



Apple Transparency Report

Reporting period: 1 April 2025 - 31 December 2025

In accordance with Section C of Code of Practice for Online Safety - App Distribution Services ("CoP"), this online safety report provides information reflecting users' experience on the App Store¹. This report covers the period between 1 April 2025 and 31 December 2025.

User Experience on the App Store

The App Store is a place for users to discover and download their favorite apps and, from its inception, was designed to protect users of Apple devices by creating a safe and trusted environment offering a wide variety of curated apps. Every app has an app "product page", which contains a range of information provided by the app developer, including developer and app information; app icons, screenshots, and previews; a privacy policy URL; support links; an age rating; and data handling practices. The App Store also provides customer rating and review information on the app product page. If the user has downloaded the app, they see a link to the Report a Problem feature, which lets customers request a refund, report a quality issue, or report a scam or fraud, or offensive, illegal or abusive content.

Unlike social media, gaming, or communication platforms, users cannot upload or publish content on the App Store (other than text in user reviews), nor communicate with other App Store users. Additionally, every app and every app update submitted to the App Store is closely reviewed by both automated systems and human experts trained to ensure that apps offered on the App Store are safe, provide a good user experience, protect user privacy, and use approved business models. Post publication, apps are subject to ongoing monitoring and multiple controls ensure that Apple can take action when it is alerted to potentially problematic developers or apps. Additional detail regarding App Store security is [here](#).

App Review supplements a range of measures that Apple has implemented to keep the App Store a safe and trusted place for all users, including tools and resources to help users make informed decisions about which apps to download, make purchases safely, and receive customer support when users need it most, including to report problems with an app or to report suspicious activity. Additional detail regarding these measures is [here](#).

Publicly Available Resources

Apple has published multiple resources for users of the App Store, including a dedicated [Online Safety webpage](#) in Singapore that provides information on reporting unlawful or harmful content on the App Store, parental controls, App Store age ratings, and App Review Guidelines (the "Guidelines"). Other publicly available resources to help guide users of the App Store are included throughout this report.

App Submissions and Age Ratings

As part of the App Review submission process, developers are required to answer predefined age rating questions and self-assess how often specific content categories, such as "realistic violence" or "sexual content or nudity", appear in their app, as well as whether their app offers certain features, such as gambling or purchasable loot boxes. Based on this self-assessment, a specific age rating is provided to the developer for their app.

¹ This report is provided by Apple Distribution International Limited

The App Store uses five age rating categories that help users make informed decisions about how appropriate an app may be : 4+, 9+, 13+, 16+, and 18+. For example, apps with profanity or crude humor may incur ratings of 9 or 13+ depending on content frequency, while apps with frequent simulated gambling or realistic violence are assigned the highest rating of 18+. The App Store does not allow apps with graphic sexual content and nudity or prolonged graphic or sadistic realistic violence. See <https://developer.apple.com/help/app-store-connect/reference/app-information/age-ratings-values-and-definitions/>. Further, all information available on an app's product page — including metadata, descriptions, and imagery must adhere to a 4+ age rating even if the app is rated higher. This establishes a baseline level of protection for all users, regardless of account type or whether child safety features are enabled.

Apple also makes available to its users the Made for Kids category, which gives parents a section of the App Store with age-appropriate apps held to even higher standards for privacy and safety, and which helps parents and their children discover age-appropriate apps tailored to their needs. Developers can assign the Made for Kids category to apps and games designed for minors under age 12 and thereafter assign an appropriate age band (5 and under, 6-8, or 9-11), ensuring that their app will appear in the Kids category when users browse the App Store. Apps in the Made for Kids Category are subject to additional requirements specifically to protect minors. This includes limitations on payment opportunities, external links and prohibitions on sharing identifiable data with third parties. Apps not in the Made for Kids Category cannot use metadata like "For Kids," nor imply that the main audience for the app is children. This means that, on the App Store, parents and guardians are empowered to accurately identify appropriate apps for their children. Requirements and restrictions are detailed in the App Review Guidelines. When a developer selects Made for Kids and chooses the appropriate age range for the app, this selection cannot be changed once App Review approves the app, and all subsequent updates must comply with the Kids category guidelines. See also, <https://developer.apple.com/app-store/categories/>.

Age ratings also work alongside device parental controls and form the foundation upon which device app restrictions are based. As discussed further below, these age ratings are integrated across Apple's operating systems and work with parental control features like Screen Time and Ask to Buy.

