

ONLINE SAFETY ASSESSMENT REPORT 2026

Designated App Distribution Services



AGE
18+
Years Old



Table of Contents

01	Key Findings at a Glance and What This Means for Users		2
02	Executive Summary	Introduction	4
		Overall Assessment	4
		Key Findings	5
		Conclusion and Next Steps	12
03	Main Report	Introduction	13
		Code of Practice for Online Safety - App Distribution Services	14
		Aim of the Online Safety Assessment Report	15
		Methodology	15
		Detailed Assessments of Designated App Distribution Services	17
		Apple App Store	17
		Google Play Store	23
		Huawei AppGallery	30
		Microsoft Store	36
		Samsung Galaxy Store	41
Annex A: Code of Practice for Online Safety - App Distribution Services		46	

Key Findings at a Glance and What This Means for Users



Age Assurance Present and Generally Well Implemented

	Credit Card	Singpass	Government ID	Facial Age Estimation	Email Verification	Account / Behavioural Signals
Apple App Store	✓		✓			✓
Google Play Store	✓		✓	✓	✓	✓
Huawei AppGallery	✓					
Microsoft Store		✓	✓	✓		
Samsung Galaxy Store	✓					

All five Designated App Distribution Services (D-ADSs) implemented the Age Assurance (AA) methods approved by IMDA to establish users' age or age range with reasonable accuracy. These AA methods were proposed by the D-ADSs in accordance with IMDA's guidelines.

Key Observations

Baseline safety measures in place and no systemic breaches of ADS Code but IMDA's testing found weaknesses.



1. Age Assurance



Measures present, generally well implemented and could not be easily circumvented, except for a small percentage of **Huawei AppGallery** users.

2. Enhanced Protections for Children



Default restrictions from downloading 18+ apps were present, except for limited instances on **Huawei AppGallery** and **Microsoft Store**.

3. Effectiveness of App Review



65 apps containing or facilitating harmful content that violated policies and should not have been allowed across all **five D-ADSs**, indicating weaknesses in content moderation and app review processes.

4. Appropriateness of App Age Ratings



24 apps containing 18+ content wrongly age-rated as below 18+ on **Apple App Store**, **Google Play Store** and **Huawei AppGallery**, indicating weaknesses in age-rating processes.

5. Effectiveness of User Reporting and Resolution Measures



User reporting channels present but notification of report outcomes inconsistent/lacking across **all five D-ADSs**. No notification to users who downloaded apps within the previous six months that the app was subsequently removed for violations on **Google Play Store** and **Samsung Galaxy Store**.

6. Accountability



All D-ADSs submitted the required accountability metrics for the first year but **Google Play Store**, **Huawei AppGallery**, and **Samsung Galaxy Store** need to provide better metrics.

What This Means for Users

While designated app stores have safeguards to help protect users under 18, everyone can play a part in fostering a safer online environment, especially for children.

Here are some practical ways parents and youths can manage their devices safely through practising healthy digital habits.



Visit the [Digital for Life website](#) for more resources on how you can manage your online safety.

Parents

Your child may still face some risk of bypassing age assurance measures or accessing 18+ apps, as safeguards may not work as intended in every instance, due to technical limitations, inconsistent implementation of safeguards, or inaccurate age ratings.



The best way to protect your child online is to understand their digital experiences and stay involved. You are encouraged to:

- 1 Stay informed of the apps that your child uses.** Be aware of the apps that your child may encounter as they explore the digital world beyond schoolwork.
- 2 Set up an age-appropriate account for your child.** Indicate your child's actual birth date. Do not create or share an adult account with your child.
- 3 Use parental controls.** These serve as an additional guardrail to manage screen use, set limits, and restrict access to inappropriate content and app downloads on your child's device. Keep the device's operating system and apps up to date.
- 4 Review first, then explore together.** Read reviews and check the app's age rating before downloading. Where possible, test and explore the app with your child.
- 5 Have open conversations.** Agree on suitable apps and content, explain why safeguards matter, and encourage your child to approach you if something online makes them uncomfortable.
- 6 Report and remove inappropriate apps.** Report inappropriate content or inaccurate age ratings to the app or app store, and delete the app where necessary. Regularly review downloaded apps to ensure that they remain age-appropriate, and refer to the app store for the most updated age ratings.

Youths



You are encouraged to take these steps when accessing apps on designated app stores:

- 1 Check before downloading.** Check age ratings and content guidelines to identify suitable apps content.
- 2 Discuss apps with your parents.** Speak to your parents about which apps to download and use.
- 3 Keep your device and apps up to date.** Install the latest operating system and app updates.
- 4 Turn on privacy and safety settings.** Adjust privacy and safety settings on your devices and accounts to limit exposure to inappropriate content.
- 5 Report and remove inappropriate apps.** Flag or report inappropriate content and delete the app where necessary.
- 6 Seek help.** Approach your parents or a trusted adult if you feel uncomfortable or encounter harms.

Executive Summary

Introduction



- 01** The Online Safety Assessment Report (OSAR) 2026 for Designated App Distribution Services (D-ADSs) sets out IMDA's first assessment of the five D-ADSs' online safety measures under the Code of Practice for Online Safety - App Distribution Services (ADS Code). The five D-ADSs are Apple App Store, Google Play Store, Huawei AppGallery, Microsoft Store,¹ and Samsung Galaxy Store. The OSAR covers the reporting period from 1 April 2025 to 31 December 2025.
- 02** IMDA's main priority as Singapore's online safety regulator is to ensure a safe online environment for all users in Singapore, particularly children. IMDA assessed whether the D-ADSs' measures were *Present, Comprehensive, and Effective*, using information from D-ADSs' annual online safety reports to IMDA, together with IMDA's own mystery shopper testing, direct testing, and operational data. This assessment focused on the D-ADSs':
- Effectiveness of age assurance measures and enhanced protections for children;
 - Effectiveness of safety measures to remove egregious and harmful apps;
 - Effectiveness of safety measures to assign appropriate age-ratings to apps; and
 - Effectiveness of user reporting and resolution measures.

Overall Assessment

- 03** **Baseline safety measures were in place across all five D-ADSs. There were no systemic breaches of the ADS Code but IMDA's testing found weaknesses in how several measures were implemented.**
- Age Assurance.** Given that this is the first time age assurance has been introduced, IMDA tested for presence of measures, ease of use and ease of circumvention. IMDA found that age assurance measures on the D-ADSs were present and generally well implemented. IMDA's sample testing also found that the measures generally could not be easily circumvented, except for a small percentage of users on Huawei AppGallery.
 - Enhanced Protections for Children.** Children were restricted from downloading 18+ apps by default on all D-ADSs except for limited instances on Huawei AppGallery and Microsoft Store that have mostly been rectified.
 - Effectiveness of App Review.** IMDA detected 65 apps containing or facilitating harmful content across all five D-ADSs that violated their own policies and should not have been allowed on their platforms. This indicates that there are weaknesses in the D-ADSs' content moderation and app review processes that can be improved.
 - Appropriateness of App Age Ratings.** IMDA detected 24 apps containing 18+ content that were wrongly age-rated as below 18+ on Apple App Store, Google Play Store, and Huawei AppGallery. This is a weakness in their age-rating processes that could expose children to age-inappropriate content or misinform parents and guardians about the suitability of apps for their children.

¹ Microsoft Store comprises five storefronts - Microsoft Store on Windows, Apps.microsoft.com Website Store, PC Games Store, Xbox console storefront, and the part of Xbox.com Website having the characteristics of an app distribution service as specified in the Fourth Schedule of the Broadcasting Act 1994.

- e. **Effectiveness of User Reporting and Resolution Measures.** All D-ADSs had user reporting channels but did not fully notify users of the outcome of their user reports. Google Play Store and Samsung Galaxy Store also did not notify users who had downloaded apps within the previous six months when that app was removed by the D-ADS for a violation.
- f. **Accountability.** All D-ADSs submitted the required accountability metrics for the first year but Google Play Store, Huawei AppGallery, and Samsung Galaxy Store will need to provide better metrics to demonstrate the effectiveness of their user reporting mechanisms.

Key Findings

Key Finding 1 – Given that this is the first time age assurance has been introduced, IMDA tested for presence of measures, ease of use and ease of circumvention. IMDA found that age assurance measures on the D-ADSs were present and generally well implemented. IMDA’s sample testing also found that the measures generally could not be easily circumvented, except for a small percentage of users on Huawei AppGallery.

04 All five D-ADSs implemented the Age Assurance (AA) methods approved by IMDA to establish users’ age or age range with reasonable accuracy. These AA methods were proposed by the D-ADSs in accordance with IMDA’s guidelines. The list of approved AA methods across the D-ADSs is at [Table 1](#).

- a. There are three main categories of AA – i) age inference using user signals, ii) age estimation via facial scans, and iii) age verification using official documents.
- b. The most common AA method, implemented by three out of the five D-ADSs, is age inference via the use of a credit card.

D-ADS	Method	Point of Age Check
Apple App Store	[Primary] Credit card, Age inference via account tenure (active account for min. 18 years) [Secondary] Government ID (passport, driving licence, NRIC, or FIN)	AA prompted upon first 18+ app download (default 18+ download restrictions if not completed).
Google Play Store	[Primary] Age Inference Model via behavioural signals (e.g. YouTube history, search history, installed apps, tenure of account) [Secondary] User chooses between: Credit card, Government ID (national ID/NRIC, passport, driving licence), Facial Age Estimation (selfie/facial image of user), Email Verification (age inference based on signals associated to user's email e.g. used for finance/mortgage)	Default U-18 restrictions until age inference is completed. Continuous analysis by age inference model in the background. Any of the secondary methods can be chosen for immediate or alternative verification / estimation at point of 18+ app download.
Huawei App Gallery	Credit card (only method)	AA prompted upon first access to the app store (default 18+ download restrictions if not completed).
Microsoft Store	User chooses between: Singpass, Government ID (national ID, driving licence, passport, residence permit) and Facial Age Estimation (selfie/facial image of user)	AA prompted upon first 18+ app download (default 18+ download restrictions if not completed).
Samsung Galaxy Store	Credit card (only method)	AA prompted upon first access to the app store (default 18+ download restrictions if not completed).

Table 1: List of D-ADSs’ AA methods approved by IMDA

05 IMDA assessed that the AA methods set out in Table 1 were effective in determining the age or age-range of users, specifically if they are above or below 18 years old, on the D-ADSs.

- a. For Apple App Store, Huawei AppGallery, and Samsung Galaxy Store, age inference via credit card was assessed to be effective as it provides a reliable age signal given that credit cards have a minimum ownership age of 18 in Singapore.² However, parents or guardians should ensure that young users under-18 do not use their credit cards to download 18+ apps.

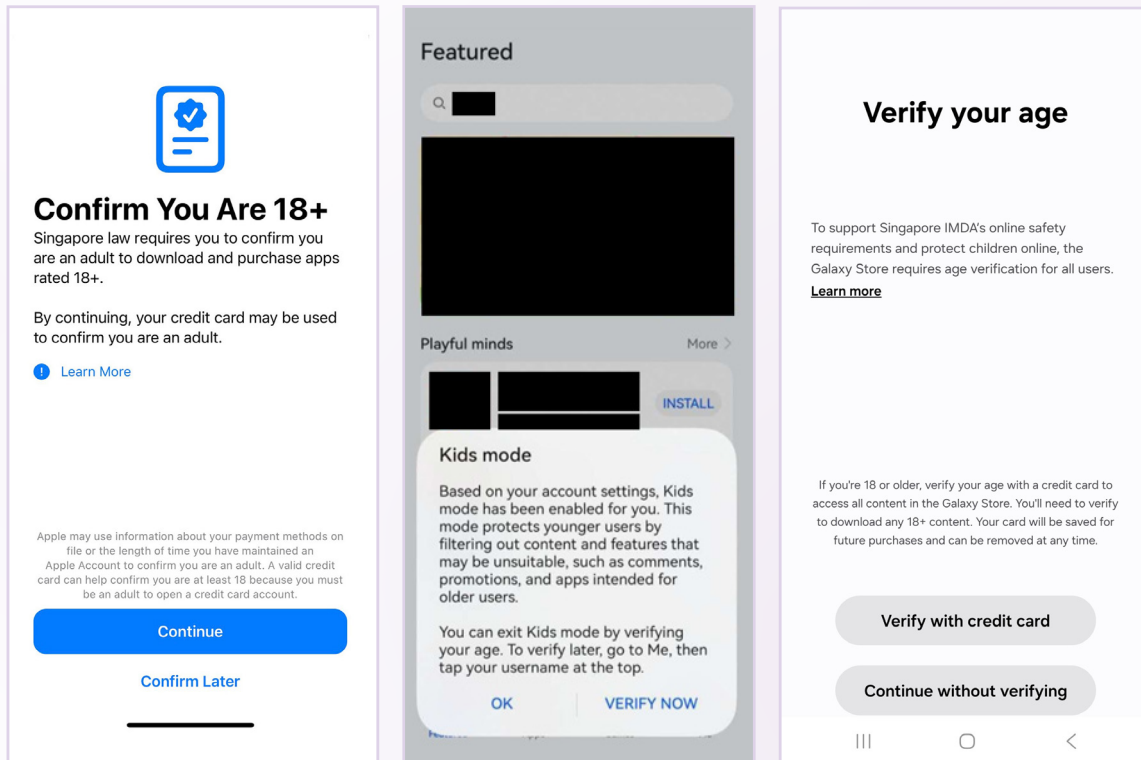


Figure 1: Credit card verification prompts on Apple App Store, Huawei AppGallery and Samsung Galaxy Store respectively

- b. For Google Play Store, all users are defaulted to a child-safe experience until its behavioural signals-based model can complete the age inference process.

