



Malaysian Communications and Multimedia Commission

**PUBLIC CONSULTATION PAPER ON THE
ONLINE SAFETY PLAN**

Publication date: 12 February 2026

Closing date for responses: 13 March 2026

TABLE OF CONTENTS

GLOSSARY	2
PREFACE	3
SECTION 1: BACKGROUND AND POLICY IMPERATIVE	4
1.1 Background	4
1.2 Problem Statement	5
1.3 Rationale	5
1.4 Scope and Application	6
SECTION 2: INTERNATIONAL BENCHMARKING	7
2.1 International Benchmarking	7
2.2 Common Regulatory Requirements	7
SECTION 3: KEY COMPONENTS	10
3.1 Risk Mitigation	11
3.2 Content Management and Moderation	11
3.3 User Empowerment and Controls	16
3.4 Child Protection	20
3.5 Transparency and Reporting	20
3.6 Governance and Accountability	22
SECTION 4: CONCLUSION	24
SECTION 5: SUBMISSION OF RESPONSES	25

GLOSSARY

Term	Definition
AI	Artificial Intelligence
BOSE	Basic Online Safety Expectations
CIB	Coordinated Inauthentic Behaviour
CMA 1998	Communications and Multimedia Act 1998
Codes of Practice	Code of Practice for Online Safety for Social Media Services and the Code of Practice for Online Safety for App Distribution Services
Commission	Malaysian Communications and Multimedia Commission
DSA	European Union Digital Services Act
EU	European Union
IMDA	Infocomm Media Development Authority
Licensed Service Providers	Licensed applications service providers and licensed content applications service providers
ONSA	Online Safety Act 2025
OSP	Online Safety Plan

PREFACE

The Malaysian Communications and Multimedia Commission (“**Commission**”) is conducting this Public Consultation to invite feedback on the proposed regulatory framework to operationalise the Online Safety Plan (“**Regulatory Framework**”).

The Online Safety Act 2025 (“**ONSA**”) was passed by Parliament on 6 May 2025 and gazetted on 22 May 2025. ONSA establishes a statutory framework to enhance and promote online safety in Malaysia, strengthen protections for children and vulnerable groups, and introduce systemic online safety measures applicable to service providers within the scope of the Act. For licensing constructs, ONSA is to be read together with the Communications and Multimedia Act 1998 (“**CMA 1998**”).

ONSA came into force on 1 January 2026, along with several subsidiary instruments to complement the Act. While section 20 of ONSA establishes duty for licensed service providers to prepare, publish and submit an Online Safety Plan (“**OSP**”), ONSA does not currently prescribe the form, content, or submission procedure for the OSP. Section 81(2)(c) of ONSA empowers the Minister to make regulations prescribing the period for the preparation of an OSP, its form, and the information it must contain.

The Regulatory Framework is intended to inform the development of future regulations on OSPs, by setting out the Commission’s proposed policy intent and guiding principles to promote clarity, consistency, and accountability.

This Public Consultation aims to solicit views from a broad range of stakeholders including industry players, civil society organisations, consumer groups, and members of the public on the policy rationale, proposed scope, overall regulatory approach and practical implementation considerations. This initiative reflects the Commission’s commitment to transparent, inclusive, consultative, and evidence-based rulemaking. The Commission thanks all participants and welcomes constructive written submissions.

SECTION 1: BACKGROUND AND POLICY IMPERATIVE

1.1 Background

The rising prevalence and complexity of online harms, including cyberbullying, child exploitation, and other harmful content, have outpaced Malaysia's existing regulatory and voluntary approaches in terms of scale, speed and complexity.

To address these challenges proactively, ONSA introduced the OSP as a core compliance instrument to demonstrate how licensed applications service providers ("**ASP**") and licensed content applications service providers ("**CASP**") (collectively referred to as "**Licensed Service Providers**") meet their duties under Part III of the Act. The OSP shifts regulatory focus from reactive, incident-led responses towards a more systematic and forward-looking approach to compliance, embedding online safety considerations across governance, operations and service design. It functions as a structured plan that outlines how service providers manage risks, implement child protection measures, empower users, and uphold transparency and accountability.

