Malaysian Communications and Multimedia Commission

PUBLIC CONSULTATION REPORT ON THE

ONLINE SAFETY PLAN

Table of Contents

GLOSSARY 2
SECTION 1: INTRODUCTION 3
1.1 Background 3
1.2 Objective 3
1.3 Scope and Application 4
1.4 Stakeholder Engagement 5
1.5 Public Consultation 6
SECTION 2: FEEDBACK FROM THE PUBLIC CONSULTATION 8
2.1 Question 1 – Proposed Content Management and Moderation 8
2.2 Question 2 – Proposed Detection and Removal Systems 12
2.3 Question 3 – Proposed Transparency in Content Moderation Systems 15
2.4 Question 4 – Proposed User-Controlled Content Filters 18
2.5 Question 5 – Proposed Interaction and Privacy Settings 22
2.6 Question 6 – Proposed User Education and Choice Architecture 25
2.7 Question 7 – Proposed Submission to the Commission 28
2.8 Question 8 – Proposed Governance and Accountability 31
2.9 Question 9 – Proposed Governance Accountability and Contact Point 34
SECTION 3: CONCLUSION 38

©2026 MCMC. All rights reserved.

GLOSSARY

Term	Definition
ASP	Applications service providers
CASP	Content applications service providers
CMA 1998	Communications and Multimedia Act 1998
Commission	Malaysian Communications and Multimedia Commission
CSAM	Child sexual abuse material
Licensed Service Providers	Licensed applications service providers and licensed content applications service providers
NSP	Network service providers
ONSA	Online Safety Act 2025
OSP	Online Safety Plan
PC	Public consultation
URL	Uniform Resource Locator

©2026 MCMC. All rights reserved.

SECTION 1: INTRODUCTION

1.1 Background

The Online Safety Act 2025 ("**ONSA**") was passed by the Dewan Rakyat on 11 December 2024 and by the Dewan Negara on 16 December 2024. ONSA was subsequently gazetted on 22 May 2025 and came into force on 1 January 2026, along with several subsidiary instruments to complement the Act.

ONSA establishes a statutory framework to enhance and promote online safety in Malaysia by regulating harmful content and providing for duties and obligations of applications service providers ("**ASP**"), content applications service providers ("**CASP**") and network service providers ("**NSP**") licensed under the Communications and Multimedia Act 1998 ("**CMA 1998**").

The rising prevalence and complexity of online harms, including cyberbullying, child exploitation, and other harmful content, have outpaced existing regulatory and voluntary approaches in terms of scale, speed and complexity. To address these challenges proactively, ONSA establishes statutory duties for ASPs and CASPs (collectively referred to as "**Licensed Service Providers**").

1.2 Objective

Under section 20 of ONSA, Licensed Service Providers are required to prepare, publish, and submit an Online Safety Plan ("**OSP**") to the Malaysian Communications and Multimedia Commission ("**Commission**"). The OSP serves as a structured mechanism for Licensed Service Providers to describe how they comply with their statutory duties under Part III of ONSA.

©2026 MCMC. All rights reserved.

Through this mechanism, Licensed Service Providers are expected to demonstrate how they manage risks, implement appropriate safety measures, protect vulnerable users, particularly children, provide accessible tools to support safer online experiences. The OSP is intended to enhance transparency, accountability, and regulatory oversight, while supporting the effective implementation of ONSA within Malaysia's evolving digital ecosystem.

1.3 Scope and Application

Section 20 of ONSA provides 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.

To implement this provision effectively, the Act empowers the Minister to prescribe regulations under section 81(2)(c) of ONSA. Pursuant to this mandate, the Commission is formulating regulations prescribing the period for the preparation of an OSP, its form, and the information it must contain.

©2026 MCMC. All rights reserved.

As outlined in the PC on OSP, the Commission identified six (6) key components that Licensed Service Providers are expected to address at an appropriate level in their OSPs, in operationalising duties under Part III of ONSA. The proposed key components are as set out in Table 1 below:

No.	Key Component
1.	Risk Mitigation
2.	Content Management and Moderation
3.	User Empowerment and Controls
4.	Child Protection
5.	Transparency and Reporting
6.	Governance and Accountability

Table 1: Key Components

1.4 Stakeholder Engagement

To support the development of the framework, the Commission convened stakeholder engagement sessions on 18 and 27 November 2025. The initial engagement comprised separate sessions for industry and non-industry stakeholders. A supplementary session was subsequently held to accommodate additional participants and to ensure broader participation and inclusivity.

In total, 64 participants representing 36 organisations attended these sessions, demonstrating stakeholders' interest in the implementation of ONSA and its subsidiary instruments.

©2026 MCMC. All rights reserved.

Across these sessions, participants generally expressed support for strengthening online safety protections under ONSA, particularly in relation to child safety. At the same time, stakeholders emphasised the importance of ensuring the framework remains practical and implementable, including the need for clear operational guidance, an appropriate balance between regulatory certainty and flexibility, and alignment with existing industry practices.

