



2025 Microsoft Store Annual Online Safety Report - Singapore Code of Practice for Online Safety: App Distribution Services

Table of Contents

1. Introduction	3
2. Microsoft Store Approach to Online Safety.....	3
3. How Microsoft Store Protects Children Online	8
4. Microsoft Store Accessible Information About Safety	14
5. MS Store User Reporting Metrics.....	15

1. Introduction

At Microsoft, we are committed to protecting our users, especially children, from harmful content and conduct, while meaningfully balancing freedom of expression, privacy, security, and accessibility. As a company that offers a wide range of consumer, educational, and enterprise services, Microsoft applies a risk proportional approach to safety. This approach recognizes that risks vary depending on a service's primary purpose, design, features, and audience and effective safeguards must be tailored to the characteristics and use cases of each service. This annual online safety report provides an overview of the safety measures in place in Microsoft Store for Singapore in line with our requirements under the Singapore Code of Practice for Online Safety: App Distribution Services.

2. Microsoft Store Approach to Online Safety

Microsoft maintains several digital online storefronts that are available in Singapore, including the Microsoft Store on Windows, the Xbox.com Store, the Apps.microsoft.com Store, the PC Games Store, and the Microsoft Store on Xbox consoles (collectively "MS Store"). Although these storefronts distribute different products and serve distinct customer needs, they share certain backend systems, including MS Store's online safety program, which uses a layered approach to mitigate harm for end users, including a thorough pre-publication application ("app") review process, user reporting, automated technology, age ratings, parental controls, and trained human reviewers, enabling us to find and take action against content or conduct that violates our terms and policies.

MS Store Content Policies

Microsoft's consumer online products, including MS Store, maintain a robust set of rules about what types of content and conduct are not allowed. The [Microsoft Services Agreement](#) ("MSA") which governs the use of Microsoft consumer products and services, has a [Code of Conduct](#) that explains what is not allowed and what to expect when accessing services like MS Store. MS Store has additional content policies that its app publishers must abide by for the apps published on its storefronts. All developers must agree to the Microsoft Application Developer Agreement, published [here](#), and are also subject to the [Developer Code of Conduct](#) and [Microsoft's Store Policies](#), all of which are publicly available.

App Distribution Service Code of Practice Harm Categories	Store Policy	Internal Breakdown
Child Sexual Exploitation and Abuse	11.15 - Child Safety	11.15.1 - Child Sexual Exploitation and Abuse (CSEA)
Graphic Violence and Gore	11.3 - Risk of Harm	11.3.5 - Graphic Violence and Gore
Suicide and Self Injury	11.3 - Risk of Harm	11.3.7 - Suicide & Self-Harm
Violent Threats and Incitement	11.3 - Risk of Harm	11.3.1 - Glamorization of Violence
Public Health Endangerment	11.3 - Risk of Harm	11.3.8 - Endangering Public Health
Bullying and Harassment	11.4 - Defamatory, Libelous, Slandorous and Threatening	11.4.2 - Bullying and Harassment
Sexual content	11.7 Adult Content	1.7 - Pornographic or Sexually Explicit content
Vice and Organized Crime	11.8 - Illegal Activity	11.8.4 - Vice and Organized Crime

Included in the Developer Code of Conduct are additional requirements that address user-generated content within the publisher’s app, such as implementing a method for proactive detection of inappropriate or harmful user generated content. The policy specifically states: If your product contains UGC, you must:

“Publish and make available to users a product terms of service and/or content guidelines for User Generated Content either in product or on your website. Provide a means for users to report inappropriate content within the product to the developer for review and removal/disablement if in violation of content guidelines and/or implement a method for proactive detection of inappropriate or harmful UGC.”

Remove or disable UGC when requested by Microsoft.

As part of our standard onboarding process, MS Store checks that apps have the necessary tools in place for proactive detection of content or content reporting mechanisms.

The chart below indicates how MS Store’s Policies map to the Code of Practice’s harmful and inappropriate content categories. A user-friendly explanation of these policies is available on our [public-facing digital safety site](#), as is a version for [teens](#).