The OSP serves three (3) key purposes:

- a) **Regulatory Assurance:** Enables the Commission to monitor compliance with statutory duties effectively.
- b) **Public Accountability:** Enhances transparency at an appropriate level, allowing users and stakeholders to understand safety measures and hold providers accountable.
- c) **Global Alignment:** Positions Malaysia in line with leading international best practices, promoting consistency and cooperation in addressing cross-border online harms.

Under section 20 of ONSA, Licensed Service Providers are required to prepare, publish, and submit an OSP to the Commission. This obligation supports safer online environments by requiring service providers to proactively manage risks, protect vulnerable users, particularly children, provide accessible safety tools, and demonstrate accountability in meeting their statutory duties. Collectively, these measures reflect Malaysia's commitment to a modern, effective, and globally aligned regulatory framework for online safety.

1.2 Problem Statement

The rapid growth of online services in Malaysia has increased user exposure to harmful content and conduct, including risks to children and vulnerable groups, cyberbullying, financial fraud and other emerging harms. While existing regulatory measures exist, they are increasingly challenged by the speed, scale, and complexity of online risks, which often transcend jurisdictional boundaries and adapt quickly to technological change. This underscores the need for a more systematic and proactive regulatory approach that places clear responsibilities on Licensed Service Providers to anticipate, mitigate, and respond effectively to online harms.

1.3 Rationale

The OSP advances transparency by documenting, at an appropriate level, the operational and technical safeguards adopted by Licensed Service Providers and facilitates effective regulatory oversight by the Commission. It also establishes clear accountability, incentivises continuous improvement, and enables proportionate supervision. Ultimately, this obligation helps bridge gaps in the current regulatory landscape by institutionalising robust protections for all users, particularly children, families and vulnerable groups, consistent with Malaysia's broader online safety objectives.

1.4 Scope and Application

Section 20 of ONSA introduces a duty for Licensed Service Providers to prepare, publish, and submit to the Commission an OSP within a prescribed period and form. Licensed Service Providers are also required to make the OSP easily accessible on their services and to ensure that it is regularly updated.

- *The rest of this page is intentionally left blank.* -

SECTION 2: INTERNATIONAL BENCHMARKING

2.1 International Benchmarking

This section outlines regulatory approaches observed across multiple jurisdictions in the implementation of online safety measures, including safety-by-design elements. Examples of such approaches may be found in instruments such as:

- a) Australia's Basic Online Safety Expectations;
- b) the European Union's Digital Services Act; and
- c) Singapore's Codes of Practice for Online Safety.

While these instruments differ in legal form and scope, they reflect common regulatory outcomes relating to risk mitigation, user empowerment, transparency and the protection of children and vulnerable users.

2.2 Common Regulatory Requirements

In Australia, the Basic Online Safety Expectations ("**BOSE**") pursuant to the Online Safety Act 2021 outline principle-based expectations for relevant online service providers to take reasonable steps to minimise unlawful and harmful material. These expectations are supported by regulatory powers relating to transparency and compliance and are supplemented by mandatory industry codes and standards for certain categories of online services, including social media, messaging, search, hosting, and other designated services.

In Singapore, the Code of Practice for Online Safety for Social Media Services and the Code of Practice for Online Safety for App Distribution Services (collectively "**Codes of Practice**") are issued by the Infocomm Media Development Authority ("**IMDA**") pursuant to section 45L of the Broadcasting Act 1994. The Codes of Practice impose outcome-oriented obligations on designated services, with a focus on mitigating harmful content and protecting users, particularly children.

The Digital Services Act (“**DSA**”) of the European Union (“**EU**”) promotes a safer and more transparent online environment by addressing illegal content and systemic risks, with additional obligations applying to services with significant reach. The framework also places emphasis on safeguards for children, including measures relating to safety, privacy, and wellbeing.

A common feature across these jurisdictions is the requirement for service providers to take reasonable steps to minimise the availability and spread of harmful or illegal content through mechanisms such as content moderation processes, accessible reporting and redress mechanisms, and transparency and accountability measures.

User safety and empowerment are also consistently reflected, including the provision of tools that enable users to manage their own safety, access clear reporting channels, the ability to control interactions and content exposure, and avenues to seek review of moderation decisions. There is also a strong emphasis on protecting children, including through safety-by-design and age-appropriate design principles.