Stakeholders also highlighted the value of complementary self-regulatory measures and the importance of continued engagement, including the provision of clear guidance and reasonable timelines to support effective implementation.

1.5 Public Consultation

On 12 February 2026, the Commission commenced a Public Consultation ("**PC**") on the proposed OSP framework. Members of the public, including service providers, industry participants and other interested parties, were invited to submit written feedback over a one-month period from 12 February until 13 March 2026, at 5:00 p.m., either in hard copy or electronic form.

Following the requests from stakeholders, the PC period was subsequently extended until 31 March 2026 to facilitate broader participation.

©2026 MCMC. All rights reserved.

In total, the Commission received **18** written submissions representing **20** respondents. The list of respondents is provided in Table 2 below:

No.	Respondents
1.	ARTICLE 19, Centre for Independent Journalism (CIJ) and Sinar Project (**Joint Submission**)
2.	Asia Tech Alliance (ATA)
3.	CelcomDigi
4.	Google
5.	Human Rights Commission of Malaysia (SUHAKAM)
6.	Institute of Strategic & International Studies (ISIS) Malaysia
7.	Malaysian Bar
8.	Malaysian Media Council (MMM)
9.	Maxis Broadband Sdn. Bhd. (Maxis)
10.	Meta
11.	Roblox
12.	TikTok Service Pte. Ltd. (TikTok Malaysia)
13.	TM Technology Services Sdn. Bhd. (TM)
14.	TT dotCom Sdn. Bhd. (TIME)
15.	UNICEF Malaysia
16.	US-ASEAN Business Council (USABC)
17.	X Corp.
18.	YTL Communications Sdn. Bhd. (YTLC)

Table 2: List of Submissions Received

The feedback received reflects a diverse range of perspectives across industry, civil society, and institutional stakeholders. A summary of the feedback received, together with the Commission's response, is presented in the following sections.

©2026 MCMC. All rights reserved.

SECTION 2: FEEDBACK FROM THE PUBLIC CONSULTATION

The PC on the proposed OSP framework generated extensive feedback from a broad range of stakeholders. Respondents generally supported the objective of strengthening online safety governance and recognised the OSP as a mechanism to enhance transparency and accountability.

At the same time, stakeholders emphasised the importance of ensuring that the framework remain clear, proportionate, and practical. In particular, the respondents highlighted the need for a risk-based approach that reflects differences in service models, and for the OSP to function as a transparency and compliance mechanism aligned with ONSA.

This section summarises the feedback received and sets out the Commission's responses on the issues raised.

2.1 Question 1 – Proposed Content Management and Moderation

Question 1

The Commission invited 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.

©2026 MCMC. All rights reserved.

Overview of the Question

Question 1 relates to how Licensed Service Providers describe their content management and moderation approaches in the OSP, including the systems, processes, and safeguards used to detect, assess, manage, and respond to harmful content.

The proposed approach is intended to ensure that Licensed Service Providers clearly describe how their moderation practices support compliance with their duties under ONSA, in a manner that is transparent, proportionate to the nature and risk profile of the service, and supportive of effective regulatory oversight.

Summary of Submissions Received

Respondents generally supported the requirement for Licensed Service Providers to describe their content management and moderation approaches in the OSP and agreed that transparency in this area is important for accountability and regulatory oversight. Many considered the proposed scope to be clear and aligned with international practice.

At the same time, respondents emphasised that the framework should remain proportionate, non-prescriptive, and flexible, reflecting differences in service design, scale, and risk profile.

A recurring theme across submissions was the need for a risk-based and service-appropriate approach. Several respondents highlighted that the same level of detail should not apply uniformly to all Licensed Service Providers, particularly where services do not host user-generated content, do not enable public interaction, or function primarily as connectivity or distribution services.

©2026 MCMC. All rights reserved.

Telecommunications operators, infrastructure-based providers, and curated content services emphasised that they do not exercise editorial or moderation control over third-party or user-generated content, therefore should not be subject to the same expectations as social media, Internet messaging, or other interactive platforms.

In this regard, respondents called for clearer differentiation between content-hosting platforms and carriers or connectivity providers. It was suggested that the OSP should allow service providers to describe their moderation and governance approaches on a "where applicable" basis, taking into account their operational role and level of control over content.

Several respondents also emphasised that the OSP should remain descriptive in nature and should not introduce substantive obligations beyond those already provided under Part III of ONSA. Concerns were raised that certain elements of the proposed framework could be interpreted as mandating specific moderation measures, including proactive detection, continuous monitoring, or broader operational safeguards not expressly required under the Act. Respondents therefore recommended that the OSP focus on describing their existing compliance approaches, rather than prescribing new technical or operational requirements.

Additional feedback focused on implementation practicality and safeguards. Some respondents recommended phased implementation to allow sufficient time for system development, testing, and refinement before full compliance. Others called for flexibility in how moderation systems are disclosed, including the use of high-level descriptions or references to existing public transparency resources, without requiring disclosure of confidential, proprietary, or security-sensitive information. Several respondents also emphasised that the OSP should function as an outcome-focused transparency and reporting mechanism, rather than a vehicle for prescriptive operational mandates.

