



Singapore Code of Practice for Online Safety Transparency Report

Submitted: June 12, 2026

Resubmitted with clarifications: October 20, 2026

Code Obligations:	For designated ADSs' input
Section A: User Safety	
Paragraph 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. <i>And</i> Paragraph 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.	Please provide information on the measures in place for all ADS users in Singapore: Google Play takes seriously our responsibility to provide a safe and trusted experience for all users and provide a platform for developers to deliver apps safely to billions of people worldwide. Google Play minimises App Distribution Service (ADS) users' access or exposure to harmful content through a comprehensive, multi-layered moderation strategy that combines advanced automated systems and human expertise. Key measures include: Clear Content Guidelines: Google Play establishes and seeks to enforce clear expectations through our Developer Programme Policies, which act as the primary framework for ensuring a safe ecosystem. Our Developer Programme Policies set out what developers can and cannot provide users on the Play platform and are the foundation upon which Play delivers apps and games safely to billions of people worldwide. These policies restrict categories of harmful content such as child endangerment, hate speech, illegal activities, and privacy violations. In order to mitigate the impact on ADS users that may arise from the propagation of harmful content, Play uses a gradient of enforcement mechanisms. When a policy breach is confirmed, Google Play applies proportionate enforcement actions based on the severity of the violation as outlined in our public facing Enforcement Policy. This can include varying levels of: - App-Level Actions: Rejecting app updates or completely removing the app from the store. - Account-Level Actions: Terminating developer accounts for repeat or egregious offenders to prevent future harm. Safeguarding our Users: Google Play wants everyone to feel secure in engaging with high quality apps on the platform. We do this with a combination of automated reviews and by having a team of experts who review apps before they are

published, and by removing apps that violate our policies. We build products and processes to improve app quality, weed out bad apps, and stay ahead of emerging challenges that may cause harm.

- **Content Ratings:**

Apps and games on the Google Play Store are assigned content ratings by an independent expert third-party, the International Age Rating Coalition (IARC). The ratings help users understand an app's maturity level and inform users of potentially objectionable content within an app.

- **Google Play Protect:**

Serving as the primary automated defense on Android devices, [Google Play Protect](#) scans applications daily to identify applications that pose a risk to user, data or device security. It warns users about potentially harmful apps and may deactivate or remove those apps from a device. These measures guard against the potential for bad actors to obtain sensitive content from a user's phone and use that content to engage in cyberbullying, harassment or sextortion.

To empower ADS users to manage their safety, Google Play provides a direct mechanism that allows users to identify and report apps that violate the [Google Play Developer Programme Policies](#) or contain illegal content.

- Users can easily submit a report directly within the potentially violative app by navigating to an app's detail page, tapping the "More" menu, and selecting "Flag as inappropriate", or they can submit a report through the [online reporting webform](#).
- This mechanism actively protects users by swiftly routing flagged issues—such as [malicious software](#) (including [malware](#)), [deceptive practices](#), or [restricted content](#) (including [user generated content](#))—directly to Google Play's specialised review teams for investigation.
- By using a combination of human reviewers and automated systems to assess these user-submitted reports, Google Play can quickly apply necessary enforcement actions like app suspension or removal, thereby mitigating potential harms and maintaining a safe, trusted ecosystem for everyone.

Google Play has mechanisms in place to provide users with rights and redress for content moderation decisions, which includes situations where Google Play decides not to take action on a user's report. When an assessment is made on a user's report, the reporter receives a Statement of Reasons (SOR) notice that includes a direct link to formally appeal the decision.

This appeals mechanism is designed to be easily accessible and user-friendly. Appeals are handled in a timely, non-arbitrary, and diligent manner under the supervision of qualified staff, rather than relying solely on automated means. If an appeal is successful, Google Play will reverse the original decision without undue delay and the reporter will receive an additional notice with the final appeal outcome. The reporter will also receive a notice if the appeal is unsuccessful.

More information about how Play works can be found [here](#).

Please provide information on any differentiated or additional measures in place for children:

As a preliminary comment, Play (and other Google services) distinguish between three main age categories in Singapore: children under 13, children between 13 and 17, and adults. Children under 13 are required to be supervised through Family Link, and when they reach 13, they will need a parent's approval before exiting supervision. As such, children between 13 and 17 may, but are not required to, be subject to parental supervision through Family Link.

Our approach to kids and families is built on the core belief that children deserve a safe, enriching digital environment. Our commitment is to empower parents with robust tools while providing children with access to high-quality, age-appropriate content. To that end, we build age-appropriate products that align with kids' and teens' developmental stages and needs, offer tools that give families flexibility to manage their unique relationships with technology, and implement policies, protections and programmes that help keep every kid and teen safer online.

Google Play

- **Policies for Children:**

We have additional requirements for apps whose audience includes children. Before an app is published on Play, the developer must certify whether children are part of the intended audience and, if so, the app must comply with the [Google Play Families Policies](#) (in addition to the standard [Play Developer Programme Policies](#)). The Google Play Families Policies establish heightened obligations for developers regarding age-appropriate content, data practices, and social app features. Apps subject to these policies must also disclose in greater detail how they use the user data they collect. Both automated protections and human reviewers enforce the Google Play Families Policies.

- **Expert Approved Programme:**
This [programme](#) identifies apps rated and approved by teachers and education specialists based on quality criteria (e.g., age-appropriateness, design). These apps are specifically made for children under the age of 13 and are highlighted in the Play Kids Tab to help families make informed choices.
- **Content Ratings and Content Restrictions:**
Content ratings on Play are provided by IARC. IARC is an independent agency administered by a group of participating regional and local ratings agencies. To receive a content rating, the developer of an app must fill out a rating questionnaire on the Play Console that asks about the nature of the app's content. IARC ratings are used to aid parental controls and to restrict access to certain content where legally required. Users can browse Play on the web without being signed into a Google Account, but must sign in to download, purchase or install content on Play, whether on the web or on mobile. Adult content is blocked for signed-in users under the age of 18 in Singapore.
- In addition, all developers may choose to use the [Restrict Minor Access](#) feature to block users determined to be under 18 from any app globally. Developers of apps involving age-inappropriate activities, like dating or matchmaking apps, are [required](#) to use this feature.

General Protections and Parental Controls

- **Supervised Accounts:**
Google's systems prevent children under the age of consent for processing personal data (i.e. 13 in Singapore) from creating a standard Google account. Instead, a child is guided through a process to create a supervised account, which requires parental involvement and management via [Google Family Link](#). To complete the account setup for a child under 13 in Singapore, a parent must provide parental consent and agree to supervise the child's account through Family Link. The resulting supervised account has default settings and parental controls managed through Family Link, ensuring an age-appropriate experience across Google products.
- **Family Link:**
This tool allows parents to supervise their child's account by setting screen time limits, managing app access, and viewing device activity. It is available for parents to manage the accounts of children under the [minimum age](#) (with mandatory supervision) and to supervise teens (with supervised accounts).

	● Advertising Restrictions: We prohibit age-sensitive ad categories from serving to users under 18, including ads that feature adult or sexually suggestive content, alcohol, or gambling and games. We also prohibit the display of personalised ads based on age, gender, or interests to any users we determine to be under the age of 18. Ads shown to these users must meet our under-18 ads policies, and may only be served based on non-personalised contextual information, such as the content on the current site a user is visiting. ● Age Assurance: As of March 31, 2026, Google has bolstered its age assurance measures in place in Singapore. In addition to a neutral age screen (date of birth without pre-populated options) during account creation, these measures include age estimation and age verification. These measures help the platform apply appropriate protections, such as high-privacy defaults and restrictions on content for minors. Please see our response to Paragraph 20, Section A: User Safety for more detail on age assurance.
Paragraph 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.	Please provide information on (a) the content guidelines and standards for app providers in place and (b) content moderation measures in place and how they are enforced or effected. Please include screenshots or evidence where possible. You may also provide information on additional measures outside (a) and (b) that meet the outcome of minimising ADS users’ access or exposure to harmful content. All ADS users in Singapore: Paragraph 12(a): Content guidelines and standards must address the categories of harmful content set out at paragraph 4 of the Code. Please map the content categories in your content guidelines to the harmful / inappropriate content categories under the ADS Code. Content Guidelines and Standards for App Providers: Google Play's safety standards are centered on the Google Play Developer Programme Policies, which serve as the primary framework to ensure a safe and trusted ecosystem for users. Before submitting an app, developers are required to ensure their apps comply with these policies and local laws. The guidelines are structured into specific categories to address various types of harmful content and practices, including:

