



FREQUENTLY ASKED QUESTIONS

The Online Safety Act 2025 (ONSA)

1. What is the Online Safety Act 2025?

The Online Safety Act 2025 (ONSA) is a new law to make the Internet safer for everyone in Malaysia by making service providers more responsible to safeguard the public, especially children, families and vulnerable groups, from online harmful content.

2. Who does this law apply to? Does it apply to users?

ONSA applies to licensed Applications Service Providers (ASPs), Content Applications Service Providers (CASPs), and Network Service Providers (NSPs) (collectively referred to as Licensed Service Providers) under the Communications and Multimedia Act 1998 (CMA 1998).

All regulatory obligations under ONSA apply to Licensed Service Providers. The Act does not apply to individual users.

3. Which service providers are deemed licensees under the current licensing framework?

Under the current licensing framework, service providers offering Internet messaging or social media services with eight (8) million or more users in Malaysia are deemed to be registered as ASP(C) licensees. Hence, these service providers fall within the scope of Malaysian regulatory requirements and the social media platforms that meet the licensing criteria are required to comply with ONSA.

4. Why was the ONSA introduced?

As more people spend time online, they are increasingly exposed to harmful content such as child sexual exploitation, online scams, cyberbullying and extremist material. ONSA was introduced to address harmful content by placing clear responsibilities on Licensed Service Providers.

ONSA helps build public trust by ensuring Licensed Service Providers take action to prevent harm, detect and respond to harmful content, and create a safer online environment for all users in Malaysia.

5. What duties do Licensed Service Providers have under ONSA?

Licensed ASPs and CASPs are required to take proactive steps to keep users safe from harmful content online. This includes, among others, implementing measures to reduce the risk of being exposed to harmful content, issuing safety guidelines, providing online safety tools for users, providing user support on their services and making it easy to report harmful content.

The Licensed ASPs and CASPs are also required to implement measures to safeguard the online safety of all users, including ensuring priority harmful content such as child sexual abuse materials (CSAM) and financial fraud related are made inaccessible to all users. In addition, the Licensed ASPs and CASPs are required to prepare and publish an Online Safety Plan that explains the safety measures.

Licensed NSPs are required to cooperate during investigations and provide reasonable technical assistance within their capabilities when required. They must also provide relevant information and allow inspections to ensure compliance with ONSA.

6. What is “harmful content” and “priority harmful content” under the ONSA?

Under the ONSA, the types of harmful content are listed in the First Schedule, as follows:

- (a) Child sexual abuse material (CSAM);
- (b) Financial fraud;
- (c) Obscene content;
- (d) Indecent content;
- (e) Content that may cause harassment, distress, fear or alarm;
- (f) Content that may incite violence or terrorism;
- (g) Content that may induce a child to cause harm to himself;
- (h) Content that promotes ill-will or hostility and may disturb public tranquillity; and
- (i) Content that promotes the use or sale of dangerous drugs.

Among these, child sexual abuse material (CSAM) and financial fraud related content are classified as “priority harmful content”. These must be made inaccessible to all users as soon as possible, given the serious harm that may arise from such content.

7. What changes will users see with ONSA?

Under the ONSA, users can expect platforms to take a more consistent and proportionate approach to online safety. This means clearer safety information and guidelines on platforms, easier ways to report harmful content, more responsive assistance and better tools and settings to control who can find, contact or interact with you.

For services that are likely to be used by children, stronger protections are expected over time. These may include safer default settings, stronger privacy protections and better controls over interactions.

8. Does ONSA require relevant Licensed Service Providers to adopt a specific technology for age verification?

The main provisions of ONSA do not require any specific type of technology that must be adopted by Licensed Service Providers.

However, the Malaysian Communications and Multimedia Commission is currently exploring potential age verification approaches, among others, with the use of official Government-issued documents such as MyKad, passport and MyDigital ID, through a regulatory sandbox process involving relevant agencies and social media platforms. This evaluation will take into account user safety, personal data protection, privacy considerations, as well as suitability within Malaysia's legal and regulatory framework.

The most appropriate age verification mechanism will be finalised through the relevant subsidiary instrument(s) under ONSA.

9. How does ONSA help parents keep their children safe online?

ONSA helps parents by requiring platforms to provide better safety tools and clearer guidance. This includes safety controls that allow parents to manage who can contact children, settings to control the type of content that can be accessed by or recommended to them, clear guidelines on safe use, as well as mechanisms for reporting harmful content and accessing user support.

10. How will Malaysians benefit from ONSA?

ONSA helps create a safer online environment for everyone in Malaysia, especially children, families and vulnerable groups.

Social media platforms are expected to act more swiftly and responsibly against harmful content and provide clearer safety standards.

ONSA strengthens protections for children, families and vulnerable users, while helping to ensure a safer and more trusted online environment for all Malaysians.

-END-