

App Store Technical Deep Dive

Final Report
March 2026

App Store Technical Deep Dive: Final Report

Contents

1. Executive summary	1
2. Introduction and objectives	6
3. Methodology	8
4. Prioritisation of app stores for review	13
5. Review of app store measures to protect children from content harmful to children	16
5.1 Overview of app store measures	16
5.2 Content policies including age ratings	17
5.3 Account setup	21
5.4 Parental controls	23
5.5 App discovery	26
5.6 App access	36
5.7 Reporting	38
5.8 Developer processes	40
5.9 Overall analysis of app stores	42
6. Digital ecosystem overview	46
6.1 Digital ecosystem map	46
6.2 Role of key actors	47
7. App stores in context	49
7.1 Overview of the different ways child users may access regulated services	49
7.2 Operating systems	50
7.3 App stores	53
7.4 Sideloaded	55
7.5 Browsers	56
7.6 Cloud gaming	59
7.7 Regulated services	61
7.8 Other supporting actors	62
8. Conclusions	64
Appendices	
A1 Glossary	67
A2 Further Details on Methodology: User Journey Testing	71

1. Executive summary

1.1 Research scope and objectives

Ofcom commissioned this research to better understand what role app stores play in children in the United Kingdom encountering content which is harmful to them, by means of regulated apps which the app stores make available.

This research is structured into two phases:

- **Phase 1** - focuses on the role of app stores; and
- **Phase 2** - aims to contextualise app stores within the broader digital ecosystem, mapping the different actors that may be involved in children accessing regulated apps.

The results set out in this report are based on research conducted by MTM London on behalf of Ofcom, with desk research and user journey testing conducted between 1 November 2025 and 15 January 2026. This research represents a snapshot in time and these findings may not reflect subsequent updates to features or policy guidelines that occurred after these periods. The findings from phase 1 are based on a set number of user-journeys and are not representative of every user journey on app stores.

The findings set out in this report are those of MTM London alone and do not reflect the views or position of Ofcom. For the purposes of transparency, we have explained the methodology for the selection of certain app stores and named them in Exhibit 3, illustrative screenshots of findings from user-journey testing on these app stores have been used throughout the report. App stores are not regulated under the Online Safety Act and the findings in the report are not intended to be a compliance assessment.

1.2 Key findings: Phase 1

App stores commonly provide access to regulated apps.¹

We prioritised twelve app stores for in-depth review from a long list of over 80, primarily based on access to and usage of the stores by the UK population, and focused on those most likely to be used by children. The app stores selected for in-depth review included: Apple App Store, Google Play Store, Samsung Galaxy Store, PlayStation Store, Xbox Store, Microsoft Store, Amazon Appstore, Nintendo eShop, Steam, Epic Games Store, Aptoide and Uptodown Market.²

We found that these app stores used a range of measures to protect children from accessing regulated apps where they may have encountered content harmful to children including:

- Prohibition of apps containing certain types of content (e.g. explicit sexual content, extreme violence, hate speech) in their Terms of Service.
- App store review of apps pre-publication to ensure all apps adhered to developer terms of service, including content policies.

¹ This report uses the term 'regulated app' to refer to apps for a regulated service, as defined in Section 161 of the Online Safety Act.

² Aptoide and Uptodown Market were selected to cover a wider range of app store types.

- Implementation of age ratings and content labels, designed to provide users with clearer visibility over the nature of content within regulated apps.
- Use of age checks such as self-declaration (and in some cases age assurance) to determine if users were over 18.
- Provision of child accounts to apply age restrictions within the app store.
- Age restrictions on apps surfaced in the discovery journey (e.g. browsing app stores) which may have reduced the likelihood that child users discovered regulated apps.
- Age restrictions that restricted apps that a child user downloaded based on age-ratings, which may have blocked access to certain regulated apps.
- User reporting tools that helped app stores identify regulated apps which may contain content harmful to children.

These measures had the potential to protect children from apps where they may encounter content harmful to them, by restricting their access to these apps, reducing their chance of discovering them and reacting following children being exposed to potentially harmful content, e.g., delisting apps.

The combination of measures used and how they were deployed in practice varied by app store, with implications for the nature and level of protection offered to children. The app stores reviewed generally fit into one of four general archetypes, distinguished by parent or guardian role, method of age check (e.g. age assurance, self-declaration), and whether age restrictions were applied automatically or required manual setup. These archetypes are differentiated by reference to the different approaches app stores took.

Exhibit 1: Archetypes of app stores reviewed

App store archetype	A: Automatic restrictions supported by age assurance	B. Automatic restrictions based on self-declared age	C. Manually enabled restrictions based on self-declared age	D. Access without account-based age restrictions
Accounts	Account required			No account required
Parent or guardian role	Parent or guardian required to set up child account and/or to give approval to download 18+ apps			Not required
Age check for 18+ users	Age assurance used	Age self-declared	Age self-declared	Not applicable
Age-based restrictions	Restrictions on accessing 18+ apps set automatically		Restrictions on 18+ apps available, requiring manual setup to turn on	Not applicable
Which app stores (note variations)	PlayStation Store Google Play Epic Games Store	Microsoft Store Xbox Store Apple App Store Amazon Appstore Samsung Galaxy Store	Nintendo eShop Steam	Uptodown Market Aptoide

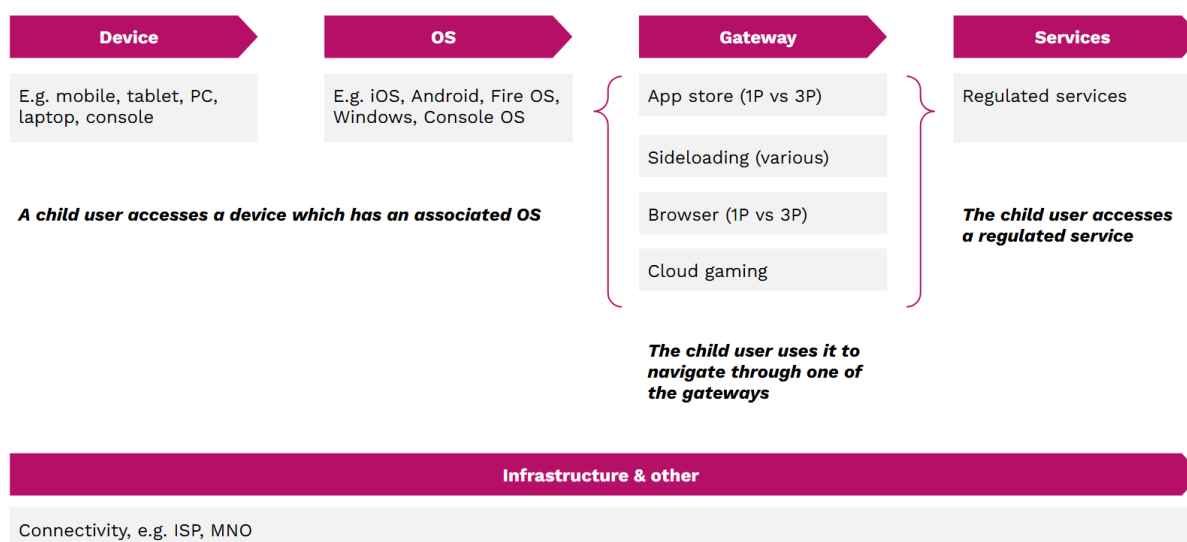
We found several potential limitations to these protective measures used by the app stores reviewed including:

- Protective measures used could vary by age group, with differences generally more pronounced between child users aged under 13 and child users aged 13-17.
- Inconsistencies in age ratings across different app stores suggested that there was the risk that not all app stores had appropriate or consistent age ratings.
- Most app stores reviewed appeared to rely on one-time account registration, with few subsequent age checks, creating a risk that if an error was made during account set up, or a child gained access to an adult account, this would not have been corrected.
- A significant proportion of app stores surfaced or recommended regulated apps with age ratings higher than account ages during user testing, including 18+ apps. This discoverability could have raised children's awareness of regulated apps, even if those users may have still been blocked from downloading the apps.

1.3 Key findings: Phase 2

There are a range of different actors beyond app stores that may play a role in how child users in the UK access regulated services. This can be illustrated through a typical child user journey which involves accessing a device with an associated operating system (OS)³, then passing through a gateway to reach a regulated service, via an internet connection from an internet service provider (ISP) or mobile network operator (MNO).

*Exhibit 2: General stages in the child user journey to access regulated services and the key actors involved**



A child user relies on on connectivity from an ISP or MNO.

