



FREQUENTLY ASKED QUESTIONS (FAQ) ON CHILD PROTECTION CODE UNDER THE ONLINE SAFETY ACT 2025

Date: 1 June 2026

TABLE OF CONTENTS:

SECTION A:	Under-16 Initiative
SECTION B:	What You Need to Know about Age Verification
SECTION C:	How Does Age Verification Work?
SECTION D:	Roles and Responsibilities
SECTION E:	Child Protection Code

Licensed service providers refer to providers of online services, including social media platforms, that hold an Applications Service Provider Class Licence under the Communications and Multimedia Act 1998. For the purposes of this document, the terms 'online service' and 'platform' are used interchangeably, where appropriate, depending on the context.

SECTION A: Under-16 Initiative

1. Why is stronger online protection for child users necessary today?

Child users today are exposed to online content, interactions and algorithm systems at an unprecedented scale and intensity.

As child users are still developing their ability to assess risks, manage online interactions and make informed decisions, they are particularly more vulnerable to online harms due to their stage of cognitive and emotional development. This includes exposure to harmful content, unsafe interactions with other users and platform features that may encourage prolonged or inappropriate use.

Stronger online protection is therefore necessary to ensure online services are designed and operated in a safer and more age-appropriate manner for child users.

2. What is Malaysia's minimum age requirement for social media account registration?

Child users below the age of 16 are not permitted to register for social media accounts.

In line with their statutory duty to protect online safety of child user under Online Safety Act 2025 [Act 866] ("**ONSA**"), social media platform providers are expected to implement reasonable measures to prevent child users below the age of 16 from creating accounts.

3. Why was the age of 16 chosen?

At the age of 16, child users are generally better able to assess risks, manage online interactions and exercise judgement in digital environments.

The minimum age reflects increasing international concern regarding child users' exposure to online harms, as well as child development considerations such as their cognitive and emotional development.

4. Is this measure meant to ban child users from the Internet?

No. The measure is not intended to prohibit child users from the Internet or to deny them access to technology.

Instead, it is aimed at promoting social media registration and age-appropriate access to certain platform features, while encouraging shared responsibility between social media platform providers, parents and guardians in protecting child users online.

5. How is age verification being introduced under ONSA?

Age verification measures are implemented pursuant to the statutory duties under Part III, section 18 of the ONSA, which requires licensed social media platform providers to protect online safety of child users.

The specific implementation measures are set out in the Child Protection Code (CPC), issued by the Commission pursuant to subsection 80(2) of the ONSA, which sets out the measures to be implemented by licensed social media platforms to ensure safe use of their services by child users, including age verification mechanisms.

6. Is Malaysia's approach consistent with the practices in other countries?

Several countries around the world, including Australia, Brazil and Indonesia have introduced or announced age restriction measures for child users, while many others such as United Kingdom, Spain, France, Thailand and South Korea are actively studying or developing comparable frameworks.

Similarly, Malaysia's approach is in line with ongoing international developments relating to online safety and age restriction measures.

SECTION B: What You Need to Know About Age Verification

7. What is age verification for social media platform providers?

Age verification refers to measures to be implemented by licensed social media platform providers that offer social media services, to ensure that only users who are verified as 16 years old and above are permitted to register for an account and access any features of the service that are appropriate for their age.

Under Malaysia's approach, relevant social media platform providers are required to implement effective age verification measures, including verification against Government-issued records, in a manner that is secure, practical and respectful of users' privacy.

8. Why is Malaysia introducing age verification for social media?

Malaysia is introducing age verification as part of its broader regulatory approach to strengthen online safety, particularly for child users.

The measure is aimed at mitigating child users' exposure to harmful content, unsafe interactions and platform features that may not be suitable for their age. It also supports stronger platform accountability in ensuring that social media services are safer and more age-appropriate for child users.

9. What do users need to do to verify their age?

Users will need to complete an age verification process before creating a social media account or continuing to use an existing account.

The process may vary between social media platform providers, but users should be given clear instructions on the steps they need to take.

10. What documents may be used for age verification?

Age verification will be conducted against Government-issued records, such as MyKad or Passport, and/or any other relevant documents recognised by

the Government of Malaysia or equivalent records issued or recognised by a competent authority in another jurisdiction.