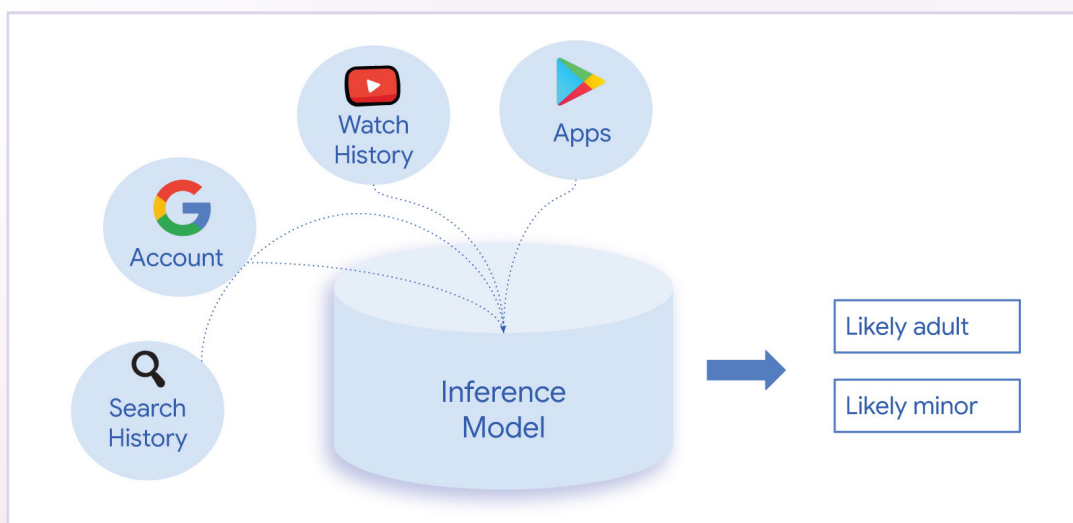


Figure 2: Google Play Store's age inference model based on behavioural signals
(Source: Google Play Store)

² The minimum age to apply for most credit cards in Singapore is 21, with the exception of student credit cards and supplementary credit cards with a minimum age of 18.

- c. For Google Play Store and Microsoft Store, age estimation methods using technology to analyse facial images have a high confidence level in determining the age or age range of users, but these should be combined with other AA methods for greater accuracy.

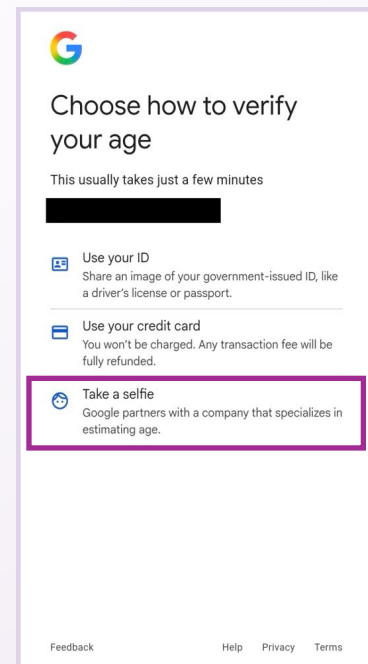


Figure 3: Facial age estimation prompt on Google Play Store

- d. For Apple App Store, Google Play Store, and Microsoft Store, age verification methods using digital ID (Singpass) or official documents are highly accurate as they are based on official and trusted sources of information.

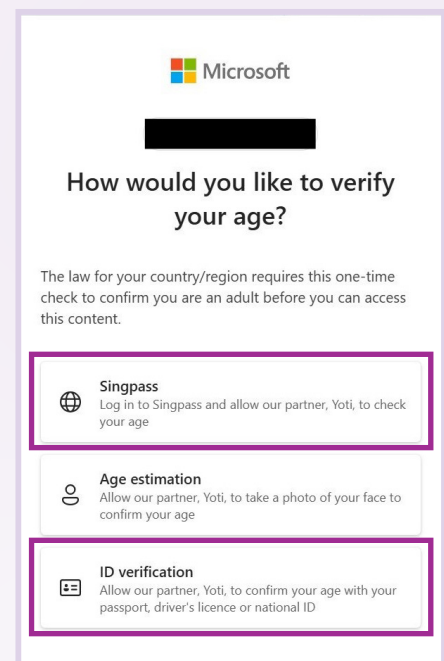


Figure 4: Age verification prompts (via Singpass or official identity documents) on Microsoft Store

- 06** IMDA tested the effectiveness of these AA methods by simulating the real-world user experience at the different stages where AA checks may be triggered. This was done using a small sample test. IMDA found that the AA methods deployed by the D-ADSs were present and sample testing found that the measures generally could not be easily circumvented. However, IMDA also notes that there is no AA method that is completely foolproof. There was one exception for Huawei AppGallery where a small percentage of users were able to circumvent AA under specific circumstances on certain versions of the AppGallery due to technical limitations. Following IMDA's engagement, Huawei AppGallery investigated the issue and updated that only 7% of its users were affected. Huawei AppGallery is committed to working with IMDA to monitor and address the issue.
- 07** The ADS Code requires AA measures to be implemented in accordance with the data protection provisions under the Personal Data Protection Act 2012 (PDPA) and relevant guidelines issued by the Personal Data Protection Commission (PDPC). Based on the information provided by the D-ADSs for this review, PDPC observed positive practices, including AA-specific notices and consent mechanisms for several AA methods, measures to limit the amount of personal data collected or retained for some AA methods, and the deletion or non-retention of certain underlying information or documents used for the age check.
- 08** The review also identified areas where more detailed information would have provided greater clarity on how personal data is handled, including how previously collected account or payment information is used for AA and how users are informed of such use, the roles and responsibilities of certain vendors, information on safeguards for particular retained AA records, and the retention and deletion rules for age-check results created through the AA process. These observations are based on the information available for this review and are not an overall assessment of the D-ADSs' compliance with the PDPA.

Key Finding 2 – Children were restricted from downloading 18+ apps by default on all D-ADSs except for limited instances on Huawei AppGallery and Microsoft Store that have mostly been rectified.

- 09** After the D-ADS establishes via its AA measures that a user is a child (below 18 years old), the D-ADS must then ensure that children are provided with enhanced protections that are age appropriate.
- 10** All D-ADSs had default restrictions to prevent children from downloading apps rated 18+ that were generally effective. However, IMDA's tests uncovered limited instances on Huawei AppGallery and Microsoft Store where these restrictions were either not present or could be bypassed due to loopholes that allowed children to turn off the restrictions. Following IMDA's engagement, Huawei AppGallery has resolved the issue, while Microsoft Store has identified the root causes and has implemented an interim solution as it works towards a permanent solution.
- 11** In addition, IMDA's tests found a loophole in Microsoft Store's parental tools that allowed children to turn off the restriction on downloading 18+ apps. Microsoft Store has identified a solution and is working towards implementing it.

Key Finding 3 - IMDA detected 65 apps containing or facilitating harmful content across all five D-ADSs that violated their own policies and should not have been allowed on their platforms. This indicates that there are weaknesses in the D-ADSs’ content moderation and app review processes that can be improved.

12 All D-ADSs had content guidelines and app review processes as required by the ADS Code. However, IMDA’s mystery shopper testing of over 7,000 apps across all the D-ADSs detected 65 apps containing or facilitating harmful content that violated the D-ADSs’ own policies.

- a. The most prevalent types of harmful content were sexual content, violent content, and content facilitating vice and organised crime. Examples included generative-AI or nudification apps, AI companion or dating apps with sexually explicit content, gambling apps involving real-money or cryptocurrency payouts, and violent or horror-themed games (Details in [Table 2](#)).

13 All 65 apps containing or facilitating harmful content were removed after IMDA’s mystery shopper user reporting or IMDA’s reporting. Overall, the number of apps identified was small relative to the large number of apps available on the D-ADSs and do not indicate any systemic failure, but the findings show that some harmful apps may still slip through existing safeguards. This shows that there is room for improvement in the D-ADSs’ content moderation and app review processes. IMDA will continue to hold D-ADSs responsible for ensuring that users’ access or exposure to harmful content on their services is minimised.

Designated ADSs	Number of Apps Removed Following IMDA's Notification	Type of Harmful Content
Apple App Store	30	• Sexual content
Google Play Store	10	• Sexual content
Huawei App Gallery	11	• Sexual content • Violent content • Content facilitating vice & organised crime
Microsoft Store	3	• Sexual content • Violent content • Content facilitating vice & organised crime
Samsung Galaxy Store	11	• Sexual content

Table 2: Apps that contained or facilitated harmful content

Key Finding 4 - IMDA detected 24 apps containing 18+ content that were wrongly age-rated as below 18+ on Apple App Store, Google Play Store and Huawei AppGallery. This is a weakness in their age-rating processes that could expose children to age-inappropriate content or misinform parents and guardians about the suitability of apps for their children.

14 All D-ADSs had the required content guidelines for children and age-rating policies. However, IMDA's mystery shopper testing of over 7,000 apps across all the D-ADSs detected 24 apps on Apple App Store, Google Play Store, and Huawei AppGallery that should have been rated 18+ under their respective age-rating policies but were assigned a lower age-rating. The apps included sexual content, content facilitating vice and organised crime, and violent content (Details in [Table 3](#)).

15 The age-ratings of all 24 apps were revised to 18+ after IMDA's mystery shopper user reporting or IMDA's reporting. Overall, this is a low number of mis-rated apps at the 18+ threshold and does not indicate any systemic failures on the three D-ADSs. IMDA will continue to hold D-ADSs responsible for ensuring that age ratings are applied accurately and consistently, so as to minimise children's access or exposure to age-inappropriate content, and to provide parents and guardians with accurate information on the suitability of apps for their children.

Designated ADSs	Number of Apps Re-rated Following IMDA's Notification	Type of Inappropriate Content
Apple App Store	11	• Sexual content • Content facilitating vice & organised crime
Google Play Store	10	• Sexual content • Content facilitating vice & organised crime
Huawei App Gallery	3	• Violent Content

Table 3: Mis-rated apps that contained or facilitated inappropriate content

Key Finding 5 – All D-ADSs had user reporting channels but did not fully notify users of the outcome of their user reports. Google Play Store and Samsung Galaxy Store also did not notify users who had downloaded apps within the previous six months when that app was removed by the D-ADS for a violation.

16 All D-ADSs provided channels for users to report harmful or inappropriate content, including in-store flagging, online webforms, hotlines or service-chat functions. However, IMDA found that all D-ADSs either inconsistently notified reporting users of the outcome of their reports or completely failed to do so. As a result, users could not tell whether their reports had been assessed or what the outcome was. Following IMDA's engagement, the D-ADSs have investigated and ensured that such processes are in place or have committed to putting them in place.

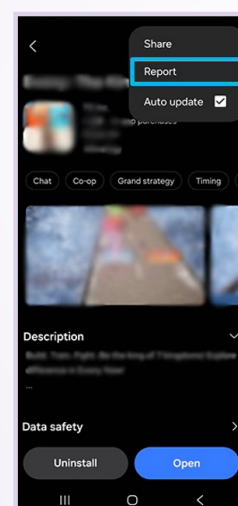


Figure 5: User reporting channel on Samsung Galaxy Store (Source: Samsung)

- 17** IMDA also found that Google Play Store and Samsung Galaxy Store did not notify users who had downloaded an app within the previous six months when the app was subsequently removed from the app store. The intent of this requirement in the ADS Code is to ensure that users are made aware that an app they have downloaded may contain or facilitate harmful content, and that the app has been removed from the app store.
- a. Google Play Store highlighted implementation challenges and said that purchases and updates would be restricted for affected apps. Google Play Store is required to put in place a notification process.
 - b. Samsung Galaxy Store has committed to implement push notifications and/or emails by Q3 2027. IMDA expects D-ADSs to close these gaps so that users receive clear outcomes and can act on identified safety risks.

Key Finding 6 – All D-ADSs submitted the required accountability metrics for the first year but Google Play Store, Huawei AppGallery, and Samsung Galaxy Store will need to provide better metrics to demonstrate the effectiveness of their user reporting mechanisms.

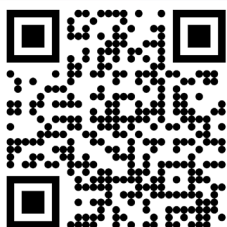
- 18** The intent of these metrics is for D-ADSs to demonstrate the effectiveness of their safety measures and reflect the Singapore users' experience on the services. All D-ADSs submitted the accountability metrics approved by IMDA for the first OSAR.
- a. Based on the submitted metrics, IMDA observed that all D-ADSs reported zero or near zero user reports on harmful or inappropriate content.
 - b. The most prevalent type of violative apps that D-ADSs took action against either proactively and/or a result of user reports, was apps with content facilitating vice and organised crime, followed by apps with sexual content.
- 19** Google Play Store, Huawei AppGallery, and Samsung Galaxy Store provided metrics that did not fully meet the intent of the ADS Code. These metrics will need to be improved in the next annual online safety report. Following IMDA's engagement, the D-ADSs have committed to exploring better metrics.
- a. Google Play Store will need to provide metrics on actions taken due to user reports broken down by policy violation, as well as absolute turnaround times for resolving user reports.
 - b. Huawei AppGallery will need to provide absolute turnaround times for resolving user reports.
 - c. Samsung Galaxy Store will need to provide absolute turnaround times for resolving user reports, with breakdown by content category.

