assessment was carried out prior to the date the code obligations come into effect or shortly thereafter. If this did not occur, service providers should be prepared to explain why they could not undertake a risk assessment sooner.

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

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

Assessing risk and categorisation in the Social Media Services Code and Equipment Code

Social Media Services Code

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]

[21] Consolidated Industry Codes of Practice for the Online Industry (Class 1A and Class 1B Material) Head Terms, cl 5.2(a).
[22] Schedule 1 – Social Media Services Online Safety Code (Class 1A and Class 1B Material), cl 5(c).

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

If this was not been done prior to this date, a risk profile notification should be sent to codes@eSafety.gov.au, with an explanation of why it could not have been done sooner (for example, the service is new or its risk tiering has changed) .

Equipment Code

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 to categorise their devices and therefore understand their applicable compliance measures under the Equipment Code.

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.

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

If a risk assessment is required under an industry code, the service provider must notify eSafety of the risk profile they have assigned to each of services or equipment types upon eSafety's request.[23] The service provider 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 service providers 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 provider about its reasons and justifications for the exemption.[24]

---

[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.

Implementing code requirements

Phase 1 Codes are designed to give service providers 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 Codes are listed in clause 4 of the Head Terms.

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

To effectively implement the applicable compliance measures, service providers 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 service providers could take, depending on the nature and functionality of their services
- be able to demonstrate that the compliance measures they have 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.

If compliance with a particular measure will result in a breach of Australian laws, or is excluded by clause 6.1 of the Head Terms, eSafety strongly encourages services providers to take appropriate alternative action.

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

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

Record keeping requirements

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

This information will help eSafety to assess whether service providers 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). Service providers should retain an appropriate amount of detail in these records to assist eSafety to assess industry code compliance.

Examples of records eSafety would expect to be available under the Phase 1 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 service provider 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 service provider is making in tools, technologies or research to enhance the safety of the service.

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

Part 3: How eSafety can assist industry participants

The Head Terms to the Phase 1 Codes state that service providers may seek guidance and information from eSafety if they are unsure which 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 can provide further information on the interpretation of a provision in an industry code or standard or the Act, but is unable to provide legal advice as to how that provision applies to a specific set of circumstances.

Where service providers are concerned about their legal position with respect to Phase 1 Codes compliance, they should seek their own legal advice.

Service providers can contact eSafety with general enquiries through the industry codes and standards compliance portal. More information about the portal can be found on eSafety's website, including how to request access.

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

eSafety will also engage – both informally and in the course of compliance assurance activities – with service providers and industry associations to understand the experiences of service providers during implementation of Phase 1 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 Codes as particular compliance and enforcement issues are identified.

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

Part 4: Communicating with eSafety

Certain measures in the Phase 1 Codes require service providers to communicate with eSafety. The key communication obligations for service providers are:

- notifying eSafety of risk profiles (Social Media Services Code and Equipment Code)
- updating eSafety about relevant changes to the functions and features of their services (Social Media Services Code, App Distribution Services Code, Equipment Code and Search Engine Services Code)
- referring unresolved complaints to eSafety (Social Media Services Code, Internet Carriage Services Code and Search Engine Services Code)
- notifying eSafety of app removals (App Distribution Services Code)
- submitting code compliance reports (applies to service providers 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 service providers covered by Phase 1 Codes to communicate with eSafety in a timely, appropriate and collaborative manner.

Phase 1 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]

Service providers can provide some of the communications listed in this section through the industry codes and standards compliance portal. More information about the portal can be found on eSafety's website, including how to request access. All other communications can be made by contacting 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 Codes is that Industry participants communicate and cooperate with eSafety in respect of matters relating to class 1A and class 1B material, including complaints.

Risk profile notifications

Unless a service provider has automatically assigned the highest risk tier to its service/s, it does not need to proactively notify eSafety of the risk profile or category for the service/s. However, eSafety can seek this information from a service provider. Further information on the notification requirements is in Part 2 of this guidance.

Relevant changes to service functionality

The Social Media Services Code, App Distribution Services Code, Equipment Code and Search Engine Services Codes each require service providers 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 Codes – to communicate and cooperate with eSafety in respect of matters relating to class 1A and class 1B material.