** In this report, "actor" is used to refer to devices, OSs, gateways – a collection of different actors that provide a way for users to access regulated services on their device including app stores, sideloading methods, browsers and cloud gaming –*

³ Operating system refers to the preinstalled system-level software that powers these devices and enable them to run software applications.

regulated services, and supporting infrastructure. The report also refers to different “actor types,” e.g. first-party (1P) versus third-party (3P).⁴

Operating systems (OS) can play a key role in child users accessing regulated services, being involved in account creation, age assurance and parental controls or age-based restrictions. In some cases, OSs may pass on age signals and apply protections to gateways and regulated services.

While app stores may be the primary gateway through which a child user accesses regulated services, there may be alternatives. These include sideloading where users download and install apps via direct publisher download, file-sharing services or other distribution channels; web browsers where users access a web version of regulated services; cloud gaming, which allows games to be streamed over the internet without the need to install each game to the user’s device; and potentially others.

There is further variety in the ways child users may access regulated services based on different actor types, e.g. open versus closed OS ecosystems, 1P versus 3P providers. Considering the main actors and differences between actor types in turn⁵:

- **OS:** Can be open, enabling multiple gateways and sign-on options to regulated services, closed, making 1P app stores the main gateway and controlling sign-on, or somewhere in between.
- **App stores:** 1P app stores appear to use OS-level accounts, inheriting age signals and parental controls, while 3P app stores are more independent and involved in account management.⁶
- **Sideloading:** Enables download and installation outside of 1P app stores, with options including direct publisher download, file-sharing services and other alternative distribution channels. Sideloading is not possible on closed or mixed OS ecosystems.
- **Browsers:** 1P browsers typically rely on OS-level accounts, inheriting age signals and parental controls, while 3P browsers may do the same but these may need to be set up separately, with the default being a signed-out experience.
- **Cloud gaming:** Integrated cloud gaming services, e.g., on consoles, appear to inherit age signals and parental controls from the console OS. Standalone cloud gaming services do not inherit age signals or parental controls, instead capturing age signals during the direct sign-up process and requiring users to set up parental controls.
- **Regulated services:** May inherit age signals from OS or app-store level accounts, or capture them via their own sign-up process, and may apply protective measures for child users themselves.

1.4 Conclusions

These research findings raised several considerations for Ofcom about the role that app stores could play in protecting children from accessing content that may be harmful to children by means of regulated apps.

⁴ In this report, ‘first-party’ refers to a gateway (e.g. app store) or regulated service that is from the same provider as the operating system on the user’s device, and any Original Equipment Manufacturer (OEM) bundled app stores that come installed with a device.

⁵ Refer to Section 7 for sources and further details.

⁶ Including in account creation, age assurance and parental controls or age-based restrictions, in some cases may pass on age signals and or apply protections to gateways and regulated services.

Firstly, relating to app store protective measures and the different combinations and ways these may have been deployed by app stores, considerations include:

- What combination of measures, if any, offers effective protection for children from encountering content harmful to them?
- How should these measures be applied, e.g. which methods of age check if any should they use?
- When should they be applied, e.g. age checks at account setup or triggered by some action later in the user journey?
- What steps should be taken, if any, to address discrepancies in age ratings across app stores?

Secondly, relating to app stores in the context of the wider digital ecosystem, we saw that, while app stores may have been the main gateway for child users to access regulated services, there were alternatives. In addition, we saw that age checks and parental controls could be managed by different actors (e.g. OSs, app stores, regulated services) and that these may have passed between actors but also may not have. Based on this, further considerations could include:

- What is the relative importance of app stores in child users accessing regulated services versus other gateways?
- What is the likelihood that protective measures applied at the app store level could be bypassed by child users by using other gateways?
- How would protective measures applied at the app store level interact with protective measures from other actors in the ecosystem?
- What is the ability of parents or guardians to understand, navigate and setup accounts and protective features, and understand where they apply across the devices, OSs, gateways and regulated services their child users may use?

2. Introduction and objectives

2.1 Research objectives

The aim of this research is to better understand what role app stores play in children in the United Kingdom encountering content harmful to children by means of regulated apps which app stores make available. It will be used to inform a statutory report that Ofcom is required to produce about the use of app stores by children.

In addressing this objective, this research is divided into two phases:

- Phase 1 examines the role of app stores in children encountering content harmful to children by means of the regulated apps they make available
- Phase 2 contextualises app stores within the broader digital ecosystem by:
 - Mapping different types of actors involved in children accessing regulated services and describing the roles they play;
 - Mapping the relevant stages of the child user journey to regulated services⁷ including key decision points and access routes;
 - Mapping the role of app stores within those journeys, as well as alternative routes to access regulated services;
 - Covering signals and backend processes shaping access to regulated services

2.2 Market context

There is a wide range of app stores available in the UK that enable users to find and access apps on a similarly wide range of devices. These include first-party app stores (e.g. owned by Apple, Google, Microsoft, Amazon)⁸, gaming stores (e.g. console stores and other stores that distribute PC games), third-party alternative app stores (e.g. Aptoide on Android) amongst a range of others, including more niche cases like APK downloads⁹ (e.g. Uptodown Market). Collectively these app stores enable access to a range of apps on mobile, tablet, PC, laptop, gaming console, smart TV, connected TV, and a range of extended reality devices. See section '4. Prioritisation of app stores for review' for more details. Generally, the variety of apps available in these stores is expansive, spanning gaming, social networking, user-to-user communication, fitness, and more.

The largest of these app stores are used widely by the UK population and, where data is available, there are indications that at least some of these stores are widely used by children too. It is also common that these app stores provide access to regulated apps, e.g. apps containing user-to-user or search content, which means that children using the app stores may be able to gain access to regulated apps. See section '4. Prioritisation of app stores for review' for more details on app store usage and availability of regulated apps.

Beyond app stores, there are a range of different actors that may play a role in child users in the UK accessing regulated services. This includes, but is not limited to, sideloading (e.g.

⁷ This includes where these services are available through apps, websites and any other digital services.

⁸ This is an app store that comes pre-installed with a device's operating system, e.g. Apple App Store with iOS and Google Play with Android.

⁹ Third-party download platforms and websites allow users to directly download Android Package Kits (APKs) - file packages used by the Android operating system to install apps.

direct publisher download, file-sharing services), web browsers, and cloud gaming services. See section '7. App stores in context' for more details.

2.3 Overview of this report

The remainder of this report includes:

- **Section 3. Methodology:** Outlining the methodology used across both phases of the research. This includes the approach taken in Phase 1 to identify, prioritise and conduct an in-depth review of app stores accessible to child users in the UK, and the approach taken in Phase 2 to map the broader digital ecosystem, the actors involved and the roles they play. It also includes the sources used, and the limitations of the research.
- **Section 4. Prioritisation of app stores for review:** Outlining the different types of app stores available and our rationale for selecting twelve app stores for in-depth review.
- **Section 5. Review of app store measures to protect children from content harmful to children:** Providing an overview of the app store measures, examining where and how these measures are deployed by different app stores, and finally categorising the app stores into archetypes based on the combination of measures they use.
- **Section 6. Digital ecosystem overview:** Mapping the different types of actors involved in child users accessing regulated services and describing the role they play.
- **Section 7. App stores in context:** Identifying the relevant stages of the child user journey to regulated services and the different ways that child users may access these regulated services, and a deeper exploration of the different actor types in the child user journey, exploring their role and how things vary based on different types of actor being involved, e.g. first-party versus third-party.
- **Section 8. Conclusions:** Summarising our observations on app stores and the broader digital ecosystem and outlining considerations for Ofcom.

3. Methodology

This section sets out the methodology used across the two phases of the research. Phase 1 focused on identifying, prioritising and reviewing a subset of app stores available to child users in the UK. Phase 2 built on this work to map the wider digital ecosystem through which child users may access regulated services, including the actors involved and the roles they play.

3.1 Phase 1 Methodology: App store review

Phase 1 focused on identifying, prioritising, and reviewing a subset of app stores available to child users in the UK. This phase consisted of four main steps:

1. A taxonomy and prioritisation of app stores.
2. A deep dive into the features and policies for each prioritised app store.
3. User journey testing of the app store experience across different age groups of children
4. An analysis of the app stores' metadata practices and any key differences between them.

Taxonomy and prioritisation of app stores

We identified an initial long list of app stores based on a range of existing Ofcom research, including Ofcom's Passive Online Measurement (2025)¹⁰ and Online Nation (2024, 2025)¹¹, and third-party sources such as TechCrunch and Business of Apps among others. This longlist was then prioritised to twelve app stores selected for further research and user journey testing (see section '4. Prioritisation of app stores for review' for more details).

