



Malaysian Communications and Multimedia Commission

**PUBLIC CONSULTATION PAPER ON
PROPOSED DRAFT CODES UNDER
THE ONLINE SAFETY ACT 2025**

Publication date: 12 February 2026

Closing date for response: 13 March 2026

TABLE OF CONTENTS

GLOSSARY	2
PREFACE	4
SECTION 1: BACKGROUND AND POLICY IMPERATIVE.....	6
1.1 Background: Regulation for Online Safety	6
1.2 Problem Statement: Proliferation of Online Harm	7
1.3 Rationale: Clarification of Online Safety Duties.....	13
1.4 Scope and Application.....	13
SECTION 2: INTERNATIONAL BENCHMARKING	15
2.1 International Benchmarking: Risk Mitigation Code.....	15
2.2 International Benchmarking: Child Protection Code	17
2.3 Adaptation to the Malaysian Context.....	18
SECTION 3: PROPOSED CODES	19
3.1 Risk Mitigation Code: Overview	19
3.2 Child Protection Code: Overview	21
3.3 Accountability	23
3.4 Public Consultation Questions: Overview	24
SECTION 4: SUBMISSION OF RESPONSES.....	25
APPENDIX 1	26
APPENDIX 2	27

GLOSSARY

Term	Definition
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].
COC	Code of Conduct (Best Practice) for Internet Messaging Service Providers and Social Media Service Providers.
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.
MCMC's User Experience Survey 2025	Survey on User Experience on Internet Messaging and Social Media Platforms 2025 commissioned by the Commission.
MCMCA 1998	Malaysian Communications and Multimedia Commission Act 1998 [Act 589].
Online Safety Plan	Online Safety Plan prepared by a Licensed Service Provider pursuant to section 20 of ONSA.
ONSA	Online Safety Act 2025 [Act 866].
parent	The parent or guardian of a child user.
PDPA 2010	Personal Data Protection Act 2010 [Act 709].

Term	Definition
PC	Public consultation.
RMC	Risk Mitigation Code.

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

PREFACE

The Malaysian Communications and Multimedia Commission ("**Commission**") is conducting this public consultation ("**PC**") to solicit feedback from the public on proposed draft codes under the Online Safety Act 2025 ("**ONSA**"), namely:

- (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**").

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, content applications service providers and network service providers, and to provide for related matters.

Specifically, applications service providers and content applications service providers licensed under the Communications and Multimedia Act 1998 ("**CMA 1998**"), which utilise internet access service to enable communication between users or to provide content, are required to comply with all duties set out in Part III of ONSA, including the abovementioned duties under sections 13 and 18.

Pursuant to this, measures to mitigate the risk of users being exposed to harmful content and measures to ensure safe use of their services by child users are to be specified in codes issued by the Commission under section 80 of ONSA. In this regard, the Commission has developed the draft RMC and the draft CPC as proposed draft codes under ONSA.

This PC reflects the Commission's commitment to transparent and consultative policymaking, in order to ensure that the final RMC and CPC are effective in enhancing and promoting online safety in Malaysia.

The Commission welcomes constructive feedback through written submissions and expresses its gratitude to all stakeholders and interested parties for their participation in this PC.

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

SECTION 1: BACKGROUND AND POLICY IMPERATIVE

1.1 Background: Regulation for Online Safety

The Commission is mandated under the Malaysian Communications and Multimedia Commission Act 1998 ("**MCMCA 1998**") 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:

- (i) the Communications and Multimedia Act 1998 [Act 588]; and
- (ii) the Online Safety Act 2025 [Act 866].

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 service¹ and social media service² 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.

To support the Licensing Framework, on 20 December 2024, the Commission published the Code of Conduct (Best Practice) for Internet Messaging Service Providers and Social Media Service Providers ("**COC**") which sets out the best practice for adoption by the relevant service providers in addressing harmful content online, as well as other relevant conduct requirement to be observed. The COC covers various areas pertaining to user safety, including both risk mitigation and child safety.

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.

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

1.2 Problem Statement: Proliferation of Online Harm

The Commission’s progress in regulating online safety comes in response to the proliferation of online harm, including child sexual exploitation and abuse, online scams and gambling, hate speech as well as cyberbullying and harassment.

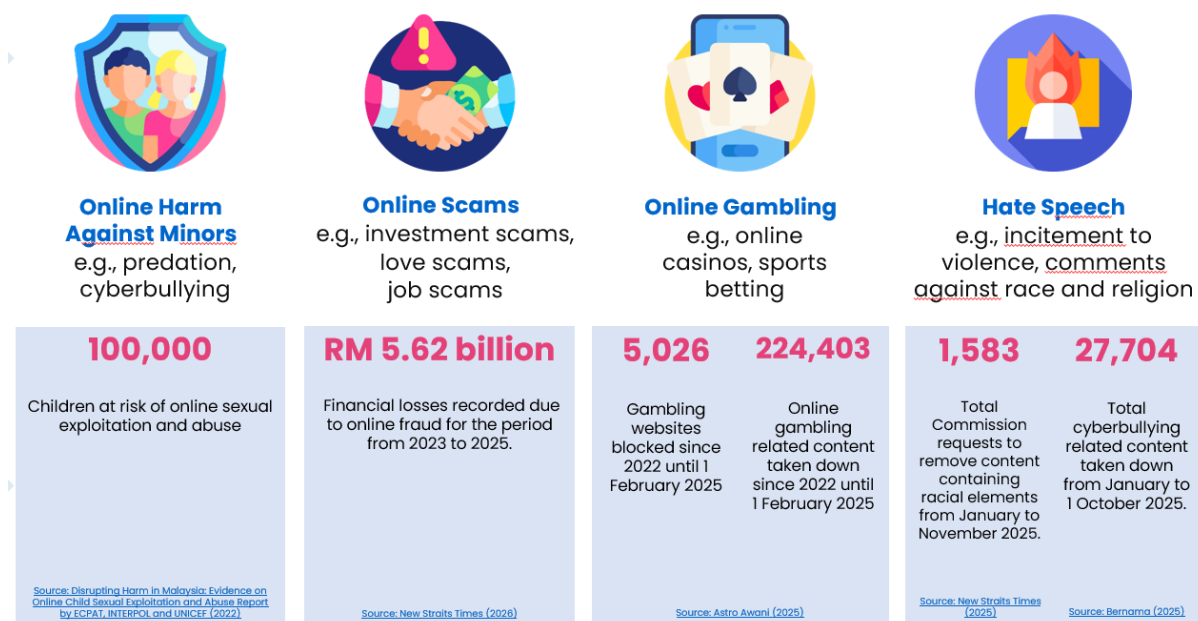


Figure 1: Types of Online Harm

Across the vast online environment, Internet messaging and social media platforms have become integral to the daily lives of Malaysians. These platforms facilitate communication between friends, family and communities, support e-commerce and livelihoods, and supply all manner of knowledge, information, and entertainment to users.