Phase 1 Codes do not require service provider to provide these updates prior to the launch of a new feature or functionality, nor do they require the service provider to disclose confidential information about the new feature or functionality to eSafety.

Compliance measures across the Phase 1 Codes vary in terms of when a service provider is required to notify eSafety of a change to service feature or functionality, and in what format.

Table 4: Notification requirements for changes to service feature or 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	Update 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 service providers 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 a service provider 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 service providers to notify eSafety within two weeks of a new feature or functionality change.

Referring complaints to eSafety

Referring complaints: 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 applicable industry code that they have not been able to resolve.[31]

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

eSafety considers this requirement will be met if the service provider directs the end-user to eSafety's industry codes and standards complaints form, which is available at eSafety.gov.au/industry/codes/complaints.

---

[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 an applicable industry code or standard: Section 199.

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

This form requires an end-user to identify whether they have already made a complaint to the service provider about their alleged non-compliance with the applicable code.

eSafety recommends that service providers give end-users who make a complaints a reference number to provide to eSafety so the complaints can be tracked by eSafety and the service provider.

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

Referring complaints: 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 service provider'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 end-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 Codes, that require industry participants to provide links or information to end-users in Australia about how to make a complaint to eSafety.

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 broader obligations on app distribution services under the Act.

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

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

Reporting on compliance

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

If a 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 an investigation and/or issue a service provider with a written direction to comply with the industry code.[36]

However, please note the information on pages 15 to 16 in relation to providers of social media services which are required to comply with the Relevant Electronic Services Standard from 22 December 2024.

Table 5: Reporting requirements under each Phase 1 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

[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.

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 • 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

eSafety's preferred approach to compliance reporting timeframes

Annual code compliance reports

Certain service providers covered by the Social Media Services Code and Equipment Code are required to submit compliance reports annually.

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

The reason for this approach is to ensure the reporting period can cover a full 12-months from the commencement of the Phase 1 Codes and to allow the applicable service providers sufficient time to collate the data and prepare the compliance report.

eSafety's preference is for all compliance reports for applicable social media services and equipment services to cover:

- a reporting period of 12 months
- consistent reporting periods (every 12 months)
- the same reporting periods for all applicable service providers (service providers that are new, or change risk profiles, should contact eSafety to agree an appropriate reporting period).

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

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

Table 6: eSafety's preferred annual 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)

***Note the information on pages 14-15 in relation to providers of social media services which are required to comply with the Relevant Electronic Services Standard from 22 December 2024.**

This approach will ensure consistency in reporting periods between years 1 and 2 and will support eSafety to understand the progress of applicable service providers towards meeting compliance measures each year. It is also expected annual compliance reporting to be easier for the applicable service providers to administer than a shorter reporting period, given other regulatory or voluntary reporting schemes they are involved in.

Having comparable data between applicable service providers in an industry section will assist eSafety to understand whether a Phase 1 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]

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 compliance reports are provided before taking investigatory or enforcement steps.

Compliance reports on request

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

[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.

Compliance report format

eSafety has developed templates that social media services and equipment services can use to submit compliance reports. Templates for other sections of the industry may also become available.

While service providers are not required to report to eSafety in a particular format, eSafety highly encourages using a code compliance report template developed by eSafety where available. This will best support service providers to provide the information eSafety requires to assess compliance and reduce the likelihood that eSafety will need to seek further information.

eSafety's Industry codes and standards compliance page contains practical guidance on how to access applicable forms or templates.

Confidentiality of information in reports

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

The Phase 1 Codes Head Terms outline that if a service provider identifies material in a 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
- personally identifiable 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 compliance reports required under the Phase 1 Codes is to assist eSafety to determine compliance with the Phase 1 Code that applies to any service and identify whether investigation and/or enforcement is appropriate and necessary. eSafety does not intend to publish compliance reports required under Phase 1 Codes as a matter of course. However, the information provided in a

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

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. 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 Codes also allow for service providers 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 of this guidance). The purpose of this is to reduce the regulatory burden on service providers and potential duplication.