©2026 MCMC. All rights reserved.

A further set of views related to freedom of expression, human rights, and child protection were also raised for considerations. Several respondents emphasised that moderation measures should be implemented in a manner that avoids over-removal of lawful or protected content, particularly where broad concepts such as "national security", "public order", or "social cohesion" are applied without clear thresholds. Concerns were also raised regarding over-reliance on automated moderation, with calls for meaningful human oversight in complex or high-impact decisions.

In addition, several respondents highlighted the need for clearer articulation of child-specific moderation risks, including grooming, sexual exploitation, cyberbullying, self-harm content, and high-risk features where children may be present. Suggestions were also made for greater transparency in moderation standards, escalation processes, local language capability, human rights due diligence, and safeguards for verified news publisher content, public interest journalism, and child sexual abuse material ("**CSAM**").

The Commission acknowledges the feedback on the proposed scope and level of detail for content management and moderation under the OSP as well as the broad support for enhancing transparency and accountability in this area. The Commission also recognises the importance of ensuring that the framework remains proportionate, practical, and responsive to different service models and risk profiles. The Commission further notes the concerns regarding the interpretation of the OSP as introducing additional operational requirements beyond those set out under Part III of ONSA and emphasises that the OSP is intended to function as a transparency and compliance mechanism in support of existing statutory duties. In addition, the Commission recognises the need for protection of confidential information and broader considerations relating to freedom of expression and child protection. These considerations will be taken into account in ensuring that the OSP requirements remain clear, balanced, and consistent with the purpose of section 20 of ONSA.

©2026 MCMC. All rights reserved.

2.2 Question 2 – Proposed Detection and Removal Systems

Question 2

The Commission invited 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.

Overview of the Question

Question 2 relates to how Licensed Service Providers describe their detection and removal mechanisms in the OSP, including the systems and processes used to identify, assess, and address harmful content.

The proposed approach is intended to ensure that Licensed Service Providers clearly describe how their detection and response mechanisms support compliance with their duties under ONSA, including, where relevant, monitoring, reporting, and response mechanisms. This is to be done in a manner that is transparent, proportionate to the nature and risk profile of the service, and supportive of effective regulatory oversight.

Summary of Submissions Received

Respondents generally supported requiring Licensed Service Providers to describe their detection and removal systems in the OSP, recognising that effective mechanisms are important to identify, assess, and address harmful content.

©2026 MCMC. All rights reserved.

Many considered the proposed scope to be clear and relevant, particularly for services that host or enable user-generated content, including where the OSP explains detection approaches, escalation pathways, human review processes, timely response, and readiness to comply with lawful directions.

At the same time, respondents emphasised that the level of detail required should remain proportionate and practical, taking into account the nature of the service, the provider's technical capabilities, and the extent of its control over content.

A key theme across the submission was the need for a risk-based and service-appropriate approach. Several respondents highlighted that the proposed framework appears more suited to social media, Internet messaging, and other interactive services that host user-generated content, but may not be directly applicable to telecommunications providers, connectivity services, or curated broadcast and streaming services.

It was noted that such services often do not host, inspect, or control user-generated content, and instead manage risks through alternative means, such as editorial review, programme classification, content advisories, Uniform Resource Locator ("**URL**") blocking in response to lawful directions, or network-level interventions. In this regard, respondents called for clearer differentiation between services with direct content visibility and control, and those that function primarily as conduits or distributors, including the adoption of a lighter-touch or "where applicable" approach where appropriate.

A number of respondents also raised concerns that the proposed drafting could be interpreted as introducing substantive obligations beyond the reporting function of section 20 of ONSA. In particular, references to proactive monitoring or continuous monitoring, or additional removal-related measures were viewed as potentially implying new detection and removal duties beyond those set out under Part III of ONSA.

©2026 MCMC. All rights reserved.

Respondents therefore recommended that the OSP remains descriptive in nature, focusing on how Licensed Service Providers explain the systems and processes used to support compliance, rather than prescribing mandatory operational measures.

Additional feedback emphasised the importance of procedural safeguards and operational clarity. Respondents highlighted the need for meaningful human oversight in moderation decisions, particularly where automated tools are used, and cautioned against risks of over-removal of lawful or protected content. It was also suggested that that the OSP should explain how providers manage false positives and false negatives, when human review is triggered, how users are notified of removal or restriction decisions, and what appeal or complaint mechanisms are available.

Further, several respondents highlighted the importance of addressing child-specific detection and removal risks. Suggestions included clearer articulation of triaging reports involving children, urgent escalation pathways, child-specific removal timeframes for priority harmful content, and measures to reduce repeated exposure through re-uploads, re-sharing, or recommendation systems. Some respondents also emphasised that the OSP should expressly address CSAM as a distinct category requiring specialised detection, reporting, takedown, preservation, and coordination arrangements, including cooperation with law enforcement and relevant hotlines.

©2026 MCMC. All rights reserved.