Feature and policy deep dive

We then conducted an in-depth review of the twelve shortlisted app stores, assessing protective measures across user-facing features, relevant app store policies and the processes used to publish, review and moderate apps. This analysis drew primarily on information published by the app stores themselves including app store guides and policy documents, as well as navigating through the app store user interface.

User journey testing

We then tested how protective features operate in practice across the prioritised app stores. User testing was conducted in MTM's test lab using a range of new or factory-reset devices, including mobile phones, PCs, consoles, and tablets. For each store, we created new user accounts registered to pseudonyms, using new email addresses and (where required) new mobile phone numbers (see Appendix 'A2. Further Details on Methodology' for details).

All devices ran the latest available version of their OS at the time of testing (see Appendix 'A2. Further Details on Methodology' for details). Where device set-up required a user's age

¹⁰ '[Children's Passive Online Measurement](#)', Ofcom (June 2025).

¹¹ '[Online Nation Report 2025](#)', Ofcom (December 2025); '[Online Nation Report 2024](#)', Ofcom (November 2025).

(e.g. when configuring a new phone), the device was factory reset before testing each new user profile. All testing was conducted in the UK.

To capture differences by age, we tested up to five age groups per app store: ages 5, 12, 14, 16 and 18. This allowed us to understand differences in user journeys across significant milestones, namely child users aged under 13, child users aged 13-17 and adult (18+) accounts. This also allowed us to understand differences within the under-13 group (selecting 5 and 12 to represent the lower and upper end of this) and within the 13-17 group (selecting 14 and 16). We also tested a sixth “guest” journey in app stores to see how far users could get through the user journey without signing in.

We followed a consistent approach across app stores, structuring the user journey around a set of core user actions:

1. Account creation: creating a new account based on user age; leaving parental controls on the default settings applied by the app store; recording which restrictions were available by age group.
2. Browsing the apps homepage: scrolling through the designated homepage and recording recommended apps. For app stores without a homepage dedicated to apps, testing focused on the games homepage instead.
3. Browsing the games homepage: scrolling through the designated homepage and recording recommended games. For app stores without a homepage dedicated to games, testing focused on the apps homepage instead.
4. Downloading an app or game: searching for a designated app or game (see below), attempting to download and doing so where possible (without accessing the app), recording any restrictions.
5. Investigating how to report an app or game: examining what reporting options were available in the app store for content harmful to children (NB: no reports were filed during user journey testing).
6. Investigating how to circumvent age restrictions: testing whether users could change date-of-birth settings and override a parental Personal Identification Number (PIN) (if a PIN was required). Our testing recorded whether app stores offered a reset option after incorrect PIN entries, but we did not attempt to bypass PIN controls or reset the PIN.

Apps were selected for user journey testing based on their availability on the app store, their popularity, the availability of user-to-user functionalities and an age rating of 18+ (see Appendix ‘A2. Further Details on Methodology’ for details on rationale).¹² The following apps were selected for download on each app store:

¹² Throughout this report, the terms ‘app’ and ‘game’ are used interchangeably when referencing platforms that host gaming content exclusively, such as the PlayStation Store or Xbox Store

Exhibit 3: Apps and games selected for user journey testing

App store	App or game selected for user journey
Apple App Store	Tinder (17+) ¹³
Google Play	Tinder (18+)
Samsung Galaxy Store	Tinder (18+)
PlayStation Store	Call of Duty: Warzone (2022 release) (18+)
Xbox Store	Call of Duty: Warzone (2022 release) (18+)
Nintendo eShop	Warframe (18+)
Microsoft Store	Reddit (18+ on Microsoft)
Amazon Appstore	Sexy Girls (Adult)
Steam	Call of Duty: Warzone (2022 release) (18+)
Epic Games Store	Warframe (18+)
Uptodown Market	Dating for Android (18+)
Aptoide	Kik (18+)

Findings from the user journey testing were recorded and are referenced throughout this report.

Several precautionary measures were taken during user testing to protect personal data and users' privacy:

- No real names were used for account creation (pseudonyms only)
- No personal data was captured in app store screenshots
- No interaction occurred with real users in any app store
- No user-generated content was viewed
- No content was created within app stores (e.g. app reviews or issue reports)

Metadata analysis

As an extension of the user journey testing, MTM also compared how app stores labelled and described apps by reviewing the age ratings and content warnings applied to the same apps across different app stores.

Eight apps were selected for the metadata analysis, based on different factors:

- Availability across app stores
- Type of app or game (e.g. social media, game, video platform)
- Age-rating of the app or game
- User-to-user and / or search capabilities within the app
- Popularity with children in the UK

¹³ User testing was completed in December 2025, while Apple was rolling out an updated age-rating system. At that time, Apple's highest age rating was 17+. The new system has since launched in the UK (as of 22/02/2026), where the highest rating is now 18+. As of February 2026, Tinder is rated 18+ on the UK Apple App Store. <https://developer.apple.com/news/?id=ks775ehf> [Accessed on 22/02/2026]

Based on these criteria, the following apps were selected: YouTube, Roblox, TikTok, Hinge, Grand Theft Auto V, Apex Legends, Google Search and Bing.

Together, these objectives and methods provided the framework for assessing how app stores may contribute to children's potential exposure to regulated apps where they may encounter content harmful to children and the extent to which age checks and protective measures were applied in practice.

3.2 Phase 2 Methodology: App stores in the context of the wider digital ecosystem review

Phase 2 focused on mapping the broader digital ecosystem through which child users may access regulated services, the different types of actors involved, and the roles they play. This phase consisted of two main steps:

1. Mapping the digital ecosystem
2. A deep dive into different actors involved in child users accessing regulated services

Mapping the digital ecosystem

We identified an initial list of the different actors involved in child users accessing regulated services based on a range of sources including the taxonomy research and user journey testing conducted during the Phase 1 research (see 'Sources' for more details). We then selected a core set of actors to map the digital ecosystem, aiming to achieve a balanced selection of actor types across OSs, regulated services, and user experiences. Here, "different user experiences" refers to variation in the parental controls offered, methods of age assurance, sign-on options, and approaches to moderating the games and apps offered by each actor.

We then mapped this digital ecosystem, which included considering the different ways that users could access regulated services and which types of actors would be involved. We then examined the role these different types of actors may play at a high level, identifying example functions, child safety measures and technical roles.

Deep dive into different actors involved in child users accessing regulated services

We examined the different routes to access regulated services via the shortlisted set of key actors and explored these actors in more depth. We considered a high-level child user journey from device to regulated service for each actor. We then investigated each actor's role in more depth and how this may have varied across different types of gateways (e.g. 1P versus 3P).

Sources

Much of the Phase 2 research draws on evidence gathered during Phase 1, including the taxonomy and prioritisation of app stores and the user journey testing. In Phase 1, the

taxonomy and prioritisation work identified a long list of app stores and highlighted several ways in which child users may access regulated apps. The user journey testing also helped identify relevant child-safety roles and the protective measures exercised by each actor.

The key sources for Phase 2 research include:

- The taxonomy and prioritisation of app stores conducted in Phase 1, drawing on Ofcom's Passive Online Measurement (2025)¹⁴ and Online Nation (2024, 2025)¹⁵, and third-party sources (e.g. TechCrunch and Business of Apps)
- The user journey testing conducted in Phase 1
- Policy documentation and user guides from relevant companies in the digital ecosystem
- Publications from regulatory bodies (e.g. the CMA and Ofcom)
- Trade press covering the technology sector (e.g. TechCrunch)

3.3 Limitations of this research

The findings in this report are subject to several limitations based on the scope and approach of the research. These include:

- The research was not intended to be exhaustive and instead focused on a defined subset of the market and ecosystem, including twelve app stores which were available in the UK in the Phase 1 research and a limited set of typical or notable actors in the Phase 2 research.
- Research relied in part on publicly available information, including policy documents, user guidance, and other published materials. This may mean that some features, internal processes, or policy details were not captured where they were not publicly disclosed.
- The user journey testing was designed to cover a set of likely actions or the representative user journey a child may take in the app store (e.g. browsing the app store home page, searching for an app, accessing the app store listing, and attempting to download the app), but did not cover all possible actions or every protective feature that app stores offered.
- This research represents a snapshot in time. Policy research was conducted between 1 November 2025 and 1 January 2026. User journey testing was conducted between 15 December 2025 and 15 January 2026. We then conducted research into the broader digital ecosystem in February and March 2026. Consequently, these findings may not reflect subsequent updates to features or policy guidelines that occurred after these periods.

¹⁴ [‘Children’s Passive Online Measurement’](#), Ofcom (June 2025).

¹⁵ [‘Online Nation Report 2025’](#), Ofcom (December 2025); [‘Online Nation Report 2024’](#), Ofcom (November 2025).

