Public Consultation Report

Proposed Gaming Sub-Code

Consultation period: 9 September to 24 October 2026

Communications and Multimedia Content Forum of Malaysia (CMCF)



Findings of the Public Consultation on the Proposed Gaming Sub-Code

Table of Contents

Executive Summary 1
Background and Context 3
Respondent Profile 5
Consultation Methodology 7
Overall Reception of the Draft 9
Key Themes and Findings 11
Written Submissions 16
Issues Requiring Further Consideration 20
Proposed Next Steps 26
Appendices 28

AT A GLANCE

Strong support

317
responses

86.8%
support at least the overall objective

65.3%
support as drafted or with some changes

80%+
agreement on 40 of 44 items

66.1%
lowest score, on children without ID

8
written submissions

Areas that require clarity

01
Age checks without identity documents
how children without documents are treated, and how a User moves off child defaults

02
Relying on Platform age signals
shared devices, family profiles and the standard age-check providers must meet

03
Teenagers' settings
what settings 13 to 17 year olds may relax themselves, and when a parent must consent

04
Randomised Reward Mechanisms and spending
parental switch-off, odds, consent and spending limits

05
Proportionate, shared responsibility
small studios, duties that follow control, and the safety contact

06
Reporting and moderation
24-hour triage, human review and protection while a report is reviewed

01
Executive Summary

This report sets out the findings of the **Public Consultation** on the proposed **Gaming Sub-Code** (the Sub-Code), conducted by the Communications and Multimedia Content Forum of Malaysia (CMCF) from **9 September to 24 October 2026**. The Sub-Code is proposed under the Malaysian Communications and Multimedia Content Code (the Content Code) and sets out standards for Online Games and Gaming Services in Malaysia, with particular attention to the safety of children.

The Public Consultation received **317 valid questionnaire responses**, 313 online and 4 on paper. **Eight written submissions** were also received: from UNICEF Malaysia; ECPAT Malaysia with the Child Rights Coalition Malaysia (CRCM) and the Online Child Sexual Exploitation and Abuse (OCSEA) Working Group; Universiti Malaya with Universiti Kebangsaan Malaysia (UM/UKM); two game developers; an academic researcher; the Institute for Democracy and Economic Affairs (IDEAS); and a joint submission on behalf of four game companies. The CMCF also held **eight town halls and dialogue sessions** with universities, a school, game developers, a regulatory body, and influencers and content creators, and promoted the questionnaire at industry and esports events. Respondents included players and members of the public, academics, esports organisers, teams and players, government agencies, educators, parents and civil society organisations.

Support for the Sub-Code is strong. **86.8%** of respondents support at least its overall objective, and **65.3%** support it as drafted or with some changes. Only **2.8%** do not support it. **88.3%** agree that Malaysia would benefit from clear standards for games.

Support is also conditional: more than half of those in support want changes or clarification, and one in five respondents (21.5%) supports the objective but wants significant changes. The feedback focused less on whether the standards are right and more on how they would work in practice. Six areas stood out:

- **Age checks without identity documents**: how a child who has no documents, or does not want to use them, is treated, and how a User moves off the protective defaults for children.
- **Relying on age signals from a phone, console or app store**: in particular, a child using a parent's device, and the standard that age-check providers should meet.
- **Teenagers' settings**: which settings 13 to 17 year olds may relax themselves, and which need a parent's consent.
- **Randomised Reward Mechanisms and spending**: parental controls over Paid Randomised Reward Mechanisms, how odds are shown, and the default spending limit.
- **Proportionate and shared responsibility**: how duties apply to small studios, and how responsibility is shared between Developers, Publishers, Platforms and parents.

- **Reporting and moderation**: what a 24-hour response to a serious incident means, human review of reports, and protection for a child while a report is reviewed.

The written submissions built on these themes, adding nuance and proposing improvements or alternatives. UNICEF Malaysia focused on children's rights across the Sub-Code; ECPAT Malaysia and CRCM on gender-based harassment, safe defaults and child-friendly reporting; UM/UKM on privacy-preserving Age Assurance, risk tiers, complaint handling and support for small Operators; the two game developers and the joint industry submission on how the standards would apply to their services, asking for flexibility in how protections are delivered; the academic researcher on disclosure for Randomised Reward Mechanisms, spending limits and enforcement; and IDEAS on age checks, moderation and complaint handling.

When read together, the public, industry and child-rights organisations largely agree on what the Sub-Code should achieve. Where views differ, it is mostly on method: how best to address long-standing problems and existing practices. Industry asks for flexibility in how these protections are delivered, while the public and child-rights organisations ask that the protections hold by default. The choice of which solution is preferable is a task for the CMCF and the Working Group.

Respondents also asked for practical and accessible support such as:

i. a plain-language summary for players and parents,

ii. a checklist for Developers,

iii. guidance on what counts as a proper age check, and

iv. a template child safety risk assessment.

The Working Group will consider all feedback provided in the Public Consultation before the Sub-Code is finalised, and the CMCF will develop supporting materials so that the Sub-Code is clear and workable from the day it takes effect.

02
Background and Context

Online games are among the most popular forms of digital entertainment in Malaysia, particularly for children and young people. Many games now combine play with chat, voice, livestreaming, player-made content, in-game purchases and advertising.

These features bring real-world social, creative and economic value. They also carry risks such as contact from strangers, exposure to unsuitable content, pressure to spend, gambling-like mechanics, and harassment. Children are most exposed to these risks and least able to manage them alone.

The Sub-Code is a proposed sub-code under the Content Code. It takes effect only on registration by the Malaysian Communications and Multimedia Commission (the Commission) under section 95(2) of the Communications and Multimedia Act 1998 (the Act), and it works alongside the Online Safety Act 2025, the Child Protection Code and the Risk Mitigation Code. It is developed under the CMCF's mandate as the designated industry forum under the Act, through a multi-stakeholder Working Group of industry, civil society, academia and government. The Sub-Code will operate under the existing **co-regulatory framework** of the Content Code.

What the Draft Covers

The draft Sub-Code released for the Public Consultation contains 14 Parts. In summary, they address:

- Which games, services and features the Sub-Code applies to, and a risk-based approach that focuses on features rather than whole games (Parts 1 and 2);
- Age ratings, technology-neutral Age Assurance, and protective default settings and parental controls for Child Accounts, including Esports (Part 3);
- Disclosure of game features and risks before download or purchase (Part 4);
- Responsible monetisation: prices in ringgit, Randomised Reward Mechanisms, spending limits and trading (Part 5);
- In-game advertising, rewarded adverts and promotion by streamers and content creators (Part 6);
- Community rules, moderation, reporting tools and protection from grooming and harassment (Part 7);
- Account security and protection from scams (Part 8);
- The responsibilities of Platforms and Operators, including Safety-by-Design, risk assessment, a Gaming Safety Officer and incident response (Part 9); and
- User responsibility, complaints, recordkeeping and cooperation, public education, and User and consumer protection (Parts 10 to 14).

Objective of the Consultation

The Public Consultation was designed to test whether the draft standards are clear, workable and proportionate, and whether they reflect what Malaysian players and parents expect of online games. It sought views both from those who would apply the Sub-Code and from the players and families it is meant to protect.

The responses point to several considerations for the next phase of drafting:

- **Age Assurance That Works and Respects Privacy**

  Age checks should be strong enough where the risk is real, without collecting more personal data than needed or locking out children who have no identity documents.

- **Safe Defaults, With Room for Families**

  Child Accounts should default to safe settings, with clear rules on what teenagers may change for themselves and what needs a parent.

- **Fair Spending and Transparent Randomised Reward Mechanisms**

  Consumers, regardless of age, should know the real cost and the odds before paying, and parents should be able to control their children's spending.

- **Proportionate and Shared Responsibility**

  Duties should follow each party's role and control, and scale to the size and risk of the service, so that small studios can comply.

Status of This Report

The Public Consultation sought views to inform the drafting of the Sub-Code. Views attributed to respondents and written submissions in this report are their own, and their inclusion does not mean that the CMCF or the Working Group agrees with them. Nothing in this report is a legal determination, including on whether any game feature amounts to gambling or how any law applies, or a statement of the jurisdiction of the CMCF or any other body.

03
Respondent Profile

Of the **317 responses** received, two thirds came from players and members of the public. Respondents could choose more than one category, so the shares in **Chart 1** add up to more than 100%. A response is counted as valid where the respondent gave a view on the Sub-Code; test entries, responses that answered only the profile questions, and earlier responses from anyone who responded more than once are not counted.

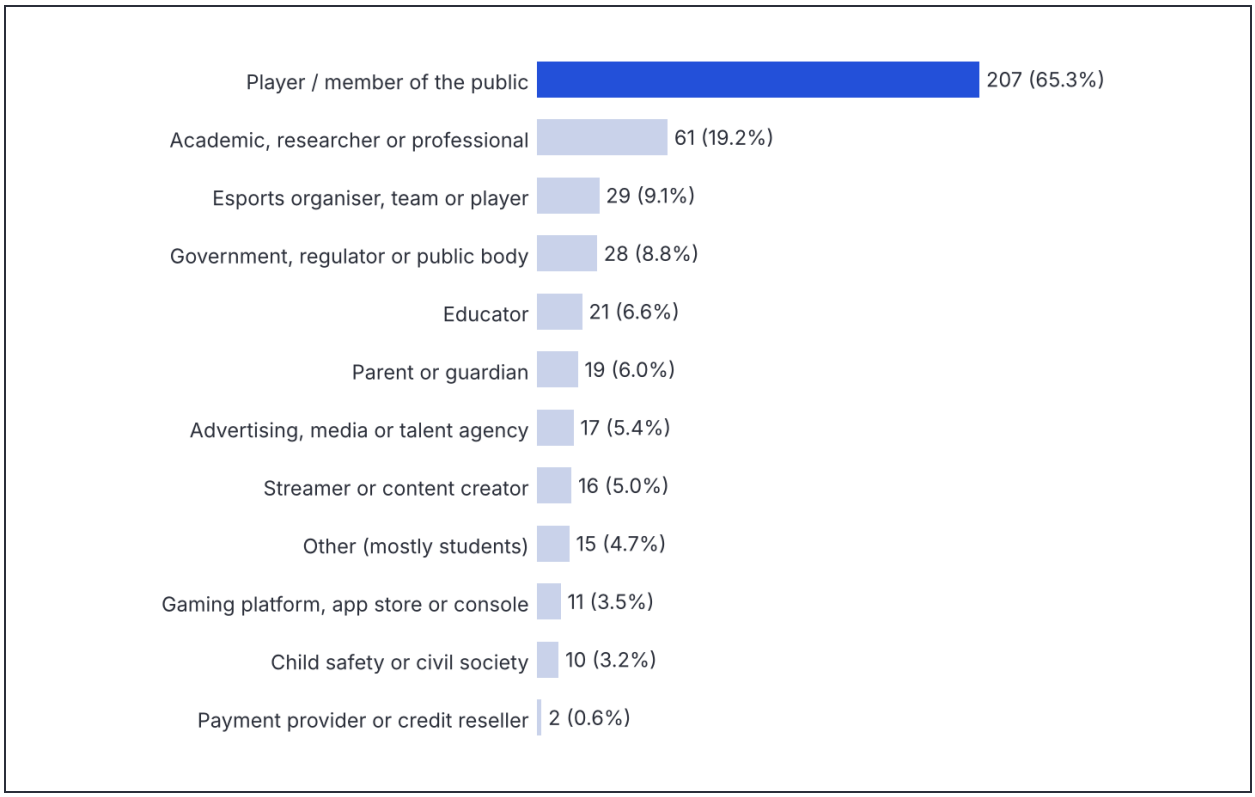


CHART 1 Number and Profile of Respondents (317 respondents; more than one category could be chosen)

Players and members of the public made up the largest group (207 respondents, 65.3%), followed by **academics, researchers and professionals** (61, 19.2%). Respondents connected with the gaming industry included esports organisers, teams and players (29), advertising, media and talent agencies (17), streamers and content creators (16), gaming platforms, app stores and console providers (11) and payment providers or credit resellers (2).

Government agencies, regulators and public bodies contributed 28 responses (8.8%), **educators** 21 (6.6%), **parents and guardians** 19 (6.0%) and **child safety and civil society organisations** 10 (3.2%). Most of those who chose “Other” described themselves as students.

The respondent base was young. Respondents aged 18 to 24 formed the largest group (67.5%), followed by those aged 25 to 34 (15.8%) and 35 to 44 (9.1%). Respondents aged 45 and above made up 5.4%, and 2.2% were below 18.

About a quarter had read all or most of the draft (26.8%), and a similar share had not yet read it (26.5%); the rest had read the parts most relevant to them or a summary.

Around 20 organisations identified themselves when responding, including universities and colleges, gaming and esports businesses, government agencies, a policy research institute, legal practices and an early-childhood education provider.

Participation was voluntary. The findings describe the views of consultation respondents and should not be treated as representative estimates of the Malaysian population or gaming industry.

04
Consultation Methodology

The Public Consultation was structured around the text of the draft rather than general opinion. It ran from **9 September to 24 October 2026** through a **bilingual questionnaire** in Bahasa Malaysia and English, available online and on paper, alongside an open invitation for written submissions.

Questionnaire Design

The questionnaire combined five types of questions, so that both views on principle and practical concerns could be captured:

- **Statements on the Draft**

  Respondents indicated how far they agreed with 44 agreement-rated items drawn from the draft, including three scenarios, grouped by the Consultation Questions in the PC Paper, from Age Assurance and Child Accounts to spending, advertising, community safety and implementation.

- **Scenario Questions**

  Short real-world situations tested how respondents would apply the proposed standards: ringgit prices beside in-game currency, a streamer promoting a Randomised Reward Mechanism, a player told the outcome of a report, and who should be responsible for a child's spending.