App Review

Apple makes clear in its [App Review Guidelines](#) that the guiding principle of the App Store is to provide a safe experience for users to get apps and that Apple accomplishes this by ensuring that every app is reviewed by experts and that an editorial team carefully curates an age appropriate experience on pages where users can discover new apps. Additionally, system parental controls are in place to ensure that the browse experience in the App Store will only display and permit the download of apps within the age restrictions set by parents on the account.

Additionally, the App Review Guidelines include rules for all developers, including that "Apps should not include content that is offensive, insensitive, upsetting, intended to disgust, in exceptionally poor taste, or just plain creepy." This policy broadly covers content like sexual content, violent content, suicide and self-harm content, and cyberbullying content for all users, not just children. The Developer Program License Agreement provides also states that applications may be rejected if they contain content or materials that are objectionable or inappropriate (see DPLA s.3.3.4(A)(iii)).

Before they're published on the App Store, all apps and app updates are subject to automated review and human review. Apple assesses whether there are any apparent inconsistencies between a developer's self-assessment and the information and screenshots provided by the developer. If Apple identifies inconsistencies with the developer's responses to the age rating questions, Apple will reject the app due to a mis-rating and ask the developer to resubmit the app for App Review with an adequate age rating, resulting from the developer's accurate self-assessment of the age rating questions.

After apps are published, the App Store continues to monitor them and can and does take action, including app takedowns, if it identifies apps that do not comply with applicable law, with the [App Review Guidelines](#) with other applicable terms and conditions — namely the [Apple Developer Agreement](#) or the [Apple Developer Program License Agreement](#) (DPLA). The App Store may also take action if alerted to concerns about an app by third parties, including via Report a Problem or Content Reports (discussed in depth below). Automated tools are used to assist App Review specialists in their ongoing monitoring of apps published on the App Store. This includes automated tools that detect malware or bait-and-switch apps that change their functionality after approval by App Review. It also includes automated tools that scan user reviews of published apps to identify concerns raised by consumers that may indicate that apps contain content incompatible with applicable law or terms and conditions. These tools are continually trained and enhanced to address new and emerging threats and to factor in learning from human-based decision-making. Any apps flagged as potentially problematic by these automated tools are escalated to human App Review specialists. These specialists then determine whether the apps violate App Store terms and conditions and, if so, what action to take — for example, app removal or developer termination. If a developer is terminated, their apps are removed from the store and can only be restored upon a successful appeal. When an app is removed or a developer is terminated, automated tools may flag additional apps or developer accounts with similarities to the removed/terminated content. These apps/accounts will also then be reviewed and potentially actioned by human specialists. No moderation actions are taken solely on the basis of automated tools.

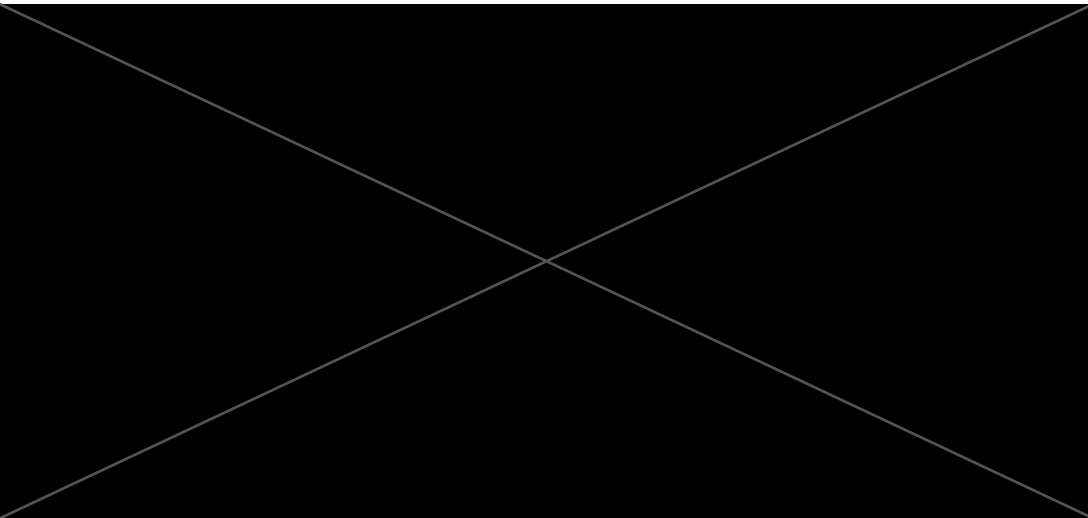
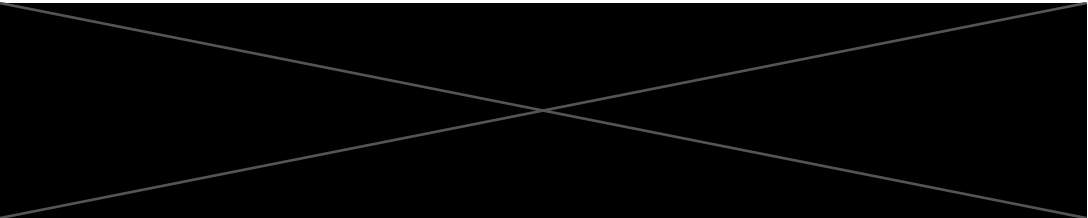
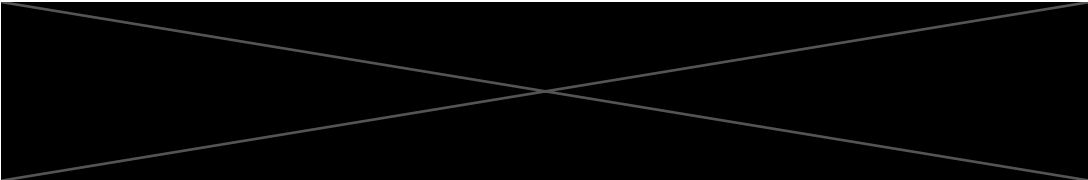
Further, Apple maintains comprehensive policies and procedures to address CSAM / CSEAM and terrorism material. All Apps and app updates are subject to the App Review process, including both automated and human review, which includes the review of product page imagery and app binary. The App Store does not allow pornographic content (see for example Guideline 1.1., which prohibits objectionable content; 1.1.4 which prohibits overtly sexual or pornographic material; 5, which requires apps to comply with all legal requirements in any location the developer makes them available). Terrorism content is also prohibited (see for example Guideline 1.1.1, which prohibits content that could harm an individual or group; 5, see above).

