Malaysian Communications and Multimedia Commission

PUBLIC CONSULTATION REPORT ON

PROPOSED DRAFT CODES UNDER THE ONLINE SAFETY ACT 2025

TABLE OF CONTENTS

GLOSSARY 2
SECTION 1: INTRODUCTION 3
1.1 Background 3
1.2 Objective 4
1.3 Scope and Application 5
1.4 Stakeholder Engagement 5
1.5 Public Consultation 6
SECTION 2: FEEDBACK ON THE DRAFT RISK MITIGATION CODE 8
2.1 General Feedback 9
2.2 Feedback on Risk Assessment 11
2.3 Feedback on Risk Mitigation Measures 12
2.4 Conclusion 15
SECTION 3: FEEDBACK ON THE DRAFT CHILD PROTECTION CODE 17
3.1 General Feedback 18
3.2 Feedback on Age Verification 19
3.3 Feedback on Content Moderation 23
3.4 Feedback on Parental Controls 25
3.5 Feedback on Privacy and Safety Settings 26
3.6 Feedback on Safe Search and Recommendation Settings 28
3.7 Conclusion 29
SECTION 4: CONCLUSION 30

©2026 MCMC. All rights reserved.

GLOSSARY

Term	Definition
AI	Artificial Intelligence.
ASP	Applications service provider.
CASP	Content applications service provider.
child	A person who is under the age of eighteen (18) years.
child user	A user identified to be a child.
CMA 1998	Communications and Multimedia Act 1998 [Act 588].
Commission	Malaysian Communications and Multimedia Commission.
CPC	Child Protection Code.
Licensed Service Provider	Applications service provider or content applications service provider licensed under the CMA 1998.
Licensing Framework	Licensing framework for Internet messaging service and social media service providers under the CMA 1998.
NSP	Network service provider
ONSA	Online Safety Act 2025 [Act 866].
parent	The parent or guardian of a child user.
PC	Public consultation.
RMC	Risk Mitigation Code.

©2026 MCMC. All rights reserved.

SECTION 1: INTRODUCTION

1.1 Background

The Malaysian Communications and Multimedia Commission ("**Commission**") is mandated under the Malaysian Communications and Multimedia Commission Act 1998 [Act 589] to supervise and regulate communications and multimedia activities in Malaysia. Under the Commission's purview are two acts that are enforced towards ensuring the online safety of users in Malaysia, namely the Communications and Multimedia Act 1998 [Act 588] ("**CMA 1998**") and the Online Safety Act 2025 [Act 866] ("**ONSA**").

In 2024, the Commission introduced the licensing framework for Internet messaging service and social media service providers under the CMA 1998 ("**Licensing Framework**"). Beginning 1 January 2025, the Licensing Framework requires Internet messaging service[1] and social media service[2] providers having eight (8) million or more users in Malaysia to apply for Applications Service Provider Class [ASP(C)] licence registration under the CMA 1998 to provide their respective applications services in Malaysia.

The Commission is also the enforcement agency for ONSA which came into force on 1 January 2026. ONSA aims to enhance and promote online safety in Malaysia by regulating harmful content and providing for duties and obligations of the applications service providers ("**ASPs**"), content applications service providers ("**CASPs**") and network service providers (**"NSPs**"), and to provide for related matters.

[1] "**Internet messaging service**" means an applications service which utilises Internet access service that enables a user to communicate any form of messages with another user.
[2] "**social media service**" means an applications service which utilises Internet access service that enables two or more users to create, upload, share, disseminate or modify content.

©2026 MCMC. All rights reserved.

1.2 Objective

Under Part III of ONSA, ASPs and CASPs licensed under the CMA 1998 (hereinafter collectively referred to as the "**Licensed Service Providers**" or individually referred to as "**Licensed Service Provider**") that utilise internet access service to enable communication between users or to provide content are required to comply with various online safety duties, including:

(i) **the duty to implement measures to mitigate risk of users' exposure to harmful content** under section 13 of ONSA; and

(ii) **the duty to protect the online safety of child users** under section 18 of ONSA.

In accordance with section 80 of ONSA, the Commission is empowered to issue any code for the purposes of ensuring said service providers' compliance with Part III duties. These codes will address regulatory gaps by clearly setting out the measures the applicable service providers are required to implement in order to comply with their online safety duties.