- **Overall View and Priorities**

  Respondents were asked to give an overall view of the Sub-Code and to select up to three areas needing further work. The online form did not enforce the limit, and some respondents chose more than three.

- **Questions for Industry**

  Respondents, particularly those answering for an organisation, were asked which requirements would be hardest to apply (up to three, a limit the online form likewise did not enforce), whether responsibilities were clear, how long they would need to prepare, and what practical support would help. These questions included an option for those to whom they did not apply.

- **Open Questions**

  All respondents were invited to identify any part of the draft that should be changed or clarified, and any issue the draft had not addressed.

Written Submissions

Eight written submissions were received, from UNICEF Malaysia; ECPAT Malaysia and CRCM, with the OCSEA Working Group; UM/UKM; two game developers, referred to in this report as

Game Developer A and Game Developer B; an academic researcher, referred to as Academic Researcher; the Institute for Democracy and Economic Affairs (IDEAS); and a joint submission on behalf of four game companies, referred to as Industry Group. The ECPAT Malaysia and CRCM submission also covered the draft Guidelines for Influencers and Brand Collaboration; only its points on the Sub-Code are reflected in this report. Each submission was read against the relevant clauses of the draft and alongside the questionnaire themes, so that a point raised in both channels is treated once. Section 07 summarises each submission, and Appendix B lists every point raised with the provision it concerns.

Town Hall Sessions

To reach both those who would apply the Sub-Code and the players and families it is meant to protect, the CMCF held eight town hall and dialogue sessions with universities, a school, game developers, a regulatory body, and influencers and content creators in gaming. It also engaged players and members of the public at games, animation and esports events. Each session introduced the draft, invited questions and discussion, and encouraged participants to respond to the questionnaire.

05
Overall Reception of the Draft

Support for the draft was broad and consistent. **88.3%** agreed that Malaysia would benefit from clear standards for games, **87.2%** felt the requirements are proportionate to risk and size, and **87.4%** felt the draft strikes the right balance between protecting players and allowing the industry to grow. **82.4%** found the draft clear enough to understand; a few respondents asked for a shorter, plain-language version for players and parents.

Overall view of the proposed Sub-Code	Respondents	Share
Support the Sub-Code as drafted	120	37.9%
Generally support, with some changes or clarifications	87	27.4%
Support the objective, but significant changes are needed	68	21.5%
Do not support the proposed Sub-Code	9	2.8%
Not sure or need more information	33	10.4%

TABLE 1 Overall View of the Proposed Sub-Code

Taken together, **65.3%** support the Sub-Code as drafted or with some changes, and **86.8%** support at least the overall objective. Only nine respondents opposed the Sub-Code outright.

Support for the Proposed Standards

Each core standard was tested through a statement or a scenario. Agreement ranged from **66.1% to 91.1%**, and disagreement exceeded 10% on only two items. Every area of the draft has majority support, and the area of age ratings and Age Assurance attracted the most disagreement, as reflected in **Chart 2**. Chart 2 adds together all the ratings given to the statements in each area and shows the share of those ratings in each category; it is not an average of the statement percentages, nor a count of individual respondents.

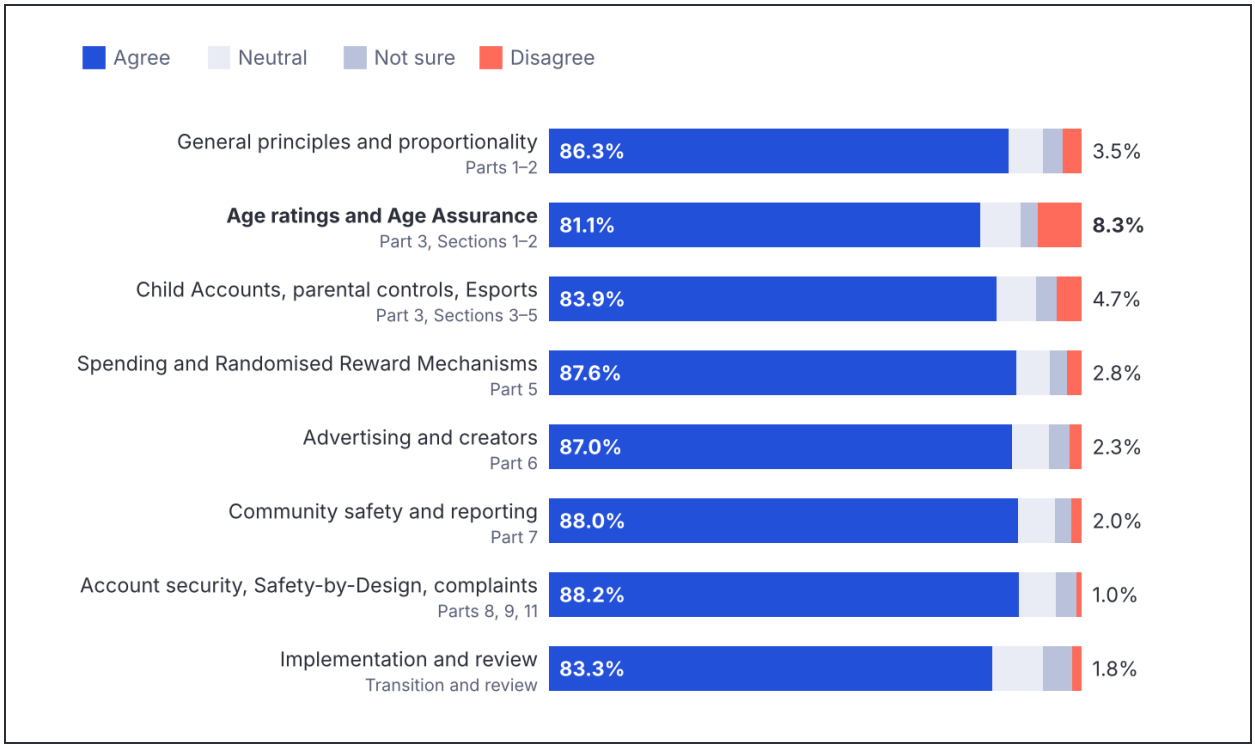


CHART 2 Share of All Ratings in Agreement, by Area of the Draft

The strongest agreement was for protecting players against account theft and scams (**91.1%**, with no respondent disagreeing), showing the real ringgit cost of a purchase before payment (**90.6%**), re-checking safety risks periodically (**90.4%**) and age-check providers meeting a recognised standard (**90.1%**).

The two clear exceptions are both about age checks. An alternative route for children without identity documents received **66.1%** agreement, with **17.1%** disagreeing, **11.1%** neutral and **5.7%** not sure. Allowing a game to rely on an age check by the phone, console or app store received **68.8%**, with **19.7%** disagreeing, the highest disagreement in the questionnaire. While **68.8%** supported reliance on phone, console or app-store age checks, **90.1%** supported requiring age-check providers to meet recognised standards. Some comments raised concerns about children using a parent's device.

06
Key Themes and Findings

Seven themes emerged from the analysis of questionnaire responses and written submissions. Each is presented below with the questionnaire results that bear on it and the main points raised.

- **Checking a Player's Age**

Age checks are the area respondents most want developed further: **56.7%** chose age checks and age ratings as an area needing work, and **55.2%** of those who answered the question on implementation selected knowing when a stronger age check is required as one of the hardest requirements to apply. Respondents strongly support showing a recognised age rating before download or purchase **(89.7%)** and ratings that show what a game contains (**88.5**%). Support is lower for treating unchecked accounts as a Child Account by default (**81.2%, with 8.6% disagreeing**) and for the rule that typing a birthday is not enough for risky features (**83.7%**).

Written comments pulled in different directions. Several respondents said that uploading MyKad, passports or facial images is disproportionate and intrudes on privacy, and asked for lighter, privacy-preserving methods; one suggested a payment-card check; another asked for identity checks at app stores before any purchase. Others pointed to a child using a parent's phone or console and inheriting an adult's age signal. At engagement sessions, participants compared the draft with the identity-based age checks now required of social media platforms.

UNICEF Malaysia and UM/UKM asked for an alternative route for children without identity documents and a way to correct a wrong result, and UNICEF Malaysia asked that age-check providers meet recognised standards. ECPAT Malaysia and CRCM and UM/UKM asked that age checks collect the minimum data needed. Both game developers and Industry Group asked that Platforms and app stores carry more of the Age Assurance task, and Game Developer A and Industry Group that strong age checks follow from the risk remaining after safeguards rather than from the presence of a feature alone. Academic Researcher asked that a Platform's age signal be relied on only where each User, not each device, has been checked, and IDEAS that age be re-checked at sensitive transactions so that an adult cannot pass a verified account to a child.

- **Children's Accounts and Parental Controls**

Respondents strongly support Child Accounts starting with the safest settings (**89.6%**), parental controls that are easy to find and use (**87.5%**) and children joining organised Esports with parental consent (**86.8%**). Support is lower for letting 13 to 17 year olds relax lower-risk settings themselves (**80.7%, with 8.4% disagreeing**) and for a parent being able to reinstate any setting at any time (**81.7%**). Child Account settings were the second most chosen area for further work (**48.5%**).

The lowest score in this area was for a parent supervising the account of a person with a disability (**77.3%**), where **17.5%** were neutral or not sure rather than opposed. Several respondents asked that adults with disabilities keep control of their own accounts, with supervision only by choice. Game Developer A and Industry Group asked that such arrangements be optional, with

safeguards against misuse, UNICEF Malaysia that they respect the person's views and dignity, and Academic Researcher that adults with full capacity not be closely supervised.

Views on teenagers differ. Some respondents asked that teenagers not relax any setting before 17 or 18, while others asked the Sub-Code to protect through defaults rather than restricting access to games. At engagement sessions, participants asked that children not be reachable by any player unless they or a parent choose otherwise. UNICEF Malaysia asked that public profiles and links to other services stay off for 13 to 17 year olds without Verified Parental Consent, and ECPAT Malaysia and CRCM and UM/UKM asked for the highest privacy settings and contacts-only communication by default. The game developers asked that voice chat with teammates during a match, and age-based controls with parental involvement, be accepted in place of fixed defaults. Academic Researcher suggested separate tiers for 13 to 15 and 16 to 17 year olds, with more choice for older teenagers.

- **Spending, Randomised Rewards and Virtual Currency**

Support is consistently high in this area. Respondents agree that the real ringgit cost, recurrence, expiry and effect of a purchase should be shown before payment (90.6%), that ringgit should be shown beside Virtual Currency (88.7%), that odds for Randomised Reward Mechanisms should be shown before payment (88.2%), that parents should be able to switch off or limit Paid Randomised Reward Mechanisms (88.5%), that Child Accounts should have a default spending limit raised only by a parent (87.8%) and that parents can require approval for every purchase (87.6%). Support for clear pricing by top-up resellers was 85.9%.

Several respondents said Paid Randomised Reward Mechanisms are a form of gambling and should be banned, and one asked that they be switched off on Child Accounts with no parental override. UNICEF Malaysia and ECPAT Malaysia and CRCM asked that Paid Randomised Reward Mechanisms be prohibited on Child Accounts. 88.5% supported parents being able to switch off or limit Paid Randomised Reward Mechanisms; the questionnaire did not ask about a prohibition.

Game Developer B asked that Paid Randomised Reward Mechanisms be available where spending and parental controls are in place, and that odds may be shown by rarity tier. Game Developer A asked that spending notifications be accepted in place of a default limit, while UM/UKM and UNICEF Malaysia asked that the limit be kept, with the amount set in guidance. UNICEF Malaysia also asked that changing odds be disclosed and that top-up resellers carry obligations. Academic Researcher asked that Paid Randomised Reward Mechanisms on Child Accounts be off until a parent approves them, that odds be shown on the purchase page, that default spending limits be set in exact figures by age and that top-up resellers be prohibited. Industry Group asked how a default limit would work where a parent already approves each purchase.

- **Advertising and Creator Promotions**

Respondents agree that in-game advertising should be clearly recognisable (**88.8%**), that a child's data should not be used for targeted advertising (**89.7%**), that rewards for watching adverts should be clearly disclosed (**89.2%**) and that streamers should disclose sponsorship and real odds (**87.6%**). Support was lower for allowing ad-funded free games to show more adverts (**79.6%**).

UNICEF Malaysia asked that the ban on Personalised Advertising cover personal data from any source, and UM/UKM supported a ban on using data collected or inferred within the service. Game Developer A asked for age-appropriate safeguards in place of a ban, and Game Developer B asked whether recommending the game's own items counts as Personalised Advertising. UNICEF Malaysia also asked that all advertising on Child Accounts be clearly marked, and Academic Researcher that advertising show a game's age rating and whether it contains Randomised Reward Mechanisms. Industry Group asked that the restriction on promoting age-restricted content apply to content directed at children.

- **Talking to Other Players, Reporting and Moderation**

Respondents agree that games with chat should have clear community rules (**89.5%**), that mute, block and report should be easy to reach during play (**88.8%**), that a player should be told the outcome of a report (**88.8%**) and that games should actively look for signs of grooming (**89.0%**). **88.8%** agree that unresolved complaints may go to the CMCF, and 84.7% agree that Operators should publish regular figures on reports received and action taken.

Respondents raised concerns about harassment and about moderation by automated tools alone, and engagement session participants asked that reporting tools and parental controls work for children, persons with disabilities and non-English speakers. Game Developer A and Industry Group asked that the 24-hour response to a serious incident be understood as acknowledgement and initial triage, and UM/UKM proposed time-bound standards by severity, beginning with acknowledgement within two hours for critical child-safety reports.