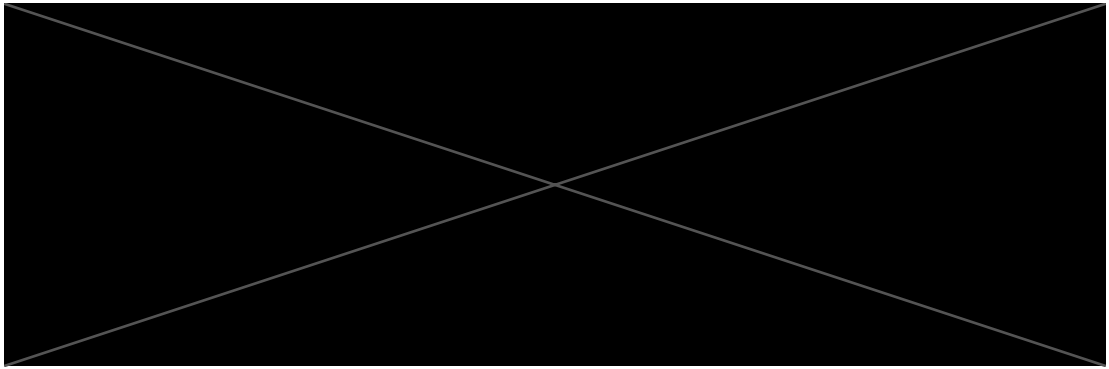
Apple also employs robust notice and action mechanisms that enable users, developers, law enforcement, or government regulators to report allegations of CSAM / CSEAM or terrorism content. Apple investigates any credible claims that a developer is not acting in accordance with the DPLA, the Guidelines or local law. Apple also maintains dedicated child safety counsel specifically to review allegations of CSAM / CSEAM content on the service. If a violation is confirmed, Apple will take appropriate action, which may include removal of the app from the App Store and removal of the developer from the Apple Developer Program. If terrorism content is found within an app, App Review will forward it to the Global Security and Legal teams, who will circulate it to proper authorities.

With respect to apps that contain user-generated content (UGC), Apple requires developers to have effective processes that monitor and mitigate the spread of harmful content on their apps. All UGC is hosted on the developers' servers, and Apple cannot moderate such content. Developers are fully responsible for monitoring and maintaining reporting systems to comply with the Guidelines, including Guideline 1.2, which requires developers to include a method through which they can prevent objectionable or harmful material from being posted and a mechanism through which users can report offensive or threatening content. These mandatory reporting mechanisms allow users to report abusive content to the developer and seek to have it removed. Guideline 1.2 also prohibits apps with UGC that are used primarily for pornographic content, physical threats, or bullying — including apps designed to generate or promote pornographic deepfake content.