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.	● Restricted Content: Prohibits apps that feature Child Endangerment, Inappropriate Content, Illegal Activities, Health Content and Services, Real-Money Gambling, and AI-Generated Content. ● Privacy, Deception, and Device Abuse: Restricts apps that are deceptive, malicious, or intend to misuse personal data, networks, or devices. ● Impersonation and Intellectual Property: Prohibits apps from misleading users by impersonating others or unfairly using someone else's work. ● Malware and Mobile Unwanted Software: Strictly prohibits code that puts users, data, or devices at risk, as well as software that is harmful to the user experience. Mapping Google Play Content Guidelines to Paragraph 4 of the Singapore Code of Practice: Based on Google Play's Restricted Content policies, the categories of harmful content outlined in paragraph 4 of the Singapore Code of Practice map to the following Play Developer guidelines. All of these specific policies are housed under the broader Restricted Content section of the Developer Policy Center: ● Sexual content: Maps to Play's Inappropriate Content policy and Child Endangerment policy. ● Violent content: Maps to Play's Inappropriate Content policy. ● Suicide and self-harm content: Maps to Play's Inappropriate Content policy. ● Cyberbullying content: Maps to Play's Inappropriate Content policy. ● Content endangering public health: Maps to Play's Health Content and Services policy. ● Content facilitating vice and organised crime: Maps to Play's Illegal Activities and Inappropriate Content policies.
---	---

All ADS users in Singapore:

Paragraph 12(b.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.

Content Moderation Measures and Enforcement:

Google Play uses a combination of human and automated evaluation to review apps and app content to detect and assess content which violates our policies and is harmful to users and the overall Google Play ecosystem. User reviews of Google Play apps also go through a combination of manual and automated review processes to determine if the user review violates the user comment posting policies (e.g., contains hate speech, sexually explicit content, spam, etc.). In addition, Google Play uses a combination of human and automated evaluation to take action on developers that pose a risk to our platform's safety. Using automated models helps us detect more violations and evaluate potential issues faster, which helps us better protect our users and developers.

- **Proactive App Review:**

Before an app or an update is made available on the platform, Google Play performs safety checks. Every app is reviewed before it goes live on Play with a combination of human and automated review. This helps us to detect and remove malicious apps. These efforts helped Play to prevent 1.75 million policy-violating apps from being published in 2025 globally.

- **Automated Scanning:**

Google Play continues to run safety checks on every app offered on the platform. These checks happen not only before an app is available on Play but also before an app is updated and continuously while the app is available on Play. Automated systems identify potential policy violations and may apply enforcement actions when there is high confidence, while more nuanced cases are routed for human evaluation.

- **Human Evaluation:**

Complex policy violations, including cases requiring contextual understanding, are routed to a global team of specially-trained analysts who conduct in-depth content evaluations. The results of these manual reviews are then used to help build training data to further improve our machine learning models.

	All ADS users in Singapore: Paragraph 12(b.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. Please see response above to Paragraph 9, Section A: User Safety. All ADS users in Singapore: Other additional measures N/A
Paragraph 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	Please <u>explain</u> how your service has made information regarding online safety easy to be accessed, including information that addresses the three sub-categories. All ADS users in Singapore: Paragraph 13(a): The Service’s content guidelines and standards. Google Play’s safety standards are centered on the Developer Programme Policies, which are presented as the primary framework for ensuring a safe and trusted ecosystem and are publicly available on our Transparency Center and Developer Policy Center. These guidelines are organised into distinct, easy-to-navigate categories such as Restricted Content (covering child endangerment, hate speech, and illegal activities) and Privacy, Deception, and Device Abuse. These policies are designed not only for developers but to provide users with transparency regarding the types of apps allowed on their devices. All ADS users in Singapore: Paragraph 13(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. Please see response above to Paragraph 9, Section A: User Safety.

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. <i>And</i> Paragraph 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.	All ADS users in Singapore: Paragraph 13(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. Please see response above to Paragraph 9, Section A: User Safety. Please <u>explain</u> how your service has made information regarding online safety easily accessible for children and their parents or guardians, including information on tools available and steps that parents or guardians may take to supervise and manage children's use of apps. Children: Google Play offers a one-stop shop for information about how Google Play works, which provides clear direction to users about where to find more information, tools and resources that help ensure online safety for children: Content Ratings: As described above in response to Paragraph 10, Google Play integrates with IARC and regional rating bodies to display content ratings on app detail pages. These ratings help children and parents understand the maturity level of content. This help center article explains how parents can restrict the content a child can download or purchase based on maturity level. Expert Approved Programme: As described above in response to Paragraph 10, Google Play's Expert Approved Programme helps highlight high-quality, age-appropriate apps and games specifically designed for children, making it easier for children and parents to find suitable content. This help center article explains how parents and children can find family-friendly content on Play. Parents or guardians: In addition to the information resources mentioned above, Google Play also provides parents with the following: Parental Controls via Family Link: Our Family Link resources provide information about the various restrictions parents can set on Google Play including purchase approvals, content filters based on maturity levels, and the ability to block or allow specific apps.
--	---

	● On-Device Parental Controls: Even without Family Link, users can set up parental controls directly within the Google Play Store app on an Android device. These controls are protected by a PIN and restrict content based on maturity ratings. These settings are device-specific. ● Educational Resources: The Google Families pages also provide families with information and resources to educate kids and teens about how to be safer online and to empower them with media literacy and digital skills. ● Data Safety Section: Google Play requires developers to provide transparency about their app’s data collection, sharing, and security practices in a “Data Safety” section on each app’s store listing as depicted below. This allows parents to make more informed decisions about apps their children use.
--	--

Data safety

The developer says that this app doesn't collect or share any user data. [Learn more about data safety](#).



No data shared with third parties

The developer says this app doesn't share user data with other companies or organizations. [Learn more](#) about how developers declare sharing.



No data collected

The developer says this app doesn't collect user data



Security practices



Committed to follow the Play Families Policy

The developer has committed to follow the Play Families Policy for this app. [See the policy](#).

Paragraph 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.

Paragraph 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

Please provide information on the measures to minimise ADS users' exposure to child sexual exploitation material. Please include screenshots or evidence where possible.

All ADS users in Singapore:

Google Play has strict policies and robust operations in place to tackle content and behaviour that is harmful or exploitative to children. Google Play's policy regarding Child Sexual Abuse Material (CSAM) can be found within the [Restricted Content](#) section of the Developer Programme Policies, specifically under the [Child Endangerment policy](#).

The core tenets of this policy mandate the following:

- **Immediate Removal for Facilitating Exploitation or Abuse:**
The CSAM policy explicitly states that "Apps that do not prohibit users from creating, uploading, or distributing content that facilitates the exploitation or abuse of children will be subject to immediate removal from Google Play. This includes all child sexual abuse materials."
- **Prohibition of Predatory Behaviour:**
Developers are strictly prohibited from using apps to endanger children. This includes any promotion of predatory behaviors such as child grooming, inappropriate targeted interactions, sextortion, trafficking, and the sexualisation of minors.
- **Enforcement and Authority Escalation:**
Google Play has processes in place to suspend the accounts of developers whose apps contain CSAM, based on investigation and instruction from Google's trained specialist teams. If Google becomes aware of content featuring CSAM, we remove it and report it to the National Center for Missing & Exploited Children (NCMEC).
- Additional [resources](#) are made available to developers to help them understand Google Play's Child Safety Standards Policy.