Conclusion and Next Steps

- 20** Since the introduction of the ADS Code in March 2025, the D-ADSs have stepped up efforts to implement online safety measures for Singapore users. This OSAR found that a baseline of safety measures is in place across the five D-ADSs. That said, these measures need to be implemented effectively to keep users safe. D-ADSs must address the weaknesses identified and remain vigilant to emerging risks.

Follow-up Actions Needed

- a. **Age Assurance.** D-ADSs should continue to ensure that their AA measures cannot be easily circumvented. Huawei AppGallery needs to continue to monitor and reduce the percentage of users able to circumvent the AA checks.
- b. **Enhanced Protections for Children.** D-ADSs should ensure that children are restricted by default from downloading 18+ apps. Microsoft Store needs to fully address the remaining instances where these restrictions could be bypassed.
- c. **Effectiveness of App Review.** All D-ADSs should improve their content moderation and app review processes to prevent apps that contain or facilitate harmful content from slipping through existing safeguards.
- d. **Appropriateness of App Age Ratings.** Apple App Store, Google Play Store, and Huawei AppGallery need to strengthen their age-rating processes to ensure that apps are appropriately rated, and that children are restricted from accessing 18+ apps containing or facilitating age-inappropriate content.
- e. **Effectiveness of User Reporting and Resolution Measures.** All D-ADSs should ensure that reporting users are notified of the outcomes of their reports. Google Play Store and Samsung Galaxy Store need to notify users who had within the previous six months downloaded app(s) that had been removed by the D-ADS for a violation.
- f. **Accountability.** Google Play Store, Huawei AppGallery, and Samsung Galaxy Store need to improve the metrics in their next annual online safety reports to demonstrate the effectiveness of their user reporting and resolution mechanisms.



IMDA's Online Safety Assessment Report and the D-ADSs' annual online safety reports are published in full on IMDA's website at www.imda.gov.sg/online-safety for public reference.

Main Report

Introduction



- 01** App Distribution Services (ADSs), also known as app stores, are key gateways to accessing apps and online content. More people, including children, use mobile devices and can access app stores to download apps easily. Therefore, there is an increased risk of exposure to harmful and age-inappropriate content for children.
- 02** Singapore has introduced regulatory measures that require online communication services to put in place safety measures to safeguard Singapore users from harmful online content.
- 03** In November 2022, Singapore passed the Online Safety (Miscellaneous Amendments) Act (OSMAA) which introduced a new section to the Broadcasting Act to regulate Online Communication Services, such as Social Media Services (SMSs) and ADSs. The Broadcasting Act empowers IMDA to direct any SMS or ADS to block access to egregious content and apps on their services respectively. The Broadcasting Act also empowers IMDA to issue legally binding Codes of Practice and designate services with significant reach or impact in Singapore to comply with such Codes of Practice.
- 04** IMDA issued the Code of Practice for Online Safety – App Distribution Services (ADS Code) which took effect from 31 March 2025. Five ADSs were designated for a start: Apple App Store, Google Play Store, Huawei AppGallery, Microsoft Store,¹ and Samsung Galaxy Store. These Designated ADSs (D-ADSs) must have in place system-wide measures to minimise Singapore users' exposure to, and mitigate the impact of, harmful content on their services.
- 05** IMDA will continue to review and strengthen Singapore's online safety framework as technology, services and online harms evolve, including assessing whether additional requirements are needed for other types of online communication services.

Code of Practice for Online Safety – App Distribution Services

- 06** The ADS Code outlines system-level measures to minimise users' exposure to harmful content. The ADS Code takes an outcomes-based approach and gives D-ADSs the flexibility to design their measures to achieve these outcomes. See [Annex A](#) for the full text of the ADS Code.

¹ Microsoft Store comprises five storefronts - Microsoft Store on Windows, Apps.microsoft.com Website Store, PC Games Store, Xbox console storefront, and the part of Xbox.com Website having the characteristics of an app distribution service as specified in the Fourth Schedule of the Broadcasting Act 1994.

Singapore's Code of Practice for Online Safety — App Distribution Services

What must Designated App Distribution Services do?

01



Enhance User Safety, Including Enhanced Protections for Children

- Minimise users' exposure to harmful content through content guidelines and effective content moderation.
- Proactive detection and removal of Child Sexual Exploitation and Abuse Material and terrorism content, and related preparatory activities.
- Age assurance measures and differentiated accounts for children with default restrictive settings.
- Safety information and parental tools.
- Policies for app providers of apps with User Generated Content (UGC) functionalities to ensure content moderation, in-app user reporting, and appropriate actions against providers where necessary.

02



Empower Users through User Reporting and Resolution

- Have effective and easy mechanisms for users to report harmful/inappropriate content.
- Assess user reports and take appropriate actions in a timely and diligent manner.
- Inform users of actions taken on their reports, and users who have within last six months downloaded apps that were subsequently removed for violations.

03



Ensure Accountability

- Submit annual online safety reports to be published on IMDA's website.
- Reports to contain clear information on online safety measures and supported by suitable data, so that users may make informed choices on their use of the respective Designated ADS.

Aim of the Online Safety Assessment Report

- 07** The first Online Safety Assessment Report (OSAR) for Designated App Distribution Services aims to inform Singapore users of:
- The online safety measures that the D-ADSs have in place, as required by the ADS Code.
 - The **Presence, Comprehensiveness, and Effectiveness** of these online safety measures to mitigate risks from harmful and inappropriate content.
 - The areas of weakness in the D-ADSs' online safety measures that they must address.
- 08** This allows Singapore users to make informed decisions for themselves and their children about the online safety risks and available safety measures when using the various D-ADSs and ensures that the D-ADSs are accountable for providing a safe experience for their users.

Methodology

- 09** The OSAR was prepared using the following sources:
- Information and data from the D-ADSs' annual online safety reports covering the period from 1 April 2025 to 31 December 2025, and
 - Empirical data such as: (i) harmful apps and content detected by or reported to IMDA by members of the public, and (ii) data from IMDA's testing of the D-ADSs' online safety measures.
- 10** The Effectiveness of the D-ADSs' online safety measures was assessed via the following methods:
- Setting up test accounts** to simulate the real-world experience of Singapore users. For example, to assess the effectiveness of the D-ADSs' child safety measures, IMDA tested whether child accounts were provided with more restrictive default settings, such as restrictions from downloading 18+ apps, how easily children could download 18+ apps, and whether parents/guardians were provided with tools to manage the experience of child accounts.
 - Mystery Shopper tests** were conducted to test the effectiveness of D-ADSs' safety measures to address harmful and age-inappropriate apps, by detecting and reporting harmful and mis-rated apps that violated the D-ADSs' content guidelines and measuring if they took the appropriate action and in a timely manner.

Examples of How Testing was Conducted

Example 1: Effectiveness of D-ADSs' Age Assurance (AA) measures

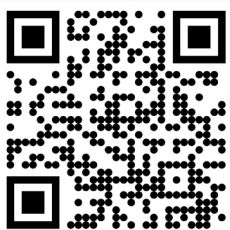
Methodology: The ADS Code requires all D-ADSs to implement AA measures to establish the age or age range of ADS user with reasonable accuracy. As a start, D-ADSs are expected to determine which users are children and prevent them from accessing apps rated 18+. For this test, IMDA tested the stage of the user journey at which the AA check was applied (e.g. upon access to the D-ADS or upon download of an 18+ app), and the robustness of the AA method(s), such as whether the method could be circumvented easily. Testing was also conducted across different device types (such as mobile and desktop) to assess whether AA was implemented consistently.

Findings: The test found that AA measures were present across all D-ADSs and largely effective in establishing the age or age range of users with reasonable accuracy, specifically if they are above or below 18 years old. The AA methods generally could not be easily circumvented, except for a small percentage of users on Huawei AppGallery. Please refer to the Executive Summary and Detailed Assessments of D-ADSs for more details on the findings.

Example 2: Effectiveness of D-ADSs' safety measures for harmful apps through app review processes to minimise users' exposure to harmful content (Mystery Shopper Test)

Methodology: The ADS Code requires D-ADSs to have content guidelines and standards that covers the six harmful content categories and content moderation measures such as review of apps before and after publication. The D-ADSs are expected to enforce their own content guidelines effectively. For this test, IMDA conducted mystery shopper testing of over 7,000 apps across all the D-ADSs to detect apps that contain or facilitate harmful content, based on the D-ADSs' content guidelines. Potentially harmful apps were reported via the D-ADSs' user reporting mechanisms, with the notification of outcome and action recorded.

Findings: The test found 65 apps that contained or facilitated harmful content across all the D-ADSs, which violated the D-ADSs' own policies and were removed after IMDA's mystery shopper user reporting or IMDA's reporting. IMDA also found that the D-ADSs either did not consistently or failed to inform users of the outcome of their user reports. Please refer to the Executive Summary and Detailed Assessments of D-ADSs for more details on the findings.



IMDA's Online Safety Assessment Report and the D-ADSs' annual online safety reports are published in full on IMDA's website at www.imda.gov.sg/online-safety for public reference.

Detailed Assessments of Designated App Distribution Services



Apple App Store

Section Ai: User safety measures for all users

- 01** Apple App Store had the required content guidelines and standards in its App Review Guidelines, and content moderation measures for all ADS users. However, there were weaknesses in its enforcement as IMDA detected 30 apps that contained or facilitated harmful content.
 - a. Apple App Store's content guidelines covered the six categories of harmful content in the ADS Code, and content moderation included a combination of human and automated reviews at multiple stages of the app life cycle (from pre-publication, updates, and monitoring existing apps on App Store).
 - b. While content moderation measures were largely effective, IMDA detected 30 apps that contained or facilitated harmful content relating to sexual content (e.g., dating, social networking, and AI chatbot/companion apps featuring sexually explicit content or interactions, gaming apps featuring AI-generated nude or pornographic content, and AI-powered apps with nudification or non-consensual intimate imagery functionalities).
 - c. Following IMDA's mystery shopper user reporting or IMDA's reporting, Apple App Store removed all 30 apps.
- 02** Apple App Store provided easily accessible and understandable online safety information through a dedicated online safety webpage on its online safety efforts, including how to report unlawful or harmful content on the App Store, parental controls, App Store age-ratings, and App Review Guidelines.
- 03** Apple App Store reported comprehensive measures to proactively detect and remove apps containing or facilitating Child Sexual Exploitation and Abuse Material (CSEM) and terrorism content and preparatory activity.

Section Aii: User safety measures for children

04 Apple App Store had the required content guidelines and standards in its App Review Guidelines and age-rating system for children. However, there were weaknesses in the application of its age-rating framework to ensure that apps are appropriately rated. IMDA detected 11 mis-rated apps that should have been rated 18+ under its age-rating policies but were assigned a lower rating instead.

- a. Apple App Store’s content guidelines and age-rating system covered the four categories of inappropriate content, and content moderation was effected by assigning appropriate app age ratings.
- b. While content moderation measures were largely effective, IMDA detected 11 mis-rated apps that contained or facilitated inappropriate content relating to sexual content (e.g., dating and social networking apps centred on romantic or sexual connections), and content facilitating vice and organised crime (e.g., gaming apps simulating criminal activities such as drug dealing and gang-related activities).
- c. Following IMDA’s mystery shopper user reporting or IMDA’s reporting, Apple App Store engaged the relevant developers on the inappropriate age ratings. All 11 apps were subsequently adjusted to higher age-ratings (18+), including one app whose age rating was adjusted by the developer.

05 Apple App Store had implemented the required Age Assurance (AA) measures using methods approved by IMDA. These included credit card check and account tenure as primary methods, with government ID verification (e.g. passport, driving licence, NRIC, or FIN card) available as a secondary method.

- a. However, public feedback identified areas where the user experience in completing AA could be improved. For example, inclusivity could be improved to ensure all users have access to at least one method of age check, as some users did not have credit cards or the required device specifications to run iOS 26 necessary for government ID verification. The lack of support for digital forms of government ID was also a limitation for users that did not possess the necessary physical government ID.