User Notice & Takedown

Customers may use the “Report a Problem” feature to submit notices of offensive, illegal, or abusive content concerning apps they have purchased or downloaded. The Report a Problem feature is displayed in the Games and Apps tabs, and on the product page of any app a user has purchased or downloaded. Users can choose from “report a scam or fraud” and “report offensive, abusive, or illegal content” options to submit their concern about content they have purchased or downloaded. Users are presented with a free text field to describe the issue they are reporting.





If a user uses Report a Problem in the App Store, they can select “Report offensive or abusive content” or “Report illegal content” from the menu of options. If they select the former, the user goes through the process flow outlined above. If they select the latter, they are redirected to the Content Reports portal. The Content Reports Portal can also be accessed directly via the [web](#).

The Content Reports portal is a central platform where individuals can file notices concerning alleged illegal content, from which communications concerning those notices are processed and sent, and in which data is consolidated for later transparency reporting purposes. Anyone in Singapore can submit concerns about alleged illegal content via the Content Reports portal, whether or not they have purchased or downloaded the app in question. Members of the public in Singapore can also use the portal to anonymously file notices concerning CSEAM content.

[REDACTED]
[REDACTED] All remaining notices will undergo manual triage before submission to App Review. Manual triage will help Apple track and understand the kinds of notices it receives, [REDACTED]
[REDACTED] and help identify possible misuse and abuse of the system. Once a notice passes through these triage systems, an automatic acknowledgment communication will be sent to the notifier.

The App Review team collaborates with relevant internal teams and partners, including the App Store Legal team when appropriate, to review, analyse, and action the notices. Once an action is taken, the Content Reports portal facilitates necessary communications to notifiers and designated appointees about the actions taken, and when necessary, to impacted consumers who purchased illegal products or services.

If a notifier disagrees with an outcome, they have the option to challenge the decision via <https://contentreports.apple.com/Complaints>. These complaints are received through a separate section of the Content Reports Portal and are routed to senior App Review analysts for review. The senior App Review analyst reviews the original notice alongside any new information provided by the complainant. These senior App Review analysts partner with relevant internal teams, including the App Store Legal team where necessary, to evaluate the complaints. Some matters may be escalated for a final review by the App Store’s Executive Review Board (“ERB”). Communications are sent to complainants as part of this process.

Apple has found that most user reports it has received that allege the presence of CSEAM or terrorism content do not identify actual CSEAM or terrorism content. Of the 11 reports received during the reporting period claiming CSEAM or terrorism content, only 1 flagged potential CSEAM content and none flagged terrorism content.

Child-Specific Defaults and Protections

Apple has default settings in place, and also makes available features that parents and guardians can use, to help their kids have age appropriate experiences, including by determining what apps their children can discover and download from the App Store.

Apple provides resources on how to set up these controls at the following webpages:

- [Set up parental controls with Family Sharing on iPhone](#)
- [Set up Child Account](#)
- [Share Age Range with Developers](#)
- [Change settings and restrictions in the App Store on iPhone](#)
- [Use parental controls to manage your child's iPhone or iPad - Apple Support](#)
- [Block apps, app downloads, websites, and purchases on iPhone](#)

Specifically, parents and guardians with Apple accounts can create “Child Accounts” for their children under 18 years of age, and to which default protections will apply. When parents or guardians set up an Apple Account for their child, the parent or guardian must authenticate with their existing (adult) Apple Account, and Apple takes additional measures to verify that they are the parent providing consent. Apple provides information about the Apple Account set up process at <https://support.apple.com/en-sg/108647>. In Singapore, only users 16 and older can create an Apple Account themselves. So if a user tries to create an Apple Account with an age of below 16 years, the user receives a pop-up screen prompting a parent to sign in and complete an account for them. Users under 16 years of age in Singapore must be part of Family Sharing.

Parents or guardians can also create Child Accounts for children aged 16 to 17 years of age in Singapore as part of Family Sharing (although, as noted above, children aged 16 to 17 years are also able to set up their own Apple Accounts outside of Family sharing).

For all accounts belonging to minors under age 18, regardless of whether they are in a Child Account, certain default protections apply. Parents can also enable additional app and content restrictions based on their child’s age.

Restrictions on Apps rated 18+: All users must verify that they are at least 18 years of age to download apps rated 18+ in Singapore. See more information on age assurance in the section below. 18+ rated apps that were downloaded prior to the implementation of age assurance and subsequently deleted are unavailable for re-download on user’s devices without age assurance. 18+ apps downloaded prior to age assurance may continue receiving updates, as they are key to maintaining the security of the app and preventing vulnerabilities from being introduced that may compromise the security of the user’s device.

App Discovery: There are default restrictions on the types of apps that children can discover on the App Store. For child accounts, apps with age ratings that exceed a user’s account age will not appear on the App Store in places like the Today, Games, and Apps tabs, or in editorial stories by default.