UNICEF Malaysia asked for hash-matching of known child sexual abuse material, moderation in the languages children use, human review before significant action on a Child Account, and direct access to the Complaints Bureau where going to the Operator first is unsafe. ECPAT Malaysia and CRCM asked that gender-based harassment be named, that reporting be built into the game, that children have instant self-protection tools while a report is reviewed, and that young players receive staged warnings. IDEAS asked for moderation that understands local slang in several languages, firm action against adults who harass children, acceptance of reports of harassment that moves from a game to other apps, and alerts to the parents of both children involved in serious misconduct.

- **Responsibility and Proportionality**

Asked who should be mainly responsible for a child's spending, the most common answer was each party for the part it controls (**31.8%**), followed by the parent (**27.0%**); no single industry party exceeded **12.9%** (Scenario G, **311** respondents). **87.2%** agree that requirements should be proportionate to risk and size. Of the **214** respondents who gave a view on whether the responsibilities of Developers, Publishers, Platforms, creators and resellers are clear, leaving out those who answered that the question did not apply to them, **73.4%** found them very or mostly clear, **18.7%** said some or significant clarification is needed, and **7.9%** were not sure.

Respondents asked that safety-contact and monitoring duties flex for small and independent studios, and at engagement sessions industry participants asked that the Sub-Code set outcomes and leave the method to Operators, supported by plain examples and checklists. Game Developer A, UM/UKM and Industry Group asked that duties follow actual control, while

Academic Researcher proposed that the Developer, Publisher, seller and promoter be jointly responsible for a child's spending so that a parent can claim against any of them. UM/UKM proposed a single entry point for complaints, UNICEF Malaysia a "no wrong door" principle, and IDEAS resolution times by severity before a complaint may go to the Complaints Bureau. Game Developer A asked that equivalent risk assessments be accepted, while UNICEF Malaysia and ECPAT Malaysia and CRCM asked for child rights impact assessments with published outcomes.

- **Implementation, Timing and Review**

Respondents support giving companies time to prepare before the Sub-Code fully applies (**83.2%**), setting specific figures in separately updatable guidance (**80.6%**) and reviewing the Sub-Code within a year and regularly after that (**86.1%**). Of the 178 respondents who gave a view on lead time, leaving out those who answered that the question did not apply to them, **32.6%** said they already meet most of the draft; **11.2%** would need up to 6 months, **19.1%** 6 to 12 months and **8.4%** more than 12 months, while **28.7%** were not sure.

UNICEF Malaysia and UM/UKM asked for a review within 12 months, and UM/UKM for phased implementation, with high-risk obligations first. Academic Researcher proposed up to six months for simpler measures and up to a year for complex ones, with guidance issued early, and a funded evaluation of whether the measures work. UNICEF Malaysia and Game Developer A asked for clarity on how the Sub-Code works alongside the Online Safety Act 2025 and related codes, and Industry Group that references to the Online Safety Act 2025 be removed or limited to context. At engagement sessions, participants asked what effect a voluntary code has, and raised excessive play and its effect on sleep and health; UNICEF Malaysia and ECPAT Malaysia and CRCM asked that streaks, night-time notifications and other design features that encourage excessive play be addressed.

Matters Raised Beyond the Scope of the Sub-Code

Some respondents and submissions raised matters beyond what the Sub-Code is designed to address, namely:

1. doxxing and stalking;
2. whether Randomised Reward Mechanisms amount to gambling under Malaysian law, which is a matter for the relevant authorities;
3. obligations on app stores, APK stores and other Platforms that are not members of the CMCF, including unregulated or illegal Platforms;
4. the licensing of services and the age rules of the Child Protection Code under the Online Safety Act 2025;
5. government supervision of in-game chat; and
6. a Malaysian age rating system for games.

These views are noted and will be considered in the CMCF's wider work, or referred to the relevant bodies, where relevant.

07
Written Submissions

Eight written submissions were received. Each brings a distinct perspective: children's rights, child protection, academic research, public policy and the experience of companies that operate games. Their main points are summarised below, and Appendix B lists all 242 points with the relevant provision. The Working Group will consider each point.

UNICEF Malaysia

UNICEF Malaysia's submission is organised around ten recommendations grounded in the Convention on the Rights of the Child and General Comment No. 25, with comparisons to approaches in Europe, Australia, Singapore and Brazil. It welcomes the draft's core framework, including Highly Effective Age Assurance, protective defaults for Child Accounts, the default spending limit and the ban on Personalised Advertising, and recommends building on it. It asks that children's rights to privacy, participation and development be recognised, that "likely to be accessed by children" be defined, and that core protections be clear expectations rather than matters to assess. On Age Assurance, it asks for recognised standards for providers, prompt deletion of data, alternatives for children without documents and a way to challenge wrong results. It asks that unknown adults be prevented from contacting children, that public profiles and links stay off for teenagers without parental consent, and that streaks and similar mechanics be off on Child Accounts. It asks that Paid Randomised Reward Mechanisms be prohibited on Child Accounts, that ringgit prices be shown, that resellers carry obligations, and that Personalised Advertising be barred whatever the source of the data. It also asks for hash-matching of known child sexual abuse material, multilingual and human-reviewed moderation, safeguards for generative AI features, child rights impact assessments, transparency reporting, child-friendly reporting with direct access to the Complaints Bureau, and a review within 12 months.

ECPAT Malaysia and CRCM, with the OCSEA Working Group

ECPAT Malaysia and CRCM, with the OCSEA Working Group, ground their submission in the Convention on the Rights of the Child and the Committee's 2026 concluding observations for Malaysia. They ask that technology-facilitated gender-based violence and misogynistic behaviour be defined and prohibited, and that games offer positive default emotes and team prompts. They ask that Child Accounts default to the highest privacy settings, that Paid Randomised Reward Mechanisms, Dark Patterns and addictive features be prohibited, and that real-money equivalents be shown at every step of a purchase. On reporting, they ask for child-friendly, trauma-informed reporting built into the game, instant self-protection tools while a report is reviewed, status updates, staged warnings for young players and links to national child protection services. They also ask for public child rights impact assessments, a two-year limit on retaining Age Assurance and safety data, and co-design of guidance with children and young people. Their submission also covered the Influencer Guidelines; those points are reflected in that consultation.

Universiti Malaya and Universiti Kebangsaan Malaysia

UM/UKM support a risk-based, proportionate framework and frame each recommendation by its legal basis. They propose four feature-based risk tiers, with company size setting the method of compliance but not the level of protection, and a free compliance toolkit for small Operators and gaming cafés. They ask that Age Assurance return only the minimum age band, with an alternative route for children without identity documents, appeals and testing across demographic groups. They ask for protective defaults, broader parental controls and information for parents before children enter tournaments; clear pricing, odds by reward category, a default spending limit set in guidance and a ban on Dark Patterns. They propose a single complaint entry point with time-bound standards by severity, responsibility that follows actual control, phased implementation, a firewall on the use of child-safety data, coverage of engagement design and cash-convertible items, a regulatory sandbox for age tokens, and a review within 12 months.

Game Developer A

Game Developer A supports the principles-based and risk-based approach, and asks that the final Sub-Code assess risk by reference to the risk remaining after safeguards, allocate responsibility by functional control, and accept equivalent safeguards rather than uniform controls. It asks that Highly Effective Age Assurance and the treatment of High-Risk Features follow from a holistic assessment rather than the presence of a feature alone; that default settings and spending controls be outcome-based, with notifications in place of a default limit and approval of every purchase; and that the ban on Personalised Advertising give way to age-appropriate safeguards. It also asks for clarity on the relationship with the Content Code and the Online Safety Act 2025, reliance on upstream age signals, a targeting-based test for marketing age-restricted content, optional supervised accounts for persons with a disability, flexible reassessment periods, a contact role for the Gaming Safety Officer, a triage meaning for the 24-hour response, and a narrower reading of several consumer protection clauses.

Game Developer B

Game Developer B comments on how Age Assurance, High-Risk Features and monetisation would apply to competitive Online Games. It asks for clearer thresholds for content presenting a significant risk of serious harm, including whether existing age-rating classifications may be relied on, and a definition of content that simulates gambling. It asks that team communication during a match, Paid Randomised Reward Mechanisms with spending and parental controls, low-value gifting and features using only general location not be switched off by default, and that app stores and Platforms be required to carry out Age Assurance and share a standard age signal. It also asks for clarity on whether recommending the game's own items counts as Personalised Advertising, that one spending-limit mechanism be accepted, that odds may be shown by rarity tier, and for a standard risk assessment template.

Academic Researcher

An academic researcher of video game regulation, drawing on studies of how rules on Randomised Reward Mechanisms have been implemented and enforced in other countries, supports the Sub-Code and asks that it set out more precisely how companies should comply.

On Randomised Reward Mechanisms, the researcher asks that odds be shown on the purchase page or one tap away, that the presence of Randomised Reward Mechanisms be disclosed on store pages and in advertising, that objective disclosure standards replace subjective wording, that Paid Randomised Reward Mechanisms on Child Accounts be off until a parent approves them, and that results be recorded for auditing. The researcher proposes default spending limits set in exact figures by age, a clear meaning of parental approval for each purchase, a ban on third-party top-up resellers, and joint responsibility of the Developer, Publisher, seller and promoter for a child's spending. Other points include separate tiers for 13 to 15 and 16 to 17 year olds, limits on Esports for children where Paid Randomised Reward Mechanisms are central to competing, disclosure of features before download, IP or location checks against foreign versions of a game, wider use of the defined term Vulnerable User, removal of Part 10 on User Responsibility, and a funded evaluation of whether the measures work.

Institute for Democracy and Economic Affairs (IDEAS)

IDEAS responded to the questions on age checks, Child Accounts, talking to other players and complaints, drawing on practices already used by major platforms. It asks for periodic re-checks of age at sensitive transactions to prevent an adult from verifying an account and then allowing a child to use it, age signals from operating systems without re-collecting identity documents, and alternative routes for children without documents. It suggests sleep modes, usage limits and accessibility features such as read-aloud tools and colour-blind modes. On moderation, it asks for systems that understand local slang in several languages, proactive detection, firm action against adults who harass children, acceptance of reports of harassment that moves from a game to other apps, and alerts to the parents of both children involved in serious misconduct. It proposes resolution times by severity before a complaint may go to the Complaints Bureau, a way to track complaints, and published figures that include serious incidents.

Industry Group

Industry Group, a joint submission on behalf of four game companies, supports the risk-based, outcomes-focused approach and asks that participants be able to meet the Sub-Code's outcomes through existing and equivalent safeguards suited to their service. It asks that references to the Online Safety Act 2025 be removed or limited to context, that risk be assessed holistically after existing safeguards, that High-Risk Features be treated as indicators rather than inherently high-risk, and that Highly Effective Age Assurance be required only where significant risk remains and be applicable to a single feature. It asks that responsibility be shared according to role and control, with Platforms able to rely on creator declarations, and that default settings and spending controls be framed as outcomes, including how a default limit works where a parent already approves each purchase. It also asks that the exclusions for APK stores, unregulated Platforms and games without specified features be removed so that comparable services face the same expectations, that developer tools be confirmed as outside scope, and for clarity on unassured accounts, the Gaming Safety Officer, the 24-hour response, the child-protection principles in Part 14 and corrective advertising.

Where the Submissions Meet and Differ

Several points were raised by more than one submission: an alternative age route for children without identity documents (UNICEF Malaysia, UM/UKM, Academic Researcher, IDEAS); keeping Age Assurance data to the minimum (UNICEF Malaysia, ECPAT Malaysia and CRCM, UM/UKM, Game Developer A, Industry Group); reliance on Platform age signals (UM/UKM, both game developers, IDEAS, Industry Group); responsibility that follows actual control (UM/UKM, Game Developer A, Industry Group); protection for players who reach games outside official app stores (Academic Researcher, Industry Group); odds shown by tier or category (UM/UKM, Game Developer B); child-friendly reporting built into the game (UNICEF Malaysia, ECPAT Malaysia and CRCM, UM/UKM); and a review within 12 months (UNICEF Malaysia, UM/UKM, Academic Researcher).

The main differences are on method. The game developers ask for equivalent safeguards in place of fixed defaults for communication, Paid Randomised Reward Mechanisms, trading and gifting, spending controls and Personalised Advertising, and Industry Group for default settings and spending controls. UNICEF Malaysia, ECPAT Malaysia and CRCM, UM/UKM and Academic Researcher ask for firm defaults, and the questionnaire supports safe default settings (**89.6**%)**,** a default spending limit (**87.8%**), parental control of Paid Randomised Reward Mechanisms (88.5%) and the ban on targeted advertising to children (**89.7%**). On Paid Randomised Reward Mechanisms, UNICEF Malaysia and ECPAT Malaysia and CRCM ask for a prohibition on Child Accounts, Academic Researcher asks that they be off until a parent approves them, and Game Developer B asks that they be available with spending and parental controls. On responsibility for a child's spending, Academic Researcher proposes that the Developer, Publisher, seller and promoter be jointly responsible, while Game Developer A and Industry Group ask that each party answer only for what it controls.

08
Issues Requiring Further Consideration

The two areas most frequently selected for further work were **age checks and age ratings** and **children's account settings and parental controls** (**Chart 3**). Of the 305 respondents who answered this question, only **8.2%** said no major changes were needed. Respondents were asked to choose up to three areas, but the online form did not enforce the limit: 85 of the 305 chose more than three, so the shares in Chart 3 add up to more than 300%. *These results reflect selection frequency* rather than a consistently limited top-three ranking.