The proposed draft codes under ONSA are:

(i) the code in relation to the duty to implement measures to mitigate risk of exposure to harmful content under section 13 of ONSA, otherwise known as the **Risk Mitigation Code** ("**RMC**"); and

(ii) the code in relation to the duty to protect online safety of child user under section 18 of ONSA, otherwise known as the **Child Protection Code** ("**CPC**").

©2026 MCMC. All rights reserved.

1.3 Scope and Application

Licensed Service Providers that utilise internet access service to enable communication between users or to provide content are required to comply with the duties set out in Part III of ONSA, including under section 13 and section 18.

The RMC will specify the measures that a Licensed Service Provider shall implement to mitigate the risk of users being exposed to harmful content in compliance of the duty under section 13 of ONSA.

The CPC will specify the measures that a Licensed Service Provider shall implement to ensure safe use of their services by child users in compliance of the duty under section 18 of ONSA.

1.4 Stakeholder Engagement

To support the development of subsidiary instruments under ONSA (including the RMC and CPC), the Commission convened a series of stakeholder engagement sessions on 18 and 27 November 2025.

The stakeholder engagement 18 November 2025 comprised of two planned sessions held separately for non-industry and industry stakeholders. To accommodate stakeholders who were unable to attend, a supplementary session on 27 November 2025 was conducted to ensure broader participation, inclusivity, and meaningful consultation. The engagement sessions recorded diverse participation, demonstrating stakeholders' interest in the implementation of ONSA.

©2026 MCMC. All rights reserved.

Across all sessions, 64 participants representing 36 organisations attended. Participants expressed support for strengthening online safety protections under ONSA, particularly for child safety, while emphasising the importance of practical operational details for subsidiary instruments, a balanced approach to regulatory certainty and flexibility, complementary self-regulatory measures, and ongoing consultation with clear guidance and timelines for smooth implementation.

1.5 Public Consultation

On 12 February 2026, the Commission commenced a public consultation ("**PC**") on the proposed draft codes under ONSA where members of the public, industry stakeholders, and other interested parties were invited to provide feedback on the proposed draft RMC and on the proposed draft CPC over a one-month period from 12 February until 13 March 2026, at 5:00 p.m., either in hard copy or electronic form. The PC period was subsequently extended until 31 March 2026 to accommodate stakeholder requests.

In total, the Commission received **21 written submissions** from **24 respondents**. The list of respondents is provided in **Table 1** below. Summaries of feedback received together with the Commission's responses are presented in the following sections.

©2026 MCMC. All rights reserved.

No.	Respondents
1	UNICEF
2	X Corp.
3	Roblox (corp.roblox.com)
4	rednote (Xiaohongshu)
5	Measat Broadcast Network Systems Sdn Bhd (Astro)
6	Maxis Broadband Sdn Bhd (Maxis)
7	TT dotCom Sdn Bhd (Time)
8	TM Technology Services Sdn. Bhd. (TM)
9	Asia Tech Alliance (ATA)
10	Human Rights Commission of Malaysia (SUHAKAM)
11	Malaysian Media Council (MMM)
12	Institute of Strategic & International Studies (ISIS) Malaysia
13	Meta
14	YTL Communications Sdn Bhd (YTLC)
15	Malaysian Bar
16	TikTok Service Pte. Ltd. (TikTok)
17	US-ASEAN Business Council (USABC)
18	Google
19	Online Child Sexual Exploitation and Abuse (OCSEA) Working Group and ECPAT Malaysia
20	CelcomDigi
21	ARTICLE 19, the Centre for Independent Journalism (CIJ), and Sinar Project

Table 1: List of Submissions Received

©2026 MCMC. All rights reserved.

SECTION 2: FEEDBACK ON THE DRAFT RISK MITIGATION CODE

In conducting the PC, the Commission sought feedback from stakeholders and interested parties through written submissions guided by the following questions:

- **Are the measures specified in the draft RMC practicable to be implemented?** *For example, are there any limitations which would prevent a Licensed Service Provider from implementing a particular measure? What are the barriers to implementation?*
- **Are the measures specified in the draft RMC effective to mitigate the risk of users being exposed to harmful content?**
- **Are there any other measures that the Commission should consider adopting to mitigate the risk of users being exposed to harmful content?**

This section summarises the feedback received and sets out the Commission's acknowledgement of and responses to the views of stakeholders.