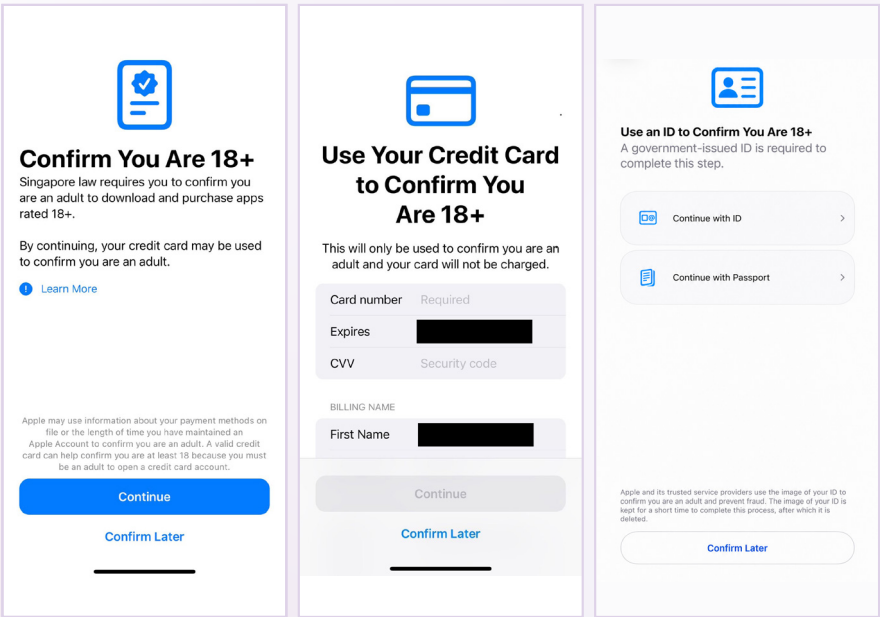


Figure 1: Apple App Store’s age assurance prompts

- b. Following IMDA's engagement, Apple shared that it is actively working on improvements for the coming year, including exploring alternative solutions for users who are unable to complete AA based on current options.

06 **Apple App Store provided child accounts with more restrictive default settings to limit children's access and exposure to age-inappropriate apps.** These included restricting the download of 18+ apps for users under 18 years of age, and restricting apps with age-ratings above a child's age from appearing by default in the App Store's recommendation feed.

- a. However, IMDA's tests found that no warnings were provided to parents and guardians on the implications of opting out of the default content restrictions for child accounts through Family Sharing, to allow apps with age-ratings above a child's age to appear in the App Store's recommendation feed. IMDA will continue to engage Apple on this issue.

07 Apple App Store's parental tools were present and comprehensive, including content filters (for both search and download) and download approval mechanisms. However, this would only be accessible if parents link their children's account via Family Sharing.

- a. Parent-linked accounts were only mandatory for users under 16 years of age. Consequently, parental tools would not be available for 16- to 17-year-old children if parents do not set up parent-linked accounts.
- b. To help make its parental tools more accessible, Apple App Store had published a guide on how parents and guardians can set up parental controls to manage their children's safety.

Section Aiii: User Safety Measures for Apps with User-Generated Content ('UGC') Functionality

08 Apple App Store reported comprehensive policies requiring UGC app providers to have content moderation measures and in-app user reporting mechanisms, and provided for appropriate actions against app providers that failed to resolve user reports in accordance with its policies. However, there were weaknesses in Apple App Store's enforcement of these requirements for UGC apps on the App Store. **During the period of assessment, IMDA found a UGC app on Apple's App Store which lacked the required content moderation and user reporting mechanisms.** Following IMDA's engagements on this issue, Apple App Store engaged with the app developer to add sufficient moderation and reporting mechanism.

Section B: User reporting and resolution

09 Apple App Store reported comprehensive reporting mechanisms in place through in-app store flagging or dedicated online webforms.

- a. However, IMDA's tests found some inconsistencies in Apple App Store's notification of reporting outcomes to users. Following IMDA's engagement, Apple App Store has investigated and ensured that such processes were in place.

Section C: Accountability

10 Apple App Store provided clear information in its annual online safety report, and metrics previously approved by IMDA.

- a. With regard to paragraph 29(a) of the ADS Code on the volume and outcomes of ADS user reports, Apple App Store provided the data broken down by the content categories, as well as CSEM and terrorism content (refer to [Table 1](#)).
- b. With regard to paragraph 29(b) of the ADS Code on the prevalence of violating or non-compliant apps on the app store that are accessible by ADS users in Singapore and app providers providing such apps, Apple App Store reported that it had detected and removed a total of 48,404 non-compliant apps (48,123 relating to content facilitating vice and organised crime, 270 relating to sexual content, 9 relating to content endangering public health, and 2 relating to violent content), and 42,536 app providers providing such apps (42,274 relating to content facilitating vice and organised crime, 251 relating to sexual content, 9 relating to content endangering public health, and 2 relating to violent content) (refer to [Table 2](#)).
 - i. Apple App Store stated that “content facilitating vice and organised crime” includes instances of gambling, and scams or fraud. Scams or fraud is one of Apple App Store’s largest categories of app removals. This includes apps removed for bait and switch manoeuvres, where apps were initially approved as standard games or utilities, such as a puzzle or calculator app, and were subsequently modified post-review with the intent of financial fraud. It also includes apps published by developers who were terminated because they shared commonalities with other terminated developers.
- c. With regard to paragraph 29(c) of the ADS Code on the time taken to review and address ADS user reports, Apple App Store provided the median time it took to take action on ADS user reports in Singapore, broken down by the content categories as well as CSEM and terrorism content (refer to [Table 3](#)).
- d. With regard to paragraph 29(d) of the ADS Code on the proactive actions in detecting and addressing violating/non-compliant apps, Apple App Store provided aggregated data that 2,093,244 apps were rejected before publication on the App Store but there was no breakdown by content categories in the additional metrics provided via a link to its Transparency Report. Apple App Store should improve the presentation of its metrics in its second online safety report by providing a breakdown of apps proactively detected and actioned across the content categories in the ADS Code.

Content Categories	Volume	Action Taken		
	Number of User Reports Received	App Removed	3 rd Party Notified ¹	No Action Taken
Sexual Content	1	0	1	0
Violent Content	0	0	0	0
Suicide and self-harm content	0	0	0	0
Cyberbullying content	0	0	0	0
Content endangering public health	0	0	0	0
Content facilitating vice and organised crime	2	0	0	2
Child sexual exploitation and abuse material	9	1	8	0
Terrorism content	3	0	3	0

Table 1: Data provided by Apple App Store for paragraph 29(a) of the ADS Code: The number of ADS user reports received and outcomes, broken down by content categories

Content Categories	Number of Apps Removed	Number of App Providers Associated with Removed Apps
Sexual Content	270	251
Violent Content	2	2
Suicide and self-harm content	0	0
Cyberbullying content	0	0
Content endangering public health	9	9
Content facilitating vice and organised crime	48,123	42,274
Child sexual exploitation and abuse material	0	0
Terrorism content	0	0

Table 2: Data provided by Apple App Store for paragraph 29(b) of the ADS Code: The number of violating or non-compliant apps and the number of app providers providing such apps, broken down by content categories

¹ Apple App Store clarified that each of the notices in this column concerned content hosted on the Telegram app. In accordance with Apple App Store's policies on user-generated content, Apple App Store forwarded these notices to Telegram for handling.

Content Categories	Median Time To Resolution
Sexual Content	3 days
Violent Content	0
Suicide and self-harm content	0
Cyberbullying content	0
Content endangering public health	0
Content facilitating vice and organised crime	4 days, 17 hours
Child sexual exploitation and abuse material	4 days, 7 hours
Terrorism content	7 days, 2 hours

Table 3: Data provided by Apple App Store for paragraph 29(c) of the ADS Code: The time taken to review and address ADS user reports broken down by content categories

Apple App Store's Response

Apple continues to build on our commitment to providing a safe and secure experience on the App Store for all users. We welcome IMDA's Online Safety Assessment Report and appreciate the collaborative approach to protecting users online.



Section Ai: User safety measures for all users

- 01** Google Play Store had the required content guidelines and standards in its Developer Programme Policies, and content moderation measures for all ADS users. However, there were weaknesses in its enforcement as IMDA detected 10 apps that contained or facilitated harmful content.
- a. Google Play Store's content guidelines covered the six harmful content categories in the ADS Code, and content moderation included a combination of human and automated reviews at multiple stages of the app life cycle (pre-publication updates, and while on the Google Play Store).
 - b. While content moderation measures were largely effective, IMDA detected 10 apps that contained or facilitated harmful content relating to sexual content (AI chatbot/companion apps featuring sexually explicit content or interactions, gaming apps featuring AI-generated nude or pornographic content, and AI-powered apps with nudification or non-consensual intimate imagery functionalities).
 - c. Following IMDA's mystery shopper user reporting or IMDA's reporting, Google Play Store removed all 10 apps.
- 02** Google Play Store provided easily accessible and understandable online safety information through its information pages such as those on Google Play Developer Programme Policies, Google Play Families Policies, Family Link and their Help Center - including how to report unlawful or harmful content on the Play Store, parental controls, Play Store age-ratings, and app review Guidelines.
- 03** Google Play Store reported comprehensive measures to proactively detect and remove Child Sexual Exploitation Material (CSEM) and terrorism content and preparatory activity.

Section Aii: User safety measures for children

- 04** Google Play Store had the required content guidelines and standards in its Developer Programme Policies and age-rating system for children. However, there were weaknesses in the application of its age-rating framework to ensure that apps are appropriately rated. IMDA detected 10 mis-rated apps that should have been rated 18+ under its age-rating policies but were assigned a lower rating instead.
- a. Google Play Store's content guidelines and age-rating system covered the four categories of inappropriate content and content moderation was effected by assigning appropriate age-ratings.
 - b. While content moderation measures were largely effective, IMDA detected 10 mis-rated apps that contained or facilitated inappropriate content relating to sexual content (e.g. AI chatbot/companion apps with "spicy" or "roleplay" elements, and dating and social networking apps centred on romantic or sexual connections), and content facilitating vice and organised crime (e.g. gaming apps simulating criminal activities such as drug dealing and gang-related activities).
 - c. Following IMDA's mystery shopper user reporting or IMDA's reporting, Google Play Store engaged the relevant developers on the inappropriate age ratings. All 10 apps were subsequently adjusted to higher age-ratings (18+).

05 Google Play Store has implemented the required Age Assurance (AA) measures using methods approved by IMDA. This included age inference via behavioural signals as a primary method, with credit card check, government ID verification (e.g. passport, driving licence, NRIC or FIN card), facial age estimation and email verification as secondary methods.

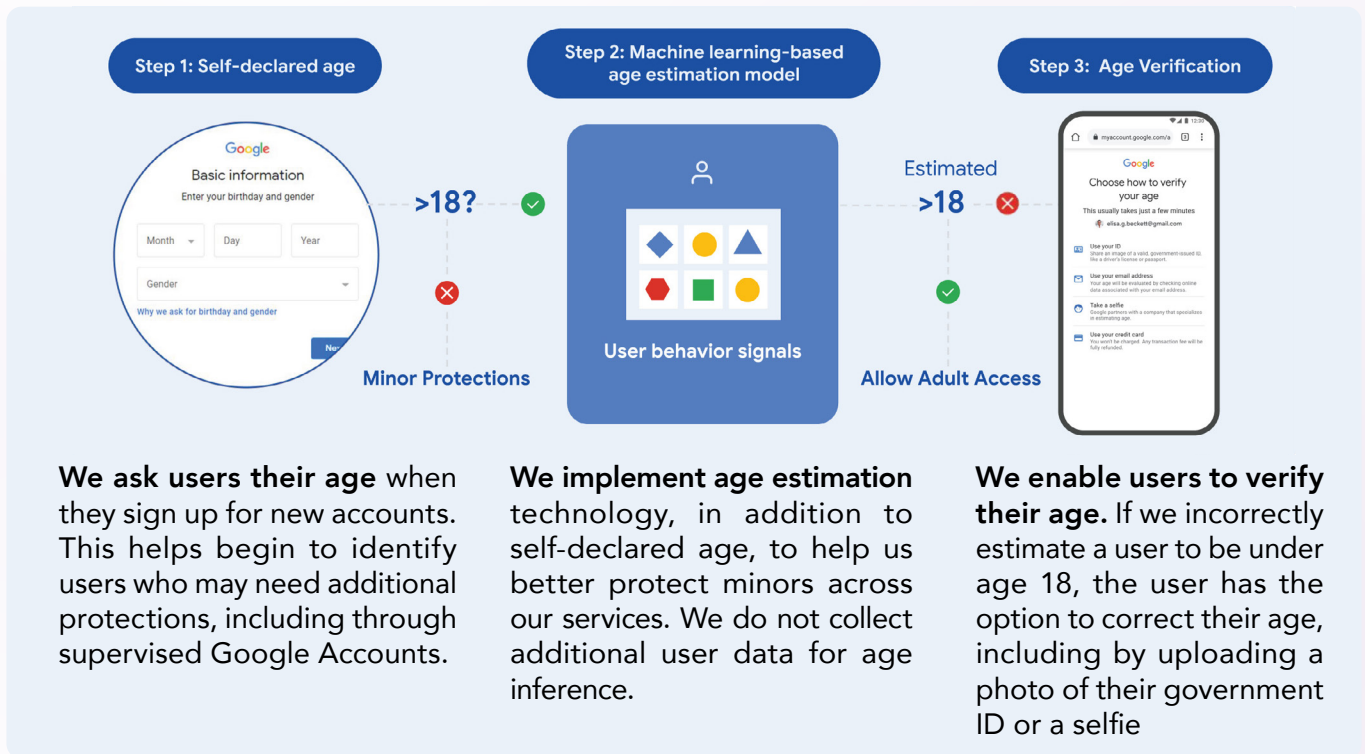


Figure 1: Google Play Store's age assurance process (Source: Google Play Store)