In 2025, the Commission commissioned a survey on User Experience on Internet Messaging and Social Media Platforms 2025 (“**MCMC’s User Experience Survey 2025**”). Conducted from May 13, 2025, to July 17, 2025, the survey engaged a total sample of 2,421 respondents for Internet messaging platforms and 2,421 respondents for social media platforms, with participants including Malaysians and foreign residents living in Malaysia aged 7 years and above, encompassing all regions nationwide.

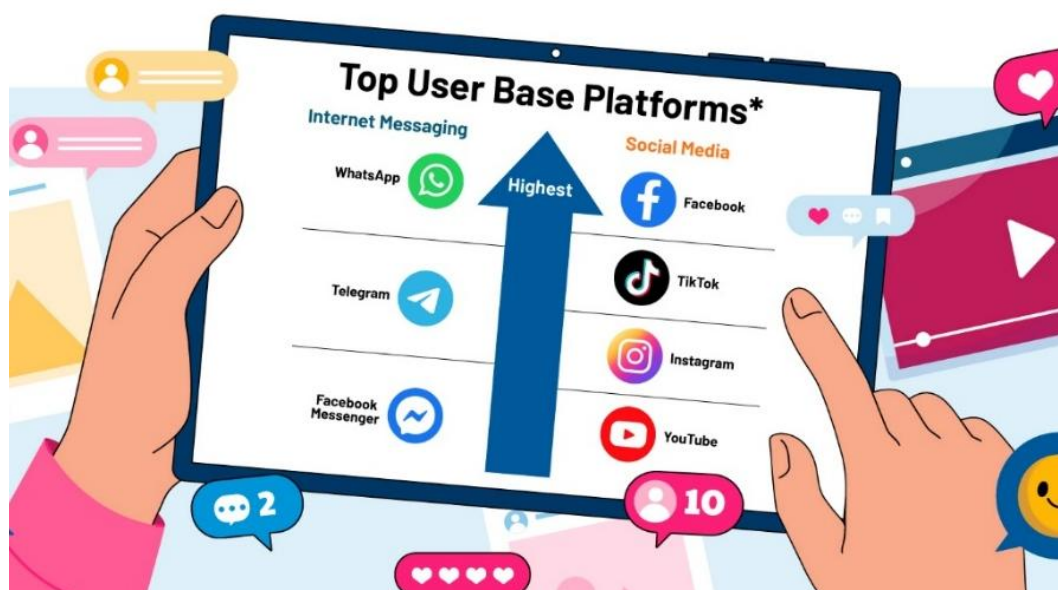


Figure 2: Top User Base Platforms in Malaysia³

³ Source: MCMC’s User Experience Survey 2025.



Figure 3: Top 5 Platforms for Children in Malaysia⁴

The survey findings indicate that many respondents regularly encounter harmful content on these platforms, with a rate of at least once a week for 52% of Internet messaging users and for 60% of social media users.

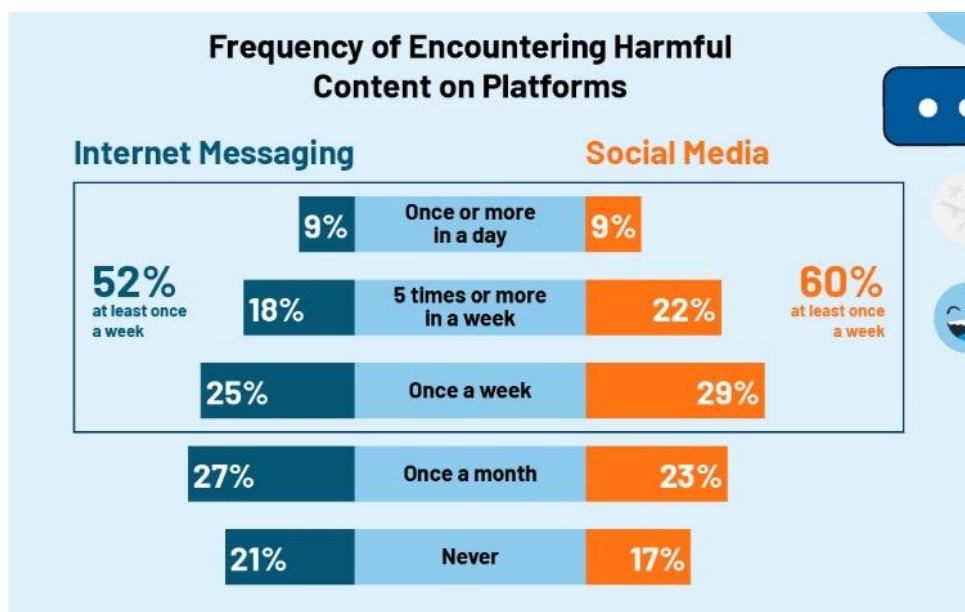


Figure 4: Frequency of Encountering Harmful Content on Platforms⁵

⁴ Source: MCMC’s User Experience Survey 2025.

⁵ Ibid.

Internet messaging and social media platforms have become breeding grounds for harmful content online, contributing to a significant upsurge in recent years. Disseminated in various forms, online harm can have serious consequences for both individuals and society.

However, while many users in Malaysia frequently encounter harmful content on Internet messaging and social media platforms (as indicated in **Figure 4** above as well as in **Figure 5** below), only 46% of respondents report the harmful content they encounter to the platforms themselves.

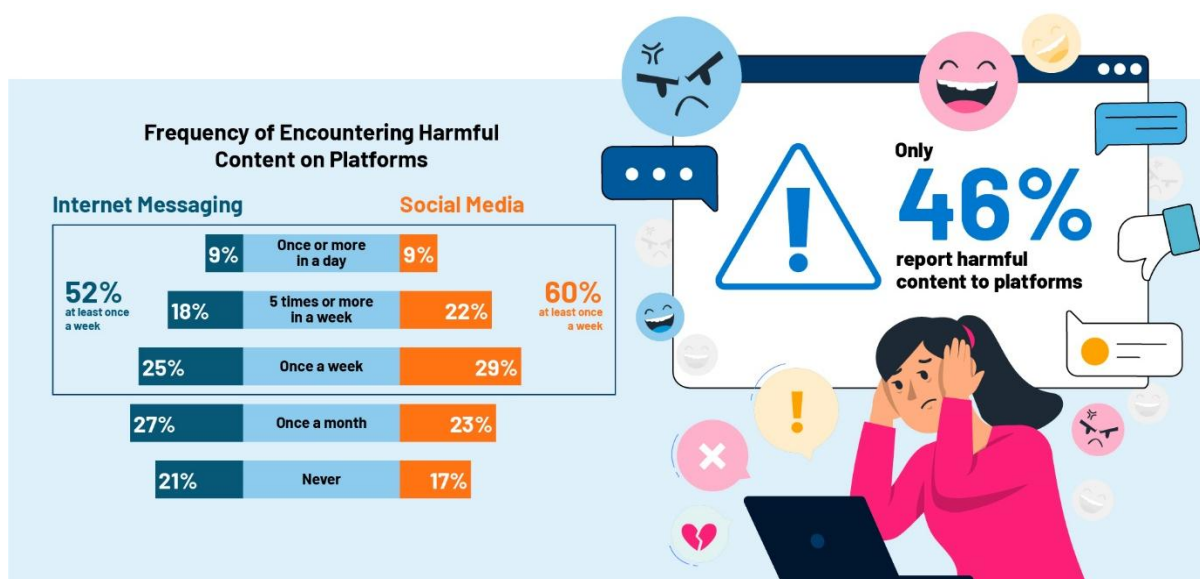


Figure 5: Reporting Harmful Content to Platforms⁶

This low response rate may be attributed to many respondents’ perceived unresponsiveness or ineffectiveness on the part of platforms, as shown in **Figure 6** and **Figure 7** below, or lack of guidance or clarity on the escalation process to the platforms.