4. Prioritisation of app stores for review

This section outlines the different types of app store available and our rationale for selecting the twelve app stores for in-depth review.

4.1 Identifying a long list of app stores

Initial research identified a long list of 82 app stores across the app store types described below (see *Exhibit 4: Taxonomy of app stores*). The long list was built by mapping the most widely used device manufacturers and OSs, then supplementing this with additional app stores referenced in industry trade press. To support analysis and prioritisation, we grouped app stores using a set of attributes with categories including:

- Ownership structure (e.g. manufacturer-owned, publisher-owned, alternative app store)
- Device distribution (e.g. TV-only app stores)
- Type of apps available (e.g. gaming stores)
- Geographic restrictions (e.g. region-limited availability)
- Store environment (e.g. in-app marketplaces, browser extension stores)
- File type and distribution model (e.g. APK downloads, Linux package repositories)

The full taxonomy of app stores includes:

Exhibit 4: Taxonomy of app stores

Type of app store	Details	Examples
First-party (1P) app stores	Owned and operated by major OSs, e.g. iOS, Android, Windows.	Apple App Store, Google Play Store, Windows Store, Amazon Appstore, Samsung Galaxy Store
Gaming stores	Console stores (e.g. for PlayStation, Xbox and Nintendo devices) and 1P app stores that users install on devices that primarily distribute games.	PlayStation, Xbox, Nintendo eShop, Steam, Epic Games Store
Third-party (3P) app stores	3P app stores that are pre-installed on devices or installed by users as alternatives to major 1P stores, e.g. iOS-alternative and Android alternative stores.	Aptoide
Geo-locked stores	1P or 3P app stores that are geo-locked and not accessible by UK users.	ONEstore, V-Appstore (VIVO)
TV app store	App stores installed on Smart TVs or accessed through TV sticks on connected TVs.	Samsung Apps Store, LG Content Store, Roku Channel Store
Publisher owned app store	Owned and operated by major publishers, typically publishing 1P titles.	EA App, GOG, Ubisoft Connect, Battle.net

In-app marketplace	Add-ons or extensions that only work inside a host app.	Slack App Directory, Zoom Marketplace, Discord, Roblox, Fortnite
Wearable devices app store	Stores for apps on wearable devices.	Garmin Connect IQ Store
Browser extension app store	Add-ons or extensions that only operate within the browser.	Chrome Web Store, Firefox Add-ons
APK downloads & open-source repositories	Direct download software distribution platforms.	Uptodown Market, APKMirror, Fossdroid, Aurora
Linux and Windows app store	Platforms for distributing Linux or Windows only software.	Flathub, Snap Store, Ninite

4.2 Prioritising app stores for a shortlist

We assessed each app store and collected data points where possible against the following indicators based on publicly available information¹⁶:

Availability of regulated apps	Access and Usage	Governance and Protections
Distributes apps with regulated content: - User-to-user - Search - Adult or Pornographic content	- Child reach or usage (as priority, where available) - UK adult reach or usage (as proxy) - Global reach or usage (as proxy where UK data is lacking)	- Parental controls - Use of an age check - Account required to access content - Billing relationship, e.g. the option to pay for services - Developer checks

We then applied ratings of high, medium, and low to access and usage data, according to the following parameters:

Measure	UK child reach or usage	UK adult reach or usage	Global reach or usage
Audience reach (#)	- High: 500k+ - Medium: 100-500k - Low: <100k	- High: 5m+ - Medium: 1m-5m - Low: <1m	- High: 300m+ - Medium: 100-300 - Low: <100m
Audience reach (%)	- High: 10%+ - Medium: 2-10% - Low: <2%	- High: 10% - Medium: 2-10% - Low: <2%	Not used

¹⁶ [‘Children’s Passive Online Measurement’](#), Ofcom (June 2025). [‘Online Nation Report 2025’](#), Ofcom (December 2025); [‘Online Nation Report 2024’](#), Ofcom (November 2025).

Following the initial taxonomy and assessment, app stores were deprioritised in Phase 1 if they lacked access to regulated apps or met any of the criteria below:

- Geo-locked app stores: Not accessible by UK users without a workaround.
- In-app marketplace: Low relevance to regulated apps and workplace-focused audiences.
- Publisher-owned app stores: Mostly 1P catalogues featuring their own titles, with limited or no 3P ecosystem.
- TV app store: Limited role for regulated apps (often YouTube or Twitch, and often pre-installed). TV user-experience, which is generally a passive, lean-back mode of consumption, likely reduces children's use of interactive features versus a mobile or tablet.
- Browser extension stores: Limited evidence of usage and scale.
- Linux and Windows app store: Low reach (Linux has a small share of users; Windows is a more niche product). Likely limited child relevance.

We prioritised twelve app stores for in-depth review based on 'Access & Usage', focusing on the app stores that were most likely to be accessed by children in the UK. In addition, two less popular app stores, Aptoide and Uptodown Market, were selected to cover a wider range of app store types which provide access to regulated apps.

Exhibit 5: App stores selected for in-depth review

Name	Access & Usage (H/M/L)	Access to Regulated Apps
Apple App Store	High	Yes
Google Play	High	Yes
Samsung Galaxy Store	High	Yes
PlayStation Store	High	Yes
Xbox Store	High	Yes
Nintendo eShop	High	Yes
Microsoft Store	High	Yes
Amazon Appstore	Medium	Yes
Steam	Medium	Yes
Epic Games Store	Medium	Yes
Aptoide	Low	Yes
Uptodown Market	Low	Yes

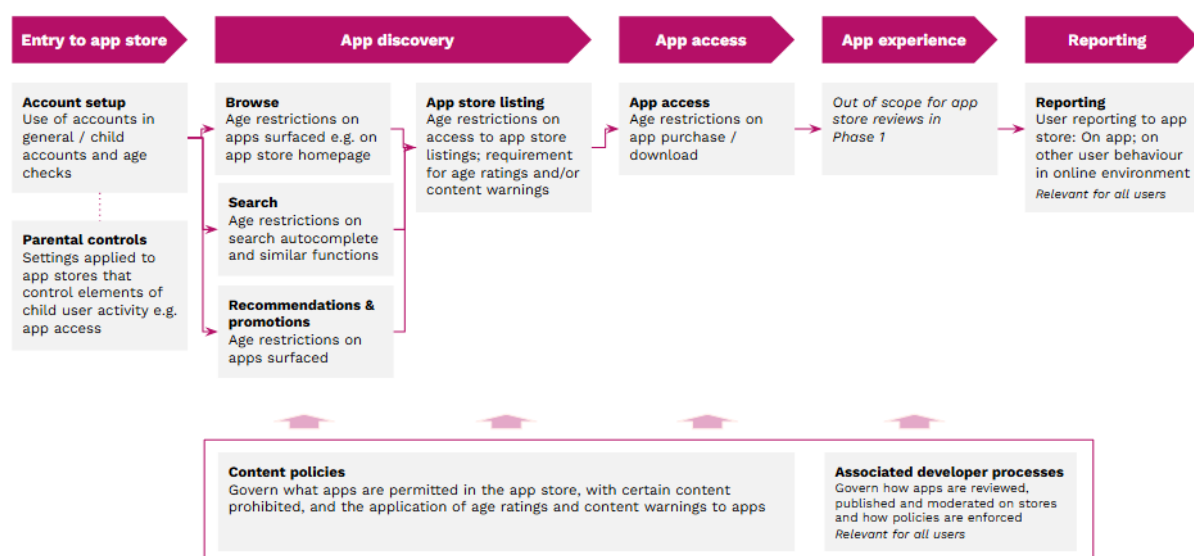
5. Review of app store measures to protect children from content harmful to children

This section provides an overview of the different protective measures implemented by the app stores we reviewed to protect children from harmful content, looking at where and how they were deployed by the different app stores. We provide an overall analysis of these app stores, categorising them into archetypes based on the combination of measures they have implemented.

5.1 Overview of app store measures

We found that the app stores reviewed used a range of measures to protect children from accessing regulated apps where they may have encountered content harmful to children, with the combination of measures used and how they were deployed in practice varying by app store. These included dedicated child accounts and age check measures; parental controls which may have, or may not have, been on by default; age-based restrictions on app discovery, access and tailored experiences within apps; mechanisms for reporting issues with apps; and a set of supporting content and developer policies and processes that governed how apps were received, published and moderated on the app stores.

Exhibit 6: Measures used across app stores to protect children, mapped against the user journey



These measures had the potential to protect children by either restricting access to regulated apps where they may have encountered content harmful to children, reducing the likelihood of them discovering these regulated apps, or in the case of reporting mechanisms, taking apps off the store.

