Australian Government
Department of Infrastructure, Transport, Regional Development and Communications

Communications and Media Group / Online Safety, Media and Platforms Division / Digital Platforms and Online Safety Branch

Frequently Asked Questions

Basic Online Safety Expectations

October 2021

This document will be updated during consultation on the Basic Online Safety Expectations as the Department receives submissions and engages with stakeholders.

Table of contents

When will the Basic Online Safety Expectations come into effect?

- Following consultation, the Minister for Communications, Urban Infrastructure, Cities and the Arts will consider submissions and make a final Online Safety (Basic Online Safety Expectations) Determination.
- It is expected to come into effect on 23 January 2022 at the same time as the *Online Safety Act 2021* (Online Safety Act) commences.

Why are the Basic Online Safety Expectations drafted broadly?

- The Basic Online Safety Expectations are broad because they apply to social media services, relevant electronic services and designated internet services.
- The Expectations are drafted so as to avoid being overly prescriptive and specific. They are not intended to impose a "one-size-fits-all" solution, but rather to allow different kinds of online services to develop their own appropriate means of complying with them.

Do I need to take every reasonable step?

- No. Where reasonable steps have been included in the Basic Online Safety Expectations, they are intended provide you with guidance about what steps you could take to meet relevant expectations and to signal some of the matters the eSafety Commissioner may ask you to report on.
- You may choose to undertake different steps that work best for you. Either way, you should be prepared to report on these steps, why they are reasonable for you and how they are effective at meeting the relevant expectation(s) and keeping users of your services safe.
- The Government expects you to consult the eSafety Commissioner and refer to any guidance published by the eSafety Commissioner in deciding which reasonable steps are most suitable for your service. Once the Basic Online Safety Expectations are finalised, the eSafety Commissioner will begin producing guidance on the expectations and reasonable steps to meet them. This guidance will be based on evidence and industry consultation.

What happens if I am taking action to make my service safer but fall short of the Expectations?

- Where you are demonstrating an effort and commitment to improving online safety, the eSafety Commissioner will take it into account when determining if you are compliant with the Basic Online Safety Expectations.
- It is recommended that you discuss the limits on your ability to meet different expectations when you consult with eSafety on reasonable steps for your service. eSafety's intention is to work collaboratively with services to support them to meet the expectations.

Will the eSafety Commissioner consult with industry before releasing its regulatory guidance?

- Yes. The eSafety Commissioner has committed to developing guidance on how it will interpret and operationalise the Basic Online Safety Expectations. This guidance will be based on evidence and consultation with industry.

Why is encryption included in the Basic Online Safety Expectations?

- The Basic Online Safety Expectations are drafted broadly to apply flexibly to existing and emerging online harms and safety issues. This includes, but is not limited to, cyber-bullying, cyber-abuse, non-consensual sharing of intimate images and harmful content in private messages.
- Encrypted communications may be used to share material or conduct activity that is unlawful and/or harmful. For example, an encrypted service could be used to share child sexual exploitation or abuse material.
- Providers of encrypted services are expected to proactively address and mitigate unlawful and harmful activity on their services. Reasonable steps might include a range of actions, such as detecting misuse through behavioural, account or online signals including routing information and metadata and closing accounts.

Am I expected to monitor my users' private communications?

- No. The Basic Online Safety Expectations focus on the systems, policies and processes that service providers may employ to prevent harm and respond to harm when it occurs.
- The Government expects that you will take action to prevent, detect and address unlawful and harmful activity. This may be achieved by identifying data or trends.
- For example, an account may be identified through behavioural signals and banned for sharing child sexual abuse material. You should then be able to show eSafety that you have systems to prevent that user from establishing a new account.

Am I expected to collect and verify proof of my users' real identities?