©2026 MCMC. All rights reserved.

2.1 General Feedback

There was express support for the Commission's efforts to strengthen online safety in Malaysia, particularly for children and vulnerable groups. Respondents also acknowledged the role of the RMC in addressing harmful content risks as part of the Commission's broader policy efforts through subsidiary instruments under ONSA.

Respondents indicated that the RMC would benefit from clearer interpretive guidance on the categories of harmful content applicable. They noted that overbroad or insufficiently defined categories could, for example, unintentionally capture lawful and socially valuable expression, including legitimate journalism such as investigative reporting on public wrongdoing or coverage of racial, religious and political tensions. On this basis, respondents encouraged the development of clearer thresholds and more workable definitions for each category of harmful content, ideally through the Commission's collaboration with the relevant service providers and other relevant stakeholders.

A related theme concerned the scope of services to which the RMC should apply. Respondents sought greater clarity on the intended scope of the RMC e.g., that it is limited to (i) applications services that enable communication between users and (ii) content applications services that provide content using internet access services.

Within this discussion, respondents submitted that the guidelines should be applied in a proportionate and service-specific way, and should be confined to user-generated content (UGC) services rather than curated, editorially controlled broadcast and Internet Protocol television (IPTV) services that are already subject to regulatory oversight under the CMA 1998, the Content Code, and the Film Censorship Board (*Lembaga Penapis Filem,* LPF).

©2026 MCMC. All rights reserved.

The RMC's approach should be role-based and proportionate, where the practicality and effectiveness of compliance will depend heavily on a service provider's functional role, technical capabilities and degree of control over content. Content-centric obligations such as content moderation, algorithm testing, advertiser verification and user-level controls are better aligned to services that host, curate or algorithmically disseminate content, and are less suitable for network or infrastructure providers that do not have visibility into, or control over, the content carried across their systems.

Many respondents favoured a risk-based regulatory approach for obligations. They observed that the practicability of compliance is likely to differ significantly between very large, well-resourced platforms and other (e.g., smaller) platforms. Accordingly, respondents called for a tiered and graduated approach that differentiates between services according to their type, functionality and systemic risk or impact. In their view, such an approach would better support effectiveness and proportionality by aligning obligations with actual risk.

Respondents also urged that the RMC should be grounded in a rights-based approach. In particular, they emphasised the importance of preserving freedom of expression, freedom of speech and the right to privacy, while ensuring that any restrictions or interventions are implemented in accordance with the principles of legality, necessity and proportionality.

Respondents drew attention to the importance of providing an adequate implementation period before compliance is enforced. One suggestion was that the relevant service providers be given 12 months from the finalisation and publication of the RMC for compliance purposes, such as to assess their obligations, adjust internal processes and deploy any necessary technical or operational changes.

©2026 MCMC. All rights reserved.

The Commission acknowledges the general feedback received on the proposed draft RMC and takes note of the views expressed in relation to interpretive clarity, scope of application, proportionality, role- and risk-based considerations, implementation timelines and rights-based principles. The Commission will consider the feedback received in the context of the overall regulatory objective and implementation of the RMC.

2.2 Feedback on Risk Assessment

Respondents generally acknowledged the importance of harmful content risk assessment as a foundational mechanism under the RMC and recognised its role in supporting a proactive and structured approach to managing online safety risks. Certain respondents further observed that elements of the RMC's risk assessment framework, particularly those relating to governance, documentation, and internal oversight, are broadly aligned with existing internal practices and compliance processes.

In relation to harmful content risk assessments, respondents stressed that these assessments should be grounded in a rights-based approach and informed by human rights impact assessment methodologies. Some respondents proposed that, in order to strengthen governance and transparency in matters affecting children, a Child Rights Impact Assessment should be mandated as part of the overall harmful content risk assessment process.

Respondents also suggested that risk assessments should be accepted where they are recognised or harmonised with frameworks used in leading online safety jurisdictions such as the European Union, the United Kingdom and Australia. This reduces duplicative compliance burdens and takes into account established good practice in comparable regulatory environments.