The Commission acknowledges the feedback on the proposed scope and level of detail for detection and removal systems under the OSP. The Commission notes the broad support for transparency in this area, while also recognising the importance of ensuring that the framework remains proportionate to different service models and consistent with the statutory purpose of the OSP under section 20 of ONSA. The Commission also notes the concerns raised regarding operational practicality, procedural safeguards, freedom of expression, and child-specific protections, including concerns that certain elements may be interpreted as introducing additional detection or monitoring obligations beyond those set out under Part III of ONSA. These views will be taken into account in ensuring that the framework remains clear, balanced, and capable of supporting effective regulatory oversight.

2.3 Question 3 – Proposed Transparency in Content Moderation Systems

Question 3

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

©2026 MCMC. All rights reserved.

Overview of the Question

Question 3 relates to how Licensed Service Providers describe their content moderation systems in the OSP, including how such systems operate and the principles, tools, and processes applied in moderating or recommending content. The proposed approach is intended to ensure that Licensed Service Providers provide meaningful and appropriate transparency to support accountability and regulatory oversight, while balancing the need to protect confidentiality, proprietary, and security-sensitive information.

Summary of Submissions Received

Respondents generally supported requiring Licensed Service Providers to explain their content moderation systems in a way that supports transparency, accountability, and regulatory oversight. Many agreed that high-level disclosure of moderation, detection, and recommendation processes can enhance user confidence and enable the Commission to better understand how harmful content risks are managed in practice. There was also broad support for the principle that transparency obligations should not require disclosure of confidential, proprietary, or security-sensitive information.

A recurring theme in the feedback was the need to ensure that transparency requirements remain proportionate to the nature of the service and the provider's operational role. Respondents noted that the proposed approach is more readily applicable to services that host, curate, or moderate user-generated content, and may be less relevant to connectivity providers or curated services that do not rely on automated moderation or recommendation systems in the same manner. In this regard, it was suggested that the OSP should allow service providers to describe their transparency measures in a way that reflects their service model, including through existing tools such as viewer information features, complaint channels, governance processes, or content advisories.

©2026 MCMC. All rights reserved.

Several respondents emphasised that the transparency expectations should be limited to meaningful, high-level descriptions, rather than detailed disclosure of operational logic, internal workflows, escalation rules, or system configurations. It was noted that excessive transparency could expose trade secrets, commercially sensitive practices, or security-sensitive information, and may be enable malicious actors to evade or reverse-engineer moderation systems. Accordingly, respondents proposed that the framework should recognise the need to balance transparency with confidentiality, commercial sensitivity, and system integrity, and that this principle should apply across the OSP more broadly.

Additional feedback focused on the quality and accessibility of transparency disclosures. Some respondents recommended that moderation systems should be explained not only for regulatory purposes, but also in a manner that is understandable to users, including how users are informed of the reasons for content removal or restriction and whether they are able to challenge moderation decisions.

Some respondents also suggested that providers should disclose, at an appropriate level, the use of automated tools, their intended purpose, the safeguards in place, and how complex or high-risk decisions are escalated to human review. Further suggestions included disclosing information relevant to the local context, such as the number and location of human moderators, language capability, training, and bias prevention measures, as well as greater transparency in relation to children, fairness, and public interest content, including the treatment of verified news publishers and journalistic content.

©2026 MCMC. All rights reserved.

The Commission acknowledges the feedback on the proposed approach to transparency in content moderation systems and notes the broad support for meaningful transparency that strengthens accountability and public confidence, while preserving confidentiality, security, and system integrity. The Commission also notes the views that transparency expectations should remain proportionate to different service models and should focus on practical, relevant, and high-level information that supports effective regulatory oversight, without requiring disclosure of confidential, proprietary, or commercially sensitive details. These views will inform the refinement of the transparency requirements to ensure they remain clear, balanced, and appropriate to the purpose of the OSP under section 20 of ONSA.

2.4 Question 4 – Proposed User-Controlled Content Filters

Question 4

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

©2026 MCMC. All rights reserved.

Overview of the Question

Question 4 relates to how Licensed Service Providers describe the availability and use of user-controlled content filters in the OSP, including how such tools enable users to manage their exposure to harmful content. The proposed approach is intended to ensure that Licensed Service Providers clearly explain how filtering options are made accessible, easy to use, and appropriately configured to support user understanding and empowerment. These tools are intended to complement broader provider-level safety measures in supporting safer online experiences.

Summary of Submissions Received

Respondents generally supported the inclusion of user-controlled content filters as part of the user empowerment component of the proposed OSP framework, recognising that such tools can help users manage their experience on a service and reduce exposure to harmful or distressing material.

Many considered the proposed approach to be broadly clear, proportionate, and practical, particularly for services that host, recommend, or algorithmically disseminate user-generated content. Respondents also agreed that the OSP should explain how such tools are made available, how users can locate and customise them, and how safety-enhancing default settings are applied where appropriate.

A recurring theme in the feedback was the need for a service-appropriate and proportionate approach. Several respondents emphasised that user-controlled content filters are most relevant to services that curate, recommend, or surface content directly to users, and may not be meaningful or applicable for connectivity providers or services that do not host or control content.