Social media platform providers must provide clear instructions on the verification process, including what information is required, how the process works and how users' information will be handled.

11. Will the age verification process be difficult or complicated?

The process is intended to be simple, secure and user-friendly. Social media platform providers are expected to provide accessible verification options and clear guidance to help users complete the process smoothly.

12. When will age verification take effect?

The age verification will be implemented by licensed social media service providers effective 1 June 2026.

13. What happens if users do not complete the age verification?

From 1 June 2026 and until the expiry of any grace period provided, users who do not complete the required age verification, or who cannot be verified as being 16 years old and above, will be unable to create a new social media account or access existing accounts or platform features.

14. Will existing child users of social media accounts need to verify their age?

Existing child users above 16 years will be required to complete age verification as part of the progressive implementation process within a grace period of six months permitted for social media service providers.

Whereas existing users identified as being under 16 years will be given a one-month period to manage, download or transfer the user's data, including photographs and videos, prior to any restriction, suspension or other action taken by the respective social media service providers.

SECTION C: How Does Age Verification Work?

15. What methods may social media platforms use to verify age?

Social media platforms must provide effective age verification measures e.g. any verification methods against Government-issued records or equivalent records recognised by a competent authority in another jurisdiction.

16. Why is Malaysia adopting a technology-neutral approach?

Malaysia adopts an outcome-based, technology-neutral and risk-based approach to allow flexibility for social media platform providers to implement solutions that are effective, secure and appropriate to their services.

No specific technology is mandated, provided that the measures implemented meets regulatory requirements, including those relating to accuracy, privacy and security.

17. Will users' personal information be protected?

The social media service providers must ensure the age verification measures are designed with due regard to the necessary protection for the personal information of its user.

Any age verification measures implemented by the social media service providers must comply with applicable Malaysian data protection laws and regulatory requirements to ensure that users' personal information is safeguarded.

In addition, social media service providers can take guidance from the established Electronic Know-Your-Customer (e-KYC) practices adopted in various regulated sectors, including applicable protocols practised by Bank Negara Malaysia, where verification checks for the purposes of age verification are conducted with appropriate safeguards and data handling requirements.

18. What personal information is required for age verification?

The CPC requires licensed social media service providers to only collect and/or process minimum personal information necessary for age verification purposes. For the purpose of determining whether a user is below 16 years old, the necessary information mainly refers to the user's age and/or date of birth.

The objective of the verification process is to confirm age eligibility and not to collect excessive personal information. In this respect, the service providers are required to verify the user's age based on records issued by the Government of Malaysia, such as the National Registration Identity Card (NRIC) or passport or any other relevant documents recognised by the Government of Malaysia or equivalent records from other jurisdictions.

19. What safeguards apply to the handling of personal information collected for age verification?

The social media service providers are expected to implement appropriate safeguards to ensure that personal information collected and processed for age verification is handled securely and responsibly.

Most importantly, the CPC requires that personal information collected for age verification should only be used for the purpose of verifying a user's age and should not be retained longer than necessary for that purpose.

20. Will international social media platform providers also need to comply with Malaysian laws?

Social media platform providers that provide its services to users in Malaysia must comply with applicable Malaysian laws and regulatory requirements, including provisions under ONSA.

This applies regardless of whether the said platform is based in Malaysia or overseas.

21. Can child users simply use their parents' accounts instead?

The use of adult accounts by child users is a recognised risk.

Social media platform providers are expected to implement reasonable and proportionate measures to prevent and mitigate such misuse, including the detection of suspicious account behaviour.

SECTION D: Roles and Responsibilities

22. What are social media platform providers required to do?

Social media platform providers that are subject to the requirement must carry out the following measures:

- implement effective age verification measures;
- introduce age-appropriate protections and safety-by-design features;
- take appropriate action on reports involving accounts belonging to users below the age of 16 and harmful content; and
- provide clear and accessible reporting mechanisms for harmful content affecting child users.

23. What happens if social media platform providers fail to comply?

Regulatory action under the ONSA, resulting in fine upon conviction and/or financial penalty of up to RM10 million, can be initiated against social media platform providers that fail to comply with applicable requirements under the CPC.