Annual forums

Certain services are required to participate in an annual forum under the Social Media Services Code, App Distribution Code and Equipment Code[42]. At the request of the industry associations**, eSafety has agreed not to enforce this requirement against service providers that do not participate in annual forums for the first year of operation of the Phase 1 Codes** (16 December 2023 – 15 December 2024). eSafety strongly encourages the industry associations to hold the annual forums required for year two (16 December 2024 – 15 December 2025) early in this period.

[41] Consolidated Industry Codes of Practice for the Online Industry (Class 1A and Class 1B Material) Head Terms, cl 7.3(d)-(e).
[42] Updated April 2025 to correct a reference to the App Distribution Code.

Part 5: How do Phase 1 Codes interact with other regulatory requirements?

eSafety has a range of legislative functions and powers to regulate harmful online content and activity, including powers to issue removal notices and investigate breaches of service providers' regulatory requirements. Some of these functions and powers interact with regulatory requirements under the codes and standards. This section outlines how Phase 1 Codes may interact with other regulatory requirements in the Act.

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 enforceable. 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.[43]

The Expectations are set out in a determination from the Minister for Communications.[44] The Basic Online Safety Expectations Determination is a regulatory instrument. In addition to the Expectations, it includes non-exhaustive examples of reasonable steps that can be taken to meet the Expectations.

The Expectations cover a broader range of online material and activity than the Phase 1 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

[43] 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.

[44] 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 include material that is illegal or refused classification[45], sexual 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 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 Codes

Compliance measures in the Phase 1 Codes and Standards) are more specific and prescriptive than those in the Expectations.

Steps taken to meet Expectations that relate to class 1 material are applicable for many compliance measures under the Phase 1 Codes. However, compliance with each compliance measure in the Phase 1 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 Codes and 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.

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 Phase 1 Codes and Standards.

More information about providing compliance reports under both the Phase 1 Codes and the Expectations is in Part 4 of this guidance.

[45] Under the National Classification Scheme.

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.

This part of the Act includes the framework for the development of industry codes and standards that are focused on reducing, at a systemic level, the risks associated with class 1 and class 2 material on online services.

It also focuses on using the Online Content Scheme for removal or restriction of specific instances of highly harmful material, referred to as 'Illegal and restricted content'. Key features include the following:

- A complaints scheme for online material that may be illegal or for which access should be restricted.
- 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.
- 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 from their services or ensure that access to certain types of class 2 material is age restricted.
- 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 a social media service, relevant electronic service, designated internet service or internet carriage service.

Interaction with the Phase 1 Codes

The Phase 1 Codes and Standards 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.

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.[46]

In addition, eSafety may give a written notice to an app distribution service requiring it to cease enabling the download of a particular app when certain requirements under the Act are met.[47]

eSafety can also give a link deletion notice to providers of 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.[48]

These powers under the Online Content Scheme complement the measures that service providers are required to comply with under the Phase 1 Codes and Standards.

Social media services, hosting service providers, app distribution services and search engine services must comply with any applicable notices issued by eSafety in relation to specific content and must also comply with the applicable Phase 1 Code.

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

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 'abhorrent violent conduct.'[49] These blocking requests and blocking notices can be issued in certain circumstances as defined by the Act.[50] They are only used where an online crisis event has been declared by eSafety under the Online Crisis Protocol.[51]

The Internet Service Providers Code operates alongside and complements the abhorrent violent conduct powers and related Online Crisis Protocol. The Internet

[46] Sections 109-110 of the OSA.
[47] Section 128 of the OSA
[48] Section 124 of the OSA.
[49] Part 8 of the Act.
[50] Sections 95, 99 of the Act.
[51] 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.

Service Providers Code requires an internet service provider to become a signatory to the Online Crisis Protocol on eSafety's request.[52]

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

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.[53]

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.

Principles

At the heart of Safety by Design initiative led by eSafety, there 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 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.

[52] Internet Service Providers Code, compliance measure 3.
[53] Section 27(1)(p)-(q) of the Act.

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.[54] 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 applicable 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.

Resources

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 assessment tools take service providers through sets of targeted multiple-choice questions, as well as information that is relevant to the overarching stream they select.[55] The multiple-choice questions ask service providers 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 the Social Media Service Code and Search Engine Services Code

Safety by Design principles and tools, although voluntary, can be used by industry participants as a way to support compliance with the Phase 1 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.[56]

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

[54] Social Media Services Code, compliance measure 4.
[55] Streams include (1) Founder CEO/Director/Founder or (2) Product/Policy/Project Owner or Manager.
[56] 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.