Identification of Harmful Content and Conduct

MS Store employs a multi-layered approach to content moderation that combines automated detection technologies and human review processes to identify and mitigate the risk that users will be exposed to harmful content within an app available in MS Store. MS Store maintains a robust certification system to ensure that content available in our store is appropriate for users. This includes making our rules and expectations clear to developers, verifying apps before publishing through both automated and human review, ongoing post-publish catalogue audits, and acting on reports of potentially violative content or conduct.

Every app submitted to MS Store undergoes Microsoft's app certification and review process. No app is published to MS Store until it is certified for publication by Microsoft. During this process, apps are tested to ensure that they are secure and safe, run properly, and comply with [MS Store Policies](#) to meet Microsoft's technical and content requirements, which addresses a wide spectrum of harms including the Code of Practice's harmful and inappropriate content (including but not limited to child sexual exploitation and abuse material, sexual content and terrorism content including material that indicates preparatory terrorism activity).

MS Store's ingestion system uses automation to review new products as well as updates using a wide range of methods, looking at both metadata and the binary packages. This includes basic scans, anti-malware, offensive word lists, machine learning, AI passes, and more. If the submission meets criteria for human review (including such criteria as unknown publishers, prior rejections, and issues arising from scans), including criteria associated with any content types that breach our policies as listed in the table above, the submission is routed to highly trained human moderators for further review. Manual reviewers confirm issues spotted in automation as they do a more thorough investigation that may include installing and using the products depending on the issues flagged. All of these activities take place before the application and updates are published to the store. Following publication, MS Store continues with a variety of automated and human audits to make sure products continue to meet content safety standards and function well. Apps that do not meet MS Store's certification requirements are rejected from publication, with detailed information provided to the publisher about the reasons for rejection so that they can correct any issues if possible and re-submit their content.

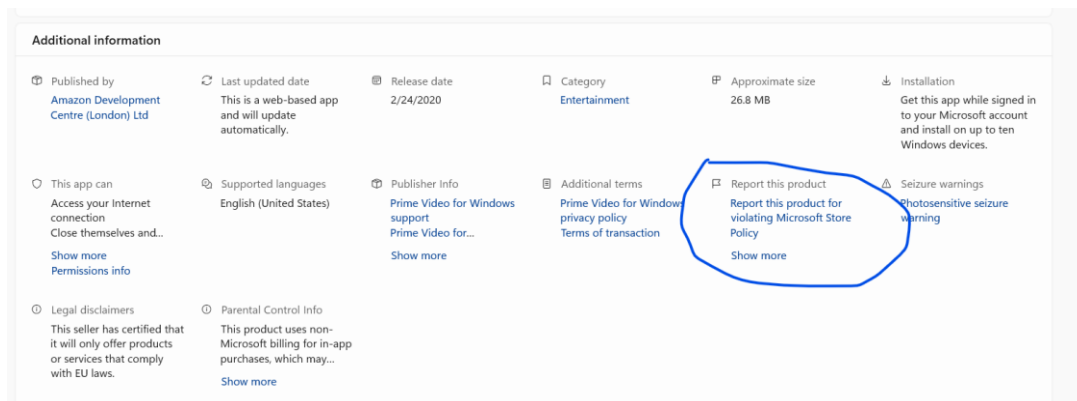
Moreover, MS Store reviews and verifies other information provided by the app publisher to ensure that information presented to consumers is accurate, including verifying information about the publisher's identity and status, reviewing the accuracy and appropriateness of details and screenshots provided for the product's listing in MS Store, and ensuring up-to-date information about any applicable additional terms and policies (such as the publisher's privacy policy and additional terms and conditions). Apps that have already been published are frequently reviewed and re-evaluated for a