©2026 MCMC. All rights reserved.

In addition, it was proposed that the concept of "situations of heightened risk" within the risk assessment framework should be expanded to include federal and state election periods.

The Commission acknowledges the feedback on harmful content risk assessment and takes note of views expressed in relation to rights-based assessment approaches, alignment with recognised frameworks, and the identification of situations of heightened risk. The Commission will consider the feedback received in the context of the overall regulatory objective and implementation of the RMC.

2.3 Feedback on Risk Mitigation Measures

With respect to risk mitigation measures, respondents indicated that the RMC is aligned with established international regulatory frameworks and reflects recognised best practices in online safety regulation.

Advertiser Verification for Paid Advertisements

With respect to advertiser verification for paid advertisements, respondents noted that not all advertisements originate from advertisers whose identity can readily be verified against government records in Malaysia. They observed that this may be difficult to implement in practice for international platforms operating across multiple jurisdictions, as well as for cross-border advertisers whose supporting documentation may differ in standards with Malaysia e.g., format, source or reliability.

For this reason, respondents generally favoured a risk-based and targeted approach to advertiser verification rather than a blanket requirement applying to all paid advertisers.

©2026 MCMC. All rights reserved.

There were respondents that noted that advertiser verification may play a useful role in mitigating harms associated with paid advertisements and online marketplaces, including scams, fraudulent goods and misleading services. One example raised was the possibility of requiring financial advertisers to demonstrate that they are appropriately licensed and legitimate entities. However, respondents also noted that further consultation would be needed to design such a framework carefully, including on questions such as who would be responsible for determining licensing validity, how advertisements would be monitored over time, how cross-border regulatory recognition would operate, and how verification status would be maintained on an ongoing basis.

Respondents further submitted that any advertiser verification requirement should remain technology neutral so that platforms may comply through self-developed systems, independent verification mechanisms, or suitably qualified third-party solutions.

Feedback also cautioned that advertiser verification requirements may have wider business and trade implications. In particular, it was noted such requirement could introduce business delay and increase compliance costs, especially for smaller platforms, and could potentially create tension with Malaysia's commitments under digital trade agreements.

AI Labelling

On Artificial Intelligence ("**AI**") labelling, respondents emphasised the current technological limitations associated with reliably detecting and labelling AI-generated content. They noted that, in practice, it is not presently feasible for platforms to identify and label such content with complete accuracy. Any labelling requirement should therefore take account of these technical constraints.

©2026 MCMC. All rights reserved.

A further concern raised was related to content generated through third-party AI tools or shared by users across different services and platforms. Respondents observed that, in such circumstances, there may be no AI label attached to the content in the first place, or any label that does exist may not be preserved when the content is reposted elsewhere. A more practical approach suggested by some respondents was for platforms to provide clear product tools and guidance that enable users and advertisers to disclose and report AI-generated content, together with distinguishable labels based on those disclosures.

Feedback also questioned the effectiveness of mandating visible, surface-level labels alone, noting that such labels may easily be edited out or stripped by bad actors. In this respect, some respondents cautioned that Government-backed universal labelling mandates could inadvertently generate false confidence among users, as content that is not labelled may be assumed to be authentic even when it has simply gone undetected. Conversely, if a very large volume of content were to carry labels, users might become desensitised to them, thereby reducing the practical value of labels when harmful manipulated images, audio or video are encountered.

Other Risk Mitigation Measures to Consider

Respondents proposed several additional mitigation measures for consideration. One such suggestion was that any requirement for pre-launch risk assessments should remain regulation-agnostic and focus on product changes that have the potential to materially increase the risk of users being exposed to harmful content on a service.

Another potential measure was that advertisements should, where appropriate, be reviewed before going live. Pre-publication reviews may serve as a critical safeguard to prevent high-risk advertisements from reaching users and causing harm.

©2026 MCMC. All rights reserved.

The Commission acknowledges the feedback on risk mitigation measures and takes note of the views expressed in relation to advertiser verification for paid advertisements, including practicability for cross-border platforms, the preference for risk-based and targeted approaches, technology neutral compliance options, and potential business and trade implications. The Commission also takes note of the feedback concerning AI labelling, including current technical limitations, challenges associated with third-party and reposted content, and views on the effectiveness of labelling approaches, as well as suggestions on additional mitigation measures such as pre-launch risk assessments and pre-publication review of advertisements. The Commission will consider the feedback received in the context of the overall regulatory objective and implementation of the RMC.

