eSafety issues first Basic Online Safety Expectations notices

Non-periodic notices have been issued to online service providers requiring them to provide details about the steps they are taking to address child sexual exploitation and abuse.

eSafety issued the notices on 29 August 2022 pursuant to section 56 of the Online Safety Act 2021. The providers have been asked to submit the information as part of the implementation of the Basic Online Safety Expectations, known as 'the Expectations'.

Why did eSafety select these providers?

In deciding which online service providers to issue a notice to, eSafety is required to consider several criteria specified in the Act:

- The number of complaints eSafety has received under the Act in relation to the service in the previous 12 months.
- Any deficiencies in the provider's safety practices and/or terms of use.
- Any previous contraventions of civil penalty provisions relating to the Expectations.
- Whether the provider has agreed to give the Secretary of the Department regular reports relating to safe use of their service.
- Any other matters the Commissioner considers relevant.

Examples of other matters the Commissioner considers relevant may include:

- A platform's reach and the profile of its users, including whether the platform is used by children.
- The measures the platform currently has in place to protect users from harm.
- The information already published by an online service provider, and any absence of information regarding a service's safety policies, processes and tools, or limited information about the impact or effectiveness of these interventions.
- Aggregated evidence from eSafety's other regulatory schemes, such as types of complaints, a provider's responsiveness to removal requests/notices, or other investigative insights regarding platform safety issues.
- Evidence of systemic harm, or evidence of key safety risks, relative to the Expectations, including from victims, charities, media, academics or other experts.

Further information is detailed in the Basic Online Safety Expectations regulatory guidance.

Key potential safety risks in a service's design were considered in this first round of notices, related to child sexual exploitation and abuse. These included whether adults could contact children on a platform, as well as features such as livestreaming, anonymity and end-to-end encryption.

eSafety intends to issue further notices in due course, so additional providers will be added over time to build a more comprehensive picture of the steps being taken across industry and the broader digital landscape.

Which providers received notices?

The purpose of a non-periodic reporting notice is to understand more about the steps companies are taking to implement the Basic Online Safety Expectations, with a view to improving transparency and accountability. eSafety has also committed to transparency in implementing the Expectations. We consider it to be important to confirm at the outset which providers have received notices.

The following providers received notices on 29 August. Each provider was given a short period to review the notice and engage with eSafety before they were issued.

Online service providers issued with non-periodic reporting notices
Apple
Meta (and WhatsApp)
Microsoft (and Skype)
Snap
Omegle

What do the notices cover?

The notices ask questions about specific Expectations, and key areas of child sexual exploitation and abuse. Some of the issues, and corresponding Expectations, are included in the following table. Not every area is relevant to every provider, so each notice is individual and will not necessarily cover all of the expectations below. Service providers are expected to take reasonable steps to implement the Expectations that are relevant to their platforms.

Areas covered by the first notices on the Basic Online Safety Expectations	Corresponding expectations in the Basic Online Safety Expectations Determination
The extent to which platforms are deploying technical tools to identify child sexual exploitation and abuse content on different parts of their service. In particular, such content that has already been confirmed and 'hashed' (digitally fingerprinted to allow for matches to be detected), as well as tools to detect 'new' or previously unseen content.	• Section 6 (Ensuring Safe Use). • Section 11 (Minimising Provision of Certain Material).
Steps taken to prevent and detect livestreamed child sexual exploitation and abuse.	• Section 6 (Ensuring Safe Use). • Section 11 (Minimising Provision of Certain Material).
Steps taken to prevent and detect the grooming of children.	• Section 6 (Ensuring Safe Use).
Steps to detect child sexual exploitation and abuse on end-to-end encrypted services.	• Section 6 (Ensuring Safe Use). • Section 8 (Encrypted Services). • Section 11 (Minimising Provision of Certain Material).
Steps taken to prevent services that allow users to remain anonymous being used for child sexual exploitation and abuse.	• Section 6 (Ensuring Safe Use) • Section 9 (Anonymous Services) • Section 11 (Minimising Provision of Certain Material).
Steps taken to prevent banned or suspended users from creating new accounts (recidivism).	• Section 6 (Ensuring Safe Use). • Section 14 (Policies and Procedures to deal with complaints).
The availability of mechanisms for users to report child sexual exploitation and abuse content or activity.	• Section 6 (Ensuring Safe Use). • Section 11 (Minimising Provision of Certain Material). • Section 13 (Mechanisms to report and make complaints about certain material). • Section 14 (Policies and Procedures to deal with complaints). • Section 15 (Mechanisms to report and make complaints about breaches of terms of use).

What happens next?

Providers have 28 days from the giving of a notice to respond, or longer as agreed with eSafety.

eSafety will provide a further update once this regulatory process has concluded. This may include publishing information received from providers where this meets the objectives of the Act.

eSafety will also publish updates as additional notices are issued.