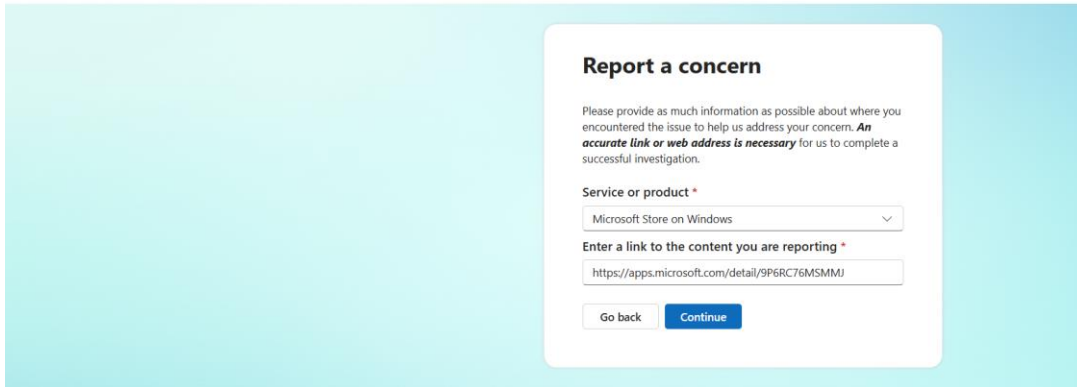
variety of reasons, including to identify and act upon instances of harmful and illegal content. This includes when an app is updated, a concern (such as an internal or external report or complaint) is raised to MS Store, and random checks.

MS Store also leverages reports from users, developers, internal audiences, and governments to identify potentially violative content and maintains a team to quickly validate and act on findings. Microsoft has a robust reporting mechanism permitting any person to quickly and easily report an app for a variety of safety and content-related potential harms, including those that pose a risk for child users.

The Report A Concern function in MS Store allows users to report content that violates Microsoft Store Policies. Users can do this by clicking on the “Report this product...” links found on the app “product detail” page and following through on the subsequent form. Microsoft also provides a centralized reporting function on our public-facing digital safety site. Reports are acknowledged by the system and reviewed by human moderators for compliance with MS Store Policy and, where needed, local law. Appropriate actions are taken swiftly where warranted. When action is taken, the developer and the complaining user are notified by the system. Complainants are able to appeal the moderation action taken as a result. Details on enforcement follow.

Customers can visit MS Store’s publicly displayed pages to find links to [report a product for harmful content](#) or violations of [MS Store Policies](#). Below are screenshots of how users can report potentially violative content; the first is in-app for MS Store and the second is through Microsoft’s Report-A-Concern tool.





Report a concern

Please provide as much information as possible about where you encountered the issue to help us address your concern. **An accurate link or web address is necessary** for us to complete a successful investigation.

Service or product *

Microsoft Store on Windows

Enter a link to the content you are reporting *

<https://apps.microsoft.com/detail/9P6RC76MSMMJ>

[Go back](#) [Continue](#)

Enforcement of Content Policies

For apps that have already been published, MS Store enforces its content policies using several types of restrictions. These restrictions can be removed at any time when the issue is resolved. In some cases, depending on the nature and severity of the issue, Microsoft may choose to not ever remove the restriction. The types of available application restrictions are:

- **Suppress:** The product is not searchable or browsable in the Store but is able to be updated by the developer to make changes to correct any issues. This is typically a temporary state.
- **Take Down:** In addition to the above, the product is not able to be re-installed by users, and the developer cannot update the product. This is typically permanent but can be adjusted based on reconsideration or appeal.

If an app is suppressed or removed for containing content prohibited by law, users who purchased and downloaded the app within the previous six months will be notified as soon as reasonably practicable. In addition, in rare cases involving persistent infringement or egregious behaviour, we may apply account-level restrictions that remove the developer's access to their account and withdraw all products associated with that account from the Store.

When an app is identified as containing illegal or policy-violating content, it is removed from the Store and an automated email is sent to the developer outlining the violative material. This notification encourages developers to contact our certification team via a dedicated email address if they wish to appeal the decision, seek further information about the violation, or work with us to resolve the issue. Furthermore, larger developers with whom we have ongoing relationships may also choose to engage their Microsoft relationship managers to discuss the matter.

Expedited removal for egregious and illegal content

Microsoft takes reports of CSEA and terrorist related material extremely seriously. Reports of illegal content are assessed based on the category of violation chosen by the reporting party, and reports of CSAM and VET Content are immediately prioritized. The average time to complete a review is less than 1 business day for all reports, and less than 3 hours for reports of CSAM/VET Content. If illegal content is detected during review, the content is immediately removed and appropriate action is taken against the app.

Additional Information

MS Store Policies and app certification criteria are available at the following link: <https://learn.microsoft.com/en-sg/windows/apps/publish/store-policies-and-code-of-conduct>.