©2026 MCMC. All rights reserved.

Telecommunications and infrastructure-based providers noted that they do not operate content feeds, recommendation systems, or platform-level filtering tools, and therefore should not be expected to provide the same type of user-controlled content filters as social media or online content platforms.

Similarly, curated broadcast and streaming services explained that user empowerment is often achieved through other embedded safeguards, such as parental controls, profile-based restrictions, programme information, and content classification systems, rather than personalised content filtering tools. Respondents therefore recommended that the OSP allow providers to describe user empowerment measures in a way that reflects their service model and level of control, including the ability to indicate where certain filtering tools are not applicable.

Several respondents also highlighted that existing public-facing resources should be recognised for the purpose of meeting transparency expectations in this area. It was suggested that service providers be permitted to fulfil part of this requirement by referring to publicly available help centre materials, safety resources, community standards, or transparency centres that already explain how filtering tools, privacy settings, reporting tools, and user controls operate, thereby avoiding unnecessary duplication of technical information in the OSP.

Additional feedback focused on accessibility and user understanding. Respondents recommended that filtering tools should be easy to understand, easy to locate, available in multiple languages, and accessible to persons with disabilities. It was also suggested that the OSP should explain how such tools operate for different user groups, particularly children and parents, including whether filters are enabled by default for child accounts, how categories and labels are presented, and whether younger users are provided with simplified explanations.

©2026 MCMC. All rights reserved.

Some respondents further suggested that the OSP should clearly explain the limitations of content filters in plain language, so that users do not assume that such tools alone can fully ensure safety. This includes describing whether additional precautionary steps are taken when users, particularly children, search for or are exposed to high-risk content.

Finally, respondents highlighted that user empowerment tools should not displace provider responsibility. Several respondents emphasised that content filters and other user controls should be treated as complementary safeguards, rather than substitutes for platform-level safety measures and that the framework should avoid implying that users bear primary responsibility for filtering out harmful content.

The Commission acknowledges the feedback on the proposed approach to user-controlled content filters and notes the broad support for providing users with meaningful tools to manage their experience on a service. The Commission also notes the views that the framework should remain proportionate to different service models, support accessibility and user understanding, and recognise that such tools complement broader provider-level safety measures. These views will be taken into account in ensuring that the proposed OSP framework remains practical, clear, and appropriate across different categories of Licensed Service Providers.

©2026 MCMC. All rights reserved.

2.5 Question 5 – Proposed Interaction and Privacy Settings

Question 5

The Commission invited views on whether the proposed approach to 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.

Overview of the Question

Question 5 relates to how Licensed Service Providers describe interaction and privacy settings in the OSP, including the tools and controls available to users to manage their online interactions, visibility, and personal boundaries. The proposed approach is intended to ensure that Licensed Service Providers clearly explain how such settings support user understanding and control, including the application of safety-enhancing defaults and appropriate safeguards, particularly for children and higher-risk interactions.

©2026 MCMC. All rights reserved.

Summary of Submissions Received

Respondents generally supported the proposed approach to describing interaction and privacy settings in the OSP, recognising that such settings are important in helping users manage their online interactions, privacy, and personal boundaries. Many considered the proposed approach to be broadly clear, proportionate, and practical, particularly for services that facilitate user-to-user engagement, public interaction, or personalised content exposure. Respondents also agreed that explaining these settings in the OSP could support user understanding, strengthen accountability, and demonstrate how Licensed Service Providers enable users to exercise greater control over their online experience.

A recurring theme in the feedback was the need for a service-appropriate and proportionate approach. Several respondents emphasised that interaction and privacy settings are most relevant to services that include messaging, commenting, tagging, public account visibility, or other interactive features. Telecommunications and connectivity providers, as well as curated broadcast and streaming services, noted that they do not generally operate such platform-level interaction controls and therefore should not be expected to implement or describe them in the same way as social media or Internet messaging services.

In this regard, respondents suggested that the OSP should allow service providers to indicate where such controls are not applicable and to instead describe alternative safeguards that are more relevant to their service role, such as parental management tools, controlled subscriber access, privacy policies, customer education, or compliance with existing data protection requirements.

©2026 MCMC. All rights reserved.

Several respondents also highlighted the importance of ensuring that interaction and privacy settings remain meaningful and understandable to users. It was suggested that Licensed Service Providers should explain, at a high level, how users can control who may contact them, interact with them, discover their accounts, as well as how such controls influence content visibility and exposure. Respondents also noted that tools such as block, mute, restrict, and reporting functions should be effective, accessible, and capable of providing timely protection.

Additional feedback focused on how data, behaviour, algorithmic systems influence user interactions and visibility. Some respondents suggested that providers should explain, at an appropriate level, whether users are able to adjust or opt out of personalised recommendations or profiling, and how such systems may affect exposure to content and interaction with others.

Child-specific safeguards were also emphasised as key consideration. Several respondents supported the inclusion of safety-enhancing default settings for child users and recommended that the OSP should clearly explain these measures, including default privacy settings, restrictions on contact from unknown users, limit on account discoverability, and accessible reporting mechanisms. Respondents also highlighted the importance of presenting such information in a manner that is understandable to different age groups.