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

Part 6: eSafety's approach to assessing compliance and enforcement

Monitoring and assessing compliance

eSafety will monitor compliance with Phase 1 Codes. This monitoring will inform any decision eSafety makes to commence an investigation and/or issue a direction to comply with a Phase 1 Code under the Act.[57]

eSafety may assess and investigate, on its own initiative or in response to complaints, whether a service provider has complied with the applicable Phase 1 Code.[58]

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.[59] 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 demonstrated.[60]

Information eSafety will take into account

eSafety may take a range of information into account when monitoring and assessing the compliance of service providers with Phase 1 Codes.: These are some examples:

- Complaints made directly to eSafety about potential non-compliance with obligations.[61]
- Information from unresolved user complaints about potential non-compliance referred to eSafety by Tier 1 social media services.[62]
- Service providers' compliance reports provided to eSafety.
- Information obtained through eSafety's other regulatory mechanisms (such as the Industry Standards, the Basic Online Safety Expectations and complaints data about illegal and restricted online content).

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

- Information that service providers already publish voluntarily or as part of international transparency initiatives.
- Information from stakeholders such as researchers, non-government organisations, law enforcement agencies and/or other governments.
- Information obtained through any routine assessment initiated by eSafety. For example, eSafety may check whether Tier 1 and Tier 2 social media services have reporting and complaints mechanisms in place for class 1A and class 1B material.

eSafety's approach to assessing compliance

In assessing a service provider's compliance with a Phase 1 Code, eSafety will consider whether the actions the service provider has taken fulfil the applicable compliance measures

Service providers 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 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 listed in the Head Terms and will also consider the following:

- The risks related to the service and the proportionality of the steps taken by a service provider in meeting a compliance measure, relative to the risks.
- Whether a service provider can demonstrate that they are, or are effectively working towards, meeting the objective or outcome of a compliance measure. While service providers 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 Code.[63] But where the steps taken by the service provider 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 provider are not reasonable for its service.
- Whether a service provider 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 that compliance measures are having on the generation, access and distribution of class 1A material as a priority – to the extent that compliance with obligations is targeted to specific harms, eSafety will focus on obligations related to addressing and mitigating the most seriously harmful material (predominantly child sexual exploitation material and pro-terror material) and the detection and removal of that material

[63] Consolidated Industry Codes of Practice for the Online Industry (Class 1A and Class 1B Material) Head Terms, cl 5.3.

- will not assess compliance with optional compliance measures[64]
- 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.

What happens if a service provider is not complying with an industry code?

eSafety will ordinarily take the following steps to help identify whether a service provider is not complying with a Phase 1 Code:

Step 1: Actively monitor compliance with the Phase 1 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 content on the applicable service/s.

Step 2: Commence an assessment and/or investigation. This could include informally approaching a service provider to obtain further information, or the use of information-gathering powers under the Act.[65] The assessment or 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 service provider has contravened or is contravening a Phase 1 Code that applies to them.

Step 4: The eSafety Commissioner or relevant delegate gives a written direction to comply with a Phase 1 code under the Act.[66]

Step 5: If a service provider does not comply with the written direction, eSafety will determine whether to take additional compliance and enforcement steps.

Non-compliance may lead to enforcement action, including civil penalty proceedings.[67]

---

[64] Compliance with optional enforcement measures may be taken into account by eSafety when considering whether or not a Phase 1 Industry Code is deficient.
[65] Sections 199, 203 of the Act.
[66] Section 143 of the Act.
[67] Section 143(2) of the Act.

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.

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

Review rights

A service provider may seek either internal review or external review by the Administrative Review 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 Codes

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

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.

[68] Sections 220, 220A of the Act.
[69] Section 220(19) of the Act, referring to decisions under Section 143.

Enforcement options

eSafety takes a graduated approach, where appropriate, to compliance and enforcement. We strive to balance the protection of Australians against ensuring no undue burden is imposed on service providers.