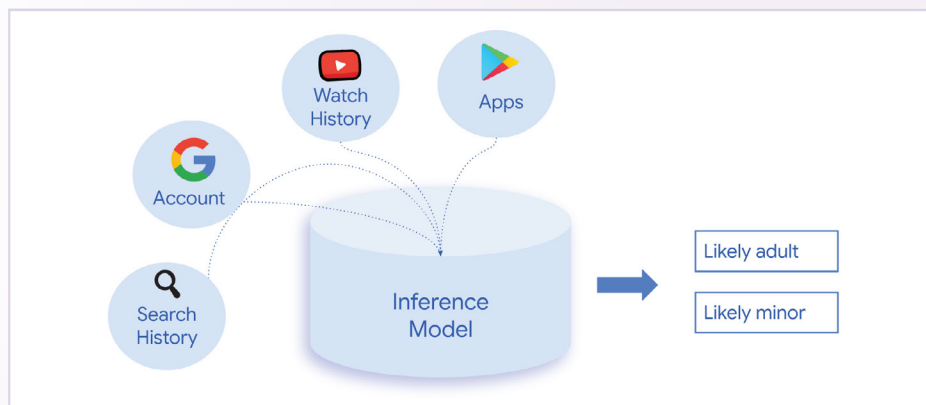


Figure 2: Google Play Store's age inference model based on behavioural signals (Source: Google Play Store)

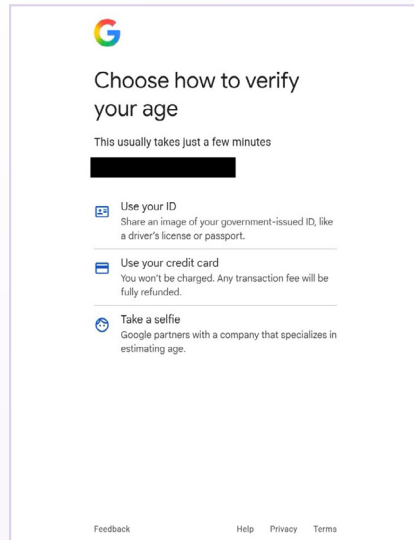


Figure 3: Google Play Store's secondary methods of age assurance

06 Google Play Store provided child accounts with more restrictive default settings to limit children's access and exposure to age-inappropriate apps. This included restricting the download of 18+ apps for users under 18 years of age, and restricting children from searching for 18+ apps.

- a. However, IMDA's tests found that no warnings were provided to parents and guardians on the implications of opting out of the default content restrictions for child accounts through Google Family Link to allow children to search for and view apps with age-ratings above a child's age. In response to IMDA's engagements, Google Play Store stated that the baseline protection to restrict all under 18 users in Singapore from browsing, downloading and purchasing apps that are rated 18+ does not depend on the choices made by parents. Notwithstanding the baseline protections in place, the ADS Code requires that clear warnings of implications be provided when opting out of the default settings of children accounts. Google must provide these warnings.

07 Google Play Store's parental tools were present and overall comprehensive, including content filters (for both search and download), screen time limits and download approval mechanisms. However, the full suite of parental tools would only be accessible if parents link their children's account via Google Family Link.

- a. Parent-linked accounts are only mandatory for users under 13-years-old. Consequently, parental tools may potentially be absent for 13- to 17-years-old children if parents do not set up parent-linked accounts.
- b. The process of linking a child's account via Family Link was detailed, including multiple steps and verification, which could cause friction for parents wishing to use the full suite of parental tools.
- c. Since the reporting period, Google Play Store has introduced limited parental tools directly on Android devices running Android 17, including the ability to limit or block app usage, and apply Google Play content restrictions. Settings are protected by a parent PIN, without the need to set up Google Family Link. Parents are encouraged to utilise the tools provided by Android 17 and Google Family Link to manage their children's usage of the Google Play Store.
- d. To help make its parental tools more accessible, Google Play Store had published a guide on how parents and guardians can set up parental controls to manage their children's safety.

Section Aiii: User safety measures for apps with user generated content ("UGC") functionality

- 08** Google Play Store reported comprehensive policies requiring UGC app providers to have content moderation measures and in-app user reporting mechanisms, and provided for appropriate actions against app providers that failed to resolve user reports in accordance with its policies. However, there were weaknesses in Google Play Store's enforcement of these requirements for UGC apps on the Play Store. **During the period of assessment, IMDA found that two UGC apps on the Play Store lacked required features such as content moderation and user reporting mechanisms.** Following IMDA's engagements on this issue, Google Play Store engaged with the relevant app developers to implement the required features on the apps.

Section B: User reporting and resolution

- 09** Google Play Store reported comprehensive reporting mechanisms in place through in-app store flagging or dedicated online webforms. Their report also detailed the resolution mechanisms which included a mandatory Statement of Resolution ("SOR") which would be issued to all user reports explaining the action taken or otherwise. This SOR also functioned as the basis of the appeal mechanism should the user disagree with the decision made by Google Play Store.
- a. However, IMDA's tests found some inconsistencies in Google Play Store's notification of reporting outcomes to users. Following IMDA's engagement, Google Play Store has investigated and ensured that such processes were in place.
- 10** Google Play Store also did not report having a process in place to inform users who had downloaded a reported app (within the last six months) that the app had been removed due to a violation.
- a. In response to IMDA's engagements on this issue, Google Play Store stated that the implementation of user notifications was challenging due to significant technical and operational complexity. Google Play Store further asserted that safeguards against suspended apps are in place, with users unable to view the app store's listing, download or update the app, or make any in-app purchases, which significantly reduces the user's ability to use the app and accelerates the natural end to the app's lifecycle. Google is required to put in place a notification process.

Section C: Accountability

11 Google Play Store provided the information and metrics previously approved by IMDA for its first annual online safety report.

- a. With regard to paragraph 29(a) of the ADS Code on the volume and outcomes of ADS user reports, Google Play Store provided the volume of user reports broken down by the content categories¹ (refer to [Table 1](#)).
- b. With regard to paragraph 29(b) of the ADS Code on the prevalence of violating or non-compliant apps on the app store that are accessible by ADS users in Singapore and app providers providing such apps, Google Play Store reported that 46,276 enforcement actions were taken against apps available in Singapore for violations of their policies in relation to harmful content categories (20,814 relating to content endangering public health, 20,623 relating to content facilitating vice and organised crime, 4,473 relating to sexual content, 365 relating to violent content and 1 relating to cyberbullying content), and 0 app providers providing such apps (refer to [Tables 2 and 3](#)).
- i. Google Play Store stated that while enforcement actions were taken against developers with apps available in Singapore, none of those enforcement actions fell within policies that cover the harmful and inappropriate content categories in the ADS Code.
- c. With regard to paragraph 29(d) of the ADS Code on the proactive actions detecting and addressing violating/non-compliant apps, Google Play Store reported that 46,237 of the 46,276 enforcement actions taken against apps available in Singapore for violations of their policies in relation to harmful content categories were taken after automated detection by automated models, while the remaining 39 enforcement actions were taken after non-automated detection by human reviewers (refer to [Table 4](#)).

12 With regard to paragraph 29(a) of the ADS Code on the volume and outcomes of ADS user reports, Google Play Store's metric for outcomes of ADS user reports will need to be improved in the next annual online safety report.

- a. For the reporting period, Google Play Store stated that enforcement actions were taken on 1,415 user reports of policy violations without breakdown by content categories. Google Play Store's metric approved for the first annual online safety report, "number of ADS user reports for policy violation by Singapore ADS users that resulted in an enforcement action without further breakdown by policy violations" did not fully meet the intent of the ADS Code.
- b. Following IMDA's engagement, Google Play Store has committed to providing user report enforcement actions broken down by policy violation under Singapore's Harmful Content Categories for future online safety reports.

¹ Google Play Store uses the term "Policy Violation".

13 With regard to paragraph 29(c) of the ADS Code on time taken to review and address user reports, Google Play Store's metric will need to be improved in the next annual online safety report.

- a. For the reporting period, Google Play Store stated that it had reviewed 96% of user reports within 7 days. Google Play Store's metric approved for the first annual online safety report, "percentage of ADS user reports that meet Service Level Agreement (SLA) standards in reviewing Singapore ADS user reports, without further breakdown by policy violations as SLA will be applicable to all policy violations" did not fully meet the intent of the ADS Code.
- b. IMDA will continue to engage Google on providing a better metric such as an absolute turn around time for reviewing and addressing user reports, with a breakdown by content categories.

Content Categories	Number of User Reports Received
Sexual Content	21
Violent Content	0
Suicide and self-harm content	0
Cyberbullying content	0
Content endangering public health	0
Content facilitating vice and organised crime	211

Table 1: Data provided by Google Play Store for paragraph 29(a) of the ADS Code: The number of ADS user reports received and outcomes, broken down by content categories

Content Categories	Number of Enforcement Actions
Sexual Content	4,473
Violent Content	365
Suicide and self-harm content	0
Cyberbullying content	1
Content endangering public health	20,814
Content facilitating vice and organised crime	20,623

Table 2: Data provided by Google Play Store for paragraph 29(b) of the ADS Code: The number of violating or non-compliant apps, broken down by content categories

Content Categories	Number of Enforcement Actions
Sexual Content	0
Violent Content	0
Suicide and self-harm content	0
Cyberbullying content	0
Content endangering public health	0
Content facilitating vice and organised crime	0

Table 3: Data provided by Google Play Store for paragraph 29(b) of the ADS Code: The number of app providers providing such apps, broken down by content categories²

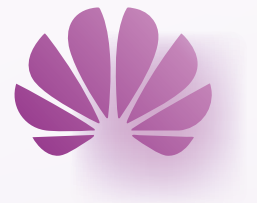
Content Categories	Number of Actions Taken (After Automated Detection)	Number of Actions Taken (After Non-Automated Detection)
Sexual Content	4,459	14
Violent Content	364	1
Suicide and self-harm content	0	0
Cyberbullying content	1	0
Content endangering public health	20,814	0
Content facilitating vice and organised crime	20,599	24

Table 4: Data provided by Google Play Store for paragraph 29(d) of the ADS Code: The number of violating or non-compliant apps that were proactively detected and addressed, broken down by content categories

Google Play Store's Response

Play appreciates the continued engagement with the Singapore government on online safety and we remain committed to protecting Singaporeans online.

² Google Play Store noted that it took enforcement actions against developers with apps available in Singapore during the reporting period. However, none of those enforcement actions fell within policies that cover the harmful and inappropriate content categories in the ADS Code.



Section Ai: User safety measures for all users

01 Huawei AppGalley had the required content guidelines and standards in its AppGalley Review Guidelines, and content moderation measures for all ADS users. However, there were weaknesses in its enforcement as IMDA detected 11 apps that contained or facilitated harmful content.

- Huawei AppGalley's content guidelines covered the six categories of harmful content in the ADS Code, and content moderation included a combination of human and automated reviews at multiple stages of the app life cycle (pre-publication, updates, and "special re-tests").
- While content moderation measures were largely effective, IMDA detected 11 apps that contained or facilitated harmful content relating to sexual content (e.g., dating apps with sexual emphasis, gaming apps with sexually suggestive categories, and apps with sex tips), violent content (e.g., gaming apps inciting horror/fear) and content facilitating vice & organised crime (e.g., Jackpot gambling app with real-money pay-out).
- Following IMDA's mystery shopper user reporting or IMDA's reporting, Huawei AppGalley removed all 11 apps.

02 Huawei AppGalley did not have the necessary public resources and information on its content moderation and user reporting measures. Following IMDA's engagement, Huawei AppGalley published public resources and information on its Community page for consumers, to explain its content moderation measures and user reporting channels. Baseline public resources and information on its content guidelines were also present via its published AppGalley Review Guidelines.

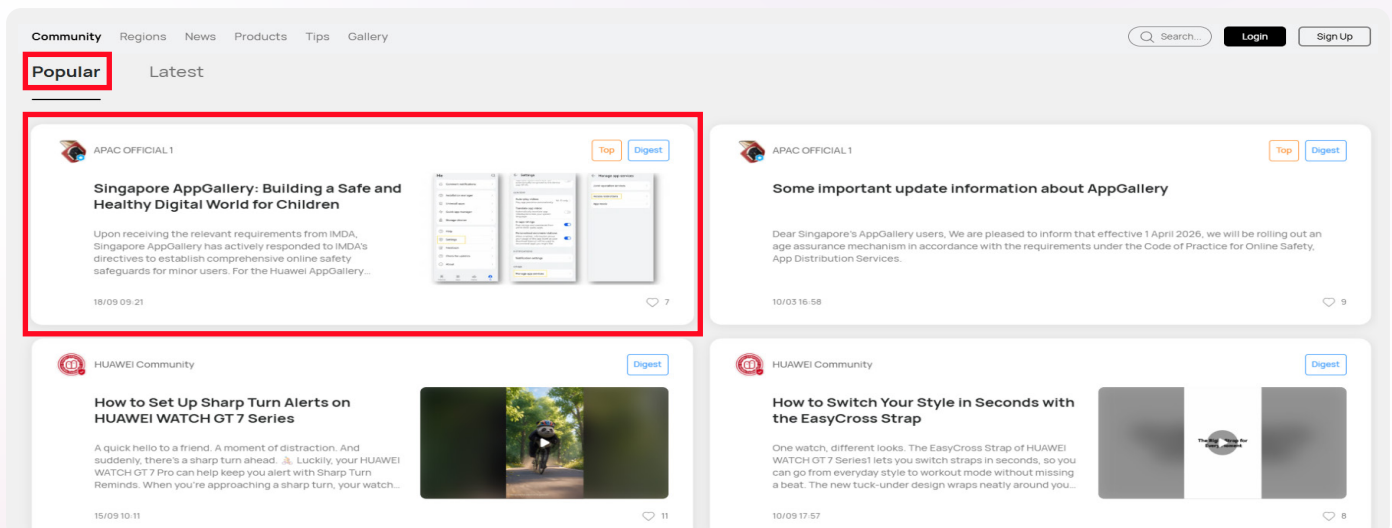


Figure 1: Public resource on Huawei AppGalley's Community page for consumers, to explain its content moderation measures and user reporting channels (Source: Huawei AppGalley)

03 Huawei AppGalley reported comprehensive measures to proactively detect and remove apps containing or facilitating Child Sexual Exploitation Material (CSEM) and terrorism content and preparatory activity.