Google Play relies on a combination of people and technology to flag CSAM. Flags can come from our automated flagging systems, human reviews or from users. To proactively detect policy violations, including CSAM, all apps and updates to apps are reviewed before going live. These reviews are performed by a combination of specialised human reviewers and advanced machine learning models that are continuously updated.

updates are released on the Service, and suspending or removing apps containing or facilitating such content or activity from the Service.	Upon detection of CSAM, the following actions are taken: • If CSAM is developer-provided, the app is immediately removed, and the developer account is terminated. • If CSAM is found within User-Generated Content (UGC) inside an app, Google typically warns the developer to remove the content. Failure to do so results in immediate removal of the app. • All confirmed CSAM is reported to NCMEC. Google prioritises the swift removal of CSAM and treats it with the highest urgency due to the severity of the potential harm. Please provide information on the measures to minimise ADS users' exposure to <u>terrorism content</u>. Please include screenshots or evidence where possible. All ADS users in Singapore: Google Play's policy regarding terrorism content can be found within the Restricted Content section of the Developer Programme Policies, specifically under the Inappropriate Content policy. Google Play explicitly does not permit terrorist organisations, or any other dangerous organisations or movements that have engaged in, prepared for, or claimed responsibility for acts of violence against civilians, to publish apps on the platform for any purpose. The policy strictly prohibits apps that feature content related to violent extremism. This includes a ban on any content that is related to planning, preparing, or glorifying violence against civilians, such as content that promotes terrorist acts, incites violence, or celebrates terrorist attacks. When enforcing this policy, Google Play utilises a robust process that spans from initial detection to severe account-level penalties as described below: • Detection and Human Evaluation: Google Play relies on a combination of advanced automated models and human evaluation to proactively review apps and app content. While automated systems help detect potential violations at scale, cases requiring nuanced understanding—such as determining if violent content qualifies for an Educational, Documentary, Scientific, or Artistic (EDSA) exception—are flagged for review by a team of specially-trained operators and analysts.
---	---

- **Expedited Action:**

Because of the severe real-world risks associated with terrorism and violent extremism, reports and activities related to this type of content are assessed and actioned on expedited timelines.

- **Gradient of Enforcement Actions:**

Depending on the specifics of the violation, Google Play will apply strict enforcement actions at both the app and developer account levels as described here and below:

- **App Rejection or Removal:** A new app or update containing extremist content will be rejected and blocked from publishing, or an existing app will be completely removed from the Play Store so users can no longer download it.
- **App Suspension:** Egregious violations result in the app being suspended. This removes the app and counts as a "strike" against the developer's account standing.
- **Account Termination:** Serious violations of the policy, or an accumulation of strikes, will result in the termination of the developer's Google Play account. When an account is terminated, all of the developer's apps are removed from the store, and any related developer accounts are also permanently suspended.

Violent Extremism

We do not permit terrorist organizations, or other dangerous organizations or movements that have engaged in, prepared for, or claimed responsibility for acts of violence against civilians to publish apps on Google Play for any purpose, including recruitment.

We don't allow apps with content related to violent extremism, or content related to planning, preparing, or glorifying violence against civilians, such as content that promotes terrorist acts, incites violence, or celebrates terrorist attacks. If posting content related to violent extremism for an educational, documentary, scientific, or artistic purpose, be mindful to provide relevant EDSA context.

Paragraph 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.

Paragraph 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

Please provide information on the measures to protect ADS users from preparatory child sexual exploitation and abuse activity. Please include screenshots or evidence where possible.

All ADS users in Singapore:

Please see our response above to Paragraphs 14 and 16, Section A: User Safety.

Please provide information on the measures to protect ADS users from preparatory terrorism activity. Please include screenshots or evidence where possible.

All ADS users in Singapore:

Please see our response above to Paragraphs 14 and 16, Section A: User Safety.

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.	
Paragraph 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	Please provide information on the measures, and include screenshots or evidence where possible. Children: Paragraph 17(a): Sexual content Google Play takes a multi-pronged approach to the protection of children on our platform, including in relation to app content and functionalities that may be harmful to children. This approach consists of baseline protections for all users, including robust policies and enforcement mechanisms, app review processes, content ratings and transparency measures as explained above in our responses to Paragraphs 9, 12 and 13. In particular, Google Play’s Inappropriate Content policy prohibits apps that contain or promote sexual content, violent content, suicide and self-harm content, and cyberbullying content. On top of this, adult content is blocked for signed-in users under the age of 18 in Singapore. We apply further protections for users under 13, including through mandatory parental supervision and specific policies for apps aimed at users under 13. Before an app is published on Play, the developer must certify whether children under 13 are part of the intended audience and, if so, the app must comply with the Google Play Families Policies (Play Families Policies) in addition to the standard Developer Programme Policies. Note that the Play Families Policies apply regardless of whether an account is participating in Family Link. The Play Families Policies establish heightened obligations for developers regarding age-appropriate content, data practices (such as restrictions on the use of precise location data and no personalised ads for children), warnings for augmented reality, and social app features. There are also heightened obligations for any monetising or advertising on apps that are targeted at children. Apps subject to these policies must also disclose in greater detail how they use the user data they collect. A dedicated enforcement workstream enforces the Play Families Policies, using both automated protections and human reviewers. If an app is not intended to be used by children, but we find that its listing on Play contains elements that unintentionally appeal to children, we require the developer to take extra steps to comply with the Play Families Policies. Misrepresentation by a developer of any information about their app in the Play Console, including in the Target Audience and Content section, may result in removal or suspension of their app.

The appropriateness of content for children is based on the target audience for a particular app and the assigned IARC content rating and is governed by the publicly available [Restricted Content](#) section of the Developer Programme policies.

IARC provided Google Play with the following information regarding their content rating system for inclusion in this report.

Content categories which IARC utilises for assessing the appropriate age rating for an app:

[IARC](#) has many content categories that are used to assess the age appropriateness of a product. These categories vary based on the context and/or the type of product being assessed. Below is a high-level overview, but many of these categories have extensive follow-up assessments for more detail and context.

For Games

- Violence, Blood, or Gory Images
- Fear
- Sexuality, Suggestiveness, or Dating Games
- Gambling Themes, Simulated Gambling, or Real Gambling
- Language
- Controlled Substances
- Crude Humor
- Digital Purchases, Cash Convertible Rewards, or non-fungible tokens (NFTs)

For Social or Communication Products

- Assess content policies, e.g.:
 - Whether app is primarily a dating product
 - Whether app permits sharing of nudity
 - Whether app permits sharing of real-world, graphic violence
- Assess moderation policies, e.g.:
 - Whether there is chat moderation
 - Whether user has the ability to report disruptive users

For Other Types of Products

- For developer-created content and user-generated content, a combination of the above
- For streaming content/digital storefront content, an assessment of the permitted content within the catalog, e.g.:
 - Whether the featured content can contain violence, how graphically it may be depicted, etc.
 - Whether the featured content can contain sexual material, whether it permits nudity, etc.
- Whether the product focuses on promoting age-restricted experiences (e.g., an app that displays the location of nearby tobacco shops)

How IARC's content categories map to the 4 types of inappropriate content:

IARC does not produce a single output based on the content assessment. There are many different outcomes that may be triggered based on the various inputs and combinations of inputs made by the developer. IARC generates different ratings across the world based on local requirements and/or norms established by its [participating rating authorities](#). (For more information on How IARC Works, please visit globalratings.com.) For regions that do not have a participating rating authority in IARC, IARC generates generic ratings for display in those regions.

How IARC's age ratings provide a stricter standard for inappropriate content for children:

The age ratings produced by IARC are intended to provide information for parents to make informed decisions about the age appropriateness of games and apps for their children. Using a combination of IARC rating information (which consists of an age rating, content descriptors and interactive elements) and tools like Google's parental controls, parents can foster an age-appropriate experience for their children.

To receive a content rating, the developer of an app must fill out a rating questionnaire on the Play Console that asks about the nature of the app's content. If a developer misrepresents their app's content in the questionnaire, Google Play may remove or suspend that app. If a developer does not agree with the rating assigned by IARC, they can appeal that rating directly to IARC.

While the IARC rating system provides a standardized framework for age-rating apps globally, Google Play's developer policies serve as an overarching safety baseline that all apps must meet to be distributed on our platform. Even if certain graphic violence is theoretically permissible under IARC rating categories, Google Play's global [Inappropriate Content policy](#) strictly prohibits sexual and violent content across the entire store. This dual-layered approach ensures

that IARC ratings help parents make informed choices, while Google Play’s policies and enforcement processes help mitigate risks that harmful or extreme content enters the platform in the first place.

Google is committed to providing a safe experience for children on Google Play by combining the IARC system with our own robust developer policies. The risk of access or exposure to suicide and self-harm content and cyberbullying content most often arises in apps that allow for the uploading and sharing of user-generated content (UGC) and/or communication between users. When obtaining their IARC rating, the developer is responsible for disclosing whether they allow for user interaction and/or UGC and is responsible for moderating content on their apps under Google Play’s [User Generated Content policy](#). For Social or Communication Products, IARC assesses whether the developer has appropriate content moderation measures and policies before assigning an age rating. Independent of IARC’s rating determination regarding the age appropriateness of an app, Google Play strictly prohibits apps that promote self harm and suicide and apps that contain or facilitate threats, harassment, or bullying in its [Inappropriate Content policy](#):

Bullying and Harassment

Policy Summary

You must not create apps containing or facilitating harassment, exploitation or bullying of any kind. Please review the full policy and examples to ensure compliance.