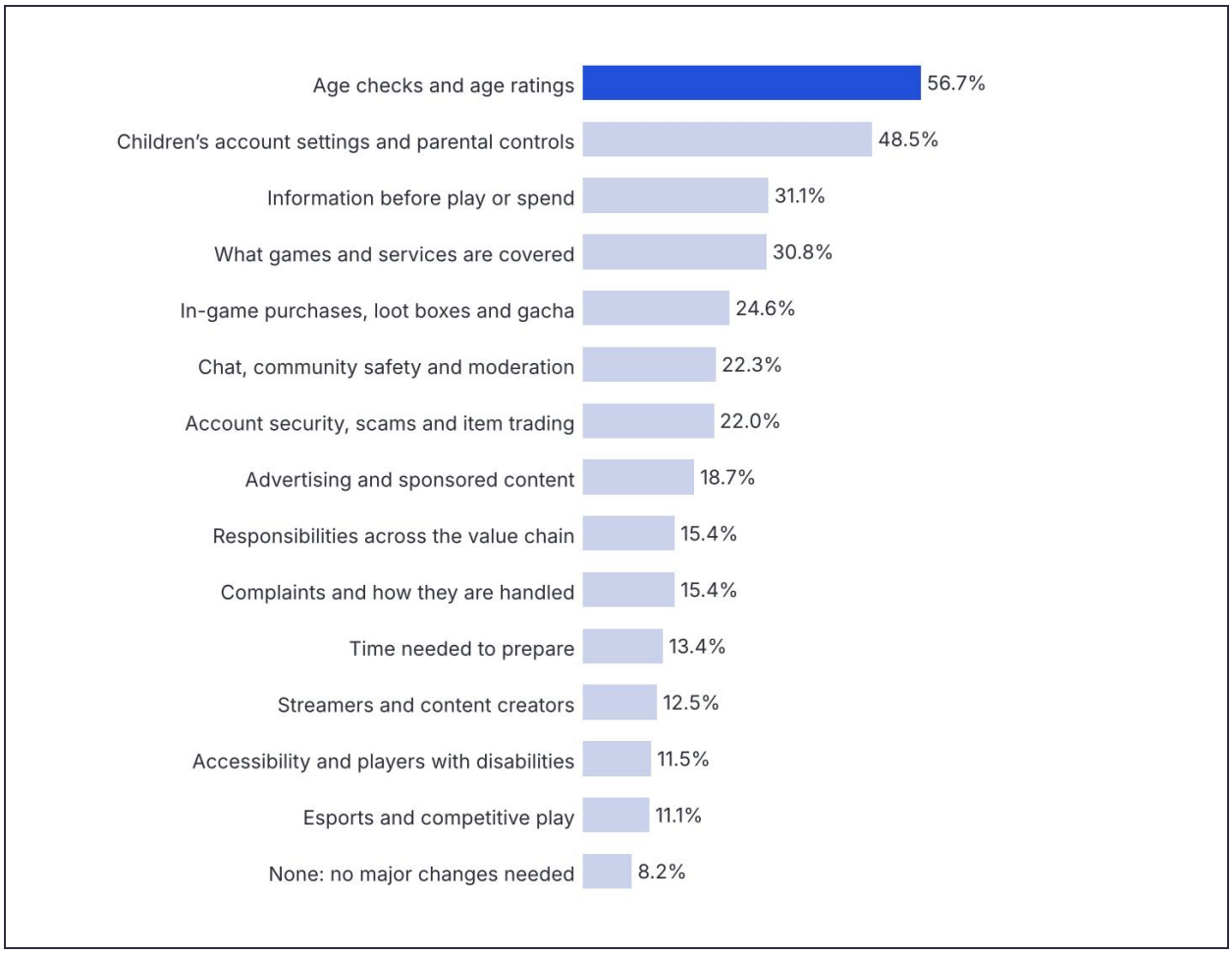


CHART 3 Areas Most Needing Further Work or Clarification (305 respondents; up to three choices requested, not enforced)

Of the 248 respondents who answered this question, leaving out those who answered only that it did not apply to them, the requirement most often selected as hardest to apply was **knowing when a stronger age check is required**, followed by relying on age signals from a platform, app store or console, and default settings for children's accounts (**Chart 4**). Appointing a safety contact and keeping risk assessments and records were selected least often. As with Chart 3, the limit of three was not enforced, and 60 of the 248 chose more than three.

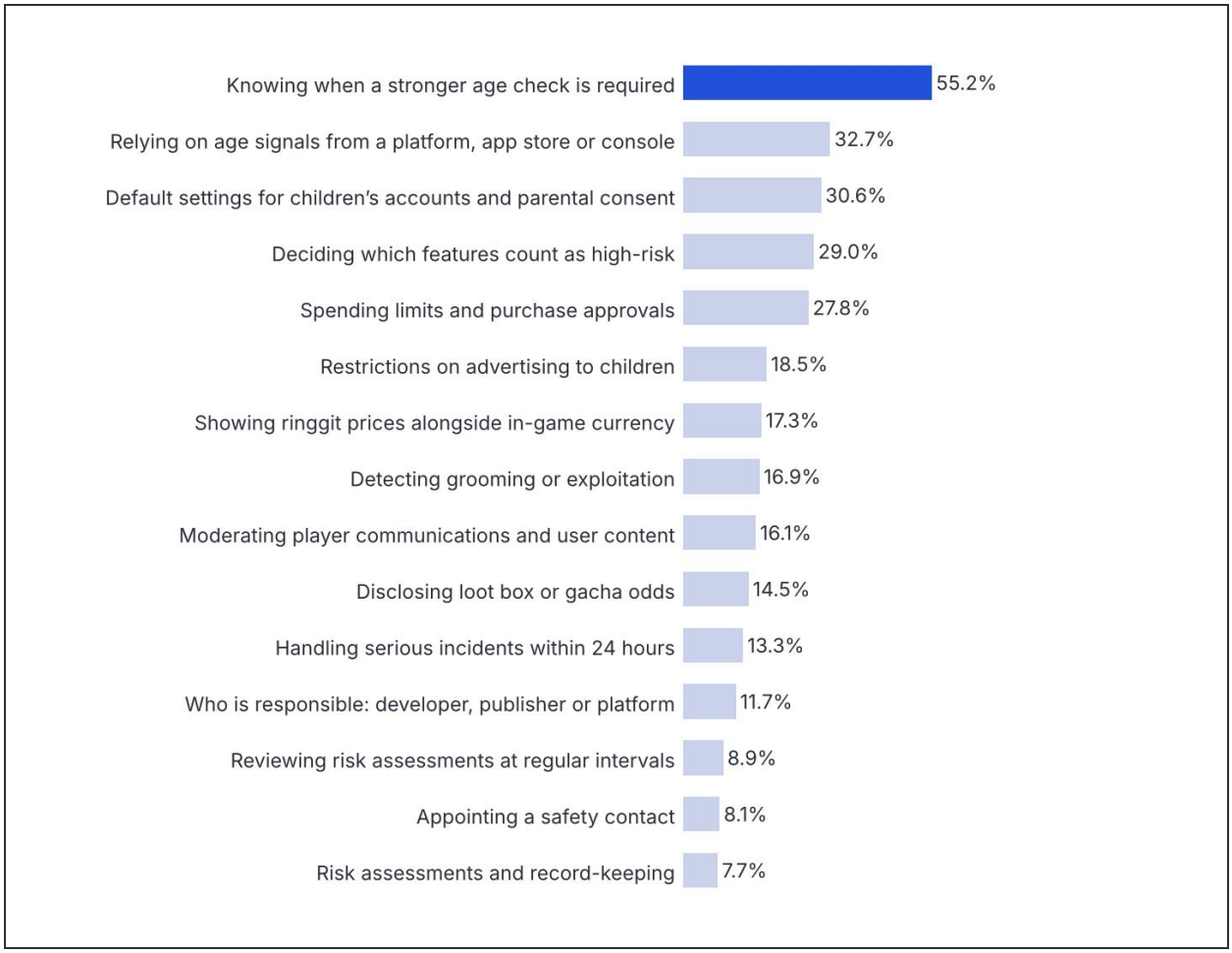


CHART 4 Requirements Hardest to Apply (248 respondents; up to three choices requested, not enforced)

Drawing the questionnaire findings and written submissions together, the following issues need deliberation by the Working Group before the Sub-Code is finalised. Most are questions of calibration and alignment rather than disagreement. The source of each is noted.

- **Children Without Identity Documents**

  How the Sub-Code should state the position of a child who has no identity documents, or does not wish to use them, including that such a child can still play on protective default settings, how a User moves off those settings, and how such a route is kept from being used to bypass protections. **Raised by:** questionnaire; UNICEF Malaysia; UM/UKM; Academic Researcher; IDEAS.

- **Content Categories and Thresholds**

  How the content categories used in risk assessment should be defined, when content presents a significant risk of serious harm, what counts as content that simulates gambling, whether existing age-rating classifications may be relied on, and whether the restriction on promoting age-restricted content should cover only content directed at children. **Raised by:** UNICEF Malaysia; Game Developer B; Industry Group.

- **Platform Age Signals and Shared Devices**

  When a game may rely on an age signal from a phone, console or app store, including where a child uses a parent's device; what standard age-check providers should meet; how much information a Platform should share with a game; and whether age should be re-checked during use. **Raised by:** questionnaire; UNICEF Malaysia; UM/UKM; Game Developer A; Game Developer B; Academic Researcher; IDEAS; Industry Group.

- **Privacy in Age Assurance**

  How to keep the personal data collected for age checks to a minimum and delete it promptly, whether government identity documents should be one method among several, and how methods are tested for accuracy and bias. **Raised by:** questionnaire; ECPAT Malaysia and CRCM; UNICEF Malaysia; UM/UKM; Game Developer A; Industry Group.

- **Teenagers' Settings and Parental Consent**

  Which settings 13 to 17 year olds may relax themselves, whether 13 to 15 and 16 to 17 year olds should be treated differently, whether links to other services and public profiles need a parent's consent, and whether voice chat with teammates during a match should be allowed. **Raised by:** questionnaire; UNICEF Malaysia; ECPAT Malaysia and CRCM; UM/UKM; Game Developer A; Game Developer B; Academic Researcher.

- **Equivalent Safeguards**

  Whether, and on what conditions, an Operator may meet the Sub-Code's outcomes through equivalent safeguards in place of fixed default settings. **Raised by:** Game Developer A; Game Developer B; Industry Group.

- **Paid Randomised Reward Mechanisms and Spending**

  How parental control of Paid Randomised Reward Mechanisms should work for children of different ages; whether one parental consent may cover both spending and Paid Randomised Reward Mechanisms for teenagers; how odds, including changing odds, are disclosed; whether spending notifications can stand in for a default spending limit; whether limits should be set in fixed figures by age; and how a default limit works where a parent approves each purchase. **Raised by:** questionnaire; UNICEF Malaysia; ECPAT Malaysia and CRCM; UM/UKM; Game Developer A; Game Developer B; Academic Researcher; Industry Group.

- **Personalised Advertising and In-Game Offers**

  Whether the ban on Personalised Advertising to children should cover data from any source, including inferred interests, and how it applies to a game's own in-game offers. **Raised by:** questionnaire; UNICEF Malaysia; UM/UKM; Game Developer A; Game Developer B.

- **Proportionality for Small Studios**

  How duties such as a safety contact, active monitoring and risk assessment scale to the size and risk of a service, whether thresholds should be set in guidance, and how a sufficiently high minimum standard is kept for all services. **Raised by:** questionnaire; UM/UKM; UNICEF Malaysia; Game Developer A; Game Developer B; Academic Researcher.

- **Allocation of Responsibility**

  How responsibility follows each party's role and control, or whether responsibility for a child's spending should be joint so that a parent may claim against any party, including tournament and venue organisers and Platform-level systems; how complaints that involve more than one party are handled; and the role and liability of the Gaming Safety Officer. **Raised by:** questionnaire; Game Developer A; UM/UKM; UNICEF Malaysia; Academic Researcher; Industry Group.

- **User Responsibilities**

  Whether Part 10 should place responsibilities on Users, who include children, or be removed. **Raised by:** Academic Researcher.

- **Reporting, Moderation and Incident Response**

  What a 24-hour response to a serious incident requires; when human review is needed; how reporting, temporary protection and graduated responses should work for children; how moderation handles local languages and harassment that moves to other apps; and how long Operators have to resolve a complaint before it may go to the Complaints Bureau. **Raised by:** questionnaire; Game Developer A; UM/UKM; UNICEF Malaysia; ECPAT Malaysia and CRCM; IDEAS; Industry Group.

- **Persons With Disabilities**

  How supervision of the account of a person with a disability can respect the person's autonomy, with supervision only by choice and safeguards against misuse, and whether Operators may decide not to offer supervised accounts. **Raised by:** questionnaire; Game Developer A; UNICEF Malaysia; Academic Researcher; Industry Group.

- **Transparency and Impact Assessments**

  Whether Operators should publish figures on reports and action taken or their impact assessments, which Operators this should apply to, and whether assessments under other regimes should be accepted. **Raised by:** questionnaire; UNICEF Malaysia; ECPAT Malaysia and CRCM; UM/UKM; Game Developer A; IDEAS; Industry Group.

- **Engagement Design and Generative AI**

  Whether the Sub-Code should address play-time, night-time notifications, penalties for not returning to a game, and generative AI features. **Raised by:** questionnaire; UNICEF Malaysia; ECPAT Malaysia and CRCM; UM/UKM; IDEAS.

- **Commencement, Transition and Review**

  How long companies should have to prepare, when and how the Sub-Code should be reviewed, and whether compliance and the effectiveness of the measures should be monitored. **Raised by:** questionnaire; UNICEF Malaysia; UM/UKM; Academic Researcher; Industry Group.

- **Scope and Excluded Services**

  Whether Operators should take reasonable steps, such as location checks, so that Users in Malaysia who install a foreign version of a game, including through APK files, still receive the Sub-Code's protections; and whether developer tools fall outside the Sub-Code. The

Sub-Code cannot impose obligations on APK stores or unregulated Platforms that are not members of the CMCF. Raised by: Academic Researcher; Industry Group.