More information about Microsoft's app certification process is available at the following link: <https://learn.microsoft.com/en-sg/windows/apps/publish/faq/get-your-app-certified>.

More information about Microsoft's Digital Safety program is available at the following link: <https://www.microsoft.com/en-sg/digitalsafety>, which details Microsoft's digital safety efforts, inclusive of MS Store.

3. How Microsoft Store Protects Children Online

For almost two decades, Microsoft has been a global leader in protecting children online through its efforts to combat online child sexual exploitation and abuse ("CSEA"). Microsoft's approach is grounded in the recognition that this is a whole of society challenge, demanding coordinated action across government, law enforcement, technology providers, civil society, and survivor support organizations. Our work reflects a simple but non-negotiable principle: children must be able to participate in digital services without being exposed to grooming, sexual abuse imagery, exploitation, or other harms. At the foundation of our work is a comprehensive policy framework that prohibits the use of any Microsoft service to exploit or harm children. We maintain a strict zero tolerance stance on CSEA, grooming, and emerging forms of CSEA, including AI-generated material. These policies are enforced globally and apply across Microsoft's consumer services, including MS Store.

Parental Controls and Family Safety

MS Store utilizes Microsoft's layered, ecosystem-wide framework that combines parent-child account creation at device or service set up, parent attestation of age for children below the local age of digital majority, and parental consent and controls flows

to protect child users from content harmful to them such as sexual content, violent content, suicide and self-harm content, and cyberbullying content. Together, these layers provide a consistent, privacy-respecting foundation for enforcing age-based protections across services.

Microsoft's consumer services, including MS Stores, allow for the creation of linked parent/guardian and child accounts in a "Family Group". Microsoft's Family Safety parental supervision and child safety protections are anchored to MSA based identities (i.e., parent and child accounts) and apply consistently across the Microsoft ecosystem, including MS Store. MS Store uses the parental control settings available through Microsoft Family Safety, which are managed by the parent account linked to the child. These controls allow parents to tailor their child's experience by setting screen time limits, restricting purchases and app downloads, applying web filtering, and requiring parental approval before a child can access apps or content above the age rating set for that child. Together, these settings help parents supervise how their child interacts with digital content and create a safer, more age-appropriate experience across Microsoft services, including MS Store. When a child account is first created, these controls are all restricted by default and can only be viewed or changed by the linked parent account. Through Microsoft Family Safety, parents can add additional restrictions by choosing apps to filter based on age-appropriateness, ensuring children only access suitable content suitable for their age. Parents set the maturity rating limit for each child (for instance, "only allow apps and games rated for ages 10 and under"), and content above that level will be blocked.

MS Store does not permit the use of demographic data, including age, for the targeting of advertisements, promotions or recommendations and as a result, children are not exposed to targeted advertising on the platform.