⁶ Source: MCMC’s User Experience Survey 2025.

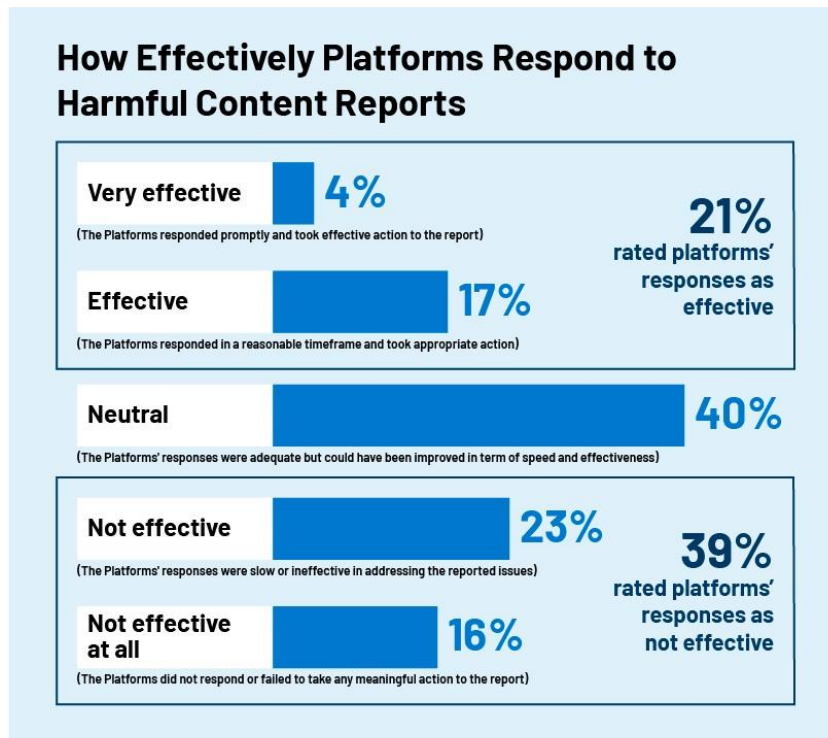


Figure 6: How Effectively Platforms Respond to Harmful Content Reports⁷

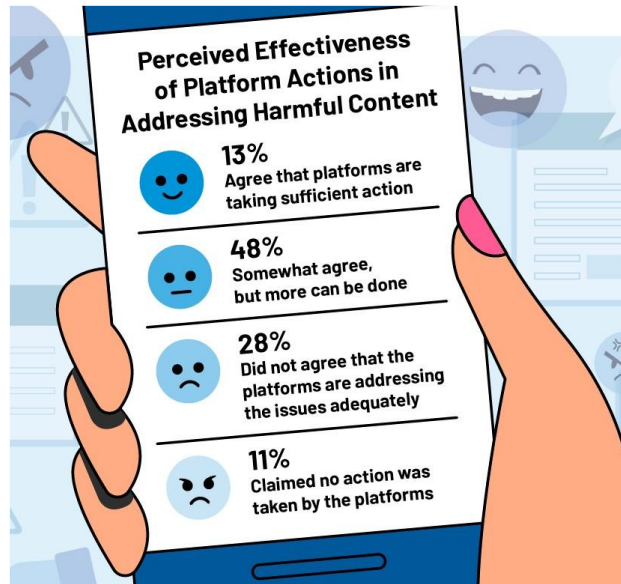


Figure 7: Perceived Effectiveness of Platform Actions in Addressing Harmful Content⁸

⁷ Source: MCMC's User Experience Survey 2025.

⁸ Ibid.

Apart from that, MCMC’s User Experience Survey found that when it comes to child safety, there is majority support for mandatory parental controls on platforms (**Figure 8**). Further, with regards to children’s access to platforms, there is clear demand for measures to be strengthened, beyond mere self-declaration. This ensures that younger users are kept out of such spaces while they remain impressionable and more susceptible to online harm.

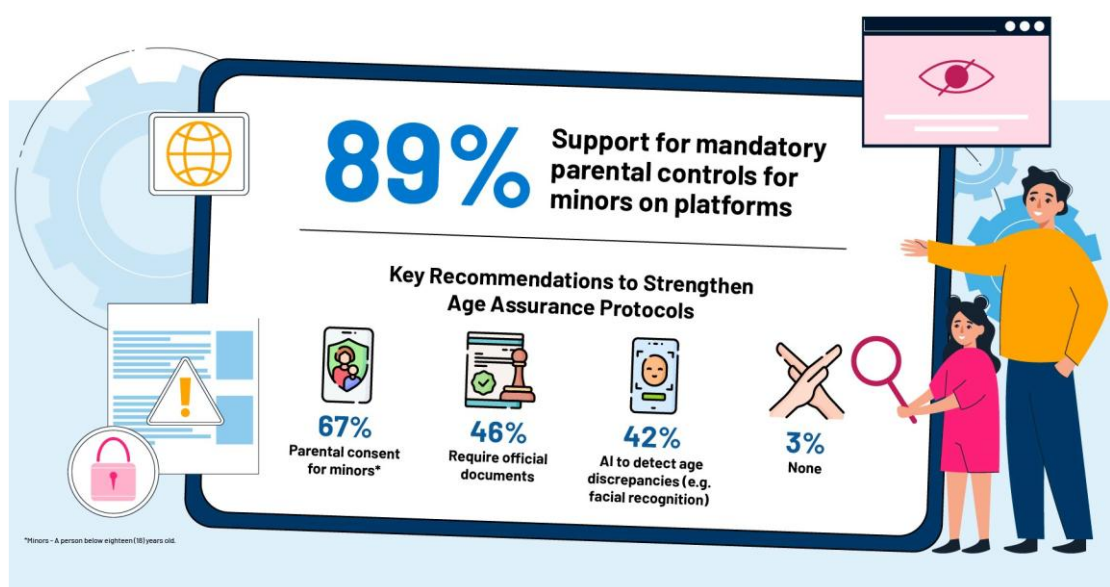


Figure 8: Building Safer Online Spaces for Children⁹

It is incumbent on the Commission to intervene where service providers have not been able to ensure that users can enjoy the benefits of being online without compromising their safety and security.