5.2 Content policies including age ratings

Overview

App store content policies govern which apps are permitted in the app store, with certain types of content being prohibited for all users. They also govern what information is provided to users about apps, including age-ratings and content warnings. Generally, these policies are integrated into the app store's broader 'Developer Terms of Service'. They often mandate specific protective measures, such as age ratings, which then facilitate the enforcement of age-based restrictions during app discovery and access.

How this works

Most app stores state that they prohibit certain harmful content entirely in their ToS, including content harmful to children. As an illustrative example:

Exhibit 7: Illustrative examples of content prohibited by app stores for all users

Example App Store	Content prohibited for all users includes: ¹⁷
Google Play	Sexual content & profanity; hate speech; violence; violent extremism; sensitive events; bullying and harassment; dangerous products (e.g. sale of explosives, firearms); marijuana (e.g. sale of marijuana); tobacco and alcohol (e.g. sale of tobacco or nicotine products). ¹⁸
Xbox Store	Risk of harm; defamatory, libelous, slanderous and threatening; offensive content; alcohol, tobacco, weapons and drugs; adult content; illegal activity; excessive profanity and inappropriate content. ¹⁹
Amazon Appstore	Sexually explicit content; regionally restricted content; user-generated content without adequate user safeguards; hateful or harassing content; inaccurate or misleading medical content; alcohol and tobacco (including e-cigarettes); real-money gambling, gaming and competitions; bitcoins & other crypto-currencies; sensitive events; illegal & harmful content; violence; terrorism & violent extremism. ²⁰

In addition to these content policies, all the app stores reviewed had an age rating system for apps. Most used the PEGI rating system²¹ for the UK, but a few had their own systems, for example, Apple App Store, Samsung Galaxy Store, Amazon Appstore, and Steam. These systems assigned age ratings based on certain types of content (e.g. violence) and features (e.g. messaging) within the app.

¹⁷ Developer terms of service presented in table were captured on 16/02/2026.

¹⁸ <https://support.google.com/googleplay/android-developer/answer/16944162?hl=en>. [Accessed on 17/03/2026]

¹⁹ <https://learn.microsoft.com/en-us/windows/apps/publish/store-policies#111-general-content-requirements>. [Accessed on 17/03/2026]

²⁰ <https://developer.amazon.com/docs/policy-center/restricted-content.html> [Accessed on 17/03/2026]

²¹ PEGI (Pan European Game Information) system used to give apps and games age ratings <https://pegi.info/>.

Exhibit 8: Rating system for each app store reviewed

App store(s)	Rating system	Age bands	Types of content
Google Play PlayStation Store Nintendo eShop Xbox Store Microsoft Store Epic Games Store ²² Aptoide Uptodown Market ²³	PEGI	PEGI 3 PEGI 7 PEGI 12 PEGI 16 PEGI 18 Parental guidance recommended	Content: discrimination, drugs, fear, horror, bad language, sex, violence Features: in-game purchases, gambling, advertising, messaging, user interaction, user generated content, location sharing
Apple App Store ²⁴	Store's own rating system	4+ 9+ 13+ 16+ 18+	Content: profanity, references to alcohol or tobacco or drug use, sexual content, gambling, realistic violence, medical or treatment focused content Features: unrestricted web access, user-generated content, loot boxes, simulated gambling
Samsung Galaxy Store	Store's own rating system	All ages 4+ 12+ 16+ 18+	Content: sex, violence, horror & fear, bad language, tobacco & alcohol Features: gambling without real cash or currency
Amazon Appstore	Store's own rating system	All ages Guidance suggested Mature Adult	Content: violence, drugs, nudity, sex, intolerance, profanity, simulated gambling Features: account creation, personal information collected, advertisements, gambling, location detection or location-based services, user generated content, user to user communication
Steam	Store's own rating system	Not rated Mature content Adult content	Content: sexual themes, nudity, strong language
	Also allows developers to include PEGI rating on Store listing	PEGI 3 PEGI 7 PEGI 12 PEGI 16 PEGI 18 Parental guidance recommended	Content: violence, sex

²² Epic Games Store does not publish public documentation requiring non-Fortnite games to use the PEGI rating system; however, all titles reviewed on the Epic Games Store displayed PEGI ratings.

²³ Uptodown Market's documentation states that a PEGI age rating is optional.
<https://support.uptodown.com/hc/en-us/articles/360053260491-How-to-publish-an-app-on-Uptodown>
[Accessed 26/01/2026].

²⁴ Apple updated its age rating system for apps and games in July 2025 to provide more granular age ratings.
<https://developer.apple.com/news/?id=ks775ehf> [Accessed 26/01/2026].

The app stores all displayed age ratings on app store listings and most also displayed warnings for certain types of content and features within apps. Based on user journey testing, exceptions to this included Samsung Galaxy Store, Amazon Appstore, Aptoide and Uptodown Market, which showed age ratings but did not show content or feature warnings.

There was some inconsistency in how apps were rated across app stores, based on reviewing the metadata of a sample of apps. This included the use of Parental Guidance and similar warnings versus specific age ratings, or significant differences in the age ratings for certain apps across app stores.

Exhibit 9: Consistency of app ratings across app stores reviewed

App	Age ratings across app stores	Differences in age ratings
YouTube	• Parental Guidance (Google Play, Xbox Store, Nintendo eShop) • 13+ (Apple App Store) • 12+ (Uptodown Market) • 3+ (Aptoide)	YouTube, TikTok & Roblox: • Parental Guidance used in some cases, flagging a variety of user-generated content or curated content, versus age ratings in others; • Lower age ratings by Aptoide and Uptodown Market
TikTok	• Parental Guidance (Google Play, Microsoft Store, Amazon Appstore) • 13+ (Apple App Store) • 12+ (Samsung Galaxy Store) • 3+ (Uptodown Market, Aptoide)	
Roblox	• Parental Guidance (Google Play, PlayStation Store, Xbox Store, Microsoft Store, Amazon Appstore) • 13+ (Apple App Store) • 12+ (Samsung Galaxy Store, Uptodown Market) • 3+ (Aptoide)	
Hinge	• 18+ (Apple App Store, Google Play Store) • 16+ (Uptodown Market)	• Lower age rating by Uptodown Market
Grand Theft Auto V	• 18+ (PlayStation Store, Xbox Store, Microsoft Store, Steam, Epic Games Store) • Guidance Suggested (Amazon Appstore)	• Generally rated 18+, versus 'Guidance Suggested' for Amazon Appstore
Apex Legends	• 16+ (PlayStation Store, Xbox Store, Nintendo eShop, Epic Games Store) • Parental Guidance (Steam) • 12+ (Uptodown Market)	• Generally given age ratings versus 'Parental Guidance' by Steam; • Lower age rating by Uptodown Market
Google Search	• 16+ (Apple App Store) • 3+ (Google Play, Uptodown Market)	Google Search & Bing: • Higher age rating by Apple

Bing	• 16+ (Apple App Store) • 3+ (Google Play, Microsoft Store, Uptodown Market, Aptoide)	versus other app stores
------	--	-------------------------

There was also inconsistency in the content warnings provided alongside age ratings. Taking Roblox, Grand Theft Auto V and Google Search as examples, not all content warnings were flagged by every app store:

Exhibit 10: Content warnings given for selected apps and games

Example App or Game	What content warnings were given ²⁵ and by how many of the app stores reviewed ²⁶
Roblox	Violence (1 out of 5 stores), Weapons (1/5), Fear (1/5), Gambling (5/5), Advertising (2/5), Messaging (1/5), User Generated Content (1/5), Users Interact (4/5)
Grand Theft Auto V	Violence (5 out of 5 stores), Bad Language (5/5), Gambling (3/5), In-app Purchases (4/5), Online Gameplay
Google Search	Contains Advertising (1 out of 2 stores), Unrestricted Web Access (2/2), In-app Purchases (1/2)

Related to these content policies, most app stores also had advertising policies which put age restrictions on advertising within apps (including Apple App Store, Google Play, Samsung Galaxy Store, Xbox Store, Microsoft Store and Amazon Appstore²⁷). This generally involved requiring developers to ensure ads were appropriate for the app's age rating.

Protection offered and limitations

Content policies and associated developer processes are designed to mitigate children's exposure to certain harmful content that is prohibited in apps, e.g. explicit sexual content, extreme violence, or hate speech. Age ratings may also enable various age restrictions used by app stores. These are used, along with content warnings on app store listings, to help users better understand the nature of content within apps.

There may be limitations to how effective these protections are, however, based on inconsistencies in how age ratings and content warnings are applied in practice:

- An inconsistency in age ratings across app stores could reduce users' understanding of the nature of content within apps;
- An inconsistency in applying content warnings and omitting them entirely in some cases implies a risk that users are less well informed about the nature of content within apps and may not be aware of content that is harmful to children

²⁵ The exact wording of the warning may vary for some app stores.