2.4 Conclusion

Overall, the feedback received reflects broad recognition of safeguards against harmful content online, while also underscoring that any resulting obligation in relation to risk assessment and risk mitigation measures should be proportionate and grounded in operational realities. Respondents consistently called for clearer definitions of harmful content, greater certainty as to the services captured by the RMC, and a more differentiated approach that reflects the varying roles and capabilities of different categories of services.

Respondents expressed that measures should remain risk-based, preserve fundamental rights, technology neutral, and sufficiently flexible to accommodate evolving harms, business models and technical constraints. In particular, respondents highlighted the practical limitations of absolute or highly prescriptive requirements in areas such as advertiser verification and AI labelling.

©2026 MCMC. All rights reserved.

Taken together, the overall feedback does not challenge the policy intent of enhancing online safety through risk assessment and risk mitigation. Rather, it points towards the value of a framework that is clear, rights-respecting, and implementable in practice.

The rest of this page is intentionally left blank.

©2026 MCMC. All rights reserved.

SECTION 3: FEEDBACK ON THE DRAFT CHILD PROTECTION CODE

In conducting the PC, the Commission sought feedback from stakeholders and interested parties through written submissions guided by the following questions:

- **Are the measures specified in the draft CPC practicable to be implemented?** *For example, are there any limitations which would prevent a Licensed Service Provider from implementing a particular measure? What are the barriers to implementation?*
- **Are the measures specified in the draft CPC effective to ensure safe use of their services by child users?**
- **Are there any other measures that the Commission should consider adopting to ensure safe use of their services by child users?**

This section summarises the feedback received and sets out the Commission's acknowledgement of and responses to the views of stakeholders.

©2026 MCMC. All rights reserved.

3.1 General Feedback

Respondents expressed support for the Commission's objective to strengthen online safety for children through the introduction of the CPC and acknowledged the CPC's role in as an important regulatory instrument to enhance protections for children in the online environment. Feedback indicated that the CPC complements existing regulatory and platform-level measures aimed at improving child safety outcomes as well as supports a more structured and consistent approach to safeguarding children across online services.

Respondents urged for greater clarity of the services that would fall within the scope of the CPC e.g., whether the framework is intended to apply to (i) application services that enable communication between users, and (ii) content application services that deliver content, using internet access services. Respondents observed that the effectiveness of the proposed requirements would depend substantially on the operational characteristics of the relevant service, and they cautioned against applying identical expectations across markedly different service types.

Respondents submitted that broadcast and curated over-the-top services typically do not rely on open user uploads and instead manage access through upstream editorial classification, electronic programme guide descriptors, scheduling, and parental control personal identification numbers. In their view, these services should be treated distinctly from open, user-generated environments.

Respondents emphasised that although the proposed measures may be practicable for application service providers and content application service providers, they would not be practicable for network service providers. Certain measures cannot realistically be implemented by entities that neither control nor operate those applications.

©2026 MCMC. All rights reserved.

Respondents also recommended that a reasonable implementation timeline be provided following finalisation and publication of the CPC. A transition period of 12 months was regarded as important for facilitating smoother compliance and promoting regulatory certainty.

The Commission acknowledges the general feedback received on the proposed draft CPC and takes note of the views expressed in relation to clarity of service scope, differentiation between user-generated and curated services, and the practicability of implementing the proposed measures for different categories of service providers. The Commission will consider the feedback received in the context of the overall regulatory objective and implementation of the CPC.

3.2 Feedback on Age Verification

Open Access for Social Media

There were respondents that advocated to allow all users under 18 years old access to services subject to appropriate safeguards. In other words, these respondents favoured an under-18 safety standard, rather than prohibiting access for users under-16.

Respondents favouring a universal child safety standard argued that such an approach would enable stronger automated protections without requiring invasive data collection. In their view, removing a hard age barrier would reduce the need for age-assurance or age-verification systems that entail the collection and processing of personal data.

©2026 MCMC. All rights reserved.