The introduction of the Licensing Framework in 2024 brought relevant service providers within the Commission’s regulatory ambit, and the enforcement of ONSA now establishes a clear and enforceable mandate on online safety duties for applicable service providers. However, regulatory gaps remain in translating these duties into actionable steps and in setting baseline expectations for the Commission when enforcing them.

⁹ Source: MCMC’s User Experience Survey 2025.

1.3 Rationale: Clarification of Online Safety Duties

Under Part III of ONSA, applications service providers and content applications service providers licensed under the CMA 1998 are required to comply with the duty to implement measures to mitigate risk of users' exposure to harmful content under section 13 of ONSA, as well as 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.

1.4 Scope and Application

The duties set out in Part III of ONSA, including the duty to implement measures to mitigate risk of exposure to harmful content under section 13 of ONSA and the duty to protect online safety of child user under section 18 of ONSA, are required to be complied with by applications service providers and content applications service providers licensed under the CMA 1998 (hereinafter collectively referred to as the "**Licensed Service Providers**" or individually referred to as "**Licensed Service Provider**"), which utilise internet access service to enable communication between users or to provide content, as the case may be.

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 draft RMC is provided in **Appendix 1**.

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. The draft CPC is provided in **Appendix 2**.

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

SECTION 2: INTERNATIONAL BENCHMARKING

Online harm is not unique to Malaysia. The global increase in online harm has led many countries to regulate online platforms to enhance user safety, particularly for children, and to address harmful and illegal content.

This section outlines regulatory approaches observed across multiple jurisdictions in the implementation of online safety measures, including safety-by-design elements. While these instruments differ in legal form and scope, they reflect common regulatory outcomes relating to risk mitigation and child protection.

2.1 International Benchmarking: Risk Mitigation Code

Australia

In Australia, the eSafety Commissioner (eSafety) maintains a register of industry codes and industry standards for illegal online material. Schedule 1 – Social Media Services Online Safety Code (Class 1A and Class 1B Material) requires certain providers of social media services to adopt appropriate features and settings that are designed to mitigate the risks to Australian end-users related to harmful material.

eSafety is also a strong advocate of safety by design, for which they published the Safety by Design Principles, encompassing service provider responsibilities, user empowerment and autonomy, as well as transparency and accountability.

European Union

The European Commission's Digital Services Act (DSA) requires providers of very large online platforms to put in place reasonable, proportionate and effective mitigation measures, tailored to specific risks as described in the DSA. Among others, such platforms must test and adapt their algorithmic systems, place prominent markings on generated or manipulated content, and take awareness-raising measures for the benefit of users.

United Kingdom

The United Kingdom's Online Safety Act 2023 requires providers of user-to-user services to carry out a suitable and sufficient illegal content risk assessment. Pursuant to that, the Office of Communications (Ofcom) published its Risk Assessment Guidance and Risk Profiles to help online service providers regulated by the Online Safety Act 2023 comply with the illegal content risk assessment duties. Ofcom further recommends that such risk assessments be reviewed at least every twelve (12) months.

Other International Benchmarks

Singapore's Code of Practice for E-Commerce Services under the Online Criminal Harms Act 2023 set verification requirements for advertisers for the sales of goods and/or services. Further, the World Economic Forum's *Insight Report on Digital Safety Risk Assessment in Action: A Framework and Bank of Case Studies* sets out a risk assessment framework comprising risk identification, risk reduction, and harm mitigation, which is applicable across a broad range of digital services.

2.2 International Benchmarking: Child Protection Code

Australia

In Australia, the Basic Online Safety Expectations (BOSE) framework under the Online Safety Act 2021 sets principle-based expectations for platforms to keep children safe, supported by eSafety's powers to demand transparency reports, compel improvements to age checks, and enforce standards against exposure to harmful content. Further, as of 10 December 2025, age-restricted social media platforms are required to take reasonable steps to prevent Australians under the age of 16 from creating or keeping an account.

European Union

The DSA requires platforms to take appropriate and proportionate measures to protect minors, including restricting targeted advertising based on profiling, ensuring privacy-by-default settings, and providing accessible parental controls. The European Commission also published guidelines in 2025 to expand on these obligations by calling for robust age-assurance systems and safe recommendation design.

United Kingdom

The United Kingdom's Online Safety Act 2023 establishes a statutory duty of care for online service providers, requiring platforms to deploy effective age-assurance mechanisms, mitigate risks of harmful and addictive design features, and set privacy and safety by default for children. The Children's Safety Codes developed by Ofcom under the Online Safety Act 2023, require online service providers to implement effective algorithmic risk controls, establish accessible and robust reporting mechanisms, and provide tools that enable parental oversight and empowerment.

2.3 Adaptation to the Malaysian Context

The CMA 1998 and ONSA provide the key legal and regulatory frameworks for adapting regulatory approaches observed across multiple jurisdictions to the Malaysian context.

The Commission is also guided by feedback obtained from the 2024 public consultation on its COC. The COC covers various aspects of user safety, including risk assessment and mitigation as well as child safety measures. Feedback from stakeholders including industry players, non-governmental organisations, civil society organisations, and law enforcement agencies continues to inform the Commission on priority issues within the Malaysian context in developing the RMC and the CPC.

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

SECTION 3: PROPOSED CODES

This section briefly outlines the draft codes that are the subjects of this PC. PC questions are included within the drafts in **Appendix 1** and **Appendix 2** to solicit feedback on the draft codes.

3.1 Risk Mitigation Code: Overview

The RMC is to be issued by the Commission under section 80 of ONSA for the purpose of specifying the measures that Licensed Service Providers shall implement to mitigate the risk of users being exposed to harmful content in compliance of the duty under section 13 of ONSA. The draft RMC is provided in **Appendix 1** and the measures specified in the RMC are divided into two (2) parts:

- (i) Part 1: Risk Assessment.
- (ii) Part 2: Risk Mitigation.

- **Part 1: Risk Assessment**

The RMC requires Licensed Service Providers to conduct suitable and sufficient harmful content risk assessment of their service. In conducting harmful content risk assessment, Licensed Service Providers are required to consider the characteristics of their service as set out in the RMC.

The RMC further specifies that where the service, or any part of the service, is likely to be accessed by child users, Licensed Service Providers must also consider characteristics of the service specific to child users in conducting harmful content risk assessment.

The RMC also imposes additional requirements to the harmful content risk assessment such as the skills and qualifications of the risk assessment team, annual review and update of harmful content risk assessment, making and keeping records of harmful content risk assessments, as well compliance with the PDPA 2010.