- **Relationship With Other Laws**

  How the Sub-Code works alongside the Online Safety Act 2025 and the Child Protection Code, including its age rules, whether references to that Act should be removed or limited to context, and which other laws it should refer to. Whether Randomised Reward Mechanisms amount to gambling is a matter for the relevant authorities. **Raised by:** questionnaire; UNICEF Malaysia; UM/UKM; Game Developer A; Industry Group.

Support for Implementation

Respondents were clear about the support they need. Of the 227 who answered, leaving out those who answered only that it did not apply to them, the option most often selected was a plain-language summary for players and parents, followed by a checklist for developers, guidance on what counts as a proper age check and a template child safety risk assessment (**Chart 5**).

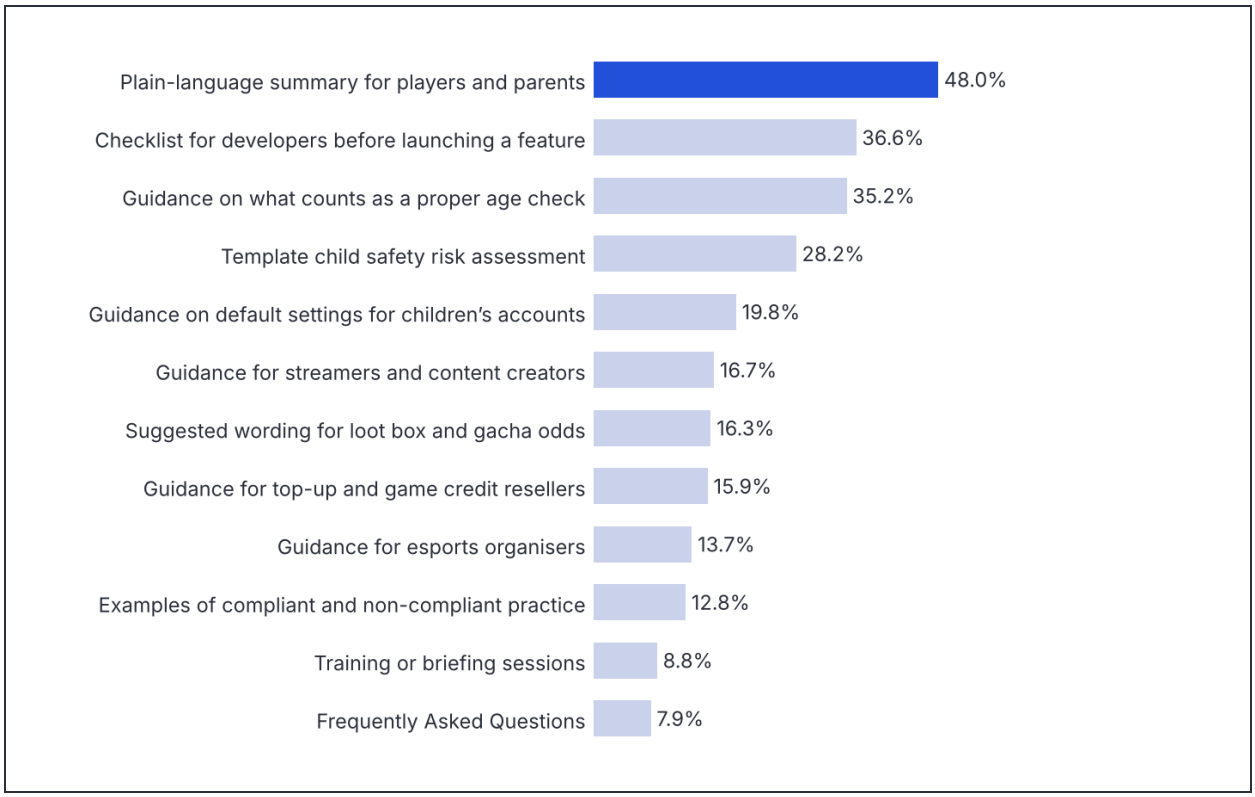


CHART 5 Practical Support Most Wanted (227 respondents; more than one choice allowed)

The CMCF intends to develop the following alongside the final Sub-Code: a plain-language summary for players and parents; a checklist for Developers; guidance on age checks and on default settings for Child Accounts; a template child safety risk assessment; guidance for streamers and content creators, top-up resellers and Esports organisers; and an FAQ, including on the legal status of the Sub-Code.

09
Proposed Next Steps

The Public Consultation confirms strong public support for the direction of the Sub-Code. The task now is to make the standards clearer where respondents found them uncertain, and easier to apply in practice.

Next Steps

- **Working Group Deliberation**

  The Working Group is considering the Public Consultation findings and written submissions, and how each issue in Section 08 should be resolved.

- **Final Draft**

  The CMCF will prepare the final draft of the Sub-Code reflecting the Working Group's decisions.

- **Submission and Registration**

  The final draft will be submitted to the Commission for registration under the Communications and Multimedia Act 1998.

- **Consultation Outcomes**

  When the final Sub-Code is released, the CMCF will publish a summary of the main changes made in response to the Public Consultation.

- **Implementation Support**

  The CMCF will publish the implementation materials described in Section 08, and the Sub-Code will allow time to prepare before it fully applies.

- **Awareness**

  The CMCF will hold awareness and briefing sessions for Developers, Publishers, Platforms, creators, parents and players once the Sub-Code is published.

Acknowledgement

The CMCF thanks everyone who took the time to respond to this Public Consultation: players and members of the public, parents, educators, game developers and esports organisations, platforms, creators, government agencies, academics, students and civil society organisations. We are particularly grateful to UNICEF Malaysia, ECPAT Malaysia, CRCM and the OCSEA Working Group, Universiti Malaya and Universiti Kebangsaan Malaysia, the Institute for Democracy and Economic Affairs (IDEAS), the two game developers, the academic researcher and the four game companies that made a joint submission, for their detailed written submissions, and to the universities, programmes and partners who hosted and supported the engagement sessions.

Their input will help ensure that the final Sub-Code is clear, practical and worthy of the trust that players and parents place in online games.

10
Appendices

Appendix A: Summary of Questionnaire Findings

The table below sets out the level of agreement with each statement and scenario in the questionnaire, grouped by the Consultation Questions in the PC Paper. Figures are shares of the respondents who answered each statement, shown in the column "n". Question 8 was answered through Scenario G, reported in Section 06. "Agree" combines strongly agree and agree; "Disagree" combines disagree and strongly disagree; "Neutral" is neither agree nor disagree. Rows may not total exactly 100% because of rounding. Clause references are to the draft released for the Public Consultation.

Statement or scenario	Draft provision	n	Agree	Neutral	Disagree	Not sure
Question 1: Overall Approach						
Malaysia would benefit from clear standards for games	Part 1, Objectives	316	88.3%	4.7%	3.5%	3.5%
The Sub-Code is clear enough to understand	Whole draft	306	82.4%	8.8%	3.6%	5.2%
Strikes the right balance between protection and industry growth	Part 1, cl. 2.2	309	87.4%	4.9%	4.2%	3.6%
Requirements proportionate to risk and size	Part 2, cl. 2.9; Part 3, cl. 2.2(c); Part 9, cl. 4.3	312	87.2%	7.4%	2.6%	2.9%
Question 2: Checking a Player's Age						
Typing a birthday is not enough for risky features	Part 3, cl. 2.4	306	83.7%	6.5%	6.9%	2.9%
A game may rely on an age check by the phone, console or app store	Part 3, cl. 2.5	314	68.8%	8.6%	19.7%	2.9%
Show a recognised age rating before download or purchase	Part 3, cl. 1.1, 1.3	310	89.7%	5.8%	1.9%	2.6%
The rating should show what the game contains	Part 3, cl. 1.2	313	88.5%	6.7%	1.6%	3.2%
Unchecked accounts treated as a child's by default	Part 3, cl. 2.13–2.14	313	81.2%	8.0%	8.6%	2.2%
Age-check providers must meet a recognised standard	Part 3, cl. 2.5	312	90.1%	5.4%	1.9%	2.6%

Statement or scenario	Draft provision	n	Agree	Neutral	Disagree	Not sure
Alternative route for children without identity documents	No express provision	316	66.1%	11.1%	17.1%	5.7%
Question 3: Children's Accounts and Parental Controls						
Children's accounts start with the safest settings	Part 3, cl. 3.8	307	89.6%	4.9%	2.9%	2.6%
Teenagers aged 13 to 17 may relax lower-risk settings themselves	Part 3, cl. 3.9	311	80.7%	6.8%	8.4%	4.2%
A parent can reinstate any setting at any time	Part 3, cl. 3.10	311	81.7%	8.7%	6.8%	2.9%
Parental controls easy to find and use	Part 3, cl. 3.3–3.4	312	87.5%	6.1%	2.6%	3.8%
Children can join organised esports with parental consent	Part 3, cl. 5.1–5.2	311	86.8%	6.4%	2.6%	4.2%
A parent may supervise the account of a person with a disability	Part 3, cl. 3.11	308	77.3%	11.7%	5.2%	5.8%
Question 4: Spending, Randomised Rewards and Virtual Currency						
Show real ringgit cost, recurrence, expiry and effect before purchase	Part 5, cl. 1.1–1.3	307	90.6%	3.6%	2.3%	3.6%
Scenario D: ringgit shown next to virtual currency	Part 5, cl. 1.4	310	88.7%	6.5%	2.6%	2.3%
Loot box and gacha odds shown before payment	Part 5, cl. 2.1(b), 2.3(a)	313	88.2%	6.1%	2.6%	3.2%
Parents can switch off or limit paid loot boxes	Part 5, cl. 2.3(c)	313	88.5%	5.8%	2.9%	2.9%
Default spending limit on children's accounts, raised only by a parent	Part 5, cl. 3.4	312	87.8%	6.1%	2.6%	3.5%
A parent can require approval for every purchase	Part 5, cl. 3.2; Part 3, cl. 3.3(h)	314	87.6%	7.6%	2.2%	2.5%
No countdown timers or pressure tactics aimed at children	Part 5, cl. 3.5–3.6	311	83.6%	8.7%	3.9%	3.9%
Top-up resellers clear on price and mindful of the buyer	Definition only; no express obligation	312	85.9%	7.1%	3.8%	3.2%
Question 5: Advertising and Creator Promotions						
In-game advertising clearly recognisable	Part 6, cl. 1.3	313	88.8%	5.1%	1.9%	4.2%

Statement or scenario	Draft provision	n	Agree	Neutral	Disagree	Not sure
No targeted advertising using a child's data	Part 6, cl. 2.3	311	89.7%	5.5%	0.6%	4.2%
Rewards for watching adverts clearly disclosed	Part 6, cl. 3.1–3.2	314	89.2%	6.4%	1.9%	2.5%
Scenario E: streamer discloses sponsorship and real odds	Part 6, cl. 4.1–4.2	315	87.6%	7.3%	1.6%	3.5%
Ad-funded free games may show more adverts	Part 6, cl. 2.4	314	79.6%	10.5%	5.4%	4.5%
Question 6: Talking to Other Players						
Clear community rules for games with chat	Part 7, cl. 1.1–1.2	313	89.5%	5.8%	2.2%	2.6%
Mute, block and report easy to reach during play	Part 7, cl. 2.2(a), 3.4	312	88.8%	6.7%	2.2%	2.2%
Scenario F: player told the outcome of a report	Part 7, cl. 3.5	313	88.8%	7.3%	0.6%	3.2%
Games actively look for signs of grooming	Part 7, cl. 2.2(i)	310	89.0%	6.5%	1.9%	2.6%
Responsibility for off-platform communities depends on control	Part 7, cl. 2.4–2.5	311	83.9%	8.7%	2.9%	4.5%
Question 7: Accounts, Safety and Complaints						
Protect against account theft and scams; alert players	Part 8, cl. 1.1–1.3	304	91.1%	6.2%	0.0%	2.6%
Think about safety when designing a feature	Part 9, cl. 2.1	312	89.7%	6.1%	0.3%	3.8%
Re-check safety risks periodically	Part 2, cl. 2.10; Part 9, cl. 2.3	311	90.4%	4.8%	1.0%	3.9%
Named safety contact for games with player communication	Part 9, cl. 4.1–4.3	312	84.6%	8.7%	2.2%	4.5%
Unresolved complaints may go to the Content Forum	Part 11, cl. 2.1	313	88.8%	6.1%	1.3%	3.8%
Publish regular figures on reports and action taken	No express provision	308	84.7%	10.1%	1.0%	4.2%
Question 9: Implementation, Thresholds and Review						
Companies given time to prepare before full effect	No transitional provision	310	83.2%	8.1%	1.6%	7.1%
Specific figures set in separately updatable guidance	Part 5, cl. 3.4(b); Part 9, cl. 4.3(d)	309	80.6%	11.3%	2.9%	5.2%

Statement or scenario	Draft provision	n	Agree	Neutral	Disagree	Not sure
Review within a year, then regularly	No express review provision	310	86.1%	9.0%	1.0%	3.9%

TABLE 2 Agreement with Each Statement and Scenario

Appendix B: Points Raised in Written Submissions

The table below lists each of the 242 points raised in the written submissions and the provision of the draft it concerns. The points are recorded as made and will be considered by the Working Group before the Sub-Code is finalised. For the joint submission from ECPAT Malaysia and CRCM, only the points on the Sub-Code are listed. Both game developers commented on an earlier draft; their points are shown against the corresponding provision of the draft released for the Public Consultation. The two game developers, the academic researcher and the four companies that made the joint industry submission are not named.