Full Policy

We don’t allow apps that contain or facilitate threats, harassment, or bullying.

[Examples of common violations](#)

- Bullying victims of international or religious conflicts.
- Content that seeks to exploit others, including extortion, blackmail, etc.
- Posting content in order to humiliate someone publicly.
- Harassing victims, or their friends and families, of a tragic event.

Violence

Policy Summary

Apps that contain gratuitous violence or dangerous activities are prohibited. You must not promote representation or encouragement of such material. Apps that depict fictional violence in the context of a game, such as cartoons, hunting or fishing, are generally allowed. Please review the full policy to ensure compliance.

Full Policy

We don’t allow apps that depict or facilitate gratuitous violence or other dangerous activities. Apps that depict fictional violence in the context of a game, such as cartoons, hunting or fishing, are generally allowed.

[Examples of common violations](#)

- Graphic depictions or descriptions of realistic violence or violent threats to any person or animal.
- Apps that promote self harm, suicide, eating disorders, choking games or other acts where serious injury or death may result.

Through these complementary layers of IARC ratings and Google Play policies, we help protect children from harmful content.

	Children: Paragraph 17(b): Violent content Please see our response above to Paragraph 17(a), Section A: User Safety. Children: Paragraph 17(c): Suicide and self-harm content Please see our response above to Paragraph 17(a), Section A: User Safety. Children: Paragraph 17(d): Cyberbullying content Please see our response above to Paragraph 17(a), Section A: User Safety.
Paragraph 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.	Please <u>provide details</u> on the measures and include <u>explanations</u> on how they apply to content targeting including, but not limited to, in-app advertisements, promoted apps and app recommendations. Children: Google Play employs a multi-layered approach to protect children from being targeted with harmful content and inappropriate advertisements. Advertising: When developers advertise their apps, we make sure that the ads are well-marked. In addition, Google does not permit personalised ads for children, and the Play Families Policies impose specific advertising restrictions on apps whose audience includes children. Anyone can report ads that are inappropriate for the age group it was designed for here. Promoted apps and app recommendations: As explained in our Help Center, to make it easy for users to discover and navigate apps on Play, we take many factors into account when organising and ranking apps, such as: • <u>Relevance:</u> We show apps that are relevant to the page a user is on or what they have searched for using details provided by developers. This includes, for example, an app’s title, description, category, images, content and functionality.

	● <u>Quality of the app experience:</u> We show apps that have a good in-app user experience based on user feedback (for example, user ratings, reviews and engagement). ● <u>Editorial value:</u> We curate recommendations based on what is noteworthy and interesting. Play includes a dedicated space for children under 13 which only contains high-quality, age-appropriate content reviewed as part of our Expert Approved Programme. ● <u>User experience:</u> We show apps that perform well in the Play Store and that users continue to enjoy after installation. ● <u>Mature content:</u> Content that is not appropriate for children is filtered out of app recommendations in a number of ways: ○ All apps and games rated 18+ in Singapore are blocked for all users under 18 and therefore cannot be accessed through search results. ○ Developers can opt into Play's Restricted Minor Access feature, which restricts their apps to an adults-only audience globally, and prevents users under 18 from downloading or purchasing an app, continuing a subscription, or making new purchases on an app that is already installed. ○ Parents who manage their child's account through Family Link may choose to apply additional protections, such as filtering or blocking apps with certain content ratings. As parents are free to choose which protections apply to their child's account, the effect on the child user's search results will vary depending on the options the parent selects.
--	---

Paragraph 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.

Please describe the settings/tools and explain how they are robust and set to more restrictive levels by default for children. Do include screenshots or evidence where possible.

Children:

Users can access most Google products, including Play, using a central Google Account. Users can browse Play on the web without being signed into a Google Account, but must sign in to download, purchase or install content on Play, whether on the web or on mobile. Google uses age assurance measures to identify Google Account users who are minors. As explained further in response to Paragraph 20, below, Google enhanced the age assurance measures implemented in Singapore in early 2026.

In Singapore, children below the age of 13 cannot create their own Google Account. Instead, their parent or guardian must set up their account through [Family Link](#). While children aged 13 or above can create their own [Google Account](#), their account can also be set up by a parent through Family Link or subsequently linked to their parent's account on a voluntary basis. Children with supervised accounts that reach the age of consent will remain supervised until a parent provides approval to exit supervision or the account holder turns 18. Some of the parental controls under Family Link include screen time management where parents can set daily screen time limits, and app and content filters, which provide real time notifications to approve or deny any app downloads or in-app purchases a child attempts to make from the Play Store.

In order to provide flexibility to parents regarding how they manage their families' relationships with technology, Google empowers parents to set up voluntary parental supervision for users aged 13-18. Even without supervision, accounts for users ages 13-18 have default protections applied, including age restrictions for certain types of content (see our response to Paragraphs 10 and 18) and the disabling of personalised ads. In particular (as mentioned in our response to Paragraph 22, below), all children under the age of 18 are blocked from browsing, downloading and purchasing apps that are rated 18+ by default, regardless of whether they have parental supervision enabled on their account.

Using Family Link, parents can also choose to [block any app](#) for a user under the age of 18 whose account is supervised by a parent, including apps that have already been downloaded by their supervised user. Parents also have the option to set up [device-level parental controls](#) on Android devices.

Google takes any reports of potential inconsistencies in the application of content restrictions very seriously and actively investigates the specific apps flagged by regulators and/or users. Google remains committed to working closely with IMDA to ensure a highly consistent, safe, and age-appropriate experience for all young users in Singapore.

Paragraph 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.

Please describe in detail how and where the Service has implemented age assurance, and ensured the reasonable accuracy of it, in accordance with the Service's age assurance implementation plan that IMDA has agreed to.

Children:

Google has for many years required users to provide their age when signing-up for a Google account to help ensure children receive age-appropriate experiences including enhanced privacy, content and wellbeing protections.

In early 2026 in Singapore, Google rolled out additional age assurance measures to help identify users under the age of 18. These measures are implemented at the Google Account level and therefore apply to Play as well as other Google services, which is important to ensure that age-appropriate protections are carried across all Google services.

Google adopts a multi-pronged approach to age assurance, including a combination of:

- **Age declaration (age screen):** We ask users to provide their date of birth when creating their Google Account. This request is presented in a neutral manner which does not encourage users to state that they are over 18, and prevents users from back-buttoning and changing their age in the flow. This step has been part of the Google account sign-up process for several years.
- **Age estimation (process establishing a user is likely to be over or under a certain age):** Unless the user declares themselves to be under 18 (in which case they are treated as being under 18), Google will also use our age estimation model to assess the likelihood that the user is above or below 18.
 - The age estimation model only uses information that we have already collected and stored in the course of normal business operations, in line with the purposes described in our [Privacy Policy](#), which enables us to increase our confidence about whether the user is likely to be over 18 without collecting more data than that which we would otherwise process.
 - We continually train and improve our age estimation model to ensure it is as accurate as possible.
- **Age verification:** We go further and apply age verification methods in specific circumstances.

For example, below is the screen shown to users as a part of the email verification flow.



Verify your age with your email address

Email address:
tywinbolton.232764@gmail.com



Google will share your email address with our third-party partner, VerifyMy

VerifyMy will share your email address with its third-party partners to review sites and apps where you've previously used this email address, in accordance with their [privacy policy](#).

[Learn how VerifyMy estimates age](#)



You need to be 18 or older to verify

Google will use the confirmation from VerifyMy to ensure you have an age-appropriate experience, in accordance with our [privacy policy](#).

[Learn more about age verification](#)



Your age is verified immediately

If VerifyMy can't confirm you're 18 or older, you can try other available options to verify.



Your email messages are private

Your email messages aren't read. Our partner doesn't save your email address or use it for any purpose except to verify your age.