In addition, some respondents recommended that the framework provide clearer guidance on identifying services likely to be accessed by children, using a high-level and non-prescriptive approach based on relevant factors rather than rigid thresholds.

A further set of views related to alignment with existing legal and policy frameworks. Some respondents cautioned against duplicating obligations that already arise under data protection requirements and recommended that the OSP framework be interoperable with existing privacy and governance obligations.

©2026 MCMC. All rights reserved.

Others proposed that, for certain service types, user empowerment in this area may be better supported through customer awareness initiatives or guidance on how to activate privacy and interaction controls on commonly used devices or third-party platforms. There were also suggestions that the OSP should address risks arising from predictive analytics and personalised recommendations systems, particularly for child users, where such systems may contribute to harmful exposure or exploitative engagement patterns.

The Commission acknowledges the feedback on the proposed approach to interaction and privacy settings and notes the broad support for empowering users with practical controls over their online interactions and privacy. The Commission also notes the views that the application of these expectations should remain proportionate to the functionality and operational design of the service, while ensuring that safeguards are meaningful, understandable, and supportive of user control. These views will be taken into account in ensuring that the framework remains clear, practical, and appropriate across different service environments.

2.6 Question 6 – Proposed User Education and Choice Architecture

Question 6

The Commission invited views on whether the proposed approach to 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.

©2026 MCMC. All rights reserved.

Overview of the Question

Question 6 relates to how Licensed Service Providers describe user education measures and choice architecture in the OSP, including how users are informed about safety-related features, risks, and decision-making tools. The proposed approach is intended to ensure that Licensed Service Providers clearly explain how users are supported through accessible guidance, contextual information, and design practices that promote informed and safety-enhancing choices, without misleading users or undermining user safety.

Summary of Submissions Received

Respondents generally supported the proposed approach to describing user education and choice architecture in the OSP, recognising that informed user decision-making is an important part of online safety. Many agreed that users should be provided with clear and accessible guidance on safety-related features, settings, and risks, and that the OSP should explain how service providers support users in understanding and using those safeguards.

Several respondents also considered the proposed approach to be broadly clear, proportionate, and practical, particularly for services that host, curate, or recommend content and provide users with direct interaction or choice over their online experience.

A recurring theme in the feedback was the need for a flexible and service-appropriate approach. Several respondents emphasised that user education and choice architecture should reflect the nature of the service and should not be implemented through a single prescribed model. It was noted that different services such as gaming platforms, curated broadcast services, or connectivity-based services may deliver safety guidance through different means, including terms and conditions, help centre materials, customer portals, parental dashboards, in-service notices, or contextual prompts, rather than standardised onboarding flows or interface-driven nudges.

©2026 MCMC. All rights reserved.

Accordingly, respondents recommended that the OSP should allow Licensed Service Providers to describe user education measures in a way that reflects their operational design and user journey.

Several respondents also highlighted the need for greater clarity on certain concepts, particularly the meaning of "higher risk features." It was suggested that the framework should provide indicative examples rather than fixed definitions, enabling service providers to identify such features in a structured and proportionate manner while retaining flexibility to apply judgement based on their services.

Others recommended that user education should not be limited to onboarding but should also be provided at relevant moments of heightened risk, including when users engage with features or settings that may have safety implications.

Additional feedback focused on accessibility, user understanding, and child-specific safeguards. Several respondents recommended that user education materials and safety information should be easy to understand, available in multiple languages, and accessible to different age groups, including the use of age-appropriate explanations, child-friendly language, and additional prompts or safeguards for child users.

A further theme in the feedback was that user education and choice architecture should complement, and not replace, broader provider-level safety measures. Several respondents stressed that such measures should form part of a wider online safety strategy that includes platform-level safeguards, content moderation, and privacy protections. Respondents also noted that design choices and recommendation systems can shape user exposure to risks and suggested that OSP should describe how providers help users understand why content is shown to them and how such systems are assessed to avoid manipulation or unsafe outcomes.

©2026 MCMC. All rights reserved.

At the same time, respondents cautioned against overly prescriptive user interface or design requirements, on the basis that such mandates may constrain innovation and may not suitable across all service types.

The Commission acknowledges the feedback on the proposed approach to user education and choice architecture and notes the broad support for helping users make informed and safety-enhancing decisions when using online services. The Commission also notes the views that these measures should remain flexible, proportionate, and appropriate to the nature of the service, while ensuring that safety information is accessible, understandable, and responsive to different user needs, including those of children. These views will be considered in ensuring that the framework remains practical, clear, and effective in supporting user empowerment.

2.7 Question 7 – Proposed Submission to the Commission

Question 7

The Commission invited 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.

©2026 MCMC. All rights reserved.

Overview of the Question

Question 7 relates to the proposed submission and update arrangements for the OSP, including the timelines for initial and annual submission, as well as the requirement to update the OSP where there are material changes to the service.

