Fact sheet: Post consultation changes to the Relevant Electronic Services Standard

June 2024

21 June 2024

Following consultation with industry, civil society organisations and other stakeholders the eSafety Commissioner (eSafety) has registered the Online Safety (Relevant Electronic Services – Class 1A and Class 1B Material) Industry Standard 2024 (known as the '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. It 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.

This fact sheet outlines some of the key changes made to the scope and obligations of the RES Standard following consultation. More information about the consultation – including submissions and summaries of the roundtables – can be found at: eSafety.gov.au/industry/codes/standards-consultation.

Key changes to the scope and services covered by the RES Standard

Section (current reference)	Details of change
5 Application of this industry standard	**Removal of a subsection.** This section no longer includes subsection (2) covering the test relating to a service's predominant functionality in determination of the application of the RES Standard or another industry standard or code. A provider of a relevant electronic service will only be required to comply with the RES Standard for that service.
6 General Definitions	**Combining of two categories.** For clarity, open communications RES and closed communications RES categories have been combined into 'Communication RES'. This includes email services, online messaging services (including chat) and some video conferencing services.

Section (current reference)	Details of change
Technical feasibility definition	**Removal of a section and amendment to approach.** The former Section 7, which included the technical feasibility definition, has been removed. Consistent with the approach in other legislation, technical feasibility is now undefined in the RES Standard and will maintain its 'ordinary meaning' under the law.

Key changes to the obligations applying to RES categories

Section (current reference)	Details of change
20 Detecting and removing known pro-terror material	**Removal of a service type.** Based on assessment of proportionality and risk, this section no longer applies to dating services.

Changes to the RES Standard's obligations

Section (current reference)	Consultation draft obligations	Details of change
19 Detecting and removing known child sexual abuse material **20 Detecting and removing known pro-terror material**	A service provider was not required to use a system, process or technology where it was not technically feasible for the provider to do so, under former sections 20(3) and 21(3).	**Amendment to section numbering and addition of further exceptions.** Former Sections 20(3) and 21(3) are now Sections 19(3) and 20(3) respectively. The obligation remains the same, but a service provider is also not required to implement a process, system or technology under any of these circumstances: • If it is not reasonably practicable to do so. (This change is based on feedback that technical feasibility alone was inadequate to encompass broader impediments that a service provider might encounter in implementing a technology, such as cost or business model limitations. However, those impediments alone would not be enough to demonstrate that something is not reasonably practicable – the extent of the challenges faced by service providers must be balanced against the severity of risks and harm to end-users.) • If doing so would introduce a systemic weakness or vulnerability into the service. • If the service is end-to-end encrypted and doing so would build a new decryption capability into the service or render methods of encryption used in the service less effective. (This change is based on feedback that end-to-end encrypted services require an explicit reference).

		If any of these circumstances apply, a provider must take appropriate alternative action.
11 Determining what is appropriate **19 Detecting and removing known child sexual abuse material** **20 Detecting and removing known pro-terror material** **21 Disrupting and deterring child sexual exploitation material and pro-terror material**	'Appropriate' and 'appropriate action' were used in some obligations to ensure that services could comply in a way which was suitable to their circumstances and the potential harms.	**Amendment to section numbering and addition of a further consideration.** Former section 12 is now Section 11. In considering whether something is 'appropriate', Section 11 now includes a consideration of whether it is proportionate to the level of risk to the online safety of end-users in Australia. (This change incorporates feedback that some obligations were not proportionate or feasible for particular service providers.) In addition, the wording in Sections 19-21 has been amended to ensure that matters like proportionality are considered when providers implement 'appropriate' systems to: • detect and remove known child sexual abuse material and known pro-terror material (Sections 19 and 20) • disrupt and deter child sexual exploitation material and pro-terror material (Section 21).
13 Terms of use	Services were required to have 'terms of use' in place regarding class 1A and class 1B material, and to take appropriate action to respond to breaches of their terms of use, under the former Section 14.	**Amendment to section numbering and addition of clarifying wording.** Former Section 14 is now Section 13. The obligation remains the same, but wording has been added at Section 13(3) to provide clarity that 'terms of use' has a commonly understood meaning and that a different name may be used by the service provider as long as it has the same contractual effect as 'terms of use' and incorporates the obligations for dealing with breaches set out in Section 13(2).

28 Mechanisms for end-users and account holders to report and make complaints to providers **29 Dealing with reports and complaints – general rules** **30 Dealing with reports and complaints – additional rules for pre-assessed and Tier 1 RES**	Service providers had to provide a mechanism, tool or process that enabled end-users in Australia to report to the service material that breached its terms of service, under former Sections 27 and 28.	**Amendment to section numbering, and clarification and addition of obligations.** Former Sections 27 and 28 are now Sections 28 and 29 respectively. Section 28 now clarifies that services need to provide one or more tools that enable end-users to both: • report to the service any class 1A or class 1B material that breaches its terms of service, and/or • make a complaint to the service about its non-compliance with the RES Standard. Section 29 consolidates the obligations for review of reports and complaints, requiring providers to respond promptly to acknowledge reports and complaints under Section 28 and take appropriate and timely action in relation to a report or complaint. Section 30 has been introduced to require Pre-assessed and Tier 1 services to review the outcome of a report or complaint about class 1A and class 1B material accessible on or through the service, if requested by an end-user, and: • the review must be conducted by a person other than the person who conducted the investigation into the initial report • the provider must take appropriate action to facilitate the review.
36 Commissioner may require compliance reports – pre-assessed RES and Tier 1 RES	Annual compliance reports were required to be provided to eSafety by pre-assessed RES and Tier 1 RES and had to include the amount of child sexual exploitation and pro-terror material removed by the service	**Amendment to section numbering, addition of detail and change to the obligation.** Former Section 37 is now section 36.

	and how it was detected, under former Section 38.	Annual compliance obligation changed to on request of the Commissioner to facilitate more targeted reporting. To provide greater clarity, the content required in annual compliance reports now specifically includes: • the amount of child sexual exploitation material and pro-terror material identified by the provider in relation to the service • the way any of these materials were identified • details of the action taken by the service provider in respect of these materials • the number of complaints made to the provider about the service's compliance with the RES Standard during the reporting period • if applicable, a statement of the extent to which it was not technically feasible or reasonably practicable for the provider to detect or remove class 1A class 1B material from the service and why.