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 a service provider that they have failed to comply with the requirements of a Phase 1 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 Code.[70]
- **Written direction to comply:** A provider can be given a written direction to comply if eSafety is satisfied that it has contravened or is contravening the requirements of a Phase 1 Code that applies to its service/s.[71] Failure to comply with a written direction may result in additional compliance action.
- **Enforceable undertakings:** An enforceable undertaking is available where a service provider has failed to comply with a direction to comply with a Phase 1 Code. A service provider may enter into an agreement with eSafety to ensure compliance with a Phase 1 Code. Once accepted by eSafety, the undertakings that a service provider 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 a service provider to take certain actions, or to refrain from taking certain actions. An injunction is available where a service provider has not complied with a direction to comply with a Phase 1 Code.[73]
- **Infringement notices:** Infringement notices are notices that set out the particulars of an alleged contravention and specify an amount to be paid. If it is not paid, eSafety may commence civil penalty proceedings. Infringement notices may be issued by eSafety and do not require the involvement of a Court.[74]

---

[70] Section 144 of the Act.
[71] Section 143 of the Act.
[72] Section 164 of the Act.
[73] Section 165 of the Act.
[74] Subject to requirements in the *Regulatory Powers (Standard Provisions) Act 2014*.

- **Civil penalty orders:** These require payment of a financial penalty and can be directed towards service providers that do not comply with a Phase 1 Code.[75] A civil penalty order can only be made by a Court following civil penalty proceedings.
- **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 a social media service, 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 Code) on two or more occasions over the past 12 months, and that 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.[76] 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.

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

Annexure A

Indicative comparison between the requirements in the Social Media Service Code and the RES Standard.

Obligation	Application to RES Standard	Application to SMS Code
Division 2—Compliance measures		
Terms of Use	✓ s 13	✓ Minimum compliance measures (MCM) 30, 31
Systems and processes for responding to breaches of terms of use: class 1A material	✓ s 14	✓ MCM 2
Responding to class 1A material	✓ s 15	✓ MCM 3
Notification of child sexual exploitation material and pro-terror material	✓ s 16	✓ MCM 1
Resourcing trust and safety functions	✓ s 17	✓ MCM 4
Safety features and settings	✓ s 18	✓ MCM 6, 7
Detecting and removing known child sexual abuse material and pro-terror material	✓ s 19-20 Requires systems, processes and technologies.	✓ MCM 8, 9 Requires systems, processes and/or technologies.
Disrupting and deterring child sexual exploitation/abuse material and pro-terror material	✓ s 21	✓[2] MCM 10
Development programs	✓ s 22	*Partly*[3] MCM 14, 16
Participation in an annual forum	✗	✓ MCM 15
Systems and processes for responding to breaches of terms of use: class 1B material	✓ s 23	✓ MCM 11
Responding to breaches of terms of use: class 1B material	✓ s 24	✓ MCM 12
Giving information about the Commissioner to end-users in Australia	✓ s 25	✓ MCM 21

Division 2—Compliance measures (CONTINUED)		
Responding to and referring certain unresolved complaints to the Commissioner	✓ s 26	✗
Dedicated section of service for online safety information	✓ s 27	✓ MCM 22
Division 3—Reports and complaints		
Mechanisms for end-users and account holders to report, and make complaints, to providers	✓ s 28	✓ MCM 25
Dealing with reports and complaints—general rules	✓ s 29	✓ MCM 26-28
Dealing with reports and complaints—additional rules for some services	✓ s 30	✗
At least annual reviews of effectiveness of its reporting systems and processes	✗	✓ MCM 29
Unresolved complaints about non-compliance to be referred to the Commissioner	✓ s 31	✓ MCM 18
Division 4—Requirements for reporting to the Commissioner		
Documents about risk assessments and other information	✓ s 32	✓ MCM 32, 33
Reports relating to technical feasibility and practicability of compliance with provisions of Division 2	✓ s 33	✗
Notifying changes to features and functions	✓ s 34	✓ MCM 19
Reports on outcomes of development programs	✓ s 35	✗
Annual compliance reporting by providers of Tier 1 Social Media Service	✗	✓ MCM 32
Commissioner may require compliance reports	✓ s 36	✗