No thanks

I agree

[Feedback](#)

[Help](#)

[Privacy](#)

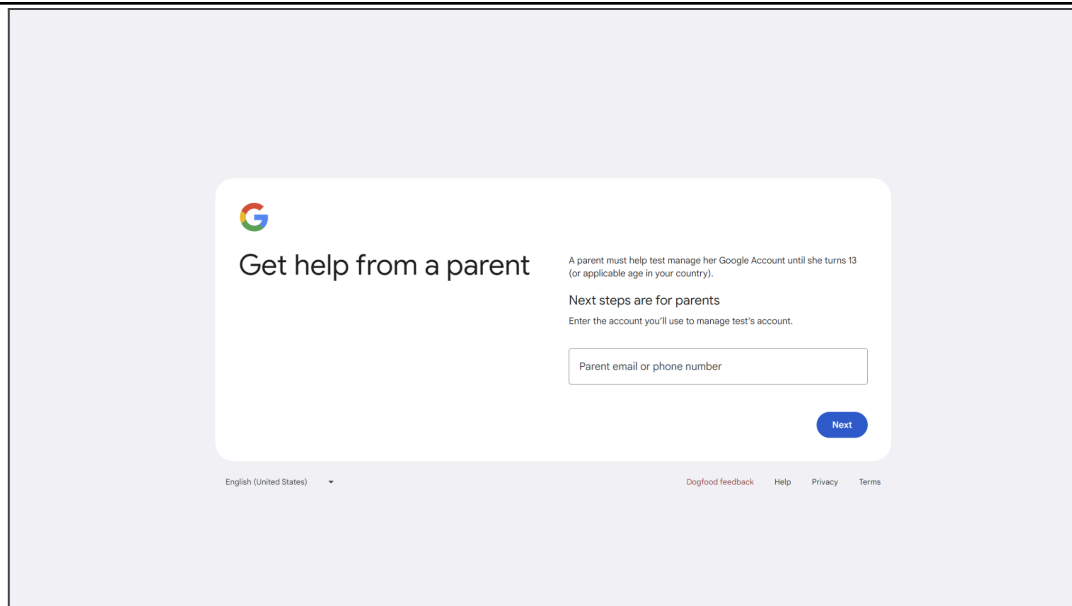
[Terms](#)

Users with questions or concerns about the protection of their data can visit the Privacy Help Center or contact Google by filling out this [web-form](#).

	Please provide information on how the implementation of age assurance has complied with the data protection provisions under the Personal Data Protection Act 2012 (“PDPA”) and the relevant advisory guidelines issued by the Personal Data Protection Commission, such as the Advisory Guidelines on the PDPA for Children’s Personal Data in the Digital Environment. Children: Google’s age assurance approach primarily uses information that we have already collected and stored in the course of normal business operations, in line with the purposes described in our Privacy Policy. When a user chooses to verify using an additional method such as email verification, they are shown a screen that provides information about the processing that will occur to support age assurance, including a link to the Google Privacy Policy.
Paragraph 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	Please provide information on the clear warnings of implications in place for children and parents who opt out of default settings. Please include screenshots or evidence where possible. Children: There are several protective settings that are on by default for supervised users and that vary by age as explained below. Each setting is explained through the parental control interface, which includes links to help center articles where parents can learn more about the implications for the different setting options and controls. Children under 13 • <u>Content Filters (Parental Controls):</u> These are set by default and are tied to the Google account, applying across all devices where the child is signed in. Only a parent can modify these settings. When a parent adjusts the content filter settings, a pop-up appears explaining which content will be affected by the change. • <u>Downloads:</u> By default, parental approval is required for a user under 13 to acquire <i>any</i> content on Google Play, whether free or paid. Only parents can change this setting and are required to re-enter their password as a confirmation step. • <u>Account Creation:</u> Children under 13 are prohibited from setting up a Google Account without the consent of their parent. If a user determined to be under the age of 13 attempts to create an account they will be prompted during the setup flow to get help from a parent (see screenshot below).

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.



Children aged 13-17 with parental supervision

- Purchase controls: Parental approval is needed for all paid content by default. If a parent decides to disable this control, they are presented with a range of options for purchase approvals as depicted below.

← Purchase & download approvals

When Charlie uses the family payment method, require my approval for:

- ☒ All content
Approval required for all content
- ☐ Paid content only
Approval needed for all paid content, including in-app purchases
- ☐ In-app purchases only
Approval required only for purchases made inside apps, such as coins in games
- ☐ Never
You won't approve any purchases or downloads. You'll still get email receipts for anything Charlie buys using the family payment method

Previous downloads and content shared through Family Library won't require approval. Purchase approvals do not apply when using alternate billing and external offer systems. [Learn more](#)

Parents can find more information about default settings and parental controls on the [Google Play](#) and [Family Link](#) Help Centers. If a parent elects to remove supervision for a child who is over 13 but under 18, they will be alerted as shown below:

Stopping supervision

This will remove supervision from [REDACTED] Google Account and any devices that are being supervised

☐

I understand that if I continue, I will no longer be able to manage [REDACTED] Google Account or devices

After stopping supervision, the parent will receive a further alert by way of email notification about the change in supervision. See the example below.

Subject: (You/(Parent name)) stopped Family Link supervision for (Child name)

Banner: (Child name)'s Google Account & devices are no longer supervised

Body copy:

Hi (Parent name),

(You/(Parent name)) recently stopped Family Link supervision for (Child name)'s Google Account [REDACTED]@gmail.com and supervised devices.

You'll no longer be able to use Family Link to supervise your child's compatible devices and their Google Account, including:

Account settings & controls

- Control what devices your child signs in to with their Google Account
- Manage settings like Web & App Activity and Location History that controls how Google collects and processes your child's data
- Control whether your child can give third-party apps access to their account

Apps on supervised devices

- Approve app requests from Google Play
- Block apps you don't want your child to use

Location

- Check where your child is with their supervised devices

Screen time on supervised devices

- See which apps your child uses, and for how long
- Set daily device limits
- Remotely lock devices when it's time to study or sleep

Google Chrome, Search and Play filters

- Block or allow sites on Chrome
- Turn on/off SafeSearch
- Manage what your child can browse, purchase, or download on Google Play

YouTube

- See a dashboard showing info about your child's channel activity
- Get notifications when your child does things like post videos and live streams

If this was a mistake, you and (Child name) can set up supervision again from Family Link.

Signature:

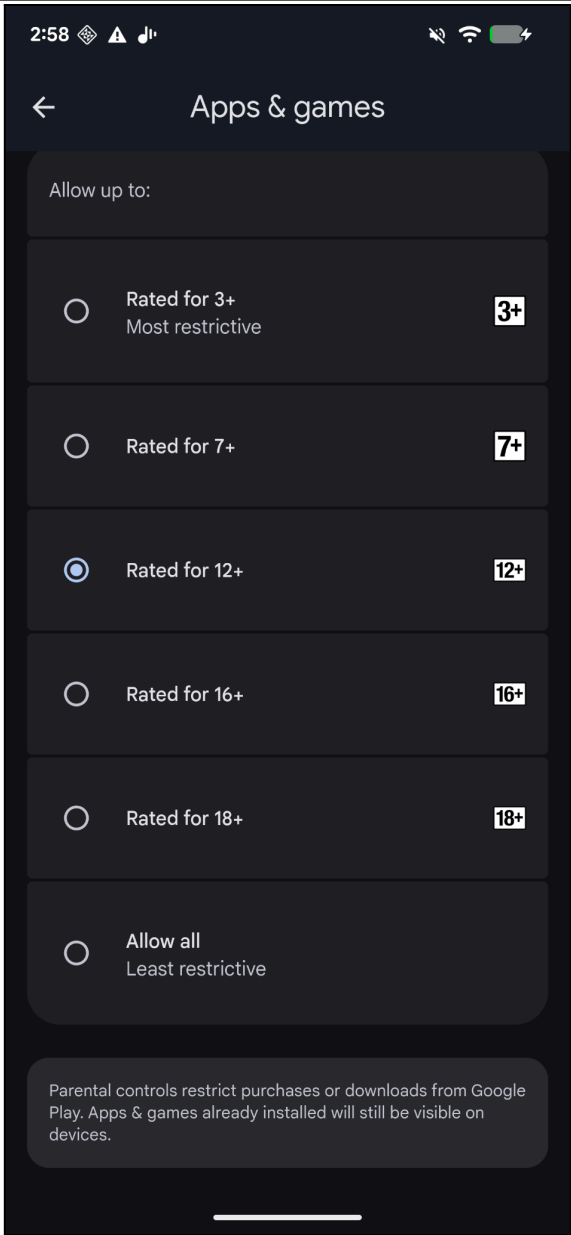
The Family Link team

Footer:

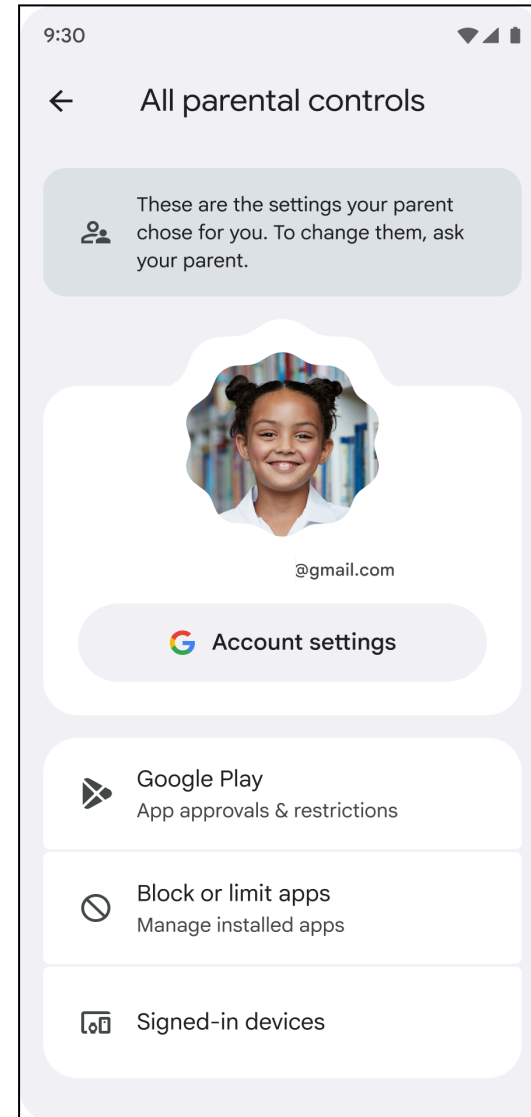
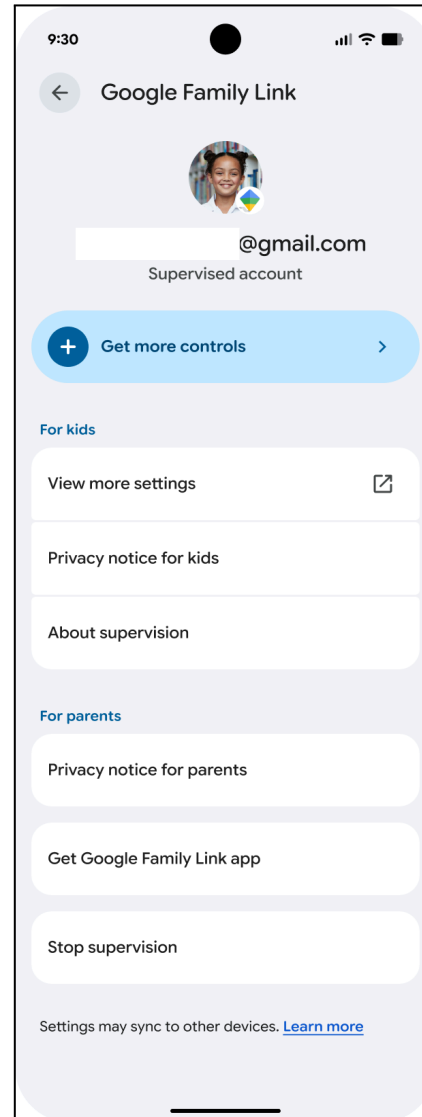
© 2018 Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043
You received this mandatory email service announcement to update you about important changes to your Google product or account.

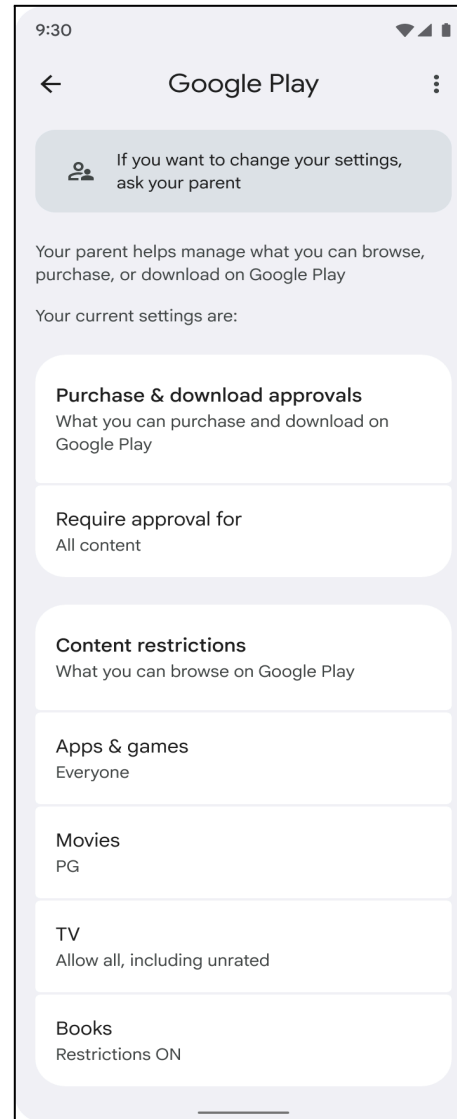
HELP CENTER

	All children under 18 In Singapore, in the Play store, all children under the age of 18 are blocked from browsing, downloading and purchasing apps that are rated 18+ by default, regardless of whether they have parental supervision enabled on their account. If a parent chooses to enable access to content rated 18+ for a child user under supervision, the child user will be able to search for the app and view the app page, but will not be able to download or purchase the app. Below is an example of the screen a parent sees when selecting content restriction settings for their supervised child:
--	--



In addition, supervised children can always view the content filter settings their parents have selected at familylink.google.com or in the Family Link app as shown below:





Please **describe in detail** the information and tools available on your service for children and parents/guardians to (i) manage children’s safety; and (ii) effectively minimise children’s access or exposure to, and mitigate the impact of, harmful and inappropriate content.

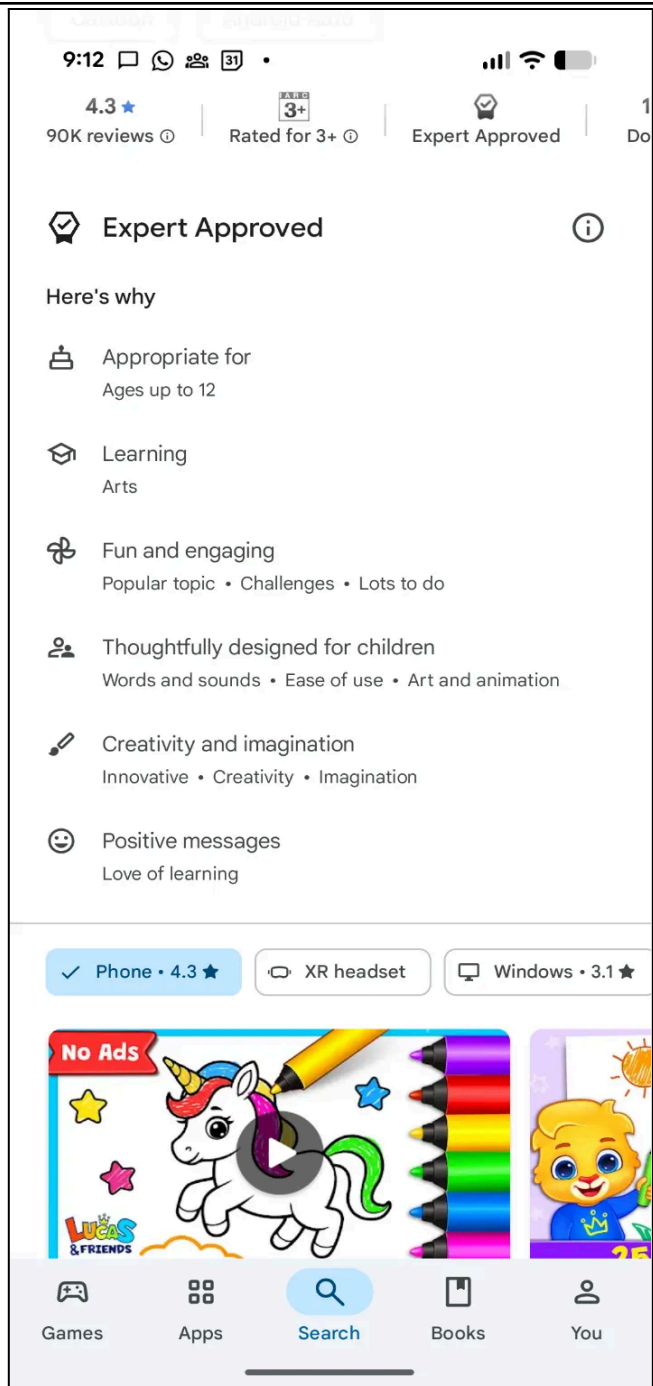
You may also provide information on additional measures outside the sub-categories paragraphs 22(a) and 22(b) that meet the outcomes described in paragraph 22 of the Code.