Section Aii: User safety measures for children

04 Huawei AppGallery had the required content guidelines and standards in its AppGallery Review Guidelines and age-rating system for children. However, there were weaknesses in the application of Huawei AppGallery's age-rating framework to ensure that apps were appropriately rated. IMDA detected 3 apps that should have been rated 18+ under Huawei AppGallery's age-rating policies but were assigned a lower rating instead.

- Huawei AppGallery's content guidelines and age-rating system covered the four categories of inappropriate content and content moderation was effected by assigning appropriate age ratings.
- While content moderation measures were largely effective, IMDA detected 3 mis-rated apps that contained or facilitated inappropriate content relating to violent content (e.g. gaming apps encouraging dangerous activities).
- Following IMDA's reporting, Huawei AppGallery engaged the relevant developers on the inappropriate age-ratings. All 3 apps were subsequently adjusted to higher age-ratings (18+).

05 Huawei AppGallery had implemented the required Age Assurance (AA) measures using a credit card check approved by IMDA. However, IMDA's sample tests found that a small percentage of users were able to circumvent the AA under specific circumstances on certain versions of the AppGallery due to technical limitations.

- Following IMDA's engagement, Huawei AppGallery investigated the issue and updated that only 7% of its users were affected. Huawei AppGallery has committed to working with IMDA to monitor and address the issue.

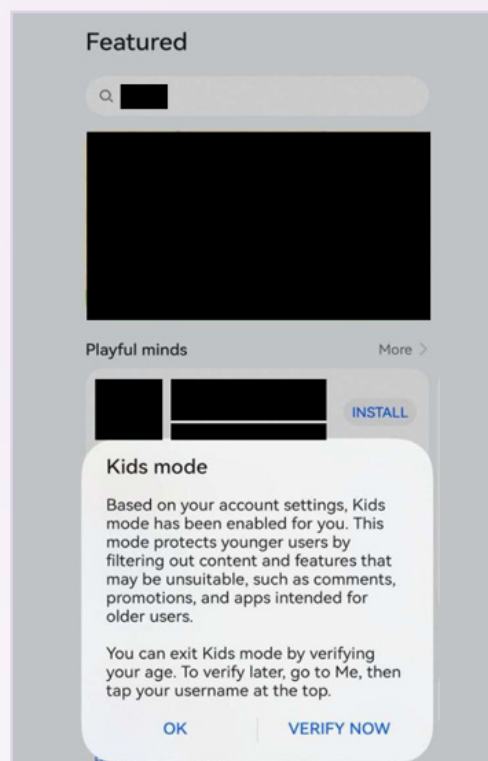


Figure 2: Huawei AppGallery's age assurance prompt

06 Huawei AppGallery provided child accounts with more restrictive default settings to limit children's access and exposure to age-inappropriate apps, including default restrictions on downloading 18+ apps. While these restrictions were largely applied, IMDA's tests found limited instances where restrictions were not present. Following IMDA's engagement, Huawei AppGallery has resolved the issue.

- 07** Huawei AppGallery’s parental tools were present and comprehensive via “Digital Balance” under the child’s device settings, including setting of screen time limits for Huawei AppGallery, blocking of specified apps and app download approvals.
- However, the “Digital Balance” feature was not mandatory and would only be accessible if parents took the initiative to set-up the “Digital Balance” settings.
 - To help make its parental tools more accessible, Huawei AppGallery had also published information on its “Digital Balance” for children in its community page.

Section Aiii: User safety measures for apps with user generated content (“UGC”) functionality

- 08** Huawei AppGallery reported comprehensive policies requiring UGC app providers to have content moderation measures and in-app user reporting mechanisms, and provided for appropriate actions against app providers that failed to resolve user reports in accordance with its policies. During the period of assessment, there were no violative UGC apps on Huawei AppGallery detected by or reported to IMDA.

Section B: User reporting and resolution

- 09** Huawei AppGallery reported comprehensive reporting mechanisms in place through in-app store reporting, customer hotline, or customer service chat functions.
- However, IMDA’s tests found that Huawei AppGallery did not provide notifications of reporting outcomes to users. Huawei AppGallery reported that it previously did not have a relevant process to inform users of the outcome of their reports given that it did not receive any user reports in 2025. Huawei AppGallery stated that it has since launched a “standard customer service support process” to provide the outcome to user reports under the user’s “feedback history”.

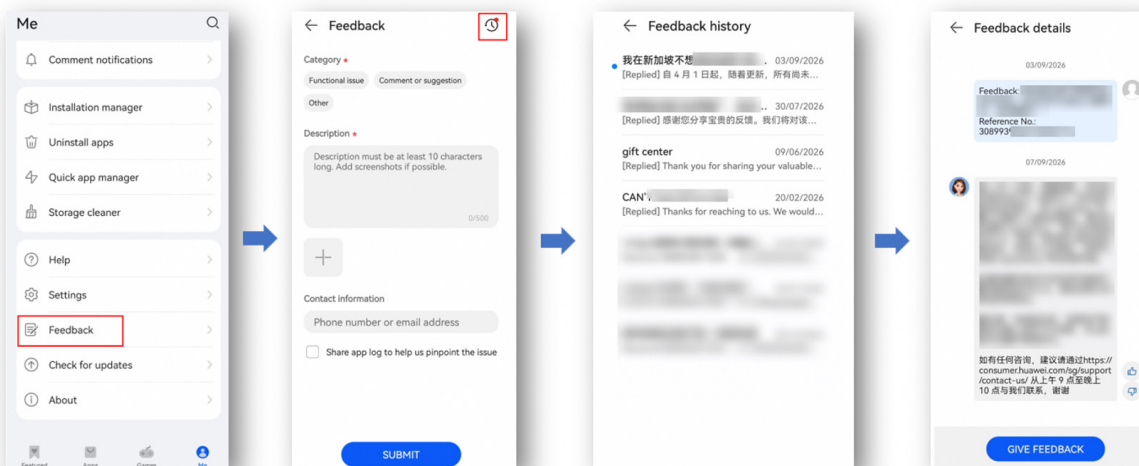


Figure 3: Huawei AppGallery’s response process to user reports (Source: Huawei AppGallery)

Section C: Accountability

10 Huawei AppGallery provided clear information in its first annual online safety report, and metrics previously approved by IMDA.

- With regard to paragraph 29(a) of the ADS Code on the volume and outcomes of ADS user reports, Huawei AppGallery reported zero user reports received (refer to [Table 1](#)).
- With regard to paragraph 29(b) of the ADS Code on the prevalence of violating or non-compliant apps on the app store that are accessible by ADS users in Singapore and app providers providing such apps, Huawei AppGallery reported it had detected and removed a total of 380 non-compliant apps (28 relating to sexual content and 352 are relating vice & organised crime), and 309 app providers providing such apps (28 relating to sexual content and 281 relating to vice & organised crime) (refer to [Table 2](#)).
- With regard to paragraph 29(d) of the ADS Code on the proactive actions in detecting and addressing violating/non-compliant apps, Huawei AppGallery provided the same data as that for paragraph 29(b) of the ADS Code i.e. 380 non-compliant apps (28 relating to sexual content and 352 are relating vice & organised crime) (refer to [Table 4](#)).

11 With regard to paragraph 29(c) of the ADS Code on time taken to review and address user reports, Huawei AppGallery's metric will need to be improved in the next annual online safety report.

- For the reporting period, Huawei AppGallery had zero user reports and hence, related data on time taken to review and address such reports was zero (refer to [Table 3](#)). Huawei AppGallery's metric approved for the first annual online safety report, "number of ADS user reports processed within the Service Level Agreement (SLA) time period of 7 business days broken down by content categories" did not fully meet the intent of the ADS Code.
- Following IMDA's engagement, Huawei AppGallery stated that it has added the relevant SLA processing time fields and that the data can be categorised, extracted, and provided for future online safety reports.

Content Categories	Total volume of ADS user reports received	Volume of ADS user reports assessed to be harmful / inappropriate with action taken	Volume of ADS user reports assessed to be not harmful / inappropriate with no action taken
Sexual Content	0	0	0
Violent Content	0	0	0
Suicide and self-harm content	0	0	0
Cyberbullying content	0	0	0
Content endangering public health	0	0	0
Content facilitating vice and organised crime	0	0	0

Table 1: Data provided by Huawei AppGallery for paragraph 29(a) of the ADS Code: The number of ADS user reports received and outcomes, broken down by content categories

Content Categories	Volume of violating or non-complaint apps accessible by ADS users in Singapore	Volume of apps providers providing violating or non-compliant apps accessible by ADS users in Singapore
Sexual Content	28	28
Violent Content	0	0
Suicide and self-harm content	0	0
Cyberbullying content	0	0
Content endangering public health	0	0
Content facilitating vice and organised crime	352	281

Table 2: Data provided by Huawei AppGallery for paragraph 29(b) of the ADS Code: The number of violating or non-compliant apps and the number of app providers providing such apps, broken down by content categories

Content Categories	Number of ADS user reports processed within the Service Level Agreement (SLA)
Sexual Content	N/A (0 user reports)
Violent Content	N/A (0 user reports)
Suicide and self-harm content	N/A (0 user reports)
Cyberbullying content	N/A (0 user reports)
Content endangering public health	N/A (0 user reports)
Content facilitating vice and organised crime	N/A (0 user reports)

Table 3: Data provided by Huawei AppGallery for paragraph 29(c) of the ADS Code: The number of ADS user reports processed within the SLA time of 7 business days, broken down by content categories

Content Categories	Volume of violating or non-compliant apps accessible by ADS users in Singapore proactively detected and addressed
Sexual Content	28
Violent Content	0
Suicide and self-harm content	0
Cyberbullying content	0
Content endangering public health	0
Content facilitating vice and organised crime	352

Table 4: Data provided by Huawei AppGallery for paragraph 29(d) of the ADS Code: The number of violating or non-compliant apps that were proactively detected and addressed, broken down by content categories

Huawei AppGallery's Response

Comprehensively building a robust cybersecurity defense line for minors, Huawei AppGallery in Singapore actively responded upon receiving requests from the IMDA. It has established a minor age verification mechanism for AppGallery in the Singapore service region, supplemented by tiered content moderation requirements and a healthy smartphone usage mode supporting parental controls over children's device usage, thereby providing minors with a safe, green, and healthy digital living environment.



Section Ai: User safety measures for all users

01 Microsoft Store¹ had the required content guidelines and standards in its Microsoft Store Policies, and content moderation measures for all ADS users. However, there were weaknesses in its enforcement as IMDA detected 3 apps that contained or facilitated harmful content.

- a. Microsoft Store's content guidelines covered the six categories of harmful content in the ADS Code and content moderation measures included a combination of human and automated reviews at multiple stages of app life cycle (pre-publication app certification, updates, and "random checks").
- b. While content moderation measures were largely effective, IMDA detected 3 apps that contained or facilitated harmful content relating to sexual content (e.g., gaming app with sexual challenges), and content facilitating vice & organised crime (e.g., BlackJack gambling app with crypto currency pay-out).
- c. Following IMDA's mystery shopper user reporting or IMDA's reporting, Microsoft Store removed all 3 apps.

02 Microsoft Store provided easily accessible and understandable online safety information through the Microsoft Digital Safety Site, including its content guidelines, content moderation and user reporting measures. Information on its content guidelines was also present via its published Microsoft Store Policies.

03 Microsoft Store reported comprehensive measures to proactively detect and remove apps containing or facilitating Child Sexual Exploitation Material (CSEM) and terrorism content and preparatory activity.

Section Aii: User safety measures for children

04 Microsoft Store had the required content guidelines and standards in its Microsoft Store Policies and age-rating system for children covering the four categories of inappropriate content in the ADS Code. Content moderation was effected by assigning appropriate age-ratings. During the period of assessment, there were no cases of mis-rated apps that were inappropriately age-rated as suitable for children according to its age-rating policies, detected by or reported to IMDA.

¹ Microsoft Store comprises five storefronts - Microsoft Store on Windows, Apps.microsoft.com Website Store, PC Games Store, Xbox console storefront, and the part of Xbox.com Website having the characteristics of an app distribution service as specified in the Fourth Schedule of the Broadcasting Act 1994.