This ensures that social media platform providers are accountable and take effective steps to implement age verification, strengthen accountability and provide safer online experiences for child users.

24. Will parents or guardians of child users' be penalised for non-compliance?

No. Regulatory action is not intended to be imposed on parents or guardians for non-compliance.

However, parents and guardians are strongly encouraged to exercise appropriate supervision and guidance over their child users' online activities and digital usage.

25. What role do parents and guardians play?

Parents and guardians play an important role in guiding child users' online behaviour and supporting safer digital habits.

This includes:

- monitoring online usage;
- setting appropriate boundaries;
- using available parental control tools; and
- educating child users about online risks and responsible online behaviour.

26. What other measures is the government taking to improve child users' online safety?

Age verification forms part of a broader online safety strategy, which also includes:

- stronger accountability of social media platform providers;
- enhanced reporting and complaint mechanisms;
- nationwide digital literacy and online safety programmes; and
- collaboration with industry, schools, parents and communities.

This ensures that online safety is addressed holistically across the ecosystem.

27. Which social media platform providers will be subjected to the age restriction measures under the CPC?

The requirement applies to licensed social media service providers with eight (8) million users or more in Malaysia.

This includes social media platforms such as Facebook, Instagram, TikTok and YouTube.

28. Are there measures to address child users from moving to other unregulated social media services?

To address such possibility, additional social media platforms may be brought within scope over time where necessary.

SECTION E: Child Protection Code

29. What is the Child Protection Code?

The Child Protection Code ("CPC") sets out the steps that licensed online service providers must take, under section 18 of ONSA, to ensure safe use of their services by child users. This includes ensuring age-appropriate access and enhanced protections for child users on their services.

30. Why was the CPC introduced?

Child users are increasingly being allowed to use online platforms, including social media platforms, by their parents and guardians for communication, learning and entertainment. Yet, as child users are still developing the skills and awareness to safely navigate online platforms, they may be more vulnerable to harmful content, such as child exploitation and cyberbullying, compared to adult users. As such, the CPC in line with section 18 under Part III of ONSA, requires the relevant social media platforms to ensure the safe use of their services by child users.

31. What is MCMC's power to issue the CPC?

The Malaysian Communications and Multimedia Commission ("**MCMC**") is empowered under section 80 of ONSA to issue any code for the purposes of compliance of duties under Part III of ONSA. In line with section 18 under Part III of ONSA, the CPC specifies the measures that the relevant licensed online service providers shall implement to ensure the safe use of their services by child users.

32. How does the CPC interact with other duties under Part III of the ONSA?

The contents of the CPC are intended to support and complement other duties of the licensed online service providers as provided under Part III of the ONSA. Compliance with the CPC does not replace or reduce other obligations under the ONSA.

33. When is the effective date of the CPC?

The effective date of the CPC is **1 June 2026**. Licensed social media service providers will be informed of the relevant timelines and requirements in relation to the verification process.

34. Which online service providers are required to comply with the CPC?

The CPC applies to licensed service providers, which utilise Internet access service to enable communication between users or to provide content, licensed under the Communications and Multimedia Act 1998 (CMA 1998), including providers of social media service.

35. Who is considered a “child user” under the CPC?

A “child user” means a user identified to be a child as defined under ONSA. ONSA defines “child” to mean a person who is under the age of 18 years.

36. Who is considered a “parent” under the CPC?

Under the CPC, “parent” means the parent or guardian of a child user.

37. What is considered “harmful content” under the CPC?

“Harmful content” refers to the categories of content listed in the First Schedule of ONSA which are:

- a) child sexual abuse material;
- b) financial fraud;
- c) obscene content;
- d) indecent content;
- e) content that may cause harassment or distress;
- f) content that may incite violence or terrorism;
- g) content that may induce a child to cause harm to himself;
- h) content that may promote feelings of ill-will or hostility amongst the public; and
- i) content that promotes the use or sale of dangerous drugs.

38. How will child users in Malaysia benefit from the CPC?

Child users can expect a safer online experience as licensed online service providers are expected to provide enhanced safeguards on their services catered specifically for child users. The CPC supports broader efforts under ONSA to strengthen online safety protections for child users, families and vulnerable users.