Ref.	Point raised	Draft provision
UNICEF Malaysia		
UNI-1	Recognise children's rights to privacy, to have their views given due weight, and to healthy development through play in the General Principles.	Part 1, cl. 2.5–2.6
UNI-2	Define "likely to be accessed by children" by whether children are reasonably foreseeable Users, drawing on the factors in the PC Paper.	Part 1, cl. 5.1
UNI-3	Turn protections framed as "assess whether" or "review whether" into clear expectations. Proportionality should shape how risks are addressed, not whether.	Part 2, cl. 3.4; Part 5, cl. 2.4, 3.3; Part 6, cl. 2.5, 3.3
UNI-4	Apply a baseline of protection wherever High-Risk Features are likely to be accessed by children, whatever the size of the service or its stated age limit.	Part 2, cl. 2.9, 3.3
UNI-5	Define the content categories precisely, in particular "mature or adult themes", so that they do not lead to over-restriction of age-appropriate information.	Part 2, cl. 2.5(g), 2.6
UNI-6	Retain the core Age Assurance framework, including Highly Effective Age Assurance, the rule against self-declaration alone, equal assurance across access routes and child defaults for unassured accounts.	Part 3, cl. 2.3–2.5, 2.11, 2.13–2.14, 2.16
UNI-7	Confirm that "any other information reasonably available" includes in-game indicators that an account may belong to a Child, without requiring more data collection.	Part 1, cl. 5.1
UNI-8	Recognise Age Assurance providers only where they meet standards such as ISO/IEC 27566-1:2025 and IEEE 2089.1-2024, are independently tested, and publish key findings of their impact assessments.	Part 1, cl. 5.1
UNI-9	Where only an age range is known, apply the settings for the youngest age in that range.	Part 3, cl. 2.16
UNI-10	Use Age Assurance data only for that purpose and delete it promptly.	Part 3, cl. 2.10
UNI-11	Offer alternatives such as age estimation or vouching by a parent, guardian or trusted institution to children without government-issued documents. Where none is available, apply Child Account defaults rather than exclude the child.	Part 3, cl. 2.13–2.14
UNI-12	Provide a clear and accessible way to challenge an incorrect age assessment.	Part 3, Section 2.0

Ref.	Point raised	Draft provision
UNI-13	Evaluate periodically whether Age Assurance methods still meet the accuracy, robustness, reliability and fairness criteria.	Part 3, cl. 2.3
UNI-14	Clarify how ratings will be presented where recognised classification frameworks apply different minimum ratings.	Part 3, cl. 1.1, 1.6
UNI-15	Make disclosure of High-Risk Features mandatory wherever a Gaming Service has them.	Part 4, cl. 1.1–1.3
UNI-16	Make the duty to stop unknown adults contacting Child Accounts a clear obligation covering messages, friend requests and invitations, and expect the contact safeguards wherever children are likely to access interaction features.	Part 3, cl. 3.6, 4.2
UNI-17	Define "Established Contact" so that a stranger does not become one by an accepted friend request, and apply cooldowns before new accounts can contact Child Accounts.	Part 3, cl. 3.8(b)
UNI-18	Keep public profiles and third-party links off by default for 13 to 17 year olds unless a parent gives verified consent.	Part 3, cl. 3.8(e)–(f), 3.9; Part 2, cl. 3.2
UNI-19	Consider distinct account types by age or developmental stage rather than a single threshold at 13.	Part 3, Section 3.0
UNI-20	Notify parents of significant safety changes, such as new friend connections, and protect parental controls with a PIN or equivalent.	Part 3, cl. 3.3–3.4
UNI-21	Actively introduce parents to parental controls and core safety settings at account creation, in accessible formats and languages, and give children safety onboarding.	Part 3, cl. 3.5, 3.12
UNI-22	Switch off, or do not use on Child Accounts, mechanics that penalise children for not returning, such as streaks, loss of progress and expiring rewards.	Part 3, cl. 3.8; Part 14, cl. 5.1(i)
UNI-23	Commit to safeguarding guidance for youth Esports covering rest and schooling and, where children earn income, the Children and Young Persons (Employment) Act 1966.	Part 3, cl. 5.3
UNI-24	Ensure supervised-account arrangements for children with disabilities respect their views, dignity and evolving capacities.	Part 3, cl. 3.11
UNI-25	Prohibit Paid Randomised Reward Mechanisms on Child Accounts, removing the parental consent option, and prohibit their promotion in ways likely to appeal to children.	Part 3, cl. 2.14, 3.8(c), 3.9
UNI-26	If parental consent is kept, require disclosure of odds that change after repeated attempts.	Part 5, cl. 2.3(a)
UNI-27	Extend the ban on manipulative purchase design to artificial scarcity and prompts that encourage children to ask adults to buy items.	Part 5, cl. 3.5
UNI-28	Show the ringgit equivalent beside every Virtual Currency price, let Users buy only the currency they need, and avoid bundles that leave unusable balances.	Part 5, cl. 1.4
UNI-29	Retain the default spending limit, set conservatively, with parental approval of each purchase as an additional safeguard.	Part 5, cl. 3.4
UNI-30	Require confirmation and authentication before stored-payment purchases, a simple refund route for unauthorised purchases, and no account lock over a good-faith payment dispute.	Part 5, cl. 3.2–3.3

Ref.	Point raised	Draft provision
UNI-31	Make clear that the default restriction on trading and gifting also stops Child Accounts receiving gifts. Where enabled with consent, limit gift value and frequency, restrict gifts from new accounts and detect suspicious patterns.	Part 2, cl. 3.2(c)
UNI-32	Delete clause 4.5, which duplicates clause 4.1 and frames it as an aspiration.	Part 5, cl. 4.5
UNI-33	Do not use pay-to-progress or pay-to-win mechanics on Child Accounts, or make social participation or belonging depend on paid content.	Part 5
UNI-34	Place proportionate obligations on Third-Party Virtual Currency Resellers: clear pricing, age-appropriate sale of high-value top-ups, fraud prevention, complaints and cooperation on refunds.	Part 1, cl. 5.1; Part 5
UNI-35	Align the ban on Personalised Advertising with its definition so that it covers personal data from any source, including inferred characteristics.	Part 6, cl. 2.3
UNI-36	Do not extend the free-to-play advertising exemption to Child Accounts without age-appropriate frequency limits and restrictions on rewarded advertising.	Part 6, cl. 2.4
UNI-37	Name alcohol, tobacco and vaping products, firearms and unhealthy food among products that advertising accessible to children should not promote.	Part 6, cl. 2.2(f)
UNI-38	Clearly mark all advertising, rewarded advertising, product placement, branded items and sponsored modes on Child Accounts.	Part 6, cl. 1.3, 3.4
UNI-39	Keep creator promotion consistent with the Influencer Guidelines, and require Operators and Publishers to pass the game's code of conduct to the creators they engage.	Part 6, cl. 4.1, 4.3
UNI-40	Detect, remove and report known child sexual abuse material, including through hash-matching. Keep any wider detection defined, necessary and proportionate, with particular care for private communications.	Part 7, cl. 2.2(i)
UNI-41	Moderate in the languages children use on the service, supported by human moderators with local knowledge.	Part 7, cl. 1.4, 3.2
UNI-42	Evaluate detection tools, including for bias; limit them to child-safety purposes; and have a human review flagged content before action that significantly affects a child, with an accessible appeal.	Part 7, cl. 2.2(i), 3.3
UNI-43	Use layered moderation across text, voice, gameplay, usernames, avatars and User-generated Content.	Part 7, Section 2.0
UNI-44	Respond to children who break rules with restorative, graduated and appealable measures.	Part 7, cl. 3.3; Part 9, cl. 5.2
UNI-45	Detect banned Users who re-register, and support cross-industry signal sharing consistent with data protection law.	Part 7, Section 2.0
UNI-46	Do not direct Child Accounts to external communities without equivalent protections.	Part 7, cl. 2.2(g), 2.4–2.5
UNI-47	Address identity-based harms in community standards, monitor disproportionate harm or sanctions, and test protections with diverse children.	Part 7, cl. 1.2; Part 3, cl. 3.5

Ref.	Point raised	Draft provision
UNI-48	Include generative AI features in the Child Safety Risk Assessment, with pre-deployment testing, prevention of harmful or sexualised content, disclosure when a child is interacting with AI, and labelling of AI content that may resemble real people.	Part 9, cl. 2.3
UNI-49	Do not make AI features that may foster emotional dependency, give harmful advice or encourage self-harm available to Child Accounts unless shown to be safe.	Part 9, cl. 2.3–2.4
UNI-50	Specify what counts as Prior Moderation of User-generated environments, and keep detecting harmful environments after publication.	Part 2, cl. 3.2(e)
UNI-51	Confirm that voice in immersive environments, avatar proximity and private virtual spaces are High-Risk Features.	Part 2, cl. 3.2(a), 3.5
UNI-52	Retain Safety-by-Design and address foreseeable risks to children before features are deployed and throughout the life of the service.	Part 9, cl. 2.1
UNI-53	Broaden the risk assessment into a child rights impact assessment, informed by children's views, with guidance on scope and method.	Part 9, cl. 2.3
UNI-54	Require mitigation matched to the risks identified, measure the real-world effect of safeguards, and require services with a significant child User base to publish a summary of assessment outcomes.	Part 9, cl. 2.1, 2.3
UNI-55	Require larger Operators and Platforms to report periodically on child Users, Age Assurance, default settings, parental-control uptake, detection, reports, response times and referrals.	Part 9
UNI-56	Require the Gaming Safety Officer to have child-protection competence and authority to act.	Part 9, cl. 4.1, 5.2
UNI-57	Make reporting free, built into play, in child-friendly language, confidential and non-retaliatory, with no evidence demanded of children, bystander reporting, reference numbers, timeframes and outcome updates.	Part 7, cl. 3.1, 3.4–3.5
UNI-58	Explain why content or accounts are restricted, offer review by a different reviewer, and tell Users about external routes to remedy.	Part 7, cl. 3.3
UNI-59	Confirm that children, caregivers and representatives may go directly to the Complaints Bureau where engaging the Operator first is unsafe, impractical or likely to delay protection.	Part 11, cl. 2.1
UNI-60	Connect children in distress with support, including national helplines.	Part 9, cl. 5.2(e)
UNI-61	Do not penalise children for reporting harm, even if they breached rules or circumvented controls.	Part 7, Section 3.0
UNI-62	Adopt a "no wrong door" principle: a participant receiving a complaint about a child's safety or spending acts on its part and refers the rest promptly.	Part 9, cl. 1.4; Part 11
UNI-63	Contracts between participants may allocate, but should not extinguish, responsibility for design, monetisation, purchase authorisation, refunds and promotion.	Part 9, cl. 1.3–1.4

Ref.	Point raised	Draft provision
UNI-64	Explain how the Sub-Code relates to the Online Safety Act 2025, the Child Protection Code and the Risk Mitigation Code, including which services are licensed and how the age-13 thresholds sit with under-16 registration requirements.	Part 1, cl. 6.4–6.5
UNI-65	Refer also to the Sexual Offences Against Children Act 2017, the Children and Young Persons (Employment) Act 1966 and consumer protection law.	Part 1, cl. 6.4
UNI-66	Consult on and publish guidance before obligations take effect.	General
UNI-67	Resource the Complaints Bureau with relevant expertise, including children's rights, enable it to monitor compliance, and consult children on guidance.	Part 11
UNI-68	Conduct a first review within 12 months and regularly after, informed by transparency reports, complaints and children's views.	New provision
ECPAT Malaysia and CRCM, with the OCSEA Working Group		
ECP-1	Define and prohibit technology-facilitated gender-based violence and misogynistic behaviour, including emotional abuse, gender policing and voice shaming, and misogynistic slurs.	Part 7, cl. 1.2
ECP-2	Provide positive, supportive default emotes and team communication prompts that help young players counter toxic behaviour.	Part 7, cl. 1.4
ECP-3	Default Child Accounts to the highest privacy settings, disabling public profile indexing, precise location tracking and unsolicited messages from unknown players.	Part 3, cl. 3.8
ECP-4	Prohibit Paid Randomised Reward Mechanisms and Dark Patterns that exploit children's developing impulse control.	Part 5, Section 2.0; cl. 3.5
ECP-5	Show real-world currency equivalents alongside Virtual Currencies at every step of a transaction.	Part 5, cl. 1.4
ECP-6	Prohibit features that promote addiction, such as infinite loops, non-essential late-night notifications and visibility-based rewards that pressure children for peer approval.	Part 3, cl. 3.8; Part 9, cl. 2.4
ECP-7	Make reporting child-friendly and trauma-informed, appropriate to age and gender, accessible to children with disabilities and from marginalised communities, with minimal steps.	Part 7, cl. 3.4
ECP-8	Build reporting directly into the gameplay interface, in an interactive, low-bandwidth and age-appropriate flow.	Part 7, cl. 3.4
ECP-9	Use moderation tools and prompts that recognise grooming, bullying and child sexual abuse material, and connect at-risk players to national child protection and referral pathways.	Part 7, cl. 2.2(i); Part 9, cl. 5.2
ECP-10	Offer immediate self-protection tools, such as mutual mute, session isolation and temporary screen blur, while a report is reviewed.	Part 7, cl. 3.3–3.4
ECP-11	Give children who submit reports status updates in child-friendly language.	Part 7, cl. 3.5
ECP-12	Use a staged warning system with educational moments for young players, rather than blanket bans or immediate account termination.	Part 7, cl. 3.3