Respondents also expressed concern that a blanket prohibition on social media access for children under 16 could amount to discrimination against children and could unduly interfere with their rights to access information and freedom to express themselves as protected by the Federal Constitution. In this regard, respondents considered that a restrictive age-based access model may not strike an appropriate balance between child safety and the rights of children. They further observed that age restrictions may not achieve their intended effect in practice, as children may turn to workarounds or migrate to less regulated services, while legitimate users could be wrongly flagged through imperfect age-assurance processes.

Minimum Age for Social Media

Certain respondents supported an age threshold of 13 that would be more consistent with prevailing industry practice, instead of the proposed minimum age of 16 for account registration.

Age Assurance

A significant body of feedback supported the adoption of age assurance methods, rather than a single, prescriptive age-verification model. Respondents argued for age assurance grounded in a proportionate and risk-based framework, in which the level of assurance expected of a service corresponds to the level of harm or risk posed by that service. On this view, the CPC should permit Internet messaging service providers and social media service providers to adopt reasonable, proportionate and risk-based age-assurance measures tailored to their service design, user base, and risk profile.

©2026 MCMC. All rights reserved.

Respondents also advocated a multi-layered age-assurance strategy. Instead of relying solely on hard identifiers for all users and use cases, they recommended a framework that allows platforms to combine a range of signals and interventions. Such layered systems can help detect and remove underage accounts even where age has initially been misrepresented and can evolve as patterns of circumvention change over time. This approach was regarded as better suited to balancing child protection objectives with privacy safeguards.

Feedback also drew attention to international approaches as possible points of reference. It was noted that Australia's Social Media Minimum Age framework requires platforms to take reasonable steps without mandating a single technical method; that the United Kingdom's Online Safety Act 2023 requires effective age-assurance mechanisms without prescribing a specific technology; and that the European Union's Digital Services Act requires appropriate and proportionate measures to protect minors.

Age Verification

A consistent theme across submissions was that mandatory verification against government-issued records are not aligned with the principles of data minimisation and the protection of user privacy. Respondents cautioned that such a requirement could oblige platforms, or their third-party vendors, to collect, process and potentially retain highly sensitive personal information for all users, the majority of whom are adults. In their view, this would create concentrated repositories of sensitive data and materially heighten exposure to privacy breaches and cybersecurity incidents. Some respondents further argued that the potential harm arising from a large-scale data breach involving government-issued identification records of millions of Malaysian users could far outweigh the intended benefits of the proposed child safety intervention. In support of data minimisation, it was recommended that the CPC should expressly state that age verification is not required where a service already has reasonable confidence in a user's age.

©2026 MCMC. All rights reserved.

Related concerns were raised about proportionality, human rights, and transparency. Respondents observed that it remains unclear how a mandatory age-verification regime would be proportionate to the actual risks of harm, and whether it would be compatible with obligations to respect and protect privacy. Mandatory identity verification linked to platform activity could create infrastructure capable of tracking how individual citizens access and consume information online. They also noted that there was insufficient publicly available information regarding the procurement process of appointing any third-party vendor that might be tasked with implementing age-verification measures.

Concerns were also expressed regarding equitable access. Identity-based verification may exclude users who do not possess government-issued identification, who share devices within households, or who face accessibility, documentation, or socioeconomic barriers to digital verification systems. Respondents noted that such outcomes could disproportionately affect vulnerable or marginalised groups, including undocumented persons and refugees, and could therefore undermine inclusive access.

Respondents cautioned that age verification should not be treated as a singular or definitive solution. They observed that international experience suggests that no one technical method can entirely prevent age misrepresentation or circumvention, particularly given the adaptability of young users in navigating technical controls and bypass verification requirements.

©2026 MCMC. All rights reserved.

Operational and compliance burdens in implementing age verification were another concern. Respondents submitted that building and maintaining secure age verification infrastructure would be costly and technically complex, and that such obligations could fall particularly heavily on smaller or emerging platforms, thereby raising barriers to entry and reducing competition. Some also considered that a tightly prescribed verification model may not be sufficiently future-proof in a rapidly evolving technological environment.