²⁶ Figures in brackets show how many app stores gave this warning / the total number of app stores where the app was reviewed.

²⁷ For other stores reviewed the policy is either not clear based on publicly available information (PlayStation Store, Nintendo eShop, Aptoide) or not relevant because the app store does not support in-game ads (Steam).

5.3 Account setup

Overview

In general, the account setup process requests information about users including their age. This can then be used as the basis for applying protections for children according to their age throughout the rest of the user journey.

Relevant measures included accounts being required to access the store or to download apps, the availability of dedicated child accounts, the requirement for parents or guardians to set up these child accounts, and age assurance for adult accounts.

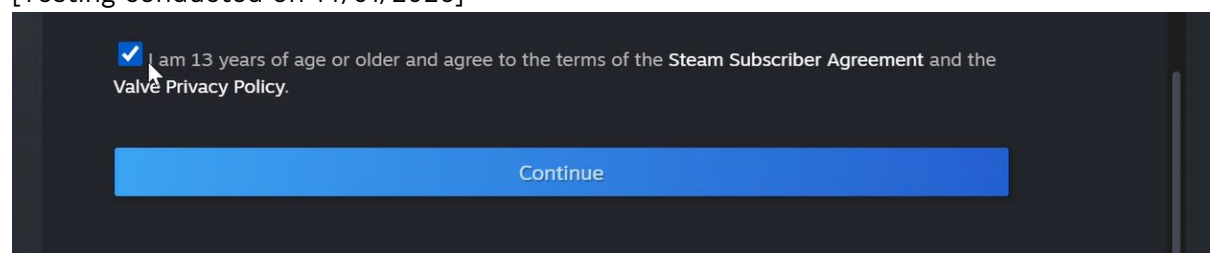
How this works

Most of the app stores reviewed required users to have accounts, except for Aptoide and Uptodown Market. Of these, some required an account to access the app store (e.g. Google Play, Xbox Store, Nintendo eShop, Samsung Galaxy Store, PlayStation Store and Amazon Appstore based on the devices used in user journey testing), while others let users explore the app store and only prompted them to create an account when attempting to purchase or download an app (e.g. Apple App Store, Microsoft Store, Steam, Epic Games Store).

In turn, most of the app stores reviewed offered dedicated child accounts which required a parent or guardian to set them up, generally capturing date of birth in the process. Variations on this include:

- Differentiating between child users aged under 13 and child users aged 13-17, such as not requiring a parent or guardian to set up accounts for users aged 13-17, e.g. Apple App Store, Google Play, and Epic Games Store;
- Only prompting to create a parent or guardian account when child users attempted to download 18+ rated apps, e.g. Xbox Store and Microsoft Store, where child users could ask for parent or guardian approval to download 18+ apps;
- Applying a minimum age for account creation, e.g. users had to be 13+ for Steam and Samsung Galaxy Store and 7+ for PlayStation Store;
- Not capturing date of birth, e.g. Steam only asked for confirmation via a tick-box that the user was over 13.

Exhibit 11: Steam, 13+ year-old user account signing up for an account
[Testing conducted on 14/01/2026]



For users who declared that they were over 18, most app stores relied on self-declaration of age. Where used, age assurance could be applied to the account setup process, when users accessed certain apps and content, or for a parent account setting up a supervised child account.

Only four of the reviewed app stores required a user to complete age assurance to determine whether they were an adult: the PlayStation Store, Google Play Store, Xbox Store and Steam. Epic Games relied on self-declaration when a user created an account, but did require a parent or guardian to complete age assurance when setting up a supervised “cabined” account for a child.

Exhibit 12: How different app stores deployed age assurance for 18+ accounts

App Store	Where age assurance is used	Method of age assurance
PlayStation Store	Required 18+ users to verify age during account setup.	Neutral age gate Facial age estimation, government issued ID, or mobile number. ²⁸
Google Play	Required users to verify age as 18+ when accessing 18+ apps for the first time. Also required parent or guardian to verify age when setting up child accounts for under 13s.	Neutral age gate Facial scan, government issued ID, or credit card (note: credit card only used when setting up child accounts).
Xbox Store	Required users to verify age as 18+ when attempting to access social features on Xbox (e.g. communicating with friends, accessing 3P services like Discord, etc). ²⁹	Neutral age gate For accessing social features: Facial age estimation, government issued ID, mobile number, or credit card.
Steam	Required users to verify as 18+ to access ‘mature content games’ or their associated community hubs on Steam. ³⁰	Accessing ‘mature’ category content required a credit card.
Epic Games Store	Required parent or guardian email for verified parental consent when setting up under 13 (“cabined”) accounts i.e. access to certain content and functionalities was disabled for such users (e.g. communicating with other players) until a parent or guardian provided consent. ³¹ Parents had to verify their age to provide consent for “cabined” accounts.	Neutral age gate Only for parents providing consent for “cabined” child accounts, not for child users: Facial age estimation, government issued ID, or credit card.

²⁸ This verification relies on the age information a mobile provider has on file for a user who is the owner of the phone contract.

²⁹ Xbox is still rolling out age verification as of 18/12/2025. <https://support.xbox.com/en-GB/help/family-online-safety/online-safety/UK-age-verification>; <https://www.theverge.com/news/714458/microsoft-xbox-age-verification-uk-social-features>. [Accessed on 26/01/2026].

³⁰ Steam Support, Age Assurance under the UK Online Safety Act. <https://help.steampowered.com/en/faqs/view/292B-3DA3-CFC8-97F6>. [Accessed on 26/01/2026].

³¹ <https://www.epicgames.com/site/en-US/cabinedaccounts>. [Accessed on 11/03/2026].

Protection offered and limitations

The combination of dedicated user accounts, including child accounts, and age signals for those accounts, provides the basis for applying age-based restrictions within the app store and within third-party services that receive age signals.

Another benefit of how age assurance during the account set up process typically works is that it can prompt parents or guardians to think about setting up a dedicated account for their child and applying parental controls.

There are several limitations in how these measures were deployed at account creation for children across the app stores reviewed:

- Account creation was not required (Aptoide, Uptodown Market);
- Reliance on self-declaration of age for children (Apple App Store, Nintendo eShop, Samsung Galaxy Store, Aptoide, Microsoft Store, Amazon Appstore, Steam, Xbox Store, Epic Games);
- App stores in general relied on a one-time setup of accounts, with limited age checks for children.

5.4 Parental controls

Overview

Parental controls are tools which enable parents or guardians to exercise control over the types of experiences children are having online, including by controlling the type of content they can access. Within app stores, these controls may include restricting the discovery, download, or purchase of apps for child accounts. In some cases, parental controls may extend beyond the store to manage broader device usage, e.g., screentime.

How this works

The app stores reviewed all had some form of parental controls, except for Uptodown Market. Generally, app stores integrated parental controls into the child account setup process (Google Play, Apple App Store, PlayStation Store, Xbox Store, Microsoft Store, Nintendo eShop), but the prominence of these controls varied by store.

Some app stores highlighted parental controls at the start of account set up (e.g. Google Play, PlayStation Store), while others required parents to configure them manually after an account has been created (e.g. Epic Games Store) with certain features restricted until consent had been provided. Additionally, the attention and input required from parents during the parental control set-up process varied. Some app stores toggled all parental controls on by default for a child account (e.g. Google Play), while others required parents to manually turn on each control (e.g. Nintendo eShop).

For example, after requiring users to enter their date of birth in account setup, Google Play immediately prompted under 13s to pass the device to a parent or guardian who could review and customise protective measures applied to the account. On the Epic Games Store, parental controls were configured independently of the initial account set up. While users under 13 could create their account and browse the store, parents had to complete the age assurance and parental control processes via a link sent to their email.