Ask to Buy: Ask to Buy allows parents to approve app downloads and purchases requested by the child, including in-app purchases, on the App Store. It is enabled by default for any Child Accounts under 16 in Singapore and can be enabled for any family member under 18 by the Family Organizer or another parent / guardian in the family group. If a child initiates a

download or purchase on their device, parents receive a request to approve it on their own device. If they choose to approve it, the download or purchase will be added to the child's account. If they decline, the process stops there (i.e. App Store will not complete the download or purchase).

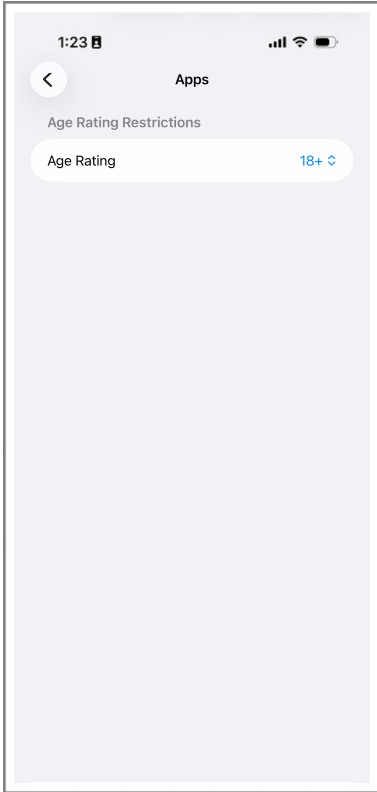
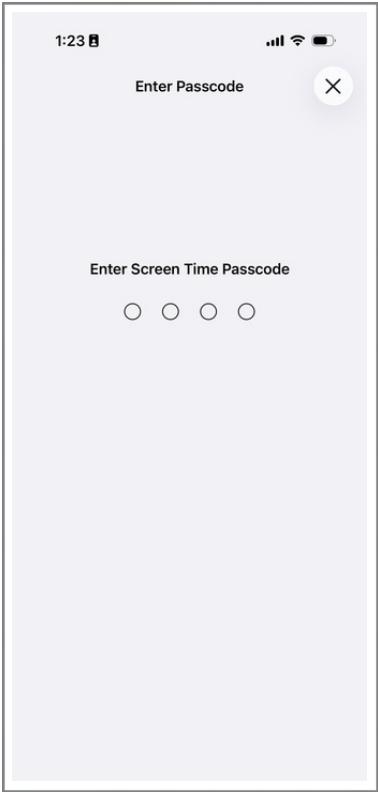
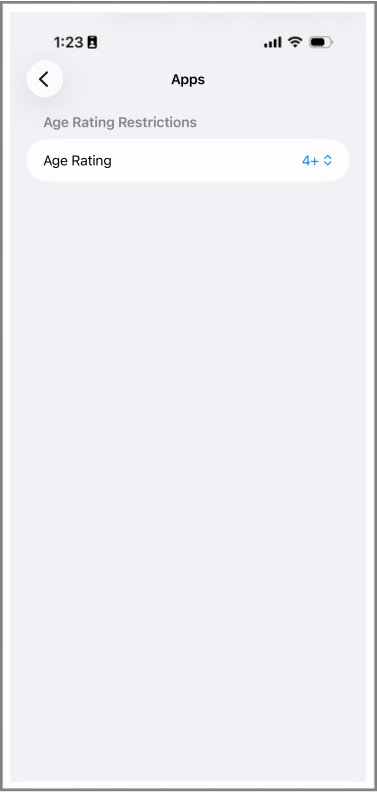
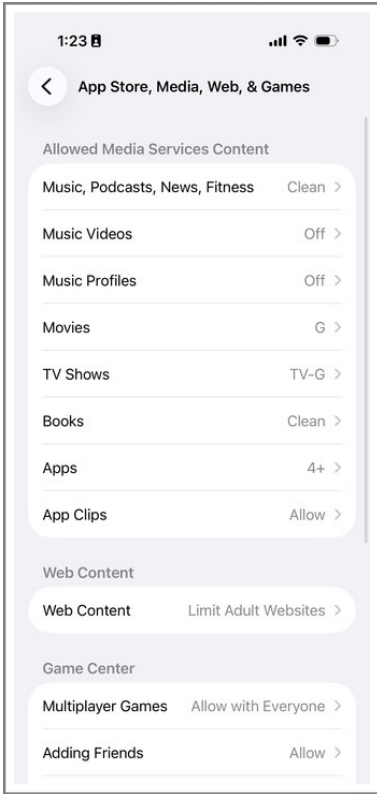
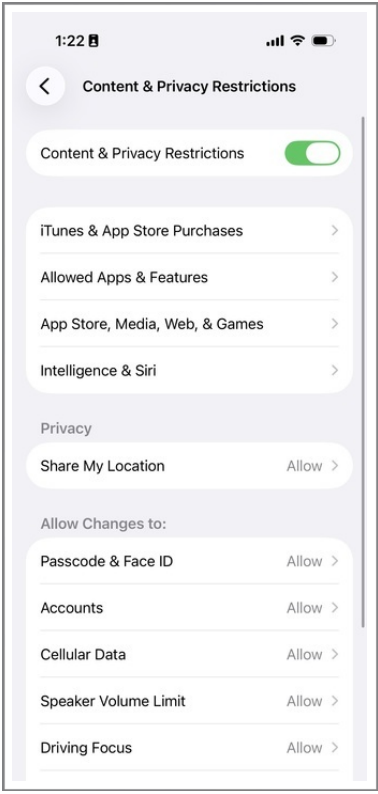
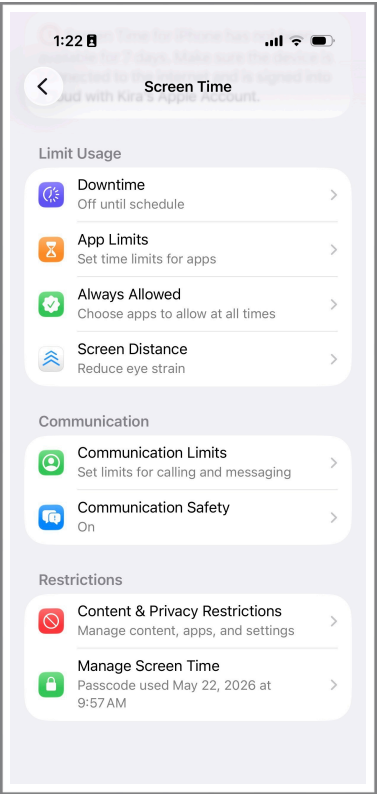
Content & Privacy Restrictions: Parents can use Screen Time's Content & Privacy Restrictions feature to restrict the download of certain types of content, such as apps with specific age ratings. For example, a parent can restrict their 12 year old child from downloading an app with a 16+ age rating. In addition, when children within Family Sharing browse apps on the App Store, they are not shown apps with age ratings higher than age levels set by their parents in the places where Apple features apps on the App Store (such as on the Today, Games, and Apps tabs, or in our editorial stories and collections). This feature can also be used to fully restrict the downloading of apps via the App Store. Parents can also manually adjust what children can access in Screen Time Content & Privacy Restrictions.