Ref.	Point raised	Draft provision
ECP-13	Require Platforms and game Publishers to conduct and publicly disclose child rights impact assessments before designing games, algorithms, monetisation models or campaigns aimed at children.	Part 9, cl. 2.3
ECP-14	Apply strict data minimisation to data collected for Age Assurance or safety, with a maximum retention period of two years and strong encryption.	Part 3, cl. 2.10
ECP-15	Require cooperation with national child protection mechanisms, social work networks and frontline responders to support child victims, using trauma-informed methods.	Part 9, cl. 5.2(d)–(e)
ECP-16	Co-design safety guidance with diverse children, young people, parents, child rights organisations and experts, including child-friendly versions of the Sub-Code.	General
Universiti Malaya and Universiti Kebangsaan Malaysia (UM/UKM)		
UMK-1	Adopt four feature-based risk tiers, from low risk to services combining several High-Risk Features or professional Esports involving children, with a common baseline of child protection.	Part 2, cl. 2.9
UMK-2	Let company size set the method and burden of compliance, not the minimum level of child protection, with a simplified route for small Operators.	Part 2, cl. 2.9; Part 9, cl. 4.3
UMK-3	Provide a free compliance pack for small Operators and gaming cafés, and use SME Corporation Malaysia definitions, with any micro-Operator threshold defined separately.	General
UMK-4	For High-Risk Features, do not rely on self-declared age alone. Providers should return only the minimum age band needed, and Operators should not receive or keep full identity documents.	Part 3, cl. 2.4–2.5, 2.10
UMK-5	Allow Operators to rely on qualifying age signals from Platforms, consoles or app stores rather than repeat identity collection.	Part 3, cl. 2.5
UMK-6	Where age cannot be assured, keep the account in child-safe mode without access to High-Risk Features.	Part 3, cl. 2.13–2.14
UMK-7	Provide an alternative route for children without identity documents, such as school, UNHCR or welfare-agency documents or verification by a responsible adult, with anti-fraud controls.	Part 3, cl. 2.2(b), 2.10
UMK-8	Provide a correction and appeal route where a User is placed in the wrong age band.	Part 3, Section 2.0
UMK-9	Specify the required outcome and assurance level rather than a particular provider.	Part 3, cl. 2.5
UMK-10	Default Child Accounts to contacts-only communication, non-public profiles, blocked external links and protective monetisation settings, with paid randomised-reward prompts and personalised re-engagement notifications off.	Part 3, cl. 3.8
UMK-11	Extend parental controls to spending, communications, privacy, play time, reporting history and High-Risk Features, accessible to Users with disabilities, with standard notices in Bahasa Malaysia and English.	Part 3, cl. 3.3–3.5
UMK-12	Provide break prompts and tools to manage continuous play, with any fixed duration set in guidance.	Part 3, cl. 3.3(a)

Ref.	Point raised	Draft provision
UMK-13	Before parents consent to a child joining a tournament, show the prize structure, entry fee, communication environment, adult participation, livestreaming and valuable items involved.	Part 3, Section 5.0
UMK-14	Show the real-money value, recurrence, expiry, restrictions and gameplay effect before payment, with a clear real-money equivalent for Virtual Currency.	Part 5, cl. 1.1–1.4
UMK-15	Disclose the probability of each material reward category before payment and prohibit misleading odds; let parents disable Paid Randomised Reward Mechanisms and require approval for purchases.	Part 5, cl. 2.3
UMK-16	Apply a default spending limit to Child Accounts, with the amount set in guidance; parents may lower it, and increases need verified parental authorisation.	Part 5, cl. 3.4
UMK-17	Prohibit Dark Patterns directed at children, including false urgency, “last chance” pressure, social exclusion and status pressure, hidden recurring charges, confusing conversions and countdown timers.	Part 5, cl. 3.5–3.6
UMK-18	For Esports involving children, disclose entry fees and prize conditions, do not replace an advertised prize with a Randomised Reward Mechanism, and set rest and fatigue standards with the relevant ministry.	Part 3, Section 5.0
UMK-19	Assess additional risks where virtual items can be transferred, sold or cashed out, and apply stronger disclosure, parental controls and fraud prevention to cash-convertible items.	Part 2, cl. 3.2(c); Part 5, Section 4.0
UMK-20	Whether a Randomised Reward Mechanism is gambling should depend on its structure, consideration and convertibility, not on randomness alone.	Part 5, Section 2.0
UMK-21	Disclose sponsored creator content upfront in the language of the promotion and repeat it in livestreams; consider a standard disclosure label.	Part 6, cl. 4.1
UMK-22	Prohibit Personalised Advertising to Child Accounts using data collected or inferred within the service, and commercial messages that exploit fear, shame, exclusion or inexperience; creators should not misrepresent odds.	Part 6, cl. 2.3, 4.2
UMK-23	Keep mute, block, restrict and report available during play, with specific reporting routes for sexual harassment, grooming, solicitation, threats and doxxing.	Part 7, cl. 2.2(a), 3.4
UMK-24	Use proportionate automated detection with human review for grooming indicators, consider gendered patterns of abuse in risk assessments, and actively moderate open-lobby tournaments involving children.	Part 7, cl. 2.2(i), 3.3
UMK-25	Provide one visible complaint entry point with three priority levels: critical child-safety reports acknowledged within two hours and triaged with protective action within 24 hours; urgent account or financial harm within 48 hours; and other issues within seven days.	Part 9, cl. 5.2; Part 11
UMK-26	Do not suspend or disadvantage a child for a good-faith safety report; preserve evidence; and notify parents where this would not increase risk.	Part 7, cl. 3.3–3.5

Ref.	Point raised	Draft provision
UMK-27	Publish aggregate figures on child-safety reports, response times, action taken and repeat-abuse trends, without personal data.	Part 7
UMK-28	Allocate responsibility by actual control across Platforms, Publishers, Developers, creators and tournament organisers, behind a single front door for complaints, without creating new strict civil liability.	Part 9, cl. 1.3–1.4
UMK-29	Phase implementation: high-risk obligations within six months for large or high-risk services, and the rest within twelve months for smaller Operators, with support.	New provision
UMK-30	Review the Sub-Code within twelve months of registration and periodically after.	New provision
UMK-31	Test Age Assurance for accuracy, including across demographic groups, provide a simple way to challenge a result, and do not restrict Users on an automated decision that cannot be reviewed.	Part 3, Section 2.0
UMK-32	Do not use data collected for Age Assurance, parental controls or safety for advertising or monetisation.	Part 3, cl. 2.10; Part 6, cl. 2.3
UMK-33	Cover engagement features such as streaks, time-limited reward loops and re-engagement notifications in risk assessments for child Users.	Part 9, cl. 2.3–2.4
UMK-34	Allow a qualifying age signal to be reused across services: verify once and disclose only the minimum age attribute.	Part 9, cl. 3.4
UMK-35	Pilot novel mechanisms such as privacy-preserving age tokens in a regulatory sandbox before finalising requirements.	General
Game Developer A		
GDA-1	Where the Sub-Code and the Content Code address the same gaming-specific matter, read them consistently and apply the more specific Sub-Code provision.	Part 1, cl. 6.4
GDA-2	Delete the clause on the Online Safety Act 2025 and its codes, or state that the references are for context only and do not import or extend obligations.	Part 1, cl. 6.5
GDA-3	State that excluding a service from the Sub-Code does not affect other applicable law.	Part 2, cl. 1.4
GDA-4	Require Highly Effective Age Assurance by reference to the risk remaining after safeguards, not automatically because particular content or a High-Risk Feature is present.	Part 2, cl. 2.7
GDA-5	Limit duties on access routes to those within the Operator's reasonable control, allow reliance on upstream age signals without repeat checks, and assess anti-circumvention by reasonable measures.	Part 3, cl. 2.11–2.13, 2.15–2.16
GDA-6	Replace "deemed to be High-Risk Features" with characteristics that may indicate heightened risk, assessed holistically, including existing safeguards and residual risk.	Part 2, cl. 3.2; definition of High-Risk Feature
GDA-7	Do not require communication features to be switched off for a group of Child Accounts where age-based restrictions, parental controls, reporting and moderation give equivalent protection.	Part 3, cl. 4.1–4.3; Part 7, cl. 2.1–2.3

Ref.	Point raised	Draft provision
GDA-8	Where games on a service are made by other creators, require reassessment only for changes within the Operator's control, with creator-level changes handled through declarations, tools and moderation.	Part 2, cl. 2.10; Part 3, cl. 1.5
GDA-9	Replace mandatory uniform default settings with an outcome-based duty that allows a combination of safeguards giving equivalent protection.	Part 3, cl. 3.8–3.10
GDA-10	Replace the default spending limit with a combination of limits, approvals, notifications, authentication or equivalent controls, with Verified Parental Consent to relax any control and no Dark Patterns.	Part 5, cl. 3.4
GDA-11	Replace the ban on Personalised Advertising to Child Accounts with age-appropriate safeguards consistent with other Malaysian law, which has no equivalent ban for comparable online services.	Part 6, cl. 2.3
GDA-12	Use a targeting-based test for marketing age-restricted content, and treat incidental display of age-appropriate thumbnails or classification information as compliant.	Part 2, cl. 2.8
GDA-13	Make supervised-account arrangements for persons with a disability optional where proportionate and feasible, with safeguards against misuse, impersonation and inappropriate access.	Part 3, cl. 3.11
GDA-14	Apply the functional-control principle throughout the Sub-Code when a requirement is shared among participants.	Part 9, cl. 1.3–1.4
GDA-15	Allow reassessment within a period proportionate to the change, with thirty days as a benchmark, and accept equivalent assessments under recognised frameworks.	Part 9, cl. 2.3
GDA-16	State that the Gaming Safety Officer performs a coordination and contact role and is not personally liable by designation alone.	Part 9, cl. 4.1; definition of Gaming Safety Officer
GDA-17	Treat the 24-hour requirement as acknowledgement and initial risk-based triage; investigation and resolution may take longer.	Part 9, cl. 5.2(a)
GDA-18	Where a Platform applies an age signal centrally, treat that as making it available; limit any shared signal to the age band or eligibility outcome.	Part 9, cl. 3.4
GDA-19	Read emotional harm, social exclusion and similar concepts as reasonably foreseeable and material harm.	Part 14, cl. 4.0
GDA-20	Assess excessive advertising by frequency, duration, placement and the service's monetisation model.	Part 14, cl. 5.1
GDA-21	Require corrective advertising only for material deception or serious non-compliance, after notice and an opportunity to respond, in proportion and according to control.	Part 14, cl. 7.1
GDA-22	Focus price transparency on the point where money is exchanged for Virtual Currency, rather than a ringgit equivalent for every transaction in Virtual Currency.	Part 5, cl. 1.4
GDA-23	Do not require parental approval of every purchase or a default spending limit; offer configurable spending notifications instead.	Part 5, cl. 3.2, 3.4
GDA-24	Accept existing safeguards, such as age-based content restrictions and restrictive defaults, as meeting the Sub-Code in place of blanket feature prohibitions.	General

Ref.	Point raised	Draft provision
Game Developer B		
GDB-1	Clarify when the content categories present a significant risk of serious harm requiring Highly Effective Age Assurance, and whether existing age-rating classifications may be relied on.	Part 2, cl. 2.5, 2.7
GDB-2	Define “content that simulates gambling”, including whether free features with random or prediction elements and no cash-out are covered, and whether gambling-like visuals should be avoided.	Part 2, cl. 2.5(f)
GDB-3	Take a more granular, risk-based approach to High-Risk Features, many of which are common and important parts of Online Games.	Part 2, cl. 3.2
GDB-4	Distinguish team and match communication from private messaging; with safeguards, it should not be switched off because participants are not Established Contacts.	Part 2, cl. 3.2(a); Part 3, cl. 3.8
GDB-5	Allow Paid Randomised Reward Mechanisms on Child Accounts where spending limits, odds disclosure and verified parental controls are in place.	Part 3, cl. 3.8(c)
GDB-6	Address trading and gifting through targeted safeguards, such as value caps, rather than default disabling, and clarify the treatment of gifts received and free items.	Part 2, cl. 3.2(c)
GDB-7	Exclude features using only general location, such as regional rankings, server allocation and matchmaking.	Part 2, cl. 3.2(f)
GDB-8	Require major app stores, operating systems and Platforms to carry out Age Assurance and transmit a standard age signal to game Operators.	Part 3, cl. 2.5, 2.13; Part 9, cl. 3.4
GDB-9	Clarify whether recommending the game’s own items based on gameplay counts as Personalised Advertising or a Commercial Communication.	Part 6, cl. 2.3
GDB-10	Clarify that one integrated spending-limit mechanism can meet both duties, with a zero limit treated as consent withheld.	Part 5, cl. 3.4
GDB-11	Confirm that odds may be disclosed by objectively defined categories, tiers or rarity levels.	Part 5, cl. 2.3(a)
GDB-12	Provide guidance or a standard template for the Child Safety Risk Assessment.	Part 9, cl. 2.3
Academic Researcher		
RES-1	Set out how companies are expected to comply with each requirement, as South Korea has done, so that implementation is consistent; for example, odds for each individual outcome.	General
RES-2	Set the minimum standard for smaller studios and lower-risk games at an appropriately high level.	Part 2, cl. 2.9
RES-3	Rely on a device, console or app-store age signal only where that Platform applies Highly Effective Age Assurance to each User rather than to the device, since devices may be shared by adults and children.	Part 3, cl. 2.5
RES-4	Require the age rating to be shown prominently in all advertising.	Part 3, cl. 1.1, 1.3