These international frameworks demonstrate a shared regulatory direction towards proactive risk management, transparency, accountability, and the protection of children and vulnerable users, while allowing flexibility in how service providers meet their obligations.

A recap of the requirements set forth by these three (3) jurisdictions is provided in Table 1 below:

International Benchmarking based on Key Components	Australia	Singapore	EU
Risk Mitigation	<i>Addressed under the Commission's <u>Code on Duties for Risk Mitigation.</u></i>		
Content Management and Moderation	✓	✓	✓
User Empowerment and Controls	✓	✓	✓
Child Protection	<i>Addressed under the Commission's <u>Code on Duties for Child Protection.</u></i>		
Transparency and Reporting	✓	✓	✓
Governance and Accountability	✓	✓	✓

Table 1: International Benchmarking based on Key Components

- The rest of this page is intentionally left blank. -

SECTION 3: KEY COMPONENTS

In this section, the Commission sets out the proposed key components to be addressed in an OSP and invites views on the appropriate scope, level of detail, and practical implementation of each component. The consultation questions under each component are intended to inform the development of the regulatory framework for OSPs, including how Licensed Service Providers should demonstrate compliance with their statutory duties under the ONSA in a clear, proportionate, and non-duplicative manner.

For avoidance of doubt, where specific duties are prescribed through Codes issued under section 80 of ONSA, the OSP is intended to describe how compliance with those duties is achieved, rather than to restate or replicate detailed operational requirements.

Based on international best practice and to operationalise duties under Part III of ONSA, the Commission identifies six (6) key components that Licensed Service Providers are expected to address, at an appropriate level, in their OSPs, as set out in Table 2 below:

Item	Key Component
3.1	Risk Mitigation
3.2	Content Management and Moderation
3.3	User Empowerment and Controls
3.4	Child Protection
3.5	Transparency and Reporting
3.6	Governance and Accountability

Table 2: Key Components under the OSP

3.1 Risk Mitigation

Risk mitigation obligations are provided for under section 13 of ONSA and are intended to be operationalised through a Code on Duties for Risk Mitigation to be issued by the Commission pursuant to its powers under section 80 of ONSA. This approach is intended to ensure alignment and to avoid overlapping or contradictory requirements for Licensed Service Providers.

3.2 Content Management and Moderation

Licensed Service Providers are required to establish robust, transparent, and accountable mechanisms to detect, assess, manage and report harmful content, pursuant to sections 16 and 19 of ONSA. Content management should go beyond reactive removal of reported material and instead reflect a more systematic approach to moderation, which may include automated systems, human review, or hybrid approaches. These practices should be proportionate to the nature, scale and risk profile of the service, and demonstrate that service providers are actively managing content risks responsibly.

For the purposes of the OSP, this component focuses on how Licensed Service Providers describe their approach to meeting content management and moderation duties under ONSA.

3.2.1 Content Moderation Obligations

At a minimum, an OSP should demonstrate how a Licensed Service Provider addresses content moderation risks, including how it:

- a) addresses priority harmful content by demonstrating how mechanisms are in place to ensure that such content is inaccessible to users;
- b) detects and mitigates harmful content proactively, through reasonable measures to minimise publication or dissemination before it reaches users;

- c) protect children through appropriate age assurance or age-appropriate measures, with enhanced safeguards for services likely to be accessed by children, ensuring that the best interest of the child are treated as a primary consideration;
- d) addresses risks arising from impersonation, account misuse, or inauthentic account activity through appropriate account integrity measures, registration safeguards, and other proportionate controls;
- e) maintain continuous moderation capability, including arrangements to monitor high-risk features such as live streaming and to respond to harmful content in a timely manner;
- f) enforce proportionate consequences for violations of platform rules relating to harmful content, including account suspension or disabling where appropriate;
- g) implement measures to deter or limit recidivism, including restricting account re-creation by repeat violators;
- h) put in place safeguards to address harmful content that could affect national security, public order, or social cohesion;
- i) address content that facilitates or promotes criminal activities, including but not limited to illegal online gambling, prostitution, scams and Coordinated Inauthentic Behaviour ("**CIB**")¹;
- j) address emerging and evolving risks, such as impersonation of public figures and the misuse of Artificial Intelligence ("**AI**") to generate harmful deepfake content;
- k) respond effectively to content flagged by the Commission by implementing clear processes to act on notifications or instructions issued under the Act; and
- l) adopt any additional moderation measures that may be prescribed by the Commission, as necessary to protect users and uphold statutory duties.