- No. The Basic Online Safety Expectations do not require users of your service to divulge their real identities, but that where reasonable, you employ processes that prevent users from exploiting anonymity or other identity shielding techniques to perpetrate abuse or post harmful content.
- The Government expects that you take reasonable steps to detect, prevent and remove the ability of suspended or banned users to exploit anonymity or identity shielding to re-register under a different or fake/imposter account. For example, you could utilise web identifiers (cookies, IP addresses, browser fingerprinting), device or hardware identifiers and other identifiers (such as account/behavioural analysis, metadata and traffic signals) to identify and stop re-registrations or fake accounts from being created.

My service is required to comply with Part 13 and Part 15 of the *Telecommunications Act 1997*. Do I need to breach my obligations under that Act to comply with the Expectations?

- No. You are not expected to disclose information that is prohibited by Part 13 or Part 15 of the *Telecommunications Act 1997* in order to comply with the Expectations.

Will I have to report on expectations that do not apply to my service?

- The Government understands that not every expectation will apply equally to every service.
- If you are required to report on actions taken to meet the Expectations, you should explain in your report where an expectation does not apply to you, and explain why.
- For example, your service may not offer encrypted messaging for users. If this is the case, you could include in your report that the additional expectation in Section 8 of the Expectations does not apply, because encrypted services are not offered to Australian end-users.

How will I report on my actions to meet the expectations in years where I do not have 'new' safety features to announce?

- Reporting on the Expectations is neither focused on, nor limited to, 'new' safety features.
- If you are required to report on the Basic Online Safety Expectations periodically, this would include an update on any new measures, an explanation of changes to existing measures and an assessment of the effectiveness and impact of ongoing measures.

Can I make a report to the eSafety Commissioner in confidence?

- Yes. Your report, or part of your report, can be made to the eSafety Commissioner in confidence if it details sensitive commercial information.
- However, the Basic Online Safety Expectations are intended to enhance transparency and accountability of service providers. Therefore, services are encouraged to make reports publicly available or to agree that the eSafety Commissioner may do so.
- The eSafety Commissioner is required to publish information about the reporting notices given and determinations made in its annual report.
- In addition, if the eSafety Commissioner forms a view that you are not complying with one or more of the expectations, they may prepare a statement to that effect.
- The Commissioner may share this statement with you, and may also publish it on their website if they consider it appropriate.

Can I appeal a reporting notice or finding of non-compliance?

- You can apply to have a decision by eSafety Commissioner to issue you with a periodic reporting notice (s.49 of the Online Safety Act) or a non-periodic reporting notice (s.56 of the Online Safety Act) internally reviewed.
- If you are not satisfied with the results of an internal review, you may apply to the Administrative Appeals Tribunal to review the matter.
- There is no penalty for not complying with the Basic Online Safety Expectations, therefore there is no power in the Online Safety Act to appeal a finding of the eSafety Commissioner that you are not complying with the Basic Online Safety Expectations.

How do the Basic Online Safety Expectations fit with other tools in the Online Safety Act to address harmful material and abusive conduct?

- The Basic Online Safety Expectations set out a benchmark for industry to protect users from online harms.
- This differs from new Industry Codes and an updated Restricted Access System (RAS) Declaration, which focus on material covered by the Online Content Scheme.
- The table below sets out how each part of the Online Safety Act addresses different types of harm.

Online Safety Act 2021—regulatory responses

Type of harm	BOSE	Industry Codes	RAS	Online Content Scheme	Cyberbullying scheme	Cyber abuse scheme	Image-based abuse scheme	AVM blocking notes
Cyberbullying of a child	✓				✓			
Cyber-abuse of an adult	✓					✓		
Non-consensual sharing of intimate images	✓						✓	
Promotion, incitement, instruction or depiction of abhorrent violent conduct	✓	✓		✓				✓
Class 1 material (refused classification)	✓	✓		✓				
Class 2 material (X18+)	✓	✓		✓				
Class 2 material (R18+)	✓	✓	✓	✓				
Sharing other harmful material	✓							
Other abusive conduct	✓							