05 Microsoft Store had implemented the required Age Assurance (AA) measures using methods approved by IMDA. This included Singpass, facial age estimation, and ID verification, provided by Yoti.

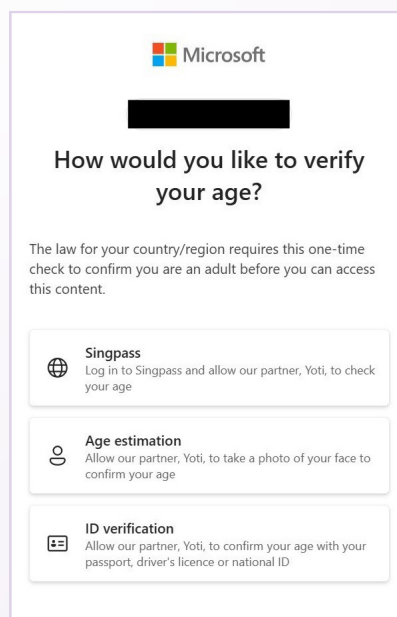


Figure 1: Microsoft Store's age assurance prompts

06 Microsoft Store provided child accounts with more restrictive default settings to limit children's access and exposure to age-inappropriate apps, including default restrictions on downloading 18+ apps. While these restrictions were largely applied across its five storefronts, IMDA's tests found limited instances where restrictions were not present. Following IMDA's engagement, Microsoft Store has identified the root causes and has implemented an interim solution as it works towards a permanent solution.

07 IMDA's tests also found a loophole in Microsoft Store's parental tools that allowed children to turn off the restriction on downloading 18+ apps. Parents who turned off these restrictions for children of their own accord were also not warned of implications of doing so. Microsoft Store is working towards solutions to fix these issues.

08 Microsoft Store's parental tools were present and comprehensive via "Microsoft Family Safety" (parent-linked accounts), including content filters (for both search and download) and download approval mechanisms.

- a. Parent-linked accounts were only mandatory for users under 13-years-old, and would only be accessible for 13- to 17-year-old children if parents took the initiative to set up the parent-linked accounts.
- b. To help make its parental tools more accessible, Microsoft Store had published toolkits and guides on how parents could utilise its parental tools to supervise and manage children's use of apps.

Section Aiii: User safety measures for apps with user generated content ("UGC") functionality

- 09** Microsoft Store reported comprehensive policies requiring UGC app providers to have content moderation measures and in-app user reporting mechanisms, and provided for appropriate actions against app providers that failed to resolve user reports in accordance with its policies. During the period of assessment, there were no violative UGC apps on Microsoft Store detected by or reported to IMDA.

Section B: User reporting and resolution

- 10** Microsoft Store reported comprehensive reporting mechanisms in place through in-app store flagging or dedicated online webforms.
- a. However, IMDA's tests found some inconsistencies in Microsoft Store's notification of reporting outcomes to users. Following IMDA's engagement, Microsoft Store has investigated and ensured that such processes were in place.

Section C: Accountability

- 11** Microsoft Store provided clear information in its first annual online safety report, and metrics previously approved by IMDA.
- a. Microsoft Store reported zero user reports received and zero non-compliant apps and app providers in relation to harmful and inappropriate content categories. Hence, all data points were zero (refer to [Tables 1 - 4](#)).

Content Categories	Total volume of ADS user reports received	Volume of ADS user reports assessed to be harmful / inappropriate with action taken	Volume of ADS user reports assessed to be not harmful / inappropriate with no action taken
Sexual Content	0	0	0
Violent Content	0	0	0
Suicide and self-harm content	0	0	0
Cyberbullying content	0	0	0
Content endangering public health	0	0	0
Content facilitating vice and organised crime	0	0	0

Table 1: Data provided by Microsoft Store for paragraph 29(a) of the ADS Code: The volume, breakdown by content category and outcomes of ADS user reports on the Service.

Content Categories	Volume of violating or non-complaint apps accessible by ADS users in Singapore	Volume of apps providers providing violating or non-compliant apps accessible by ADS users in Singapore
Sexual Content	0	0
Violent Content	0	0
Suicide and self-harm content	0	0
Cyberbullying content	0	0
Content endangering public health	0	0
Content facilitating vice and organised crime	0	0

Table 2: Data provided by Microsoft Store for paragraph 29(b) of the ADS Code: The prevalence and breakdown by content category of violating or non-compliant apps on the Service that are accessible by ADS users in Singapore; and app providers providing such apps

Content Categories	Timeliness at reviewing and addressing ADS user reports in Singapore
Sexual Content	N/A (0 user reports)
Violent Content	N/A (0 user reports)
Suicide and self-harm content	N/A (0 user reports)
Cyberbullying content	N/A (0 user reports)
Content endangering public health	N/A (0 user reports)
Content facilitating vice and organised crime	N/A (0 user reports)

Table 3: Data provided by Microsoft Store for paragraph 29(c) of the ADS Code: The timeliness of the Service's systems and processes at reviewing and addressing ADS user reports

Content Categories	Volume of violating or non-compliant apps accessible by ADS users in Singapore proactively detected and addressed
Sexual Content	0
Violent Content	0
Suicide and self-harm content	0
Cyberbullying content	0
Content endangering public health	0
Content facilitating vice and organised crime	0

Table 4: Data provided by Microsoft Store for paragraph 29(d) of the ADS Code: The effectiveness of the Service's proactive actions in detecting and addressing violating or non-compliant apps that are accessible by ADS users in Singapore.

Microsoft Store's response

Microsoft is committed to protecting our users, especially children, and enabling age-appropriate experiences, while balancing privacy, security, accessibility and freedom of expression.

Singapore was the first market in which Microsoft introduced age assurance of this kind on our Microsoft and XBOX storefronts. We are proud to have given people a choice of age assurance options including Singpass, facial age estimation using a selfie, and uploading an official government ID. Choice matters, because people have different needs, different access to documentation and different levels of comfort with each method. Being the first country also meant learning as we go, and the past year has taught us a great deal about how this works in practice for people in Singapore. There is no one-size-fits-all solution to protecting customers and we have taken those learnings forward to improve our systems, processes and the experience we offer users.

Microsoft values its positive and constructive working relationship with IMDA and the Singaporean Government. We are pleased to cooperate with IMDA on this assessment, and we look forward to working together to strengthen online safety for all Singaporean's, especially children and families.



Section Ai: User safety measures for all users

- 01** Samsung Galaxy Store had the required content guidelines and standards in its App Distribution Guide, and content moderation measures for all ADS users. However, there were weaknesses in its enforcement as IMDA detected 11 apps that contained or facilitated harmful content.
- a. Samsung Galaxy Store's content guidelines covered the six categories of harmful content in the ADS Code, and content moderation measures included a combination of human and automated reviews at multiple stages of app life cycle (pre-publication, updates, and "post-approval monitoring").
 - b. While content moderation measures were largely effective, IMDA detected 11 apps relating to sexual content (e.g. dating apps with sexual emphasis, gaming and novel apps with sexually suggestive categories).
 - c. Following IMDA's reporting, Samsung Galaxy Store removed ("suspended") all 11 apps.
- 02** Samsung Galaxy Store had baseline public resources and information on its content guidelines, user reporting and content moderation measures. However, Samsung Galaxy Store's user reporting information is limited and only available on Samsung's FAQ page for Age Assurance (AA) and online safety for children, which may not be intuitive for users seeking to report issues unrelated to AA or child safety.
- 03** Samsung Galaxy Store reported comprehensive measures to proactively detect and remove apps containing or facilitating Child Sexual Exploitation Material (CSEM) and terrorism content and preparatory activity.

Section Aii: User safety measures for children

- 04** Samsung Galaxy Store had the required content guidelines and standards in its App Distribution Guide and age-rating system for children covering the four categories of inappropriate content categories in the ADS Code. Content moderation was effected by assigning appropriate age-ratings. During the period of assessment, there were no cases of mis-rated apps that were inappropriately age-rated as suitable for children under its age-rating policies, detected by or reported to IMDA.

05 Samsung Galaxy Store had implemented the required Age Assurance (AA) measures using the credit card check approved by IMDA.

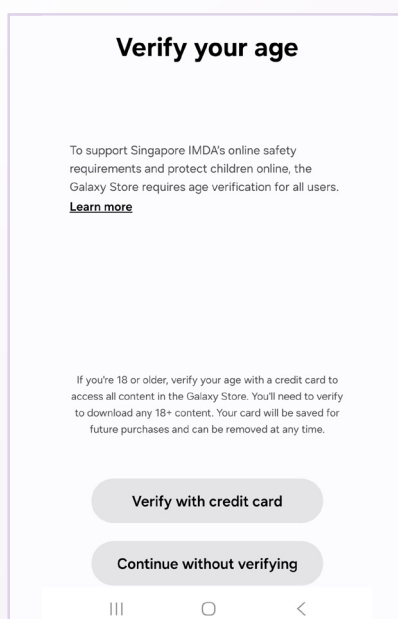


Figure 1: Samsung Galaxy Store's age assurance prompt

06 Samsung Galaxy Store provided child accounts with more restrictive settings to limit children's access and exposure to age-inappropriate apps, including restricting the download of 18+ apps for users under 18 years of age.

07 Samsung Galaxy Store's parental tools were present and comprehensive via "Samsung Kids" under the child's device settings, which enabled an environment where a specific set of apps could be curated for the child.

- However, the "Samsung Kids" feature was not mandatory and would only be accessible if parents took the initiative to set up "Samsung Kids".
- To help make its parental tools more accessible, Samsung Galaxy Store had published a guide on how parents can utilise the Samsung Kids app to manage their children's safety.

Section Aiii: User safety measures for apps with user generated content ("UGC") functionality

08 Samsung Galaxy Store reported comprehensive policies requiring UGC app providers to have content moderation measures and in-app user reporting mechanisms, and provided for appropriate actions against app providers that failed to resolve user reports in accordance with its policies. During the period of assessment, there were no violative UGC apps on Samsung Galaxy Store detected by or reported to IMDA.

Section B: User reporting and resolution

- 09** Samsung Galaxy Store reported comprehensive reporting mechanisms in place through in-app store reporting.
- a. However, IMDA's tests found some inconsistencies in Samsung Galaxy Store's notification of reporting outcomes to users. Following IMDA's engagement, Samsung Galaxy Store had investigated and ensured that such processes were in place.
- 10** Samsung Galaxy Store also reported that it had no process in place to inform users who had downloaded a reported app (within the last six months) that the app had been removed due to a violation.
- a. In response to IMDA's engagements on this issue, Samsung Galaxy Store had committed to implementing a notification system for informing users who have installed a suspended app by Q3 2027.

Section C: Accountability

- 11** Samsung Galaxy Store provided clear information in its first annual online safety report, and metrics previously approved by IMDA.
- a. Samsung reported zero user reports received and zero non-compliant apps and app providers in relation to harmful and inappropriate content categories. Hence all data points were zero (refer to Tables 1 – 4).
- 12** For paragraph 29(c) of the ADS Code on time taken to review and address user reports, Samsung Galaxy Store's metric will need to be improved in the next annual online safety report.
- a. For the reporting period, Samsung Galaxy Store had zero user reports and hence, related data on time taken to review and address such reports was zero (refer to Table 3). Samsung Galaxy Store's metric approved for the first annual online safety report, "aggregate average response and resolution time for ADS user reports, with no further breakdown by content categories" did not fully meet the intent of the ADS Code.
- b. Following IMDA's engagement, Samsung Galaxy Store had committed to explore providing the aggregate average response and resolution time for ADS user reports, with a further breakdown by content categories.

Content Categories	Total volume of ADS user reports received	Volume of ADS user reports assessed to be harmful / inappropriate with action taken	Volume of ADS user reports assessed to be not harmful / inappropriate with no action taken
Sexual Content	0	0	0
Violent Content	0	0	0
Suicide and self-harm content	0	0	0
Cyberbullying content	0	0	0
Content endangering public health	0	0	0
Content facilitating vice and organised crime	0	0	0

Table 1: Data provided by Samsung Galaxy Store for paragraph 29(a) of the ADS Code: The number of ADS user reports received, broken down by outcomes and content categories.

Content Categories	Volume of violating or non-complaint apps accessible by ADS users in Singapore	Volume of apps providers providing violating or non-compliant apps accessible by ADS users in Singapore
Sexual Content	0	0
Violent Content	0	0
Suicide and self-harm content	0	0
Cyberbullying content	0	0
Content endangering public health	0	0
Content facilitating vice and organised crime	0	0

Table 2: Data provided by Samsung Galaxy Store for paragraph 29(b) of the ADS Code: The number of apps acted upon, and the number of app providers acted upon, both broken down by content categories

Aggregate average response and resolution time for ADS user reports	N/A (0 user reports)
---	----------------------

Table 3: Data provided by Samsung Galaxy Store for paragraph 29(c) of the ADS Code: The aggregate average response and resolution time for ADS user reports without further breakdown by content categories

Content Categories	Volume of violating or non-compliant apps accessible by ADS users in Singapore proactively detected and addressed
Sexual Content	0
Violent Content	0
Suicide and self-harm content	0
Cyberbullying content	0
Content endangering public health	0
Content facilitating vice and organised crime	0

Table 4: Data provided by Samsung Galaxy Store for paragraph 29(d) of the ADS Code: The effectiveness of the Service's proactive actions in detecting and addressing violating or non-compliant apps that are accessible by ADS users in Singapore.