¹ For the purposes of this framework, CIB means a manipulative tactic where multiple fake, duplicated, or disguised social media accounts or online personas operate collectively to deceive users and manipulate public discourse

Question 1

The Commission invites views on the following:

- a) whether the proposed scope and level of detail for describing content management and moderation approaches in the OSP are clear, proportionate, and practical; and**
- b) any suggestions on additional aspects of content management and moderation that should be explained in the OSP to support transparency and effective regulatory oversight.**

3.2.2 Detection and Removal Systems

Licensed Service Providers are required under ONSA to take appropriate and proportionate measures to identify, assess, and address harmful content on their services.

For the purposes of the OSP, Licensed Service Providers should describe, at an appropriate level, the systems and processes they have in place to support the detection and removal of harmful content.

Detection and removal systems may comprise a combination of proactive and reactive measures, including:

- a) proactive monitoring designed to identify potential harmful content, which may include automated or other technological tools; and
- b) reactive measures such as reporting mechanisms, referrals from trusted flaggers, or actions taken in response to notifications or directions issued by the Commission.

For transparency and accountability, an OSP should outline:

- a) the types of detection approaches employed and their intended scope;
- b) processes for managing limitations in detection systems, including the handling of false positives and false negatives and the role of human review; and
- c) internal processes for accessing and responding to identified harmful content, including escalation pathways where appropriate.

In describing detection and removal mechanisms, an OSP should demonstrate how the Licensed Service Provider:

- a) is able to respond in a timely manner to harmful content, including priority harmful content, consistent with its duties under ONSA and any directions issued by the Commission;
- b) takes reasonable steps to reduce the risk of removed harmful content reappearing on the service;
- c) maintains oversight of high-risk service features, such as live streaming, where appropriate;
- d) ensure readiness to comply promptly with removal or takedown requests arising from notifications or directions issued by the Commission;
- e) takes into account any additional detection or removal-related measures that may be prescribed by the Commission.

Question 2

The Commission invites views on the following in relation to detection and removal mechanisms:

- a) whether the proposed scope and level of detail for describing detection and removal mechanisms in the OSP are clear, proportionate, and practical; and**
- b) any suggestions or views on additional aspects of detection or removal mechanisms that could be explained in the OSP to enhance transparency and effective regulatory oversight.**

3.2.3 Transparency in Content Moderation Systems

Transparency is an important element in promoting accountability and public confidence in content moderation practices. For the purposes of the OSP, Licensed Service Providers should describe, at an appropriate and proportionate level, how their content moderation systems operate, in a manner that supports transparency and effective regulatory oversight, without requiring the disclosure of confidential, proprietary, or security-sensitive information.

An OSP should set out:

- a) a description of the operation of content moderation, detection, and content recommendation systems in place, including the types of tools and processes used;
- b) an explanation of the principles, standards, or criteria applied when moderating or recommending content, described at a level that is consistent with confidentiality, security, and system integrity requirements;

- c) the measures adopted to ensure fairness, accuracy, and non-discrimination in content moderation decision, including mechanisms to mitigate systemic bias where relevant; and
- d) clarification of the respective roles of automated tools and human oversight in the moderation process, including escalation or review procedures for complex, high-risk or sensitive cases.

Question 3

The Commission invites views on whether the proposed approach to transparency in content moderation systems, as to be described in the OSP, is clear, proportionate, and practical, taking into account the need to balance transparency with confidentiality, security and system integrity considerations.

3.3 User Empowerment and Controls

Licensed Service Providers are subject to duties under sections 15 and 17 of ONSA to provide users with accessible and effective tools and settings that enable them to manage their online safety, including controls over content exposure, interactions, and privacy. These measures are intended to empower users to manage the risk of exposure to harmful content and to enhance individual safety when using online services.

For the purpose of the OSP, Licensed Service Providers should describe, at an appropriate level, how such user empowerment tools and controls are available and integrated into the service.

In addition, pursuant to section 14 of ONSA, Licensed Service Providers are required to provide clear, easily accessible, and regularly updated guidelines to users explaining the operation of these tools and settings. The OSP should outline how such information or guidance are provided to users in a practical and user-friendly manner.