Children:

Paragraph 22(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.

Google Play incorporates official content ratings from IARC. Google’s [Content Ratings Policy](#) explains how ratings are provided, used and assigned. Additional requirements may apply under the [Play Families Policies](#), which include heightened requirements on apps whose audience includes children under 13.

Ratings assigned by IARC are displayed clearly and visibly in each app’s page on Play. The page may also include other labels, such as an “*Expert Approved*” badge (see screenshot below), which indicates that an app has been reviewed by teachers and minors’ education and media specialists based on a range of quality criteria as part of Play’s Expert Approved programme.



	Children: Paragraph 22(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. As noted in our response to Paragraph 19 above, parents and guardians can use Family Link to manage their child’s Google Account, including with dedicated controls for Play. On Play, Family Link includes settings to limit or block the apps a child can use on certain devices, including setting app time limits, requiring approval for new apps, setting restrictions on downloading mature content, and managing social features on a child user’s Play Games profile. Parents can also use Family Link to check how much time a child is spending on apps on their Android devices or Chromebooks. In addition, purchase controls exist on Family Link and the Play app. On the Play app, parents can choose to require approval for all content, all purchases that use the family payment method, only in-app purchases, or no approvals. On Family Link, options include approval for all content, paid content only, in-app purchases only, or no approvals. Children: Other additional measures In addition to the information provided above regarding default settings and parental controls, Google Play also implements the following measures to mitigate the impact of harmful or inappropriate content to children: No personalised ads: Google Play prohibits personalised ads for any user determined to be under the age of 18. Mature content: As of March 31, 2026, Google Play blocks users in Singapore determined to be under 18 from downloading, purchasing, or searching for apps and games that are rated 18+.
Paragraph 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	Please provide information on how the Service has ensured <u>providers of UGC apps</u> have content moderation measures and in-app reporting channels in place. Please include screenshots or evidence where possible. All ADS users in Singapore: Paragraph 24(a): Content moderation measures to detect, assess, and remove harmful content in relation to the categories set out at paragraph 4 of this Code. Developers are required to abide by Google Play’s Developer Distribution Agreement, as well as our Developer Programme Policies, which include the User Generated Content Policy (UGC Policy). This policy requires developers to

the categories set out at paragraph 4 of this Code; and	implement robust, effective, and ongoing UGC moderation. If an app is found to violate our UGC Policy via automated or manual means, the app will go through our standard review processes and be enforced upon accordingly.
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.	All ADS users in Singapore: Paragraph 24(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. The UGC Policy also specifically requires developers of apps that contain or feature UGC to provide an in-app system for reporting and blocking objectionable UGC and users. Users are also able to report apps to Google Play via our reporting channel as mentioned in our response above under Paragraph 9, Section A: User Safety (see screenshot below).

	Report a Policy Violation If you believe an app on Google Play violates Google Play's Developer Program Policies , you can let us know by completing this form. For other common issues, please follow these instructions instead: • To submit feedback about an App, follow these instructions • If you want to report an app that you believe infringes on a trademark or copyright, visit our legal removal requests page. • To request an app refund or get help with downloading, using, or deleting an app, visit the Google Play Help Center. * Required field Below, you will be asked to identify the Developer Program Policy that best describes the violation you believe you've observed. We take your concerns very seriously; we ask that you do the same before completing this form. Alleging a policy violation is a serious accusation that can lead to significant consequences for both developers and users. In order to continue, please confirm the following: ☐ I have a good faith belief that the information I provide to Google is accurate and supportable. * ☐ I understand that misuse of this form, including repeated submissions of unfounded or unverifiable allegations, or a high volume of submissions within short periods of time, may result in Google restricting the processing of further submissions made by me. * Name * Application package name * ? com.example.app Please note we're only able to take action on apps published to Google Play Suspected Policy Violation * Please select the policy violation category ☐ Restricted Content ☐ Impersonation ☐ Intellectual property ☐ Privacy Violation, Deception or Misrepresentation
Paragraph 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.	Please provide information on the actions the Service has taken against <u>providers of UGC apps</u> who have failed to resolve ADS user reports. The actions taken against providers of UGC apps that do not comply with the UGC Policy vary based on severity. During the reporting period, a range of enforcement actions were taken against UGC apps that users reported, including those actions outlined in our Enforcement Policy. Please see our response above to Paragraph 9 (and Paragraph 12(b.ii)), Section A: User Safety.

Section B: User Reporting and Resolution

Paragraph 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:

Please provide information on the measures, and include screenshots or evidence where possible.

All ADS users in Singapore:

Paragraph 26(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.

Please reference our response above to Paragraphs 9, 14, 15, and 16, Section A: User Safety.

Please provide information on the measures, and include screenshots or evidence where possible.

All ADS users in Singapore:

Paragraph 26(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.

Google Play prioritises valid, non-frivolous, non-vexatious user reports by escalating them through a dedicated review process using both automated means and human reviewers specifically trained to assess for [Play Developer Programme Policy](#) violations. Furthermore, flags indicating potential CSAM or terrorist content are immediately routed to specialised teams equipped to handle this highly sensitive material.

Upon receiving a user report, Google Play acknowledges receipt and, without undue delay, notifies both the reporting user and the developer of the decision and any resulting [enforcement](#) actions. This notification serves as the Statement of Reasons (SOR) for the developer and the reporter, and is communicated via email as shown below. During the reporting period, there were no cases where a user who submitted a new, valid, non-frivolous, non-vexatious report did not receive a notification.

Google Play maintains an automated outcome notification pipeline that delivers follow-up communications to users who submit policy violation reports within mandated jurisdictions, including Singapore, in accordance with the ADS Code of Practice.

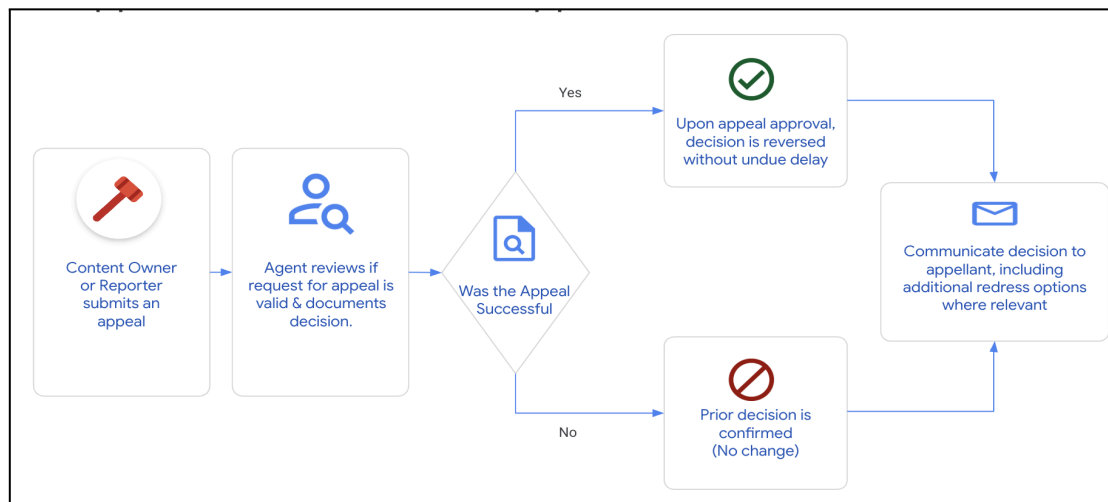
i. Swiftly removing the reported content or the app(s) containing such content from the Service, or restricting access to the reported content or app(s) on the Service; and	Following receipt of the 51 test cases referenced in the Authority’s findings, Google conducted an end-to-end audit which confirmed that Google Play’s user notification mechanism is operational and functioning as designed: All valid, uniquely identifiable, and non-spam Singapore reports received automated outcome notifications. Action that Google took on [auto-fill with app package name] From Enter email(s) BCC Enter email(s) Hi, [auto-fill with signed in first name] Thank you for submitting your policy violation report. This app has had restrictive action taken upon it. This restrictive action may be a result of yours or others reports or unrelated issues. This restrictive action may be removal from the play store or a warning before removal based on our Enforcement policy [link]. In addition, the app may have already fixed the issue as a result of this restrictive action. After a further investigation into the about [package name] app, we’ve concluded that the app violated one or more of the Play Developer Program policies [link]. We’ve informed the developer and taken appropriate action in accordance with our Enforcement policy [link]. Thank you for helping to keep users safe!
---	--

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.