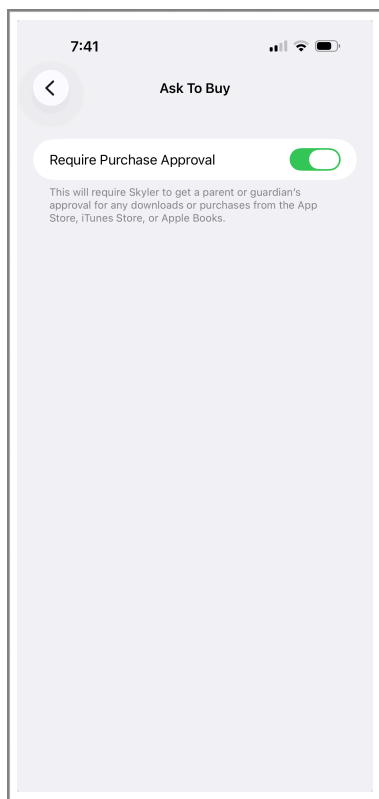
App Limits & Downtime: Screen Time's App & Website Activity features help parents better understand and make choices about how much time their children spend using apps and websites. For example, App Limits can be used to set daily time limits for certain categories of apps, such as social apps and gaming apps. Screen Time reports provide a detailed overview of how much time is spent using apps, visiting websites, and on the device overall, and which apps send the most notifications, which helps parents monitor their child's device use. Downtime lets parents block apps and notifications from launching on Screen Time enabled devices for specific time periods. If downtime is scheduled, parents can use Always Allowed to make exceptions for specific apps, like educational or mindfulness apps.

Default settings for Apple Accounts for users in Singapore 16 years of age and older: Where Apple Accounts of Singapore users with an age of 16 to 17 years are not part of Family Sharing, device level restrictions apply in addition to age restrictions on the download of 18+ apps. The default setting in Screen Time settings is that such users are not able to download apps with a higher age rating than the age associated with their Apple Account. For example, a user with an Apple Account age of 16 years old is blocked from downloading an app that is rated 18+.