3.3.1 User-Controlled Content Filters

User-controlled content filters are an important tool for enabling users to manage their exposure to harmful content. For the purposes of the OSP, Licensed Service Providers should describe, where applicable, how user-controlled filtering options are made available to support user empowerment and online safety.

An OSP should outline how the service:

- a) provide filtering tools that enable users to manage exposure to relevant content categories, including those recognised under ONSA and the service provider's terms of use;
- b) ensures that filtering tools are easy for users to locate, enable, and customise; and
- c) applies default settings that are safety enhancing where appropriate, while allowing users to adjust or disable such settings, except otherwise required or restricted by law.

Question 4

The Commission invites views on whether the proposed approach to describe user-controlled content filters in the OSP is clear, proportionate, and practical, including whether the level of explanation appropriately supports user understanding and empowerment.

3.3.2 Interaction and Privacy Settings

Interaction and privacy settings are important tools for enabling users to manage their online interactions and protect personal boundaries. For the purposes of the OSP, Licensed Service Providers should describe, where applicable, how interaction and privacy controls are made available to users to support online safety.

An OSP should outline how the service enables users to:

- a) manage interactions through settings that control, where relevant:
 - who can send direct messages
 - who can comment on, tag, or mention the user; and
 - account discoverability and visibility.
- b) mute, block, restrict, or report other users.
- c) apply safety enhancing default settings for children's accounts or services likely to be accessed by children, consistent with child safety and privacy-by-default principles.
- d) provide meaningful controls over content recommendations or content exposure features, where such features are present, including options that allow users to influence or adjust personalised content experiences.

Question 5

The Commission invites views on whether the proposed approach for describing interaction and privacy settings in the OSP is clear, proportionate, and practical, including whether the level of explanation appropriately supports user understanding and control over online interactions and privacy.

3.3.3 User Education and Choice Architecture

User education and choice architecture play an important role in supporting informed and safe user decision-making. For the purposes of the OSP, Licensed Service Providers should describe, at an appropriate and proportionate level, how users are informed about safety-related features and supported in making choices that reduce the risk of exposure to harmful content, without being misled by design practices.

An OSP should outline how the service, where relevant:

- a) provide user education materials, prompts, or guidance during onboarding and when users engage with higher risk features;
- b) explain key safety related settings and features in a clear and accessible manner, including settings relating to visibility, interactions, and content exposure;
- c) offers high-level contextual information to help users understand why certain content or recommendation are shown to them, where applicable; and
- d) adopt design approaches intended to support informed and safety enhancing user choices and avoids design practices that could undermine user safety or mislead users in relation to safety-related settings.

Question 6

The Commission invites views on whether the proposed approach for describing user education and choice architecture in the OSP is clear, proportionate, and practical, including whether it adequately supports informed and safety-enhancing user decision-making.

3.4 Child Protection

Child protection obligations are provided for under section 18 of ONSA and are intended to be operationalised through a Code on Duties for Child Protection to be issued by the Commission pursuant to its powers under section 80 of ONSA. This approach is intended to ensure alignment and to avoid overlapping or contradictory requirements for Licensed Service Providers.

3.5 Transparency and Reporting

Transparency and reporting support accountability by enabling the Commission and the public to understand how Licensed Service Providers meet their online safety obligations under ONSA. Pursuant to section 20 of ONSA, this is primarily achieved through the structured preparation, publication and submission of the OSP.

For the purposes of the OSP, Licensed Service Providers should describe, at an appropriate level, how relevant online safety measures, policies, and processes are documented and communicated through the OSP to support transparency and effective regulatory oversight.

3.5.1 Submission to the Commission

Pursuant to section 20 of ONSA, Licensed Service Providers are required to submit an OSP to the Commission in such form, manner and period as may be prescribed. The submitted OSP is subject to review by the Commission to ensure it is in line with the regulatory requirements.

For the purposes of this Public Consultation, the Commission proposes that Licensed Service Providers be required to submit their first OSP within **ninety (90) days** from the date of commencement of the regulations made under section 20 of ONSA. Thereafter, the Commission proposes that the OSP be submitted on an annual basis, unless otherwise specified.