Notably, reporters receive a SOR notice even in cases of "non-actioning"—meaning situations where Google reviews the flagged content but decides that it does not violate policies and chooses not to take any restrictive action. See screenshot below for a visual of this process.

Crucially, the SOR notice sent to the reporter includes a direct link that the reporter may use to formally appeal the decision if they disagree with the outcome.



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.	Please provide information on the measures, and include screenshots or evidence where possible. All ADS users in Singapore: Paragraph 26(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. N/A. None of the policy violations for which Google Play took enforcement action during the reporting period were determined to be so egregious or severe that user notification was necessary on top of the enforcement action already taken. We strive to balance user safety with developer due process and are continuously refining our systems. Google Play remains committed to protecting our users worldwide and robust safeguards are already in place. For example, when an application is suspended, users can no longer see the app store's listing, new users cannot download the app, and users who have already downloaded the app cannot update the app to newer versions or make in-app purchases. When a user attempts to make a purchase in a suspended app, they receive a message that says, "The item you requested is not available for purchase." These restrictions significantly reduce the user's ability to use the app and accelerate the natural end to the app's lifecycle to keep users safe. The range of enforcement actions that Google takes in response to user reports is explained in response to Paragraph 9, Section A: User Safety. Please see the response to Paragraph 29(b), Section C: Accountability for the number of enforcement actions taken on apps during the reporting period for violations of the harmful content categories set out in Paragraph 4 of the Code of Practice. There were no suspensions or terminations of developer accounts during the reporting period for violations of the harmful content categories set out in Paragraph 4 of the Code of Practice.
--	---

Please provide information on the measures, and include screenshots or evidence where possible.

All ADS users in Singapore:

Paragraph 26(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.

As mentioned in Paragraph 9, Section A: User Safety, when a user reports an app for a potential policy violation, the report is assessed by Google Play's review systems and teams. Following this evaluation, Google Play informs the reporting user of the decision and any action taken without undue delay, sending a Statement of Reasons (SOR) notice even in cases where no restrictive action was taken against the app (non-actioning). Included within this SOR notice is a direct link to an electronic appeals form.

If the reporter disagrees with the outcome of their report, they submit an appeal and provide additional information to substantiate their claim. Once submitted, the appeal is handled diligently and in a non-arbitrary manner by a human reviewer, rather than relying solely on automated systems.

Appeal non-action of a policy violation report

If you believe we've made an error in reviewing your policy violation report, you may appeal our findings by filling out this form. To report a new or different policy violation, use [this form instead](#).

* Required field

Case ID (from your email): *

Email address (should match the email of the user who completed the initial policy violation report). *

Application package name * [?](#)

You previously reported a policy violation of: *

Tell us which portion of that policy you think was violated (copy/paste from the relevant policy language). You can review our policies here: play.google.com/about/developer-content-policy/ [?](#) *

Explain briefly where in the app or app listing you found this policy violation *

Tell us how you think this policy was violated (please be specific): *

If you have specific examples of the suspected violation, including screenshots of the violative material, upload them using the option below. Do NOT upload any suspected child sexual imagery; you can submit this form without uploading additional files.

Section C: Accountability - Mandatory Information

Paragraph 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.

Please provide information on the measures, and include screenshots or evidence where possible.

All ADS users in Singapore:

Please see our response above to Paragraph 13, Section A: User Safety.

Section C: Accountability – Mandatory Metrics

Note: All data reported in this Section C is for the period April 1, 2025 to December 31, 2025 (“reporting period”), unless otherwise stated. Where breakdowns by policy violation are provided below, please note that the breakdown shown is based on Google Play’s internal categorisation, which does not exactly mirror, but broadly covers, the harmful content categories set out in Paragraph 4 of the Code of Practice. We have mapped Google Play’s internal categories to the harmful content categories set out in Paragraph 4 of the Code of Practice as closely as possible.

Paragraph 29(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;

Please provide information and insert metrics that IMDA has agreed to, broken down by the content categories and ADS user categories.

Please include accompanying explanations or footnotes to explain the metrics, where appropriate.

- a. Number of user reports for policy violation, by Singapore users, broken down by suspected policy violation. Note that Play policy violations are mapped to and subsequently reported according to the harmful content categories set out in Paragraph 4 of the Code of Practice only.

Suspected policy violation	Number of user reports
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										
	b. Number of user reports for policy violation by Singapore users, that resulted in an enforcement action											
	During the reporting period, Google Play took enforcement actions on 1,415 user reports of policy violations.											
	Note: This number includes enforcement actions taken on all user reports of policy violations during the reporting period and is not limited to enforcement actions taken solely on policies that map to the harmful content categories set out in Paragraph 4 of the Code of Practice. As a result, the number of enforcement actions on user reports cannot be compared to the total number of user reports received and reported in the table above.											
Paragraph 29(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;	Please <u>provide information</u> and <u>insert metrics</u> that IMDA has agreed to, broken down by the content categories and ADS user categories. Please include accompanying explanations or footnotes to explain the metrics, where appropriate. a. Number of enforcement actions taken for policy violation, on apps that are available in Singapore, with a breakdown by policy violation. Note that Google Play policy violations are mapped to and subsequently reported according to the harmful content categories set out in Paragraph 4 of the Code of Practice only. <table><tr><th>Policy violation</th><th>Number of enforcement actions</th></tr><tr><td>Sexual content</td><td>4,473</td></tr><tr><td>Violent content</td><td>365</td></tr><tr><td>Suicide and self-harm content</td><td>0</td></tr><tr><td>Cyberbullying content</td><td>1</td></tr></table>		Policy violation	Number of enforcement actions	Sexual content	4,473	Violent content	365	Suicide and self-harm content	0	Cyberbullying content	1
Policy violation	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
	b. Number of enforcement actions taken for policy violation, on developers with apps available in Singapore, with a breakdown by policy violation. Note that Google Play policy violations are mapped to and subsequently reported according to the harmful content categories set out in Paragraph 4 of the Code of Practice only.		
		Policy violation	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
	Note: During the reporting period, Google Play took enforcement actions against developers with apps available in Singapore. However, none of those enforcement actions fell within policies that cover the harmful and inappropriate content categories set out in Paragraph 4 of the Code of Practice.		

Paragraph 29(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	Please <u>provide information</u> and <u>insert metrics</u> that IMDA has agreed to, broken down by the content categories and ADS user categories. Please include accompanying explanations or footnotes to explain the metrics, where appropriate. Google Play reviewed 96% of user reports within 7 days¹.
---	---

¹ For certain accounts, Google Play will take more time to thoroughly review the app to help better protect users. This may result in review times of up to seven days or longer in exceptional cases.

Paragraph 29(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.

Please provide information and insert metrics that IMDA has agreed to, broken down by the content categories and ADS user categories.

Please include accompanying explanations or footnotes to explain the metrics, where appropriate.

- a. Number of actions taken for policy violation, on apps that are available in Singapore, broken down by detection method (automated or non-automated)² with a breakdown by policy violations. Note that Google Play policy violations are mapped to and subsequently reported according to the harmful content categories set out in Paragraph 4 of the Code of Practice only.

Policy violation	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

² Google Play uses a combination of human and automated evaluation to review apps and app content to detect and assess content which violates our policies and is harmful to users and the overall Google Play ecosystem. Using automated models helps us detect more violations and evaluate potential issues faster, which helps us better protect our users and developers. The policy-violating content is either removed by Google Play's automated models or by trained operators and analysts. The results of these manual reviews are then used to help build training data to further improve our machine learning models.