The Commission acknowledges the feedback on age verification and takes note of the views expressed in relation to appropriate age thresholds, the merits of age assurance as compared to prescriptive age-verification models, privacy and data protection considerations, proportionality, children's rights, operational and compliance implications and inclusive access concerns. The Commission will consider the feedback received in the context of the overall regulatory objective and implementation of the CPC.

3.3 Feedback on Content Moderation

Several respondents supported the objective of protecting children from harmful content online and acknowledged the role of content moderation and safety systems in achieving this objective. Some respondents also highlighted that platforms have already implemented a range of measures, including automated detection, human review processes, and age-appropriate safeguards, to reduce children's exposure to harmful content.

©2026 MCMC. All rights reserved.

Respondents generally supported a child safety objective grounded in reasonableness and proportionality, rather than one framed as absolute prevention of harm. They proposed that the obligation on Internet messaging service providers and social media service providers should be to take reasonable and proportionate steps to significantly reduce the risk of child users encountering harmful content, rather than to guarantee the complete elimination of such material. Respondents observed that content moderation operates in a dynamic environment in which harmful content appears in different forms and contexts, and they cautioned that no moderation system can ensure complete prevention before exposure occurs.

Some respondents warned that an absolute prevention standard could unintentionally encourages excessively aggressive automated filtering. In their view, this could lead to over-blocking of lawful content and disproportionate restrictions on legitimate expression.

There was also concern about requiring platforms to determine, prior to publication, whether content may be harmful to child users. Respondents noted that while certain categories of content, such as child sexual abuse material or content that incites violence or terrorism, are clearly harmful and already prohibited under community guidelines, other forms of content are heavily context dependent. Posts in which users share personal experiences of abuse or bullying were cited as examples of material that may be difficult to assess through automated or pre-publication processes without risking the over-removal of lawful speech. This is seen as a direct risk to freedom of expression and in contravention of Section 13(3) of ONSA.

Accordingly, mandatory pre-publication judgments in such cases is characterised as a form of pre-publication censorship that could adversely affect freedom of speech and expression, including for marginalised communities whose content may be more likely to be incorrectly flagged.

©2026 MCMC. All rights reserved.

Respondents also drew attention to the need for greater clarity in the definition of harmful content. Some considered the existing definition too broad for effective compliance, while others observed that it did not sufficiently account for the gendered dimensions of online harm, including the different ways in which harmful content may affect boys and girls.

The Commission acknowledges the feedback on content moderation and takes note of the views expressed regarding the application of reasonableness and proportionality in achieving child safety objectives, the issues with absolute prevention standards, potential impacts on freedom of expression, and concerns relating to pre-publication assessment and definitional clarity of harmful content. The Commission will consider the feedback received in the context of the overall regulatory objective and implementation of the CPC.

3.4 Feedback on Parental Controls

Respondents were generally supportive of requirements intended to ensure that parents are able to monitor and manage the online activities of child users. Parental control tools were viewed as playing an important role in enabling families to establish suitable guardrails for young people's online experiences. Several respondents noted that such tools are most effective when they operate alongside platform-level safety measures and age-appropriate product design, rather than as a standalone intervention. The proposed measures were, in general, regarded as practicable to implement and broadly consistent with current industry practice.

As a refinement, it was suggested that the CPC should require platforms to review and enhance parental control tools where necessary, rather than stipulating that such tools be "regularly updated".

©2026 MCMC. All rights reserved.

The Commission acknowledges the positive feedback on parental controls including the role of parental controls in supporting child online safety as well as their interaction with platform-level safety measures and age-appropriate design. The Commission will consider the feedback received in the context of the overall regulatory objective and implementation of the CPC.

3.5 Feedback on Privacy and Safety Settings

Respondents supported the objective of ensuring robust privacy and safety settings for child users and noted the importance of default protective settings and privacy safeguards tailored to children.

Several respondents recommended that the framework should avoid overly rigid requirements. In particular, the proposal that such settings be configured at the "most restrictive" level was seen as capable of producing unintended consequences, including constraints on a teenager's ability to participate online in age-appropriate ways as they mature. Respondents therefore suggested that the guidelines should instead focus on ensuring that default privacy and safety settings for child users are age appropriate.

Concerns were raised regarding the discoverability of legitimate content. Where indiscriminately restrictive settings could suppress recognised news content in the feeds, search results and recommended content made available to younger users.