The Commission further proposes that Licensed Service Providers be required to notify the Commission and submit an updated OSP where there are material changes affecting the service, including significant changes to the service's features, systems, terms of service, or risk environment, rather than waiting for the next scheduled submission.

The Commission may, in accordance with ONSA, require a Licensed Service Provider to provide additional information, or to revise, update, or resubmit its OSP where necessary to support effective regulatory oversight.

All information provided must be complete and accurate in all material respects.

Question 7

The Commission invites views on the proposed submission and update arrangements for the OSP, including:

- a) the proposed ninety (90) day period for Licensed Service Providers to prepare and submit the initial OSP following the commencement of the relevant regulations;**
- b) the proposed annual submission of the OSP; and**
- c) the proposed requirement for Licensed Service Providers to notify the Commission and submit an updated OSP where there are material changes to its contents.**

3.6 Governance and Accountability

Effective governance and accountability arrangements are essential to ensure that online safety obligations under the ONSA are implemented consistently and responsibly. Licensed Service Providers should describe, at an appropriate level, how governance structures, internal accountability mechanisms, and decision-making processes support compliance with ONSA, including in relation to risks affecting children, vulnerable groups and wider public.

An OSP should outline how responsibility for online safety is assigned and overseen within the organisation, including how relevant policies, processes, and design considerations are integrated into service development and operations to support effective risk management and accountability.

Question 8

The Commission invites views on whether the proposed approach to describing governance and accountability arrangements in the OSP is clear, proportionate, and practical in supporting effective oversight and compliance with obligations under ONSA.

3.6.1 Governance Accountability and Contact Point

For the purpose of the OSP, Licensed Service Providers should identify an appropriate point of accountability within the organisation responsible for overseeing compliance with online safety obligations under the ONSA and for serving as the primary contact point for engagement with the Commission on OSP-related matters.

An OSP should describe, at an appropriate level, how this accountability function supports:

- a) coordination of internal risk assessments and review processes;
- b) oversight of the implementation and internal monitoring of online safety measures; and
- c) engagement with the Commission on online safety matters, including in relation to information requests, review, or regulatory follow-up.

The OSP should record the relevant contact details for regulatory engagement. The Commission expects that the identified contact point will have appropriate seniority, expertise, and access to management functions to carry out these responsibilities effectively.

Question 9

The Commission invites views on whether the proposed approach to describing governance accountability arrangements and the identification of a regulatory contact point in the OSP is clear, proportionate, and practical in supporting effective oversight and compliance with obligations under the ONSA.

SECTION 4: CONCLUSION

This proposed regulatory framework operationalises the duty of Licensed Service Providers to prepare, publish, and submit to the Commission a structured and forward-looking compliance plan that demonstrates how online safety obligations are met, pursuant to section 20 of ONSA.

By embedding proactive planning into service design, governance and operations, the OSP framework strengthens Malaysia's capacity to enhance online safety, reduce online harms, and protect users, particularly children and vulnerable groups. It promotes systematic and effective safety measures, while upholding the principles of transparency and accountability in a rapidly evolving online environment. In doing so, the proposed approach aligns Malaysia with international best practices and contributes to the development of a safer and more resilient online ecosystem.

SECTION 5: SUBMISSION OF RESPONSES

The Commission welcomes written submissions on any aspect of this Public Consultation document. All submissions must be submitted in full no later than **5:00 PM, 13 March 2026 (Friday)**.

Stakeholders may request confidential treatment for any part of their submission that is considered proprietary, commercially sensitive, or otherwise confidential. Such requests must include clear justification and will be subject to the Commission's review.

Where confidentiality is requested, respondents must also submit a corresponding non-confidential version of the submission. All confidential information should be redacted and placed in a separate annex clearly marked as "**CONFIDENTIAL**."

If a request for confidential treatment is granted, the relevant material will be reviewed by the Commission but will not be published. However, the Commission will not accept any submission in which confidentiality is claimed over the entire document or a substantial portion thereof.

Written submissions on this matter may be provided to the Commission in either hard copy or electronic form at the following address:

Address:

The Chairman

Malaysian Communications and Multimedia Commission

MCMC HQ Tower 1, Jalan Impact, Cyber 6, 63000 Cyberjaya,

Selangor Darul Ehsan

(Attention: Regulatory Policy Division)

Email:

policy.research@mcmc.gov.my