- **Part 2: Risk Mitigation**

The RMC requires Licensed Service Providers to implement reasonable, proportionate and effective measures to mitigate the risk of users being exposed to harmful content, based on the findings of Licensed Service Providers' harmful content risk assessment conducted in accordance with Part 1: Risk Assessment. The measures include:

- (i) Content Management and Moderation;
- (ii) User Empowerment and Controls;
- (iii) Online Safety of Child User;
- (iv) Safe Design of the Service; and
- (v) Safety Policies of the Service.

Notwithstanding the measures mentioned above, Licensed Service Providers may also implement other additional measures to mitigate the risk of users being exposed to harmful content.

Licensed Service Providers must also establish an internal assurance function to continuously monitor and ensure the effectiveness of risk mitigation measures implemented under section 13 of ONSA. This includes regular reporting to the audit committee or governing body of the Licensed Service Providers.

3.2 Child Protection Code: Overview

The CPC is to be issued by the Commission under section 80 of ONSA for the purpose of specifying the measures that Licensed Service Providers shall implement to ensure safe use of their services by child users in compliance of the duty under section 18 of ONSA. The draft CPC is provided in **Appendix 2** and the measures specified in the CPC cover the following:

- (i) Age Verification;
- (ii) Content Moderation;
- (iii) Parental Controls;
- (iv) Privacy and Safety Settings; and
- (v) Safe Search and Recommendation Settings

- **Age Verification**

If the service is likely to be accessed by child users, then Licensed Service Providers are required to implement effective age verification measures to ensure that only child users whose ages have been identified as 16 years and above are permitted to (i) register for or use the service; and (ii) access any feature of the service that is appropriate for their age. In implementing effective age verification measures, Service Providers are required to subject users to verification against Government-issued records. Personal data collected and processed for the purpose of age verification must be collected and processed in compliance with the PDPA 2010.

- **Content Moderation**

Licensed Service Providers are required to implement measures to prevent child users from accessing harmful content. Such measures include establishing clear and robust systems for the detection and removal of harmful content from being accessed by child users, clear reporting channels for child users and parents, ensure reporting procedures are child-friendly, prevent child user's repeated exposure to reported/removed harmful content, and respond promptly to removal requests from the Commission or enforcement agencies.

- **Parental Controls**

Licensed Service Providers are also required to make available parental control features that enable parents to monitor and manage the online activities of child users as well as ensure all tools and settings provided to parents are user-friendly and regularly updated to remain effective.

- **Privacy and Safety Settings**

Licensed Service Providers are required to make available privacy and safety settings to ensure safe use of their service by child users. Such measures include ensuring default privacy and safety settings for child users are set to the most restrictive level, protecting the personal information and account details of child users, restricting unknown adult contact with child users, preventing child user's exposure to manipulative design features, and regularly reviewing and updating privacy and safety settings to ensure they remain effective in protecting child users.

- **Safe Search and Recommendation Settings**

Licensed Service Providers are required to ensure that search and recommendation systems on their service are suitable and appropriate for child users. Such measures include enabling safe search by default, filtering harmful content from personalised recommendation systems, enabling child users and parents to manage personalised recommendation systems, and ensuring algorithms do not display, promote, or recommend harmful content to child users.

3.3 Accountability

Pursuant to section 20 of ONSA, Licensed Service Providers are required to prepare an Online Safety Plan on their compliance of the duties under Part III of ONSA. This includes compliance of the duty to implement measures to mitigate risk of exposure to harmful content under section 13 of ONSA as well as the duty to protect online safety of child user under section 18 of ONSA.

The period, form, content, publication, and submission of the Online Safety Plan will be as provided under the regulation in relation to the duty to prepare Online Safety Plan under section 20 of ONSA. Any content addressing duties under sections 13 and 18 of ONSA must show that the Licensed Service Provider in question has implemented the measures outlined in the RMC and CPC, respectively.

Where the Licensed Service Provider has implemented any alternative measures other than the measures specified in the RMC and CPC, the Licensed Service Provider must provide their justification to the satisfaction of the Commission that the alternative measures will better mitigate the risk of users being exposed to harmful content or ensure the safe use of its service by child users, as the case may be.

3.4 Public Consultation Questions: Overview

The Commission welcomes constructive feedback concerning the draft RMC and the draft CPC from stakeholders and interested parties through written submissions. As guidance for providing feedback, the Commission has included PC questions within the draft codes in **Appendix 1** and **Appendix 2**.

In general, the Commission invites feedback on the following areas:

- **Are the measures specified in the draft codes 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 codes effective in achieving their respective online safety outcomes?** Namely:
 - (i) in relation to the RMC, to mitigate the risk of users being exposed to harmful content.
 - (ii) in relation to the CPC, to ensure safe use of their services by child users.
- **Are there any other measures that the Commission should consider adopting?** Namely:
 - (i) in relation to the RMC, to mitigate the risk of users being exposed to harmful content.
 - (ii) in relation to the CPC, to ensure safe use of their services by child users.

SECTION 4: SUBMISSION OF RESPONSES

The Commission welcomes written submissions on the draft RMC (**Appendix 1**) and the draft CPC (**Appendix 2**). All submissions must be submitted in full no later than **5:00 PM, 13 March 2026 (Friday)**.

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

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

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

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

Address:

The Chairman
Malaysian Communications and Multimedia Commission
MCMC HQ Tower 1, Jalan Impact, Cyber 6, 63000 Cyberjaya,
Selangor Darul Ehsan
(Attention: Regulatory Policy Division)

Email:

policy.review@mcmc.gov.my

APPENDIX 1

DRAFT RISK MITIGATION CODE



**MALAYSIAN COMMUNICATIONS AND
MULTIMEDIA COMMISSION**

**ONLINE SAFETY ACT 2025:
RISK MITIGATION CODE**

TABLE OF CONTENTS

1.	INTERPRETATION	2
2.	OBJECTIVE AND SCOPE OF THIS CODE.....	3
3.	PART 1: RISK ASSESSMENT	4
4.	PART 2: RISK MITIGATION	6
5.	SERVICE PROVIDER ACCOUNTABILITY.....	9
6.	REVIEW OF THIS CODE.....	10

1. INTERPRETATION

For the purpose of this Risk Mitigation Code, unless the context otherwise requires,

- (a) any terms used in this Risk Mitigation Code shall have the same meaning as in the Online Safety Act 2025 [Act 866] ("**ONSA**");
- (b) words in the singular include plural and vice versa; and
- (c) the following terms used in this Risk Mitigation Code shall have the stated meaning:

"Code" means the Risk Mitigation Code issued by the Commission under section 80 of ONSA read together with section 13 of ONSA;

"Online Safety Plan" means the Online Safety Plan prepared by a Licensed Service Provider (as defined below) pursuant to section 20 of ONSA;

"service" means an applications service or a content applications service provided by a Licensed Service Provider (as defined below); and

"Licensed Service Provider" means a licensed applications service provider or a licensed content applications service provider.

