Fact sheet: Registration of the Relevant Electronic Services Standard

June 2024

The eSafety Commissioner (eSafety) has registered the Online Safety (Relevant Electronic Services — Class 1A and Class 1B Material) Industry Standard 2024 (RES Standard). The RES Standard minimises and prevents harms associated with access and exposure to the most harmful forms of online material on these services (referred to as 'class 1A' and 'class 1B' material). It addresses gaps and enhances the safeguards in the industry's proposed code for these services, which was not accepted by the eSafety Commissioner. Background on this process can be found at: eSafety.gov.au/industry/codes/standards-consultation.

Which services does the RES Standard cover?

The RES Standard applies to relevant electronic services (RES) provided to end-users in Australia. Relevant electronic services are defined by the Online Safety Act 2021[1] as services that enable communication with other end-users by means of email, instant messaging, SMS, MMS or online chat, as well as services that enable end-users to play online games together.

What content is covered by the RES Standard?

The RES Standard covers two types of class 1 material that are associated with serious harms. These are:

- class 1A material, such as child sexual exploitation material (including child sexual abuse material) and pro-terror material
- class 1B material, such as crime and violence material and drug related material.

Australia's Online Safety Act 2021 defines these as materials that have been (or would be) Refused Classification under the National Classification Scheme, which can allow for legitimate uses of material (such as in art, research and journalism).[2]

[1] Section 13A of the Online Safety Act 2021.
[2] The National Classification Scheme is implemented through the Classification (Publications, Films and Computer Games) Act 1995.

How are services differentiated under the RES Standard?

The RES Standard recognises the different functionalities, capabilities and risks of the services covered by it. It sets out obligations that are proportionate and appropriate to the risk that class 1A or class 1B material will be accessed or generated by end-users of the service in Australia, or distributed to them using the service, or stored on the service.

Pre-assessed and **defined** categories have risk profiles deemed by eSafety. Services that do not fall within the pre-assessed or defined categories are required either to conduct their own risk assessments or assign themselves a Tier 1 risk profile. If a service assesses its risk as high, then it must assign itself a Tier 1 risk profile with the highest level of obligations. A medium-risk service can assign itself a Tier 2 profile. A low-risk service, which has minimal to no risk of being misused for class 1A or class 1B material, can assign itself a Tier 3 risk profile with minimal obligations under the RES Standard.

Pre-assessed categories	
Communication relevant electronic service	This includes services that have a predominant purpose of enabling an end-user to communicate with another end-user or to view, navigate or search for other end-users with or without already having their contact details, which does not fit the other categories in the RES Standard – specifically, online messaging services and some video conferencing services, as well as some carriage services (email but not text messaging).
Gaming service with communication functionality	A service that enables end-users to play online games with each other, and also enables end-users to share URLs, hyperlinks, images and/or videos.
Dating service	A service primarily used for dating that has a messaging function. This category does not include services that have a primary purpose of connecting end-users with escort or sex work services.

Defined categories	
Telephony RES	A Short Message Service (SMS) or Multimedia Messaging Service (MMS) provided over a public mobile telecommunications service.
Enterprise RES	A service provided to an organisation to enable end-users within that organisation to communicate with each other.
Gaming service with limited communication functionality	A service that enables end-users to play online games with each other and allows limited sharing of some kinds of material (for example, in-game images and/or pre-selected messages).

What are the key obligations of the RES Standard?

Key obligations of relevant electronic services (RES) under the RES Standard include the following:

- Pre-assessed and Tier 1 RES must implement appropriate systems, processes and technologies to detect and remove known (pre-verified) child sexual abuse material on their service. Providers are required to take appropriate alternative action where this is not technically feasible or reasonably practicable[3], or where other exceptions are applied. Providers of end-to-end encrypted services are not required to do anything that would break or weaken encryption.
- Communication RES, Tier 1 RES and gaming services with communication functionality must implement appropriate systems, processes and technologies to detect and remove known (pre-verified) pro-terror material on their service. Providers are required to take appropriate alternative action where this is not technically feasible or reasonably practicable[3], or where other exceptions are applied. Providers of end-to-end encrypted services are not required to do anything that would break or weaken encryption.
- Pre-assessed and Tier 1 RES must implement systems, processes and – where appropriate – technologies to disrupt and deter end-users from using the service to create, offer, solicit, access, distribute, or otherwise make available or store child sexual exploitation material or pro-terror material.
- Pre-assessed and Tier 1 RES with more than 1 million monthly active users must implement a development program including investment or activities designed to enhance the ability to detect child sexual abuse and pro-terror material and deter child sexual exploitation and pro-terror material on their services.
- Pre-assessed Tier 1 and Tier 2 RES must incorporate appropriate and effective features and settings that it determines would best minimise the risk of exposure to class 1A and class 1B material on the service. For certain RES, these include blocking unwanted contact, parental settings and other protections for children.

[3] Determining whether something is 'reasonably practicable' involves a balancing of the impediments that a service provider might encounter in implementing a technology, such as cost or business model limitations, against the severity of risks and harms to end-users.

- Most RES must have and enforce terms of use that prohibit end-users from using the service to solicit, access, distribute or store class 1A material or class 1B material. The terms of use in relation to child sexual exploitation material and pro-terror material can be enforced by the service provider through actions such as suspensions, restrictions, and/or terminations.
- Pre-assessed, Telephony, Tier 1 and Tier 2 RES must have systems and processes in place to allow the service to act on breaches of terms of use against class 1A and 1B material, prevent ongoing breaches and reduce the risk of further breaches.
- Pre-assessed, Telephony, Tier 1 and Tier 2 RES must provide 'in-service' reporting tools to enable end-users to make a report on class 1A or 1B material accessible on, or through, the service or in relation to a provider's non-compliance with the RES Standard.
- Pre-assessed, Tier 1 and Tier 2 RES must ensure their trust and safety functions are resourced to comply with the RES Standard and can effectively supervise the online safety of the service. In addition, these providers must have (or have access to) sufficient personnel with relevant skills, experience and qualifications to ensure compliance with the RES Standard.
- Most RES will be required to respond to notices from eSafety requiring compliance reports.

When do services have to comply with the RES Standard?

The RES Standard will come into effect on 22 December 2024*, six months after its registration by the Office of Parliamentary Counsel.

What are the consequences of not being compliant?

In the event of non-compliance, eSafety can issue a formal warning, issue an infringement notice, accept an enforceable undertaking, or seek an injunction or civil penalty in court.

After the RES Standard takes effect, if you are concerned that one or more of the obligations are not being complied with, you can make a complaint to eSafety through our website at: eSafety.gov.au/industry/codes/complaints.

* Date corrected 26 June 2024.

Complaints help eSafety to identify potential non-compliance by a service and understand wider issues around compliance with the industry codes, so we can help to keep Australians safer online. However, eSafety cannot use the industry codes and standards to resolve disputes between online services and end-users.

If you have encountered illegal content online, we encourage you to lodge a report with eSafety so this content can be removed. For more information on reporting, visit eSafety.gov.au/report.

Where can I find more information?

eSafety will publish regulatory guidance on the RES Standard prior to its commencement. All relevant information on the industry codes and standards can be found on our website at: eSafety.gov.au/industry/codes.

Industry participants may seek guidance and information from eSafety if they are unsure which industry codes or standards apply to them. However, eSafety cannot provide legal advice and industry participants who are concerned about their compliance with the RES Standard should seek their own legal advice.

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