Advertising Restrictions: Apple Search Ads doesn't serve ads to any user in Singapore whose Apple Account is registered to a minor under 16 years of age or set up as a Managed Apple Account. Nor do we collect, use, or disclose any information from them. Apple Search Ads also doesn't allow explicit targeting of people whose Apple Account is registered to a user under the age of 18." (<https://ads.apple.com/app-store/privacy>). Further, Apple's Advertising Policies bars serving ad content for real money gambling or pharmaceutical products, medical devices, and medical services to children (<https://ads.apple.com/policies>).

The screenshots below provide an overview of what users see when opting in or out of default settings in Screen Time and Ask to Buy flows.





Age Assurance

Users seeking to download apps rated 18+, or otherwise seeking to confirm their adult status, can confirm their age with a credit card that belongs to them, or by scanning their passport, driving license, National Registration Identity Card, or Foreign Identification Number (FIN) card. Debit cards and gift cards aren't supported.

If a user already has an Apple Account, Apple will check if they have a credit card on file or other eligible methods available to confirm that they are 18 or older.

If a user chooses not to confirm their age, they can continue to use their device — but they can't download apps with an age rating of 18+ until they confirm.

See more details on how users can verify their age at the following resources:

- <https://support.apple.com/en-us/126786>
- <https://support.apple.com/en-us/125662>

Apple also manages and retains personal data collected during age verification in compliance with the Personal Data Protection Act. See more detailed resources at:

- <https://www.apple.com/legal/privacy/data/en/apple-id/>
- <https://www.apple.com/legal/privacy/data/en/app-store/>

Please see the 'Contact Us' section of our privacy policy for any data protection questions relating to age assurance: <https://www.apple.com/legal/privacy/en-ww/>

If you have questions about Apple's Privacy Policy or privacy practices including where a third-party service provider is acting on our behalf, or you would like to contact our Data Protection Officer, you can contact us at [apple.com/legal/privacy/contact](https://www.apple.com/legal/privacy/contact) or call the Apple Support number (800-186-1087) for your country or region. You can also ask us questions about how to submit a privacy complaint and we will endeavor to help.

Additional Tools Available to Developers

In addition to tools available to families, Apple also provides tools to developers to ensure age appropriate experiences for users of all ages.

Family Controls Framework: The Family Controls framework enables developers' apps to use Screen Time API app extensions to implement parental controls through the Managed Settings and Device Activity frameworks.

Sensitive Content Analysis Framework: This is a tool provided to developers which enables an app to check for and blur nudity from externally-sourced images or videos before it is displayed. For example, it may be used for a messaging app to check each image it receives, or it may be used for a classroom app to evaluate uploads from personal devices to a shared location for classroom activities. Detected sensitive content is called to the user's attention and not displayed until the user decides what to do (which could include displaying the flagged content (or not) and for e.g. blocking the contact).

Declared Age Range API: As stated above, Apple has also provided parents with new options for consenting to providing developers with information about the age range of their children – enabling parents to help developers deliver an age-appropriate experience in their apps while protecting privacy. Apple provides parents with information regarding this process here: <https://support.apple.com/en-sg/122770>

PermissionKit: Apple further makes available to developers PermissionKit, which when enabled means that children have to ask their parent or guardian before chatting, following, or adding other users while in an app or game. Parents and guardians can then approve requests from their own device with one tap in Messages.

User Reports: Volume, Breakdown & Outcomes

Singaporean users can report unlawful or harmful content on the App Store — including illegal and restricted online content — to Apple at <https://contentreports.apple.com/>. If the content is hosted on a third-party app or other third-party content service, or in unsolicited promotions, users can also report it directly to the third-party provider. If the third-party provider does not resolve the reported concern, users can also escalate their issue to Apple.

1.1: Number of User Reports Categorized by CoP Categories of Harmful Content

Table 1.1 provides the number of reports received to <https://contentreports.apple.com/> - categorized by CoP categories of harmful content. Issue categories and subcategories are selected by the reporting user. As a result, the category may not accurately reflect the content concerned.

<u>CoP</u> Categories of Harmful Content	Number of User Reports Received
Child sexual exploitation and abuse material ²	9
Content endangering public health	0
Terrorism content	3
Suicide and self-harm content	0
Violent content	0
Content facilitating vice and organized crime	2
Sexual content	1
Cyberbullying content	0

² Notices submitted for this category often flag apps containing user-generated content (UGC). As described in the App Review section above, Apple does not directly moderate this content but requires apps hosting UGC to employ content moderation mechanisms where abusive content is removed promptly.