Samsung Galaxy Store's response

Samsung Singapore appreciates IMDA's assessment of the Galaxy Store and remains committed to supporting a safer online environment for users, including children and families.

Following IMDA's findings, we have taken steps to improve discoverability of information on our age assurance and app safety measures, and to update users on the review outcomes of relevant reports relating to inappropriate apps. Samsung is also working towards further enhancements, including a notification system for users who have installed suspended apps, and new features to help parents and guardians better manage children's screen time and access to apps.

Samsung will continue to engage constructively with IMDA and relevant stakeholders to strengthen user safeguards while supporting an open, trusted and innovation-friendly digital ecosystem in Singapore.

BROADCASTING ACT 1994

CODE OF PRACTICE FOR ONLINE SAFETY – APP DISTRIBUTION SERVICES

1. In exercise of the powers conferred by section 45L of the Broadcasting Act 1994, the Info-communications Media Development Authority (“IMDA”) hereby issues the following online Code of Practice (“Code”).

Title and Commencement

2. This Code is called the Code of Practice for Online Safety – App Distribution Services and shall come into effect on 31 March 2025.

Purpose of this Code

3. This Code specifies outcomes that App Distribution Services (“Service”) which are designated/will be designated under section 45K(1) of the Broadcasting Act 1994 have to meet to enhance online user safety, particularly for children, and curb the spread of harmful content on their service, including the distribution of, or online storage of harmful content on apps made available on their service.
4. The categories of harmful content include:
 - a. Sexual content
 - b. Violent content
 - c. Suicide and self-harm content
 - d. Cyberbullying content
 - e. Content endangering public health
 - f. Content facilitating vice and organised crime

Application

5. This Code applies to App Distribution Services which are designated/will be designated under section 45K(1) of the Broadcasting Act 1994.

Definitions

6. For the purpose of this Code, the following definitions shall apply:
 - a. “activity on the Service” includes (i) activity on the Service, and (ii) activity on apps, where the apps are distributed or available for download on the Service.
 - b. “ADS user” means a person who accesses the Service, including a person who downloads app(s) and app update(s) from the Service, and is not an app provider.
 - c. “app” means an application software package that includes content accessible by ADS users, or allows ADS users to access content on the Internet through the installed application software.

- d. “app provider” means a person that caused the app to be distributed or available for download by means of the Service.
- e. “child” means an individual who is below 18 years of age.
- f. “content guidelines and standards” means guidelines and policies issued by the provider of the Service on impermissible content and activity on the Service.
- g. “content on the Service” includes (i) content which is distributed or stored online on the Service, and (ii) content which is distributed or stored online on the apps, where the apps are distributed or available for download on the Service.
- h. “content moderation” means processes developed and activities taken by the provider of the Service to (i) detect, whether through the Service’s systems or in response to user reporting; (ii) assess; and (iii) address harmful content for ADS users or content inappropriate for children on the Service, in accordance with its content guidelines and standards with the aim of minimising access or exposure to, distribution of, or online storage of such content on the Service.

Obligations

- 7. The obligations are categorised into three sections:

Section A - User Safety;

Section B - User Reporting and Resolution; and

Section C - Accountability.

- 8. The measures to meet the obligations should be proportionate to the capacity and experience of ADS users to deal with the content on the Service. While adults may exercise control over the apps they install, children will need more protection to ensure a safer online space for them.

Section A – User Safety

- 9. ADS users must be able to use the Service in a safe manner. In this regard, the provider of the Service must put in place reasonable and proactive measures to (i) minimise ADS users’ access or exposure to harmful content on the Service; (ii) empower ADS users to manage their safety on the Service; and (iii) mitigate the impact on ADS users that may arise from the propagation of harmful content on the Service.
- 10. Children in particular may lack the capacity or experience to deal with the information and content available online and will need more protection to ensure a safer online space for them. In this regard, the provider of the Service must also have specific measures in place to protect children from harmful content and inappropriate content on the Service.
- 11. Measures to comply with the obligations in paragraphs 9 and 10 must include those found in (Ai), (Aii), and (Aiii) below.

(Ai.) Measures for all ADS users

Content guidelines and standards and content moderation

- 12. ADS users’ access or exposure to harmful content on the Service must be minimised via reasonable and proportionate measures. These measures include, but are not limited to, a set of content guidelines and standards for app providers, and content moderation measures that are put in place and effected by the provider of the Service:

- a. The Service's content guidelines and standards must address the categories of harmful content set out at paragraph 4 of this Code.
- b. The Service's content moderation measures must include systems and processes for the following:
 - i. Review of apps and app updates before they are released on the Service, and other reviews of apps available on the Service to ensure compliance with the Service's content guidelines and standards; and
 - ii. Appropriate action(s) to be taken when there is a breach of the Service's content guidelines and standards, which may include warning, suspending, or banning the app provider(s) from the Service.

Empower ADS users and improve safety

13. ADS users must be able to easily access information on the Service regarding online safety. Such information must be easy to understand and must include without being limited to the following:
 - a. The Service's content guidelines and standards;
 - b. The content moderation measures put in place by the provider of the Service and, in particular, the actions that may be taken by the provider of the Service to address a breach of its content guidelines and standards; and
 - c. Information on ADS users' ability to report content on the Service to the provider of the Service in relation to the categories of harmful content and inappropriate content set out at paragraphs 4 and 17 of this Code, and information on how to make such a report.

Proactive detection and removal

14. ADS users' exposure to child sexual exploitation and abuse material and terrorism content on the Service must be minimised through the use of technologies and processes. These technologies and processes must proactively detect and swiftly remove child sexual exploitation and abuse material and terrorism content as technically feasible, such that the extent and length of time to which such content on the Service is minimised.
15. ADS users must be protected from preparatory child sexual exploitation and abuse activity and preparatory terrorism activity on the Service through reasonable and proportionate steps taken by the provider of the Service to proactively detect and swiftly remove preparatory child sexual exploitation and abuse activity (such as online grooming for child sexual abuse) and preparatory terrorism activity (such as glorifying or endorsing terrorist activities and recruitment) on the Service.
16. The measures in paragraphs 14 and 15 of the Code would entail the provider of the Service taking proactive steps by primarily engaging app providers through the Service's content guidelines and standards and related processes to reduce ADS users' exposure to child sexual exploitation and abuse material and terrorism content, as well as preparatory activities related to such content. These may include requiring app providers to take steps to prevent such material or activity from being created, shared, hosted, or facilitated on their apps, conducting reviews of apps and app updates before such apps or app updates are released on the Service, and suspending or removing apps containing or facilitating such content or activity from the Service.

(Aii.) Measures for children

Content guidelines and standards and content moderation

17. Besides harmful content, children's access or exposure to inappropriate content on the Service must also be minimised through reasonable and proportionate measures. These measures include, but are not limited to, a set of content guidelines and standards for app providers and content moderation measures put in place and effected by the provider of the Service that are appropriate for children. Stricter standards must, at least, apply to the following categories of harmful content, and must be published such that they are easily accessible by ADS users:

- a. Sexual content
 - b. Violent content
 - c. Suicide and self-harm content
 - d. Cyberbullying content
18. Children must not be targeted to receive content on the Service that the provider of the Service is reasonably aware to be detrimental to their physical or mental well-being. Such content includes but is not limited to the categories of harmful content and inappropriate content set out at paragraphs 4 and 17 of this Code. In this regard, content targeting refers but is not limited to advertisements (including in-app advertisements), promoted apps and app recommendations.

Protection for children

19. Unless the Service restricts access by children, children must be provided differentiated accounts whereby the settings for the tools to minimise access or exposure to and mitigate impact of harmful content and inappropriate content on the Service are robust and set to more restrictive levels that are age appropriate by default.
20. In this regard, the provider of the Service must have in place systems and processes, including age verification, or other means of age assurance, such that the age or age range of an ADS user of an account on the Service can be established with reasonable accuracy. Age assurance must be implemented in accordance with the data protection provisions under the Personal Data Protection Act 2012 and any relevant guidelines issued by the Personal Data Protection Commission. These include the Advisory Guidelines on The PDPA for Children's Personal Data In The Digital Environment which stipulate, among other requirements, that organisations should practice data minimisation for age assurance purposes.
21. If the provider of the Service has yet to implement age assurance systems and processes, it must set out an implementation plan with relevant details that IMDA may require pertaining to how it intends to comply with the requirements in paragraph 20 read with paragraph 19, including a reasonable timeline for implementation to IMDA. The implementation plan and timeline, including any subsequent variation, is subject to agreement by IMDA.
22. Children and their parents or guardians must be provided clear warnings of the implications if they opt out of the default settings of the children accounts. Children and their parents or guardians must have access to information and tools that enable them to (i) manage children's safety; and (ii) effectively minimise children's access or exposure to, and mitigate the impact of, harmful content and inappropriate content on the Service. These must include without being limited to:
- a. Information about the apps made available on the Service that parents or guardians may use to assess the appropriateness of the apps for children. These may include description of the features and functionalities of the app, description of the type of content on the app, and consumer advice regarding such content.
 - b. Tools that parents or guardians may use to supervise and manage children's access to and use of apps. These may include user or parental controls, and search restrictions.
23. Children and their parents or guardians must be able to easily access information on the Service regarding online safety. Such information must be easily understood by children. The information must minimally include the tools available and the steps that parents or guardians may take to supervise and manage children's use of apps.

(Aiii.) Measures applicable to providers of apps with user generated content ("UGC") functionality

24. Unless the Service explicitly disallows the distribution or storage of apps with a UGC functionality, the provider of the said Service must ensure that the providers of such apps have:

- a. Content moderation measures to detect, assess, and remove harmful content in relation to the categories set out at paragraph 4 of this Code; and
 - b. An in-app channel for ADS users to report directly to the relevant app provider(s) any content on such apps in relation to the categories of harmful content and inappropriate content set out at paragraphs 4 and 17 of this Code.
25. The provider of the Service must take appropriate action(s) against app providers that fail to resolve ADS user reports in accordance with the Service's policies.

Section B – User Reporting and Resolution

26. Any individual must be able to report content on the Service in relation to the categories of harmful content and inappropriate content set out at paragraphs 4 and 17 of this Code. In this regard, the reporting and resolution mechanism provided to ADS users must be effective, transparent, easy to access, and easy to use.
- a. ADS users' reports must be assessed, and appropriate action(s) must be taken by the provider of the Service in a timely and diligent manner that is proportionate to the severity or imminence of the potential harm. In particular, timelines must be expedited for content and activity related to child sexual exploitation and abuse material and terrorism. Appropriate action(s) may include:
 - i. Swiftly removing the reported content or the app(s) containing such content from the Service, or restricting access to the reported content or app(s) on the Service; and
 - ii. Warning, suspending, or banning the app provider(s) of the reported app(s).
 - b. Where the Service receives a report that is not frivolous or vexatious, the ADS user who submitted the report must be informed of the decision and the action taken by the provider of the Service with respect to that report without undue delay, unless the ADS user had expressly opted not to be informed.
 - c. Where the Service decides to remove or disable the reported app(s) from the app store, or suspend or terminate the account of the app provider(s) of the reported app(s), any ADS user who has downloaded the reported app(s) within the last six months must be informed as soon as reasonably practical, taking into account the egregiousness or severity of the nature of the violation.
 - d. The ADS users referred to in sub-paragraph (b) must be allowed to submit requests to the provider of the Service for a review of the decision and the action taken.

Section C – Accountability

27. ADS users must have access to clear and easily comprehensible information that enable them to assess the level of safety and related safety measures afforded by the provider of the Service and make informed choices.
28. In this regard, the provider of the Service must submit to IMDA annual online safety reports to be published on IMDA's website. The provider of the Service must provide suitable information and metrics to be included in its annual online safety reports. The metrics are subject to agreement by IMDA. The annual online safety reports must reflect Singapore ADS users' experience on the Service, including:
- a. What steps the provider of the Service has taken and the effectiveness of these steps to mitigate Singapore ADS users' exposure to harmful content and inappropriate content on the Service, including descriptions of specific measures that the provider of the Service has in place to enhance online safety for ADS users in Singapore in relation to obligations in Sections A and B; and

- b. What action(s) the provider of the Service has taken in response to reports made by ADS users in Singapore.

29. The metrics in paragraph 28 may include, but are not limited to:

- a. The volume, breakdown by content category and outcomes of ADS user reports on the Service in relation to the categories of harmful content and inappropriate content set out at paragraphs 4 and 17 of this Code;
- b. The prevalence and breakdown by content category of (i) violating or non-compliant apps on the Service that are accessible by ADS users in Singapore; and (ii) app providers providing such apps, in relation to the categories of harmful content and inappropriate content set out at paragraphs 4 and 17 of this Code;
- c. The timeliness of the Service's systems and processes at reviewing and addressing ADS user reports, in relation to the categories of harmful content and inappropriate content set out at paragraphs 4 and 17 of this Code; and
- d. The effectiveness of the Service's proactive actions in detecting and addressing (including removing) violating or non-compliant apps that are accessible by ADS users in Singapore, in relation to the categories of harmful content and inappropriate content set out at paragraphs 4 and 17 of this Code.