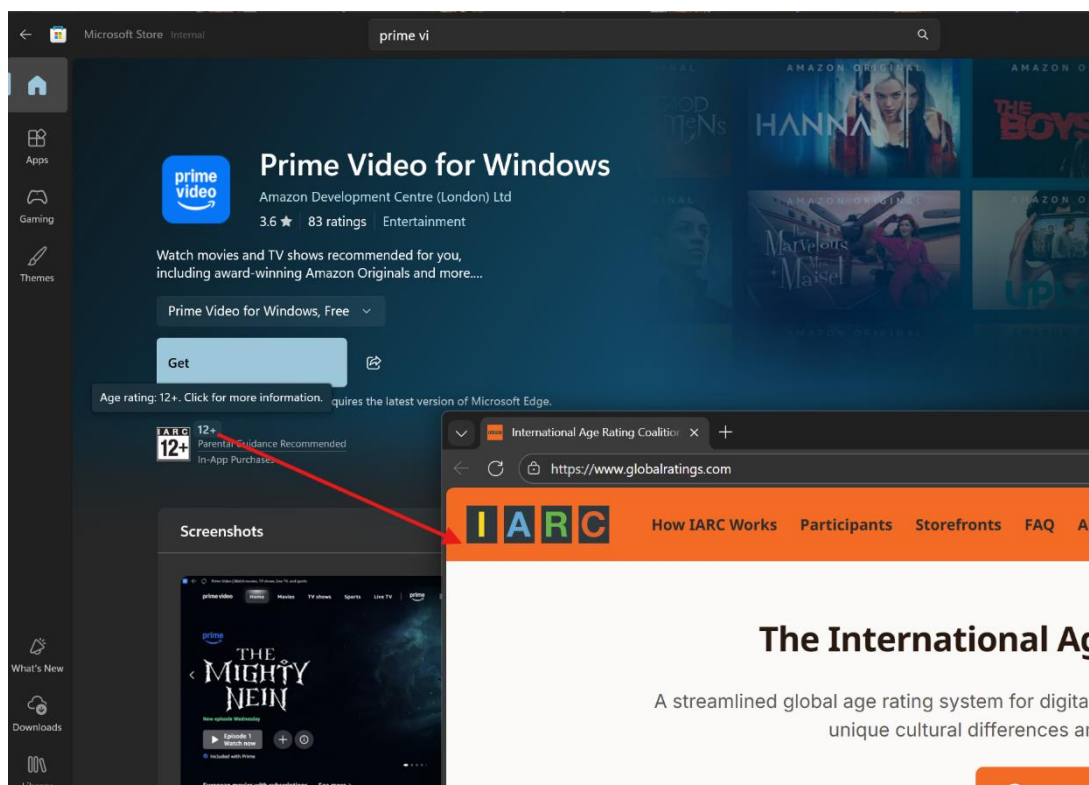
Parents can also view activity reports on MS Store regarding their children's downloads and app use and enforce "safe search" features and website filtering while children browse content linked from MS Store pages. These parental controls apply consistently to the child's Microsoft Account no matter what device the child is using to access MS Store. Parents can also choose to block access to specified apps and services.

Users must be signed in with a Microsoft Account to acquire, purchase, download, and install most MS Store apps. Users who are logged out can browse some areas of MS Store storefronts, view some product details, and install a limited number of free, appropriate-for-all-ages apps. Content that is age-gated is searchable but not purchasable or playable, for unauthenticated users.

In order to help users decide whether apps are appropriate for children, MS Store relies on app age ratings set by the International Age Rating Coalition (“IARC”). Every app or game must complete IARC’s rating process or submit existing IARC rating certificates before it can be published in the MS Store. Each “product detail” page contains links to the [IARC rating definitions](#), which provide more information on the type of content to be found based on the rating assigned to a particular app or game (3+, 7+, 12+, etc.). IARC ratings provide more information about whether the app is appropriate for child users.

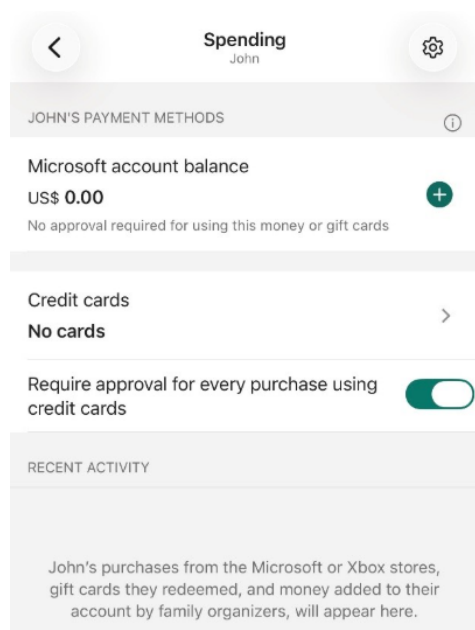
IARC implements strict age-rating categories for the variety of potentially sexual content or violent content that may be present in a particular app or game. For example, graphic sexual content and graphic violence are restricted to an IARC 18+ rating. Realistic, but non-graphic violence and non-graphic sexual content is restricted to an IARC 16+ rating. Other types of sexual and graphic content are also covered here as well.

See screenshot below for an example of where the IARC rating would sit on the product detail page for an app.