©2026 MCMC. All rights reserved.

On the proposed restriction against public visibility of a child user's "personal information and account details" unless expressly permitted with parental guidance, respondents highlighted practical and technical limitations in its implementation. Many platforms require certain limited account identifiers, such as usernames and profile images, to remain visible in order to support core platform functionality, including user recognition, prevent impersonation, and enable the safe management of follower requests. In their view, fully restricting the visibility of such elements would not be feasible without undermining essential usability and safety functions. Accordingly, it was recommended that the guidelines should instead require the availability of tools and settings that enable child users, with parental guidance, to control the public visibility of their personal information.

Respondents also noted that the concept of "manipulative design" would benefit from clearer explanation in the CPC.

With respect to the obligation on "review of features", it was proposed that the requirement be framed at the level of systemic review and improvement, rather than as a mandate for continuous or prescriptive updates to individual user settings. One suggested formulation was to require platforms to review and update privacy and safety features at reasonable, risk-based intervals to ensure their continued effectiveness in safeguarding child users.

Finally, feedback emphasised the importance of child-friendly implementation. It was recommended that platforms provide clear, accessible guidance on how safety and privacy settings operate, so that both children and parents can understand and use them effectively.

©2026 MCMC. All rights reserved.

The Commission acknowledges the feedback on privacy and safety settings for child users and takes note of the views expressed regarding age-appropriate default settings, practical and technical considerations relating to visibility of account identifiers, clarity of key concepts such as manipulative design, and the framing of review obligations. The Commission will consider the feedback received in the context of the overall regulatory objective and implementation of the CPC.

3.6 Feedback on Safe Search and Recommendation Settings

Respondents were generally supportive of measures relating to safe search and recommendation systems. These measures were seen as appropriate and capable of reducing the likelihood that child users encounter harmful content through search and recommendation functionalities.

At the same time, it was recommended that the CPC expressly incorporate standards of reasonableness and proportionality. While platforms can and should take all reasonably practicable steps to ensure that search and recommendation systems are suitable and appropriate for child users, it is not technically feasible to reduce risk to zero. Such systems are dynamic and continuously adapt in response to user behaviour, content availability and evolving patterns of harm. For this reason, enforcement should be grounded in a risk-based approach, rather than an expectation of absolute prevention.

©2026 MCMC. All rights reserved.

The Commission acknowledges the positive feedback on safe search and recommendation systems and takes note of the views expressed regarding their role in reducing the risk of child users encountering harmful content, the importance of incorporating standards of reasonableness and proportionality and the limitation of achieving absolute prevention in dynamic systems. The Commission will consider the feedback received in the context of the overall regulatory objective and implementation of the CPC.

3.7 Conclusion

Overall, the feedback received reflects broad support for strengthening online child safety in Malaysia, while also highlighting the importance of ensuring that any resulting framework is proportionate, clearly scoped, and practicable to the operational realities of different services. Respondents consistently favoured a role-based and risk-based approach that takes account of differing technical capabilities, service design and levels of control over content, rather than prescriptive or absolute obligations.

In relation to age-related measures, a significant share of feedback favoured privacy-preserving and adaptable age assurance approaches over a single mandatory age-verification model or a fixed prohibition on access below a particular age.

Taken together, the feedback suggests that respondents are not opposing stronger child safety protections as such, but are calling for a framework that is workable in practice, respectful of children's rights and evolving capacities, and capable of delivering meaningful safeguards without imposing disproportionate technical, legal or societal costs.

©2026 MCMC. All rights reserved.

SECTION 4: CONCLUSION

The Commission extends its appreciation to all stakeholders who contributed to this public consultation. The feedback received has been valuable in informing the development of the proposed codes under ONSA. Respondents provided constructive views across key areas, reflecting a shared commitment to ensure online safety in Malaysia.

The Commission will consider stakeholders' feedback in finalising the proposed codes under ONSA. The objective is to ensure that the measures in the RMC and the CPC are clear, practical and enforceable, while balancing the public interest with operational realities for industry. Once finalised, the RMC and CPC will address regulatory gaps by setting out the measures that Licensed Service Providers are required to implement in order to comply with their online safety duties.

29 April 2026

©2026 MCMC. All rights reserved.