For more information on ONSA, click [here](#).

39. Can MCMC amend the CPC after it has been issued?

Yes. MCMC may revoke, vary, revise or amend the whole or any part of the CPC from time to time, whenever necessary.

CONTENT MODERATION

40. What content moderation measures must licensed online service providers implement?

Licensed online service providers must establish clear and robust systems for the detection and removal of harmful content from being accessed by child users. They must also provide clear and accessible reporting mechanisms for child users and parents, ensure reporting procedures are comprehensible to child users, take proportionate steps to prevent repeated exposure to harmful content that has been reported or removed and respond promptly and effectively to removal requests from MCMC or any other enforcement agency.

41. Are licensed online service providers obligated to respond to requests from government agencies to remove harmful content?

Licensed online service providers must respond promptly and effectively to any request made by any enforcement agency, including MCMC, for the removal of harmful content affecting child users.

42. Are licensed online service providers required to make reporting mechanisms accessible to child users?

Licensed online service providers must provide clear and accessible reporting mechanisms for child users and their parents to make a report regarding any content that they believe is harmful content. Further, reporting procedures must be accessible and comprehensible to child users.

43. What can parents do if they find harmful content affecting their child on a platform provided by a licensed online service provider?

Parents can use the reporting tools on the platform to report harmful content directly to the licensed online service providers. Parents may also lodge complaints with MCMC or the relevant enforcement agency regarding the harmful content.

44. What obligation exists regarding repeated exposure to harmful content?

Licensed online service providers must take proportionate steps to prevent the repeated exposure of child users to harmful content that has already been reported or removed from the platform.

PARENTAL CONTROLS

45. What parental control features must licensed online service providers provide on their platforms?

Licensed online service providers must 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.

Further, all parental control tools and settings must be clear, user-friendly and easily accessible.

46. Are licensed online service providers required to review their parental control tools and settings?

Licensed online service providers must review and enhance parental control tools and settings where necessary to ensure they remain effective in safeguarding the use of their services by child users.

PRIVACY AND SAFETY SETTINGS

47. What is the default for privacy and safety settings for child users?

The CPC requires that privacy and safety settings for child users are age-appropriate and/or set to the highest level by default. This means that a child user’s privacy and safety settings should automatically be set at a level that provides them the most protective safeguards for their age.

48. Are there restrictions on direct communication between adult users and child users?

Licensed online service providers must limit direct communication features to restrict or prohibit an adult user who is not known or connected to a child user from communicating with that child user. Child users should be able to use social media platforms safely, without risking unwanted interaction with an adult user.

49. How does the CPC tackle “manipulative design features”?

The CPC requires that child users not be exposed to manipulative design features that encourage compulsive or prolonged use of the social media platform or manipulate the decisions of child users in using the platform. This addresses platform design techniques that can exploit child users’ developing judgment.

50. Can child users control the public visibility of their personal information?

Licensed online service providers must ensure the availability of tools and settings to enable child users, with the guidance of a parent, to control the public visibility of their personal information.

51. Are licensed online service providers required to review their privacy and safety settings?

Licensed online service providers are required to review and update privacy and safety settings at risk-based intervals to ensure their continued effectiveness in safeguarding child users.

52. Are licensed online service providers required to provide guidance on using privacy and safety settings?

Licensed online service providers must provide clear and easily accessible guidance and information on the use of privacy and safety settings. This ensures that even child users can understand and make effective use of the protections available on the platform.

SEARCH AND RECOMMENDATION SYSTEMS

53. What is the default setting for search and recommendation systems for child users?

Licensed online service providers must ensure that safe search functions are activated by default for child users and that harmful content is filtered from search results.

54. What can child users expect from their personalised recommendation systems?

Licensed online service providers must ensure that personalised recommendation systems are designed and operated in a manner that does not expose child users to harmful content. They must also provide child

users (and their parents) with clear and accessible options to manage personalised recommendation systems.

55. What can child users expect from how platforms' algorithms promote or display content?

Licensed online service providers must 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. This covers both the surfacing of content in search results and the promotion of content through recommendation feeds.

-END-