MS Store enforces these ratings by automatically blocking child accounts from downloading or purchasing apps rated above the child’s age. If a child tries to access a blocked app, they can send a request to the parent for approval, which the parent can approve or decline remotely. This mechanism keeps children safe by preventing exposure to violent, sexual, or other inappropriate content, while still giving families

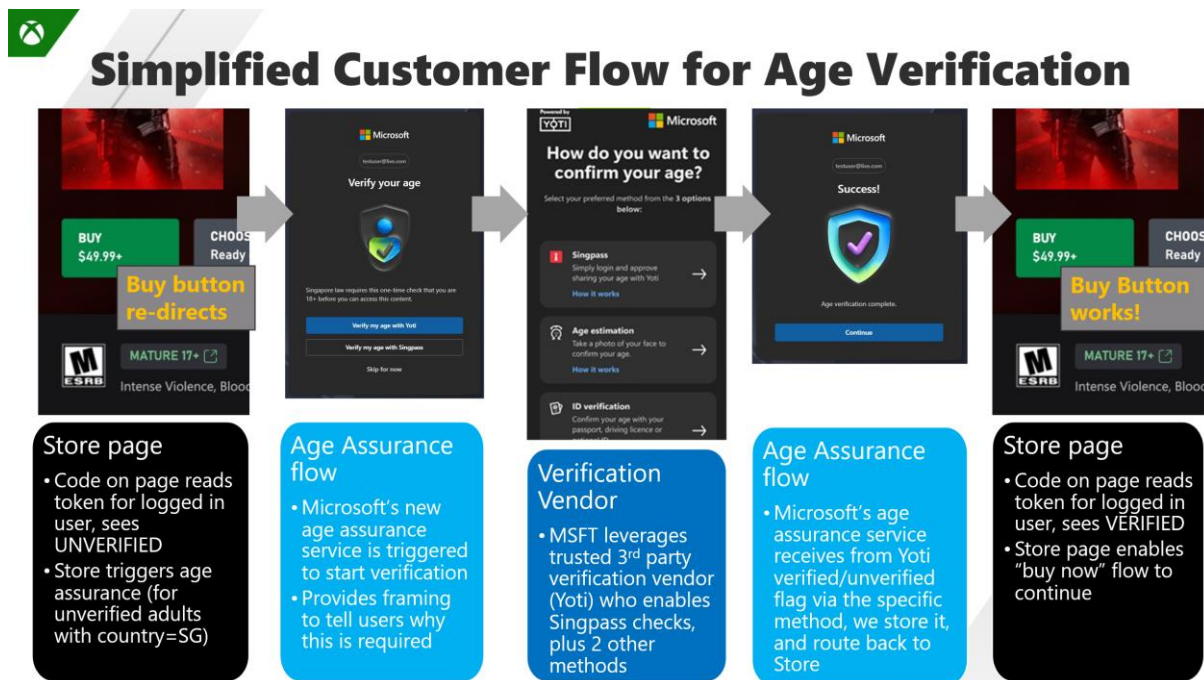
flexibility to make decisions aligned with their values and the maturity of their child. To opt out of these default restrictive content settings, a parent must intentionally turn off the setting “require approval for every purchase using credit cards,” which serves as a warning that turning this default “off” would allow child users to purchase restricted apps without parental approval - see screenshot below.



Regardless of age ratings, other types of content including a) Sexual content (b) Violent content (c) Suicide and self-harm content (d) Cyberbullying content, which may be particularly harmful to children, are prohibited from Microsoft Store entirely. Microsoft enforces its Store Policies which entirely prohibit apps or games that encourage suicide or self-harm (Policy 11.3), inappropriate interactions with children (11.15), grooming (11.15), sextortion (11.15), trafficking (11.15), and sexualization of minors (11.15). Furthermore, apps and games are prohibited from Microsoft Store if they target children and include content that facilitates or encourages cyberbullying (11.15) or promotes negative body or self-image (11.15). More information on each is available to parents [here](#).

Age Assurance

In 2026, MS Store is working with a third-party vendor, Yoti, to deploy an age assurance solution in Singapore to help mitigate the risk that child users will be exposed to harmful content within 18+ apps on its storefronts. A simplified user flow is included below, representing the three types of age assurance that will be accepted upon launch: facial age estimation, government-ID verification, and SingPass.