Exhibit 13: Google Play, 12-year-old user creating account and directed to pass device to parent

[Testing conducted on 19/12/2025]

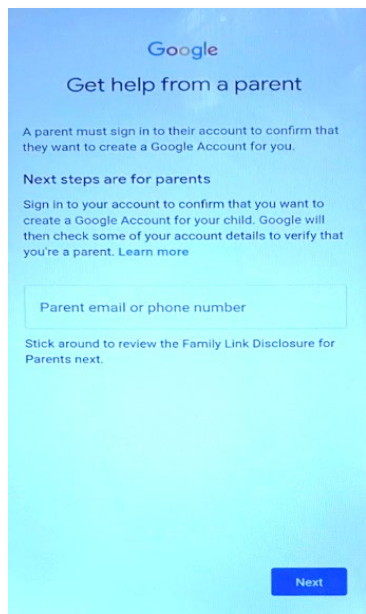
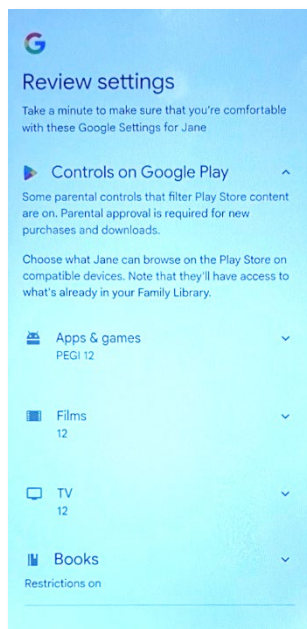


Exhibit 14: Google Play, parent reviewing parental controls for 12-year-old user account

[Testing conducted on 19/12/2025]



The parental controls observed during user testing could be applied at an account-level for children, except for Aptoide. In addition, some devices also had device level restrictions applying to all users on that device, for example:

- Nintendo eShop: Switch consoles had parental controls that applied to the device overall, separate to account-level controls operated via web or an accompanying app;
- Apple App Store: On setting up their device users were prompted to select an age category (under 13, teen aged 13-17, or adult 18+) before setting up or linking an

Apple ID. Protective features were initially enforced based on these age categories, e.g. Download controls based on app Store age ratings were set to the lowest age threshold within the given bracket.

- PlayStation Store: Parents or guardians could restrict all users from creating new, unrestricted user accounts or logging in as guests on a PS5, preventing children from circumventing parental controls.

Common parental controls included age-based restrictions on access to apps, to certain content & features within apps and the wider app store, and more general usage, e.g. screentime. An important note is that restrictions on content & features within apps may have been limited to 1P apps that were native to the app store.

Exhibit 15: Examples of app store controls

Apple App Store	A parent or guardian could restrict ability to purchase apps based on age ratings (on by default); limit who children could communicate with in apps (on by default); view activity and time spent on apps & websites (on by default); limit screentime (off by default); turn on screen distance reminders (off by default). These controls were only available for child users aged under 13.
Google Play	A parent or guardian could review and remove apps that were pre-installed on the device (e.g. Phone, Chrome, Galaxy Store) (on by default); restrict the age-rating of content in the Play store (on by default); limit screentime (off by default). These controls were only available for child users aged under 13.
Nintendo eShop	A parent or guardian could limit the sharing of account information (on by default); apply age-based restriction on purchases & downloads (off by default); restrict spending amount in the app store (off by default); restrict communication features (off by default); set limits on playtime (off by default).

Further details on age-based restrictions on access to apps are covered in sections ‘5.5. App Discovery’ and ‘5.6 App Access’ later in this report.

Focusing on age-based restrictions on access to apps, user journey testing showed that some app stores automatically applied these restrictions to child accounts during account setup, while others needed to be manually configured by parents or guardians.

Exhibit 16: Approach of app stores in applying age-based restrictions, based on ability to access 18+ app in user journey testing

Approach	Relevant app stores
Applied restrictions to child accounts automatically during account setup (to all child ages unless specified)	Google Play PlayStation Store Epic Games Store Xbox Store Microsoft Store Aptoide

	Amazon Appstore (for optional child accounts) Apple App Store (note in testing that child users aged 13-17 were able to access an 18+ app in practice) Samsung Galaxy Store (note the default restriction is self-declaration that a user is 18+ when trying to download an 18+ app or game).
Required parent or guardian to manually turn on restrictions	Nintendo eShop Steam

Protection offered and limitations

Parental controls manage various age-based restrictions offered by app stores which block access to, or reduce the likelihood of children discovering apps which may contain content harmful to children. They also give a degree of flexibility to parents or guardians in tailoring the specific experience of child users.

A potential limitation is that where parents or guardians are required to manually turn on restrictions, there was a risk that they would not realise this and did not apply controls that they otherwise may have wanted to be applied to child accounts.

5.5 App discovery

Overview

The app discovery journey covers the various ways that child users may discover apps, including browsing the app store (e.g. the homepage), searching for specific apps, seeing recommendations and promotions for apps in the app store, and the app store listing itself. Age restrictions may be used by app stores to restrict which apps are surfaced, e.g. not surfacing apps with an age rating higher than the account age.

The rest of this section is organised around the following stages of discovery:

- I. Browse
- II. Search
- III. Recommendations and promotions
- IV. App store listing

Browse: How this works

Under 'browse' we considered apps that were surfaced as users navigated through the app store, on the home page, on app category pages, 'most popular' sections etc. The user journey testing focused on apps surfaced specifically on the app store homepage and dedicated games and apps homepages where they exist.

Based on this user journey testing, most of the app stores did not appear to tailor the apps surfaced on these homepages based on age. This was judged on whether the app stores surfaced broadly the same set of apps or games to users of all ages or not.³²

Exhibit 17: App Store approach to tailoring apps surfaced to users, based on user journey testing

Approach	Relevant app stores
Tailored apps surfaced on homepage (and game and app homepages where available) by age	PlayStation Store, Apple App Store*, Amazon Appstore
Do not tailor apps surfaced by age	Microsoft Store, Samsung Galaxy Store, Nintendo eShop, Google Play, Epic Games Store, Xbox Store. Not applicable for Steam, Aptoide, Uptodown Market

*Of those that did tailor apps surfaced based on age, one still surfaced some apps with age ratings higher than the account age, raising questions about how and where age-based protective measures were applied.

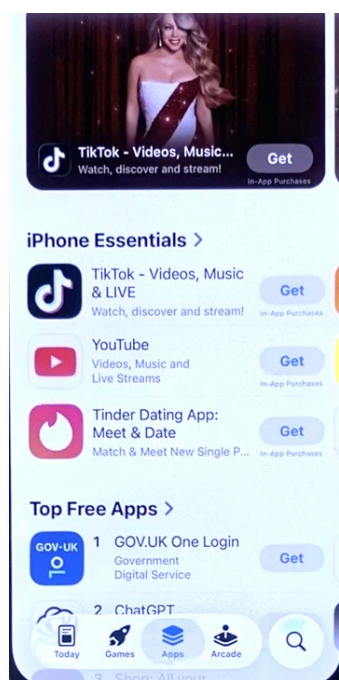
PlayStation Store adjusted the apps surfaced according to the user’s age, surfacing higher-rated games only as the user’s age increased. Child users did not encounter any games that were rated higher than their own age.

Apple App Store appeared to surface some apps to child accounts that were rated above their account age: ChatGPT (12+) surfaced for a 5-year-old user account, Call of Duty (17+) and Tinder (17+) surfaced for a 14-year-old user account, and Tinder (17+) surfaced for a 16-year-old user account despite appearing to tailor other apps.³³

³² The ±5-title threshold is applied only when user journeys were completed on the same day, and excludes any testing conducted on different days.

³³ User testing was completed in December 2025, while Apple was rolling out an updated age-rating system. At that time, Apple’s highest age rating was 17+. The new system has since launched in the UK (as of 22/02/2026), where the highest rating is now 18+. As of February 2026, Tinder is rated 18+ on the UK Apple App Store. <https://developer.apple.com/news/?id=ks775ehf>. [Accessed on 22/02/2026]

Exhibit 18: Apple App Store, 14-year-old user account exploring apps home page
 [Testing conducted 18-12-2025]



Of the app stores that did not appear to tailor apps by age, all surfaced apps with a higher age-rating than the child user's age, including 18+ rated apps.