1.2: User Reports Received Categorized by Outcome

Table 1.2 categorizes the reports highlighted in Table 1.1 by the following Outcomes: 1) Action Taken to directly remove the app or review from the App Store, 2) Action Taken to notify a third party (often the developer) of the report, or 3) No Action Taken³.

CoP Categories of Harmful Content	Action Taken: App or Review Removed	Action Taken: 3rd Party Notified⁵	No Action Taken
Child sexual exploitation and abuse material	1 ⁴	8	0
Content endangering public health	0	0	0
Terrorism content	0	3	0
Suicide and self-harm content	0	0	0
Violent content	0	0	0
Content facilitating vice and organized crime	0	0	2
Sexual content	0	1	0
Cyberbullying content	0	0	0

³ Apple has investigated these reports and determined no further action was warranted

⁴ Apple voluntarily removed the reported app from sale based on terms of service violations distinct from the reported illegal content. Apple complies with all requirements of Paragraph 26(c) of the CoP.

⁵ For this report, each of notices in this column concerned content hosted on the Telegram app. In accordance with Apple's policies on user-generated content, described in the App Review section above, Apple forwarded these notices to Telegram for handling.

User Reports: Timeliness of Review

Apple maintains the safety of the App Store by ensuring that it reviews all user reports of unlawful or harmful content on the App Store and removes any apps that are found to be malicious.

2.1: Median Time to Resolve User Reports Categorized by CoP Categories of Harmful Content

Table 2.1 provides the median time in which the App Store resolved user reports categorized by CoP categories of harmful content.

<u>CoP</u> Categories of Harmful Content	Median Time to Resolution
Child sexual exploitation and abuse material	4 days, 7 hours
Content endangering public health	0
Terrorism content	7 days, 2 hours
Suicide and self-harm content	0
Violent content	0
Content facilitating vice and organized crime	4 days, 17 hours
Sexual content	3 days
Cyberbullying content	0

Prevalence of Violating Apps & Providers

Apple proactively reviews apps submitted to the App Store and enforces its App Review Guidelines to prevent violative or non-compliant apps from reaching users in Singapore. The following metrics capture apps removed and providers associated with those removed apps during the reporting period.

3.1: Apps Removed from the App Store Categorized by CoP Categories of Harmful Content

Table 3.1 provides the number of apps removed from the App Store categorized by CoP categories of harmful content⁶.

<u>CoP</u> Categories of Harmful Content	Number of Apps Removed
Child sexual exploitation and abuse material	0
Content endangering public health	9
Terrorism content	0
Suicide and self-harm content	0
Violent content	2
Content facilitating vice and organized crime ⁷	48123
Sexual content	270
Cyberbullying content	0

⁶ The data in tables 3.1 and 3.2 was derived by mapping the Guideline cited for the app removal to a corresponding category of harmful content. For example, an app removed for Guideline 1.4 - Physical Harm would be mapped to the "Content endangering public health" category. Removals that did not map cleanly onto any category were excluded.

⁷ For the purposes of this Transparency report, 'Content facilitating vice and organized crime' includes instances of gambling and of scams or fraud. Scams/fraud is one of Apple's largest categories of app removals. This includes apps removed for bait and switch maneuvers, where apps were initially approved as standard games or utilities, such as a puzzle or calculator app, that then modified their software 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.

3.2: App Providers Associated with Removed Apps Categorized by CoP Categories of Harmful Content

Table 3.2 provides the number of app providers associated with apps removed from the App Store and categorized by CoP categories of harmful content.

<u>CoP</u> Categories of Harmful Content	Number of App Providers Associated with Removed Apps
Child sexual exploitation and abuse material	0
Content endangering public health	9
Terrorism content	0
Suicide and self-harm content	0
Violent content	2
Content facilitating vice and organized crime	42274
Sexual content	251
Cyberbullying content	0

Proactive Detection Effectiveness

In addition to the various steps Apple takes to mitigate users exposure to harmful content and inappropriate content on the App Store (as detailed under paragraph 28 above), Apple also publishes a range of metrics that can be used to assess the effectiveness of Apple's efforts to address risks relating to harmful content and inappropriate content on App Store. These metrics include for example the number of app rejections (app submissions blocked before publication on the store), apps available on the App Store, the number removed in a given period, the number of appeals and the number of apps reinstated after being removed. In 2025, Apple rejected 2,093,244 apps before publication on the App Store and removed 166,899 after publication. Additional metrics are available in the 2025 App Store Transparency Report, available [here](#), including the total number of apps available on the App Store, total number reviewed, and rejection and removal metrics broken down by App Review Guidelines sections, as well as appeals and restoration metrics.