Ref.	Point raised	Draft provision
RES-5	Work towards a Malaysian age rating system that reflects local cultural context, as China, South Korea, Japan, Singapore and Indonesia have.	Part 3, cl. 1.1
RES-6	Work with IARC and the Platforms on a questionnaire and display able to show the feature disclosures the Sub-Code requires, prioritising High-Risk Features to avoid information overload.	Part 3, cl. 1.2; Part 4, cl. 2.1–2.2
RES-7	Ensure that the alternative age route for children without documents cannot be used by other children to bypass protective features.	No express provision
RES-8	Treat 13 to 15 and 16 to 17 year olds as separate tiers, giving 16 and 17 year olds more choice, including over some higher-risk settings.	Part 3, cl. 3.9
RES-9	Limit a parent's ability to restore any setting for older teenagers, given the part games play in children's social lives.	Part 3, cl. 3.10
RES-10	Promote parental controls widely so that parents who are unaware of them can find them.	Part 3, cl. 3.3–3.4
RES-11	For children, recognise as Esports only games in which Paid Randomised Reward Mechanisms are not central to being competitive, unless an Esports version with all content unlocked is provided.	Part 3, cl. 5.1–5.2
RES-12	Avoid extensive supervision of adults with a disability who have full capacity, out of respect for their autonomy.	Part 3, cl. 3.11
RES-13	Actively monitor and enforce the display of ringgit equivalents, which consumer regulators in the United States and the European Union have required and where compliance elsewhere has been incomplete.	Part 5, cl. 1.4
RES-14	Explore with the Commission whether the odds disclosure requirement should become a legal obligation under section 99 of the Communications and Multimedia Act 1998 for companies that repeatedly do not comply, and resource the CMCF to monitor compliance.	Part 5, cl. 2.1; Part 11
RES-15	Replace subjective wording such as "clear, prominent, and understandable" with objective requirements, and do not allow odds to be shown as "<1%", following South Korea's guidance.	Part 5, cl. 2.1(b)
RES-16	Require odds on the purchase page, shown automatically or one tap away behind a button labelled "probabilities", and disclose the presence of Randomised Reward Mechanisms at the top of the store page, in advertising and on official websites and social media.	Part 5, cl. 1.1, 2.1
RES-17	Apply the additional disclosures on Randomised Reward Mechanisms required for Child Accounts to all accounts.	Part 5, cl. 2.3(a)–(b)
RES-18	Disable Paid Randomised Reward Mechanisms on Child Accounts by default until a parent or guardian approves them.	Part 5, cl. 2.3(c)
RES-19	Set default spending limits by age in exact figures, as China does: no spending under 8, about RM122 a month for 8 to 15 year olds and about RM244 a month for 16 and 17 year olds.	Part 5, cl. 3.4

Ref.	Point raised	Draft provision
RES-20	Define "each individual purchase", and let parents choose how often they approve purchases, with a default of approval for real-money spending and a weekly summary of in-game purchases highlighting Randomised Reward Mechanisms.	Part 5, cl. 3.2
RES-21	Assess whether countdown timers, last-chance messaging and similar pressure are appropriate for Vulnerable Users and adults as well as children.	Part 5, cl. 3.5–3.6
RES-22	Prohibit Third-Party Virtual Currency Resellers, given the risks of fraud and illegal skin gambling.	Part 1, cl. 5.1; Part 5
RES-23	Recognise that gamified advertising is harder for children to distinguish from the game.	Part 6, cl. 1.3
RES-24	Provide detailed guidance, developed with experts, on what Operators must do and avoid under community standards.	Part 7, cl. 1.1–1.2
RES-25	Require a Gaming Safety Officer also where a service offers Paid Randomised Reward Mechanisms or other High-Risk Features.	Part 9, cl. 4.1
RES-26	Make the Developer, Publisher, seller and promoter jointly and severally responsible for a child's spending so that a parent may claim against any of them; do not place responsibility mainly on the parent, and assume good faith in early refund requests.	Part 9, cl. 1.3–1.4
RES-27	Issue guidance well before the transition period ends, and consider phasing, with up to six months for simpler measures and up to a year for complex ones.	No transitional provision
RES-28	Ensure that guidance setting specific figures cannot easily be amended to weaken protections.	Part 5, cl. 3.4(b); Part 9, cl. 4.3(d)
RES-29	Fund the monitoring of compliance and testing of whether the measures work, with academic researchers, as part of the review.	No express review provision
RES-30	Use "Users" consistently in place of "players" and "Consumers".	Part 1, cl. 5.1
RES-31	Remove "as well as the strict letter of it" from the interpretation clause and state whether the spirit or the letter prevails.	Part 1, cl. 7.1
RES-32	Define "real-money purchases".	Part 2, cl. 3.2(d)
RES-33	Require disclosures in both Bahasa Malaysia and English without the qualifier "where reasonably practicable", and make disclosures on Randomised Reward Mechanisms for children available in all relevant languages.	Part 3, cl. 1.4; Part 4, cl. 1.4; Part 5, cl. 2.3(b); Part 7, cl. 1.4
RES-34	Note that rules based on Material Changes may be hard to monitor, as tracking significant updates has proved difficult elsewhere.	Part 3, cl. 1.5
RES-35	Give examples of non-compliant age checks, such as a confirm button as the only option or an immediate retry after a wrong answer.	Part 3, cl. 2.9
RES-36	Disclose High-Risk Features before a game is downloaded or bought, and in advertising, rather than when the feature is first encountered.	Part 4, cl. 1.3
RES-37	Treat direct exhortation of children to buy separately from pressure through Dark Patterns.	Part 5, cl. 3.5; Part 6, cl. 2.2(b)

Ref.	Point raised	Draft provision
RES-38	Remove Part 10: obligations should not be placed on Users, who include children, and responsibility should not shift from companies to Users and parents.	Part 10
RES-39	Require records of the results of Paid Randomised Reward Mechanisms to be kept for auditing against the disclosed odds.	Part 12, cl. 1.3
RES-40	Number clauses with the Part number, for example 12.1.3.	General
RES-41	Use the defined term Vulnerable User more widely, including for people experiencing gambling problems or substance use.	Part 1, cl. 1.5; Part 2, cl. 2.2, 2.5(e)
RES-42	Require IP or location checks so that Users in Malaysia who install foreign versions of a game, including through APK files, still receive the Sub-Code's protections.	Part 2, cl. 1.4
RES-43	Provide implementation guidance with example screenshots, for instance on odds disclosure.	General
Institute for Democracy and Economic Affairs (IDEAS)		
IDE-1	Include location checks in Age Assurance so that different legal age thresholds can be applied.	Part 3, cl. 2.4
IDE-2	Allow age signals from mobile operating systems without re-collecting identity documents, and consider a model for children based on MyDigital ID.	Part 3, cl. 2.5
IDE-3	Apply Highly Effective Age Assurance more widely, including facial age estimation or identity verification before open voice chat.	Part 3, cl. 2.4
IDE-4	Re-check age periodically, such as at sensitive transactions or before High-Risk Features, so that an adult cannot pass a verified account to a child.	Part 3, cl. 2.9
IDE-5	Require Developers to disclose interactive features, such as purchases, unmonitored chat and location sharing, before installation.	Part 3, cl. 1.2
IDE-6	Build alternative routes, such as facial age estimation, into Age Assurance so that stateless and refugee children are not excluded.	No express provision
IDE-7	Include sensitive content filters, daily usage limits, night-time sleep modes and limits on video chat in children's default settings.	Part 3, cl. 3.8
IDE-8	Consider Verified Parental Consent to unlock High-Risk Features, and central parental dashboards covering activity, spending, privacy and safety alerts without exposing private messages, as some platforms already provide.	Part 3, cl. 3.3–3.4, 3.9
IDE-9	Build in accessibility features such as read-aloud tools, audio descriptions, dyslexia-friendly fonts, colour-blind modes and photosensitivity warnings, with extra care over engaging features for neurodivergent and younger children.	No express provision
IDE-10	Require moderation systems that recognise local slang and offensive terms in Bahasa Malaysia, Mandarin, Tamil and Indonesian, rather than relying solely on keyword filters.	Part 7, cl. 2.2
IDE-11	Place more emphasis on automated, proactive detection, and suspend or ban adults found harassing or bullying children.	Part 7, cl. 2.2(i)

Ref.	Point raised	Draft provision
IDE-12	Allow quiet enforcement against repeat offenders, such as shadow-banning and automatic message filtering.	Part 7, Section 3.0
IDE-13	Accept reports of harassment that began in the game and moved to other apps, and take preventive action.	Part 7, cl. 2.4–2.5
IDE-14	Alert the parents of both children where a Child Account is involved in serious misconduct, collecting guardian contact details at registration and protecting them under the Personal Data Protection Act 2010.	Part 7, Section 3.0
IDE-15	Have Operators handle critical incidents directly rather than relying on the Complaints Bureau, as IDEAS considers that Operators should retain primary legal liability for hosting or facilitating illegal communication under the Online Safety Act 2025 and section 233 of the Communications and Multimedia Act 1998.	Part 9, Section 5.0
IDE-16	Set resolution times by severity, such as 7 to 14 working days for non-serious complaints, before a complaint may go to the Complaints Bureau, and define which unresolved complaints the Bureau will take.	Part 11, cl. 2.1
IDE-17	Have Operators and the Complaints Bureau verify complaints so that frivolous or bad-faith reports are filtered out.	Part 11
IDE-18	Let Users rate how complaints were handled, and give the Complaints Bureau a way for Users to track the status of a complaint.	Part 11
IDE-19	Include serious incidents in published figures, such as proactive removals and accounts closed for child-safety violations, and the accuracy of Age Assurance tools.	No express provision
Industry Group		
IND-1	Focus on the outcomes to be achieved and let participants use existing and equivalent safeguards suited to their service design, Users, risk and degree of control.	General
IND-2	Complement rather than duplicate overseas online safety regimes and the PEGI, ESRB and IARC rating systems.	General
IND-3	Remove the references to the Online Safety Act 2025, or state that they are context only, do not import or extend that Act or its codes, and that compliance is assessed solely against the Sub-Code and other applicable law.	Part 1, cl. 6.5; Part 14, cl. 4.2(c)
IND-4	Base obligations on an assessment of the risk of a feature, content or service, considered holistically with existing safeguards and the risk that remains.	Part 2, cl. 2.4–2.5
IND-5	Ensure that comparable services face equivalent expectations, so that harm is not displaced to unofficial or unregulated channels.	Part 2, cl. 1.4
IND-6	State that responsibility may be shared, with each participant applying safeguards in proportion to its role and control; Platforms should not be liable for creator decisions they cannot control in real time, may rely on creator declarations and tooling, and should be bound by a reasonable-control standard.	Part 2, cl. 1.3(b)–(d); Part 9, cl. 1.3–1.4

Ref.	Point raised	Draft provision
IND-7	Remove the exclusions for APK stores, unregulated or illegal Platforms and games without specified features, and decide whether the Sub-Code applies by the nature and severity of risk; clarify whether free games with harmful content are excluded.	Part 1, cl. 5.1; Part 2, cl. 1.4
IND-8	Confirm that developer-facing creation, testing, publishing, analytics and documentation tools are not Online Games or Gaming Services.	Part 1, cl. 5.1; Part 2, cl. 1.5
IND-9	Assess Significant Risk of Serious Harm after existing safeguards, require Highly Effective Age Assurance only where a documented assessment shows that risk remains, and apply the threshold consistently across comparable services.	Part 1, cl. 5.1; Part 2, cl. 2.7
IND-10	Apply the restriction on promoting age-restricted content to content directed at or primarily designed to appeal to children, and confirm that incidental exposure of thumbnails or classification information is compliant.	Part 2, cl. 2.8
IND-11	Treat the listed High-Risk Features as indicators of heightened risk rather than inherently high-risk.	Part 1, cl. 5.1; Part 2, cl. 3.2
IND-12	Limit responsibility for updating classification after Material Changes to matters within reasonable control, with reliance on creator declarations and Platform tooling.	Part 3, cl. 1.5
IND-13	Confirm that Platform-level age signals may be relied on without repeat checks, that Highly Effective Age Assurance may apply to a feature rather than the whole service, and that equivalent international standards qualify, with a reasonable implementation period.	Part 3, cl. 2.1–2.8
IND-14	Assess anti-circumvention by reasonable and proportionate measures rather than an absolute duty, and recognise privacy-preserving methods.	Part 3, cl. 2.9
IND-15	Limit Access Route obligations to routes within the Operator's control, allow time to address inconsistencies caused by third parties, and accept Platform-applied signals without passing them to each participant.	Part 3, cl. 2.11–2.13, 2.15–2.16
IND-16	Allow low-risk functionality on unassured, unregistered or provisional accounts, with guidance giving examples.	Part 3, cl. 2.14
IND-17	Frame the default settings for Child Accounts as outcomes, and allow equivalent combinations of safeguards.	Part 3, cl. 3.8–3.10
IND-18	Leave Platforms discretion over supervised accounts for persons with a disability, given the difficulty of identifying them and the risk that adults misuse them to pose as children.	Part 3, cl. 3.11
IND-19	Allow equivalent combinations of spending safeguards, explain how a default spending limit works with models in which a parent approves each purchase, keep guidance non-prescriptive and neutral between business models, and consider the income of Malaysian creators.	Part 5, cl. 3.4
IND-20	Accept equivalent assessments under other frameworks, treat thirty days as a benchmark, require reassessment only for changes that materially affect risk, and protect confidential information.	Part 9, cl. 2.3

Ref.	Point raised	Draft provision
IND-21	Treat a Platform's age signal as shared where it applies across its ecosystem, make each Operator responsible for applying it, and limit shared information to the age band or eligibility outcome.	Part 9, cl. 3.4; Part 3, cl. 2.5
IND-22	State that the Gaming Safety Officer has an administrative and contact role, with no personal liability and no requirement of independence, local residence or prescribed qualifications.	Part 9, cl. 4.2(a)–(c)
IND-23	Apply the 24-hour period to initial triage of reports through designated channels, starting once there is enough information to assess, possibly with acknowledgement within 24 hours and fuller triage later; contact Users and parents only where safe, lawful, appropriate and technically practicable, at the Operator's reasonable discretion.	Part 9, Section 5.0
IND-24	Treat Part 14, Section 4.0 as overarching principles, read emotional harm and similar concepts as reasonably foreseeable and material harm, and recognise that Platforms cannot assess harm that occurs off the Platform.	Part 14, Section 4.0
IND-25	Reserve corrective advertising for material deception or serious non-compliance after due process, in proportion, and allocate it according to each party's role and control.	Part 14, cl. 7.1

TABLE 3 Points Raised in Written Submissions