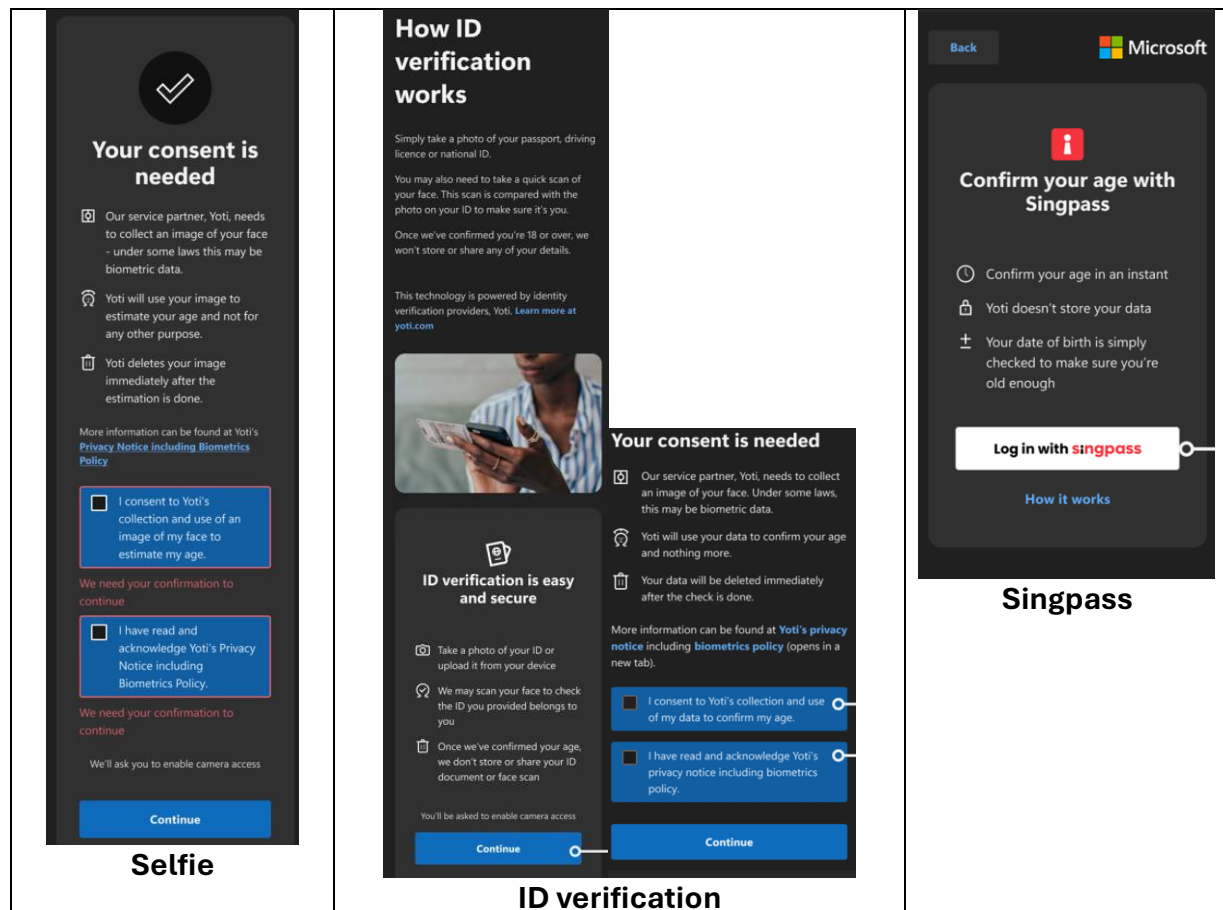
All age assurance methods offered by Microsoft have been assessed against Singapore's PDPA guidelines

- Facial Age Estimation:** A photo of the user's face, taken by a liveness selfie from the user's device, will be analysed to estimate the user's age. Users are informed prior to providing a selfie that the information is required solely for age verification purposes. The facial image and derived data are used only to perform age estimation and are not used for marketing, profiling, or any other purposes.
- Government ID Verification:** The data requested will be an image of the user's government-issued identification, uploaded by the user. Yoti performs Optical Character Recognition ("OCR") and document template detection on uploaded images. During this process, data fields, such as date of birth, are extracted from each ID document, but are purged from Yoti's system immediately following completion of the age determination. Only the date of birth is utilized for the determination of the individual's age. Additional data fields are captured and used towards document authenticity checks. A liveness selfie is also performed.
- Singpass:** MS Store's age assurance solution also offers Singpass as an age assurance option, leveraging Singapore's national digital identity system as a trusted, government-backed age verification mechanism. The Singpass integration minimises collection of personal data by only receiving a binary age attribute (e.g. above/below threshold) rather than full identity information. No underlying personal data (e.g. date of birth) is collected or stored for age assurance purposes.