2. OBJECTIVE AND SCOPE OF THIS CODE

- 2.1. The objective of ONSA is to enhance and promote online safety in Malaysia by regulating harmful content and providing for duties and obligations of the applications service providers, content applications service providers and network service providers.
- 2.2. This Code is issued by the Commission under section 80 of ONSA to specify the measures that a licensed applications service provider and a licensed content applications service provider (collectively referred to as "**Licensed Service Providers**") shall implement to mitigate the risk of users being exposed to harmful content, in compliance with the Licensed Service Providers' duty under section 13 of ONSA.
- 2.3. Notwithstanding paragraph 2.2 of this Code, as stipulated under subsection 13(2) of ONSA, the Licensed Service Providers may implement any alternative measures other than the measures specified in this Code if the Licensed Service Providers prove to the satisfaction of the Commission that the said alternative measures will better mitigate the risk of users being exposed to harmful content.
- 2.4. In accordance with subsection 13(3) of ONSA, the measures implemented by the Licensed Service Providers under section 13 of ONSA shall not unreasonably or disproportionately limit a user's expression.
- 2.5. The contents of this Code are to support and complement other duties of the Licensed Service Providers as provided under Part III of ONSA.
- 2.6. For purposes of this Code, the term "harmful content" refers to the contents specified in the First Schedule of ONSA, which are as follows:
 - 2.6.1. Content on child sexual abuse material as provided for under section 4 of the Sexual Offences against Children Act 2017 [Act 792].
 - 2.6.2. Content on financial fraud.
 - 2.6.3. Obscene content including content that may give rise to a feeling of disgust due to lewd portrayal which may offend a person's manner on decency and modesty.

- 2.6.4. Indecent content including content which is profane in nature, improper and against generally accepted behaviour or culture.
- 2.6.5. Content that may cause harassment, distress, fear or alarm by way of threatening, abusive or insulting words or communication or act.
- 2.6.6. Content that may incite violence or terrorism.
- 2.6.7. Content that may induce a child to cause harm to himself.
- 2.6.8. Content that may promote feelings of ill-will or hostility amongst the public at large or may disturb public tranquillity.
- 2.6.9. Content that promotes the use or sale of dangerous drugs.
- 2.7. The measures specified in this Code are divided into two (2) parts:
 - 2.7.1. Part 1: Risk Assessment; and
 - 2.7.2. Part 2: Risk Mitigation.

3. PART 1: RISK ASSESSMENT

- 3.1. For the purpose of implementing the measures to mitigate the risk of users being exposed to harmful content, this Code requires the Licensed Service Providers to conduct suitable and sufficient harmful content risk assessment of their services.
- 3.2. In carrying out the harmful content risk assessment, the Licensed Service Providers shall have regard to the following characteristics of their services —
 - 3.2.1. demographics of users in Malaysia;
 - 3.2.2. service design, features and functionality that may contribute to the risk of users being exposed to harmful content;
 - 3.2.3. trends, including emerging trends, in respect of online behaviour and associated threats that may contribute to the risk of users being exposed to harmful content;

- 3.2.4. utilisation of the platform in situations of heightened risk, including but not limited to, national disasters or crises; and
 - 3.2.5. such other characteristics of the service as may be necessary from time to time, as determined by the Commission.
 - 3.3. In circumstances where the service or any part of the service is likely to be accessed by child users, the Licensed Service Providers shall have regard to the following characteristics of the service in conducting harmful content risk assessment:
 - 3.3.1. demographics of child users in Malaysia, taking into account the developmental stages and vulnerabilities of child users;
 - 3.3.2. service design, features and functionality that may contribute to the risk of child users being exposed to harmful content;
 - 3.3.3. trends, including emerging trends, in respect of online behaviour and associated threats that may contribute to the risk of child users being exposed to harmful content; and
 - 3.3.4. such other characteristics of the service targeted to child users as may be necessary from time to time, as decided by the Commission.
 - 3.4. For the purpose of carrying out the harmful content risk assessment of the service, the Licensed Service Providers shall—
 - 3.4.1. ensure that there is a skilled and qualified risk assessment team established that is conducting harmful content risk assessment of the service;
 - 3.4.2. ensure that where the service or any part of the service is likely to be accessed by child users, the risk assessment team includes expertise on child online safety;
 - 3.4.3. review and update the harmful content risk assessment annually, to ensure that it remains up to date, suitable and sufficient for the purpose of implementing measures to mitigate the risk of users being exposed to harmful content;
 - 3.4.4. prepare and maintain a written record, in a clear and readily comprehensible form of all harmful content risk assessment conducted, including the methodologies applied and the findings and outcomes of each assessment; and

- 3.4.5. ensure that all personal data collected and processed for the purpose of harmful content risk assessment are collected and processed with due regard to the privacy of users and the rights of users to their personal data, in accordance with the Personal Data Protection Act 2010 [Act 709].

PC Question 1

The Commission invites views on Risk Assessment:

- a) whether the measures specified are practicable to be implemented;**
- b) whether the measures specified are effective; and**
- c) whether there are any other measures that the Commission should consider;**

for the purpose of conducting suitable and sufficient harmful content risk assessment of the services.

4. PART 2: RISK MITIGATION

4.1. Based on the findings of the harmful content risk assessment conducted by the Licensed Service Providers in accordance with Part 1 of this Code, the Licensed Service Providers shall implement reasonable, proportionate and effective measures to mitigate the risk of users being exposed to harmful content.

4.2. Pursuant to paragraph 4.1 of this Code, the measures to be implemented by the Licensed Service Providers to mitigate the risk of users being exposed to harmful content shall include:

4.2.1. Content Management and Moderation

Measures for content management and moderation are as prescribed under the regulation(s) in relation to the duty to prepare the Online Safety Plan under section 20 of ONSA.

4.2.2. **User Empowerment and Controls**

Measures for user empowerment and controls are as prescribed under the regulation(s) in relation to the duty to prepare Online Safety Plan under section 20 of ONSA.

4.2.3. **Online Safety of Child User**

Measures to ensure safe use of the service by child users are as specified in the code issued by the Commission pursuant to section 80 of ONSA, in relation to the duty to protect online safety of child users under section 18 of ONSA.

4.2.4. **Safe Design of the Service**

- (a) Implement measures that ensure the content can only be communicated on the service by a registered user.
- (b) Ensure that paid-for advertisements for the sales of goods and/or services are only permitted on the service if they are from advertisers or users (as the case may be) who are verified against Government-issued records.
- (c) Test and adapt the service's algorithmic systems, including their recommendation systems, to mitigate against the risk of users being exposed to harmful content.
- (d) Ensure that any generated or manipulated image, audio or video that closely resembles real persons, objects, places, entities or events and is likely to falsely appear authentic or truthful to a person, is clearly distinguishable through prominent labels or markings when presented on the service's online interface, and further provide an accessible functionality to enable users to identify or indicate such content.
- (e) Evaluate all service design, features and functionality to ensure that the risk of users being exposed to harmful content have been mitigated before launching or implementing a significant change to the service.