The proposed approach is intended to ensure that the OSP remains current, accurate, and reflective of the service's evolving risk profile, while supporting ongoing regulatory oversight and facilitating compliance with obligations under ONSA.

Summary of Submissions Received

Respondents generally supported the proposed submission and update arrangements for the OSP, recognising that structured and periodic submissions are important to enable effective regulatory oversight and ensure that the Commission has visibility over how online safety obligations are implemented.

Many agreed that the requirement for an initial submission, followed by ongoing updates, is appropriate in principle and reflects the dynamic nature of online services and associated risk environments.

A recurring theme in the feedback was the need for a more flexible and proportionate approach to submission timelines, particularly in relation to the proposed ninety (90) day period for the initial OSP submission. Several respondents, especially those operating complex or global services, highlighted that preparing a comprehensive and accurate OSP requires significant cross-functional coordination, data consolidation, and alignment with existing systems. As such, there were consistent recommendations to extend the timeline to at least 180 days, or to allow phased implementation or extensions where justified, in order to support meaningful and high-quality submissions.

©2026 MCMC. All rights reserved.

Respondents also raised concerns regarding the potential reporting burden associated with annual submissions and update requirements. While annual submission was generally accepted as a baseline, several respondents noted that requiring full resubmissions in cases where there are no substantive changes may result in duplicative reporting with limited regulatory value. In this regard, some suggested adopting a more proportionate approach, such as allowing annual attestations, partial updates, or limiting full resubmissions to circumstances where there are material changes to the service or its risk profile.

Another key issue raised relates to the lack of clarity on what constitutes a "material change". Respondents emphasised that without clear parameters, thresholds, or illustrative examples, this requirement may lead to inconsistent interpretation, regulatory uncertainty, and unnecessary resubmissions. Several recommended that a risk-based approach be adopted, whereby update obligations are triggered by changes that materially affect the service's risk profile, safety measures, or user exposure to harmful content.

In addition, some respondents highlighted the importance aligning submission requirements with existing operational and regulatory frameworks. Suggestions included allowing cross-referencing of information already submitted under other regulatory instruments, and providing templates or guidance to support consistency and clarity in OSP submissions. These measures were viewed as important to reduce duplication, improve efficiency, and support practical implementation.

©2026 MCMC. All rights reserved.

The Commission acknowledges the feedback on the proposed submission and update arrangements and notes the broad support for maintaining a structured and adaptive submission framework. The Commission also notes the views that timelines, update triggers, and reporting requirements should remain proportionate, clearly defined, and aligned with operational realities. These views will be considered in refining the framework to ensure that it supports effective oversight while remaining practical and manageable for Licensed Service Providers.

2.8 Question 8 – Proposed Governance and Accountability

Question 8

The Commission invited 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.

Overview of the Question

Question 8 relates to how Licensed Service Providers describe their governance and accountability arrangements in the OSP, including how internal structures, responsibilities, and decision-making processes support compliance with online safety obligations under ONSA. The proposed approach is intended to ensure that Licensed Service Providers clearly explain how oversight, risk management, and accountability are embedded within their operations to support effective and consistent implementation of online safety measures.

©2026 MCMC. All rights reserved.

Summary of Submissions Received

Respondents generally supported the proposed approach to describing governance and accountability arrangements in the OSP, recognising that clear internal responsibility and oversight are important to support compliance with obligations under ONSA. Many considered the proposed approach to be broadly clear, proportionate, and practical, particularly where it requires service providers to identify internal accountability mechanisms, management oversight, and a clear point of contact for regulatory engagement. Several respondents noted that clear governance arrangements can help ensure that online safety obligations are implemented in a structured, timely, and auditable manner.

A recurring theme in the feedback was that the OSP should allow Licensed Service Providers to rely on existing governance and compliance structures, rather than requiring the creation of entirely new organisational arrangements solely for OSP purposes. Respondents, particularly those operating curated or infrastructure-based services, noted that online safety-related oversight may already be embedded within existing regulatory, compliance, editorial, risk management, or operational governance functions.

It was therefore recommended that providers be permitted to describe these arrangements at a high level, including approval processes, escalation pathways, and management oversight mechanisms, without requiring detailed disclosure of internal organisational structures.

Several respondents also emphasised that governance expectations should remain proportionate to the provider’s service model, operational role, and degree of control over content and user interaction. Some suggested that governance and accountability requirements should be calibrated according to the provider’s nature, scale, technical feasibility, and risk exposure profile.

©2026 MCMC. All rights reserved.

In this regard, respondents noted that providers which do not operate social media or Internet messaging services should not be expected to implement governance processes beyond what is relevant to their licensable activities. It was noted that for certain service types, accountability may be demonstrated through existing governance arrangements and lawful cooperation mechanisms.

Additional feedback focused on the need for governance arrangements to support effective internal ownership of online safety across the organisation. While respondents generally supported identifying a point of accountability with appropriate seniority and expertise, some emphasised that responsibility for online safety should not rest solely with a single individual or senior management function. Instead, respondents suggested that safety-related standards and decision-making should be embedded across relevant functions and levels of the organisation, including product, design, compliance, and risk teams.