For all age assurance methods, Microsoft provides clear, easily comprehensible notifications about how data is collected. Screenshots are included below.

Users can contact Microsoft Support for data protection queries related to our age assurance solution. Contact information can be found [here](#).

The below screenshots for each age assurance method illustrate data collection notices which are clear, easily comprehensible and provide appropriate information and include a clear consent request:



To minimize the collection and retention of personal data, Microsoft's age assurance implementation is designed so that Microsoft receives only the limited age assurance information needed to enforce age-based protections and access controls. Microsoft does not receive or store the underlying identity document, facial image, payment card details, or other verification artefacts used during the verification process. Microsoft retains only the limited age assurance outcome, and not the evidence, required to support age-based protections and access controls and avoid requiring verified users to complete age verification repeatedly for the same purpose.

Yoti acts as Microsoft's independent age assurance provider for Microsoft Store Singapore and depending on the method selected by the user, Yoti may process the relevant information or evidence solely to determine whether the user satisfies the applicable age threshold. Information submitted for an age check is processed only to

complete the age verification transaction requested by Microsoft Store and is not reused by Yoti for its own research and development, marketing, profiling, or other unrelated purposes.

Microsoft's age assurance approach is based on privacy-by-design and data-minimization principles. Microsoft has implemented organizational and technical safeguards governing the use of age assurance information, including access controls, functional separation, and restrictions on use for unrelated purposes. Age assurance information is used to support age-based protections and access decisions and is not used for advertising, profiling, or artificial intelligence model training purposes. Yoti leverages independent privacy and security certifications for its age verification services, including ISO 27001, ISO 27701, and SOC 2 Type II.

Advertising to Children

MS Store also has a robust set of advertising policies contained in the MS Store [Advertising Conduct and Content Policies](#) and [App Developer Agreement](#), which requires any advertising to comply with all applicable laws, regulations and regulatory guidelines; moreover, the advertising cannot be designed to generate user clicks.

While children may encounter app recommendations, promotional placements, or curated collections that are made available to users of Microsoft Store storefronts, Microsoft Store does not target advertisements, promotions, or recommendations using demographic information, including age. Content presented on Microsoft Store product detail pages and promotional sections must be appropriate for all ages, and collections promoted for children or families are curated to include apps with appropriate age ratings. In addition, child accounts remain subject to Microsoft Family Safety settings and age-rating restrictions that limit the acquisition of age-inappropriate content. This reduces the risk that children will be exposed to harmful or age-inappropriate apps through promotional features or recommendations.

4. Microsoft Store Accessible Information About Safety

MS Store, and Microsoft generally, provides comprehensive information about online safety for users, which can be found in several locations:

- <https://www.microsoft.com/en-sg/DigitalSafety>: Details Microsoft's digital safety program and content moderation measures, inclusive of MS Store
- MS Store Content Policies are available here: [MS Store Policies](#)
- Information on how to report content that potentially violates MS Store Policies can be found here: [Report a Concern](#)

- Additional information on IARC rating definitions can be found here: [IARC rating definitions](#), which provide more information on the type of content to be found based on the rating assigned to a particular app or game (3+, 7+, 12+, etc.)
- For more information on how to leverage parental controls offered by Microsoft's Family Safety program, including information on how parents can supervise and manage children's use of apps, users can go [here](#). A short guide for parents can also be found here: <https://aka.ms/Guide-For-FamilySafety>
- For gaming-specific online safety information, parents can access the Singapore version of the [Xbox Gaming Safety Toolkit](#), which was developed in consultation with local experts including IMDA.

5. MS Store User Reporting Metrics

For the period from 1 April 2025 to 31 December 2025, MS Store received **zero** user reports concerning sexual content, violent content, suicide and self-harm content, cyberbullying content, content endangering public health, or content facilitating vice and organized crime.

During that same reporting period, MS Store did not have any non-compliant apps or app providers in relation to the harm categories outlined in the previous sentence, following the deployment of automated tools described and human review processes described above.