4.2.5. Safety Policies of the Service

- (a) Develop user-safety policies, community standards, community guidelines and/or terms of service, and ensure that such policies, etc. are fairly and consistently implemented and enforced to mitigate the risk of users being exposed to harmful content.
- (b) Adapt existing user-safety policies, community standards, community guidelines and/or terms of service, together with their implementation and enforcement, as necessary, to mitigate the risk of users being exposed to harmful content.
- (c) Ensure that the guidelines issued by the Licensed Service Providers include a description of the measures implemented by the Licensed Service Providers under section 13 of ONSA, in accordance with section 14 of ONSA.
- (d) Ensure that user-safety policies, community standards, community guidelines and/or terms of service are visible, easily accessible, regularly updated and written in clear, user-friendly language. Users should also be periodically reminded of these materials and proactively notified of changes or updates through targeted in-service communications.
- (e) Implement education and awareness-raising measures to enable users to minimise exposure to harmful content. The service should also be adapted to ensure that such information is clearly visible and easily accessible to users.
- (f) In line with section 29 of ONSA, the Licensed Service Providers shall establish and maintain clear internal procedures for the submission of a report to the relevant enforcement agency.
- (g) The Licensed Service Providers shall collaborate with enforcement agencies, regulatory bodies, civil society organisations and other relevant stakeholders, including experts on child online safety and representatives of users with disabilities, for the purpose of enhancing online user safety.

- 4.3. Notwithstanding the measures specified in paragraph 4.2 of this Code, the Licensed Service Providers may also implement other additional measures to mitigate the risk of users being exposed to harmful content.
- 4.4. The Licensed Service Providers shall establish an internal assurance function to continuously monitor and evaluate the effectiveness of risk mitigation measures implemented pursuant to section 13 of ONSA. This function shall include regular reporting to the audit committee or governing body of the Licensed Service Providers.

PC Question 2

The Commission invites views on Risk Mitigation:

- a) whether the measures specified are practicable to be implemented;**
 - b) whether the measures specified are proportionate; and**
 - c) whether there are any other measures that the Commission should consider;**
- for the purpose of implementing reasonable, proportionate and effective measures to mitigate the risk of users being exposed to harmful content.**

5. SERVICE PROVIDER ACCOUNTABILITY

- 5.1. Pursuant to section 20 of ONSA, the Licensed Service Providers shall prepare an Online Safety Plan on their compliance with the duties imposed under Part III of ONSA, including the duty to implement measures for mitigating the risk of exposure to harmful content under section 13 of ONSA.
- 5.2. The Online Safety Plan is to be prepared within the period and in such form as prescribed by the regulations made pursuant to section 81 of ONSA. The information contained in the Online Safety Plan is as prescribed in the said regulations.

- 5.3. Insofar as compliance with the duty under section 13 of ONSA is concerned, the information that is to be addressed in the Online Safety Plan shall:
- 5.3.1. demonstrate that the Licensed Service Providers have implemented the measures specified in this Code to mitigate the risk of users being exposed to harmful content; and
 - 5.3.2. where the Licensed Service Providers have implemented any alternative measures other than the measures specified in this Code, provide the justification to the satisfaction of the Commission that the alternative measures will be better to mitigate the risk of users being exposed to harmful content.

6. REVIEW OF THIS CODE

- 6.1. The Commission may revoke, vary, revise or amend the whole or any part of this Code.

APPENDIX 2

DRAFT CHILD PROTECTION CODE



**MALAYSIAN COMMUNICATIONS AND
MULTIMEDIA COMMISSION**

**ONLINE SAFETY ACT 2025:
CHILD PROTECTION CODE**

TABLE OF CONTENTS

1.	INTERPRETATION	2
2.	OBJECTIVE AND SCOPE OF THIS CODE	3
3.	AGE VERIFICATION	5
4.	CONTENT MODERATION	6
5.	PARENTAL CONTROLS	7
6.	PRIVACY AND SAFETY SETTINGS	7
7.	SEARCH AND RECOMMENDATION SYSTEMS	8
8.	SERVICE PROVIDER ACCOUNTABILITY	9
9.	REVIEW OF THIS CODE.....	10

1. INTERPRETATION

For the purpose of this Child Protection Code, unless the context otherwise requires,

- (a) any terms used in this Child Protection Code shall have the same meaning as in the Online Safety Act 2025 [Act 866] ("**ONSA**");
- (b) words in the singular include plural and vice versa; and
- (c) the following terms used in this Child Protection Code shall have the stated meaning:

"child user" means a user identified to be a child;

"Code" means the Child Protection Code issued by the Commission under section 80 of ONSA read together with section 18 of ONSA;

"Licensed Service Provider" means a licensed applications service provider or a licensed content applications service provider;

"Online Safety Plan" means the Online Safety Plan prepared by a Licensed Service Provider pursuant to section 20 of ONSA;

"parent" means the parent or guardian of a child user; and

"service" means an applications service or content applications service provided by a Licensed Service Provider.

2. OBJECTIVE AND SCOPE OF THIS CODE

- 2.1. The objective of ONSA is to enhance and promote online safety in Malaysia by regulating harmful content and providing for duties and obligations of applications service providers, content applications service providers and network service providers.
- 2.2. This Code is issued by the Commission under section 80 of ONSA to specify the measures that a licensed applications service provider and a licensed content applications service provider (collectively referred to as "**Licensed Service Providers**") shall implement to ensure the safe use of their services by child users, in compliance with the Licensed Service Providers' duty under section 18 of ONSA.
- 2.3. Notwithstanding paragraph 2.2 of this Code, as stipulated under subsection 18(2) of ONSA, the Licensed Service Providers may implement any alternative measures other than the measures specified in this Code if the Licensed Service Providers prove to the satisfaction of the Commission that the alternative measures will better ensure the safe use of the services by child users.
- 2.4. The contents of this Code are to support and complement other duties of the Licensed Service Providers as provided under Part III of ONSA.
- 2.5. For purposes of this Code, the term "harmful content" refers to the contents specified in the First Schedule of ONSA, which are as follows:
 - 2.5.1. Content on child sexual abuse material as provided for under section 4 of the Sexual Offences against Children Act 2017 [Act 792].
 - 2.5.2. Content on financial fraud.
 - 2.5.3. Obscene content including content that may give rise to a feeling of disgust due to lewd portrayal which may offend a person's manner on decency and modesty.
 - 2.5.4. Indecent content including content which is profane in nature, improper and against generally accepted behaviour or culture.