Some respondents also proposed that governance arrangements should incorporate, or have access to, relevant expertise, including child safety and human rights considerations. This may include internal review or oversight mechanisms to monitor moderation practices and track risks arising from online safety measures.

©2026 MCMC. All rights reserved.

The Commission acknowledges the feedback on the proposed approach to governance and accountability arrangements and notes the broad support for clear internal responsibility, management oversight, and effective regulatory engagement. The Commission also notes the views that governance requirements should remain proportionate, should be capable of being met through existing organisational structures where appropriate, and should reflect the provider's service model and operational role. The Commission further recognises that accountability may be distributed across relevant functions within an organisation. These views will be taken into account in ensuring that the OSP remains practical, clear, and supportive of effective oversight and compliance under ONSA.

2.9 Question 9 – Proposed Governance Accountability and Contact Point

Question 9

The Commission invited 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 ONSA.

©2026 MCMC. All rights reserved.

Overview of the Question

Question 9 focuses on how Licensed Service Providers identify and describe a governance accountability function and regulatory contact point within the OSP. This includes how the designated function supports internal coordination, oversight of online safety obligations, and engagement with the Commission. The proposed approach is intended to ensure that there is a clear and effective channel for regulatory communication, with appropriate authority, expertise, and organisational access to support compliance and accountability under ONSA.

Summary of Submissions Received

Respondents generally supported the proposed approach to governance accountability arrangements and the identification of a regulatory contact point in the OSP, recognising that a clearly defined accountability function and accessible point of contact are essential to support effective oversight, coordination, and regulatory engagement under ONSA. Many respondents considered the approach to be clear, proportionate, and practical, particularly in establishing a structured channel for communication with the Commission and ensuring internal ownership of compliance obligations.

A key theme across the feedback was the preference for flexibility in how the regulatory contact point is designated. Several respondents recommended that the requirement should not be limited to a single named individual but may instead be fulfilled through a functional or institutional contact point, such as a dedicated team, department, or role-based email alias. This approach was viewed as more operationally sustainable, particularly for large or global organisations, as it ensures continuity, avoids disruption from personnel changes, and supports timely and coordinated responses.

©2026 MCMC. All rights reserved.

Respondents also highlighted the need for clarity on expectations relating to the contact point's seniority, expertise, and authority. While there was general agreement that the contact point should have sufficient access to management and decision-making functions, some noted that further guidance would support more consistent implementation, particularly for multinational service providers with distributed governance structures. In this regard, it was suggested that the contact point may be a regional or global function with clear responsibility for Malaysia, rather than necessarily a locally based individual.

Another recurring view was that Licensed Service Providers should be permitted to leverage existing governance, compliance, and regulatory engagement structures, rather than requiring the establishment of new roles or processes solely for OSP purposes. Respondents noted that many organisations already maintain established functions responsible for regulatory compliance and engagement, and that these could serve as the designated contact point, provided accountability remains clear and effective.

Several respondents further emphasised that the accountability function and contact point should be meaningful and operationally effective, rather than purely administrative. In particular, where services are likely to be accessed by children or involve higher-risk functionalities, respondents suggested that the contact point should have access to relevant expertise, including child safety considerations, and play an active role in escalation, coordination, and review of safety-related matters. Some also proposed that governance arrangements should incorporate broader considerations such as human rights due diligence and cross-functional coordination to ensure consistent implementation of safety measures. A few respondents further suggested that, in relation to CSAM and other serious child protection matters, service providers should identify a focal point capable of liaising promptly with relevant authorities and trusted reporting channels.

©2026 MCMC. All rights reserved.

Concerns were also raised regarding proportionality, scope, and potential risks associated with the requirement. Some respondents cautioned against imposing disproportionate expectations and recommended that obligations be calibrated based on the provider's risk exposure, scale, and service characteristics. Others highlighted potential risks in requiring the identification of a named individual, including personal liability, security, and harassment concerns, and therefore supported the option of designating a role-based or departmental contact. In addition, a few respondents also questioned whether mandating a specific accountability role may extend beyond the scope of section 20 of ONSA.

The Commission acknowledges the feedback received, including the strong support for maintaining clear accountability and effective regulatory engagement, as well as the recommendations to provide flexibility in the designation of the contact point and to align requirements with existing organisational structures. The Commission also notes the concerns relating to proportionality, operational practicality, and potential risks associated with naming individuals. These views will be taken into account in ensuring that governance accountability and contact point requirements remain clear, proportionate, and effective in supporting compliance with obligations under ONSA.

©2026 MCMC. All rights reserved.

SECTION 3: CONCLUSION

The Commission extends its appreciation to all respondents who contributed to this Public Consultation. The views and recommendations received have been invaluable in informing the development of the proposed OSP framework.

The Commission will review and consider all feedback in finalising the OSP framework to ensure that it is clear, practical and enforceable, while balancing the public interest with operational realities for industry.

Once finalised, the framework will support the implementation of the Online Safety Act 2025 and contribute to a safer online environment in Malaysia.

29 April 2026

©2026 MCMC. All rights reserved.