- 2.5.5. Content that may cause harassment, distress, fear or alarm by way of threatening, abusive or insulting words or communication or act.
 - 2.5.6. Content that may incite violence or terrorism.
 - 2.5.7. Content that may induce a child to cause harm to himself.
 - 2.5.8. Content that may promote feelings of ill-will or hostility amongst the public at large or may disturb public tranquillity.
 - 2.5.9. Content that promotes the use or sale of dangerous drugs.
- 2.6. In accordance with subsection 18(3) of ONSA, the measures implemented to ensure the safe use of the services by child users shall include measures to ensure safe design and operation of the service that is, in the opinion of the Licensed Service Providers, likely to be accessed by child users—
- 2.6.1. to prevent access of a user identified to be a child to a content suspected to be a harmful content;
 - 2.6.2. to limit the ability of a user identified to be an adult from communicating with a user identified to be a child;
 - 2.6.3. to limit features that increase, sustain or extend the use of the services by a user identified to be a child;
 - 2.6.4. to prevent a user identified to be an adult from viewing the personal information of a user identified to be a child that is available on the services; and
 - 2.6.5. to control personalized recommendation systems suitable for child users.

3. AGE VERIFICATION

- 3.1. The Licensed Service Providers offering a service that is likely to be accessed by child users shall implement effective age verification measures to ensure that only users whose ages have been identified as sixteen (16) years and above, are permitted to:
 - 3.1.1. register for or use the service; and
 - 3.1.2. access any feature of the service that is appropriate for their age.
- 3.2. In implementing effective age verification measures, Licensed Service Providers are required to subject users to verification against Government-issued records.
- 3.3. The Licensed Service Providers shall ensure that such age verification measures are designed with due regard to the privacy of child users, and that all personal data collected and processed for the purpose of age verification are collected and processed in accordance with the rights of child users in relation to their personal data, including as provided in the Personal Data Protection Act 2010 [Act 709].

PC Question 1

The Commission invites views on Age Verification:

- a) whether the measures specified are practicable to be implemented;**
 - b) whether the measures specified are effective; and**
 - c) whether there are any other measures that the Commission should consider;**
- for the purpose of ensuring that only users whose ages have been identified as sixteen (16) years and above, are permitted to register and access the service.**

4. CONTENT MODERATION

- 4.1. The Licensed Service Providers shall implement measures to prevent child users from accessing harmful content.
- 4.2. For the purpose of paragraph 4.1, the Licensed Service Providers shall—
 - 4.2.1. establish clear and robust systems for the detection and removal of harmful content from being accessed by child users;
 - 4.2.2. provide clear and accessible reporting mechanisms for child users and parents to make a report to the Licensed Service Providers regarding any content that they believe is a harmful content;
 - 4.2.3. ensure that the procedures for reporting of harmful content are accessible and comprehensible to child users;
 - 4.2.4. take reasonable steps to prevent repeated exposure of child user to harmful content that has been reported or removed; and
 - 4.2.5. respond promptly and effectively to any request made by the Commission or any other enforcement agency for the removal of harmful content affecting child users.

PC Question 2

The Commission invites views on Content Moderation:

- a) whether the measures specified are practicable to be implemented;**
 - b) whether the measures specified are effective; and**
 - c) whether there are any other measures that the Commission should consider;**
- for the purpose of ensuring that child users are prevented from accessing harmful content.**

5. PARENTAL CONTROLS

- 5.1. The Licensed Service Providers shall make available parental control features that enable parents to monitor and manage the online activities of child users, including the ability to adjust settings and limits in line with the child's age, development, and evolving capacity.
- 5.2. The Licensed Service Providers shall ensure all parental control tools and settings are clear, user-friendly, easily accessible and regularly updated to remain effective in safeguarding the use of their service by child users.

PC Question 3

The Commission invites views on Parental Controls:

- a) whether the measures specified are practicable to be implemented;**
 - b) whether the measures specified are effective; and**
 - c) whether there are any other measures that the Commission should consider;**
- for the purpose of ensuring that parents are able to monitor and manage the online activities of child users.**

6. PRIVACY AND SAFETY SETTINGS

- 6.1. The Licensed Service Providers shall make available privacy and safety settings to ensure safe use of their service by child users.
- 6.2. For the purpose of paragraph 6.1, the Licensed Service Providers shall—
 - 6.2.1. ensure default privacy and safety settings for child users are set to the most restrictive level;
 - 6.2.2. ensure that the personal information and account details of child users are not publicly visible unless expressly permitted by the child user with the guidance of a parent;

- 6.2.3. limit direct communication features to restrict or prohibit a child user from communicating with a user identified to be an adult who is not known or connected to them;
- 6.2.4. ensure child users are not exposed to manipulative design features that encourage compulsive or prolonged use of the service, or manipulate the decisions of child users in using the service; and
- 6.2.5. review and update privacy and safety settings regularly to ensure their continued effectiveness in safeguarding child users.

PC Question 4

The Commission invites views on Privacy and Safety Settings:

- a) whether the measures specified are practicable to be implemented;**
 - b) whether the measures specified are effective; and**
 - c) whether there are any other measures that the Commission should consider;**
- for the purpose of ensuring safe use of the services by child users.**

7. SEARCH AND RECOMMENDATION SYSTEMS

- 7.1. The Licensed Service Providers shall ensure that search and recommendation systems on their service are suitable and appropriate for child users.
- 7.2. For the purpose of paragraph 7.1, the Licensed Service Providers shall—
 - 7.2.1. ensure that safe search functions are activated by default for child users and harmful content is filtered from search results;

- 7.2.2. ensure that personalised recommendation systems are designed and operated in a manner that does not expose child users to harmful content;
- 7.2.3. provide child users and parents with clear and accessible options to manage personalised recommendation systems; and
- 7.2.4. ensure that the design and operation of algorithms used in search and personalised recommendation systems do not display, promote, or recommend harmful content to child users.

PC Question 5

The Commission invites views on Search and Recommendation Systems:

- a) whether the measures specified are practicable to be implemented;**
 - b) whether the measures specified are effective; and**
 - c) whether there are any other measures that the Commission should consider;**
- for the purpose of ensuring that search and recommendation systems of services are suitable and appropriate for child users.**

8. SERVICE PROVIDER ACCOUNTABILITY

- 8.1. Pursuant to section 20 of ONSA, the Licensed Service Providers shall prepare an Online Safety Plan on their compliance with the duties imposed under Part III of ONSA, including the duty to protect online safety of child users under section 18 of ONSA.
- 8.2. The Online Safety Plan is to be prepared within the period and in such form as prescribed by the regulations made pursuant to section 81 of ONSA. The information contained in the Online Safety Plan is as prescribed in the said regulations.

- 8.3. Insofar as compliance with the duty under section 18 of ONSA is concerned, the information that is to be addressed the Online Safety Plan shall—
- 8.3.1. demonstrate that the Licensed Service Providers have implemented the measures specified in this Code to ensure safe use of their services by child users; and
 - 8.3.2. where the Licensed Service Providers have implemented any alternative measures other than the measures specified in this Code, provide the justification to the satisfaction of the Commission that the alternative measures will be better to ensure the safe use of its services by child users.

9. REVIEW OF THIS CODE

- 9.1. The Commission may revoke, vary, revise or amend the whole or any part of this Code.