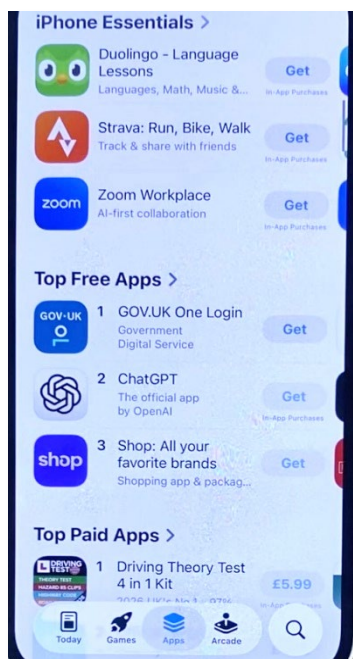
Exhibit 19: Approach to tailoring apps surfaced to users by age, based on user journey testing

Approach	Relevant app stores (with examples)
Prevented child user accounts from encountering apps with age ratings higher than the account age	Amazon Appstore (Kids Store), PlayStation Store
Child user accounts encountered apps with age ratings higher than the account age	Microsoft Store: Surfaced Call of Duty (PEGI 18) to 5-yr-old, 12-yr-old, 14-yr-old, and 16-yr-old accounts
	Epic Games Store: Surfaced Fortnite (PEGI 12), Resident Evil Requiem (PEGI 18), and Blood: Refreshed Supply (PEGI 18) to 5-yr-old, 12-yr-old, and 14-yr-old accounts
	Samsung Galaxy Store: Surfaced Bubble Cash (PEGI 18) to 14-yr-old and 16-yr-old accounts
	Steam: Surfaced Elden Ring (PEGI 18) and Fallout 4 (PEGI 18) to a 14+ account
	Xbox Store: Surfaced Roblox (PEGI 12) and Minecraft (PEGI 7) to 5-yr-old account

	Google Play ³⁴ : Surfaced Clash Royale (PEGI 7) and Solar Smash (PEGI 7) to 5-yr-old account
	Nintendo eShop: Surfaced System Shock (PEGI 18) to 16-yr-old account
	Aptoide: Surfaced Kiss of War (PEGI 16) to users with no account and signed in users
	Uptodown Market: Surfaced PUBG Mobile (PEGI 16) to users with no account and signed in users
	Apple App Store: Surfaced ChatGPT (12+) to 5-yr-old account

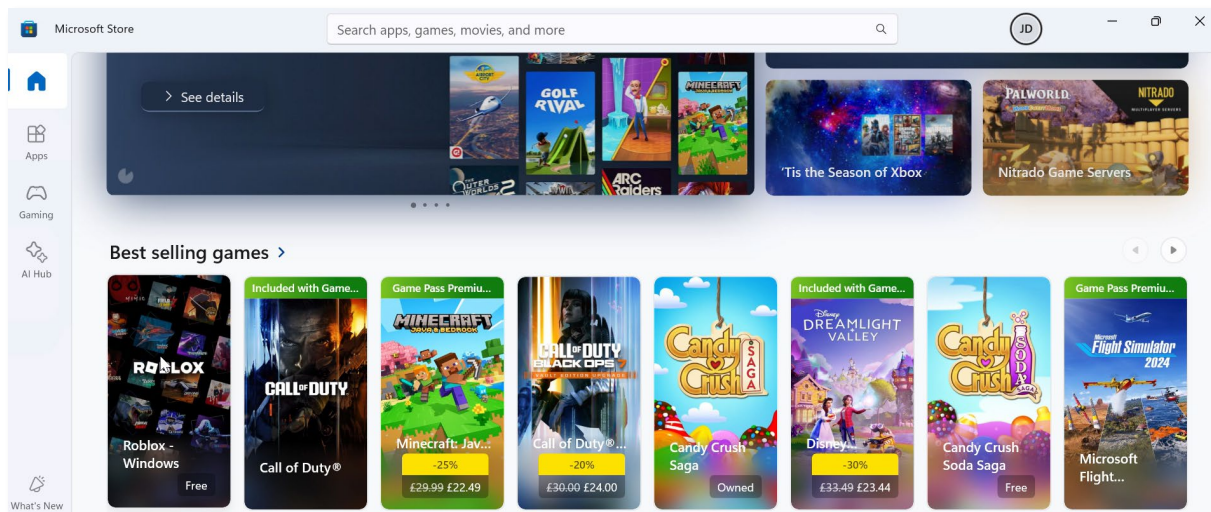
Exhibit 20: Apple App Store, 5-year-old user account exploring apps home page encountering ChatGPT (rated 12+)

[Testing conducted 18-12-2025]



³⁴ Google Play default restrictions were used during testing. Default restriction for 5-year-old was set to PEGI 12.

Exhibit 21: Microsoft store, 5-year-old user account exploring games home page encountering Call of Duty (PEGI 18)
[Testing conducted 18-12-2025]

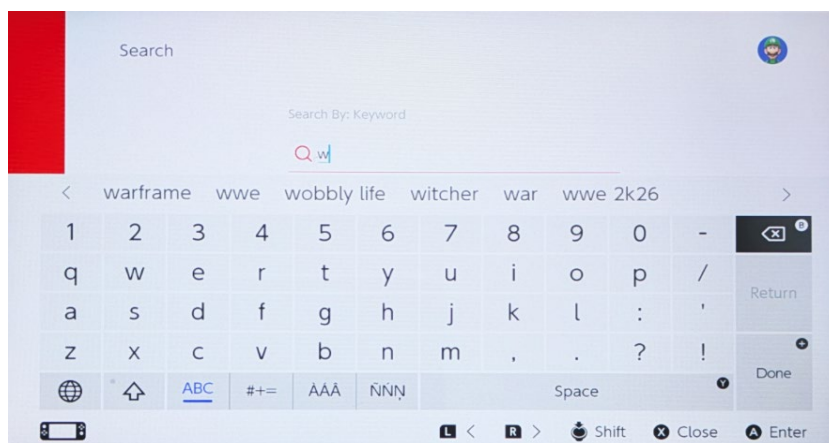


Search: How it works

The ‘search’ stage considered users looking for specific app titles on an app store’s search bar. In doing this, users typically encountered features like search suggestions or autocomplete based on a partially entered search term, search results, and related or promoted titles alongside these results. User journey testing looked at all of these as users searched for an 18+ rated app.

In testing, most of the app stores had a search autocomplete function that suggested the title of the 18+ app based on entering 1-2 letters i.e. they automatically surfaced apps that were rated higher than the user’s age (including Apple App Store, Nintendo eShop, Samsung Galaxy Store, Steam, PlayStation Store, Xbox Store, Microsoft Store, Epic Games Store, Aptoide and Uptodown Market).

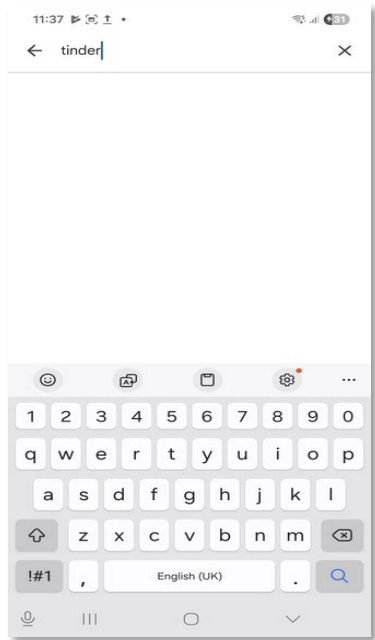
Exhibit 22: Nintendo eShop, 5-year-old user account searching “W”
[Testing conducted 17-12-2025]



Two app stores did appear to have protective measures for search:

- Google Play provided autocomplete search suggestions for Tinder to adult users but removed the feature for child users. Child users did not see any autocomplete suggestions while searching for apps in the Play Store.
- Amazon Appstore (Kids Store) recommended only age-appropriate apps in autocomplete suggestions for child users when they searched.

Exhibit 23: Google Play Store, 5-year-old user account searching for Tinder
[Testing conducted 18-12-2025]



In turn, most app stores allowed users to search for and find apps with an age rating higher than the account age, including 18+ rated apps. A few stores, however, did appear to have protective measures in place, including sharing warnings and not surfacing 18+ apps to child users.

Exhibit 24: Approach to restricting child users from accessing 18+ rated apps through search, based on user journey testing

Approach	Relevant app stores & apps
Prevented child user accounts from searching for an 18+ rated app	Google Play: Surfaced a warning message to child user accounts who searched for Tinder
	Amazon Appstore (Kids Store): Surfaced only age-appropriate apps in results for child user accounts
	Aptoide: By default, apps & games rated 18+ were not included in search results for any user
Allowed child user	Apple App Store: Tinder (17+) appeared for all users ³⁵

³⁵ User testing was completed in December 2025, while Apple was rolling out an updated age-rating system. At that time, Apple’s highest age rating was 17+. The new system has since launched in the UK (as of 22/02/2026), where the highest rating is now 18+. As of February 2026, Tinder is rated 18+ on the UK Apple App Store. <https://developer.apple.com/news/?id=ks775ehf>. [Accessed on 22/02/2026]

accounts to search for an 18+ rated app	Samsung Galaxy Store: Tinder (18+) appeared for all users
	Nintendo eShop: Warframe (18+) appeared for all users
	Steam: Warframe (18+) appeared for all users
	Epic Games Store: Warframe (18+) appeared for all users
	PlayStation Store: Call of Duty (18+) appeared for all users
	Xbox Store: Call of Duty (18+) appeared for all users
	Microsoft Store: Reddit (18+) appeared for all users
	Uptodown Market: Dating (18+) appeared for all users

Exhibit 25: Apple App Store, 12-year-old user account results for searching “Tinder”
[Testing conducted 18-12-2025]

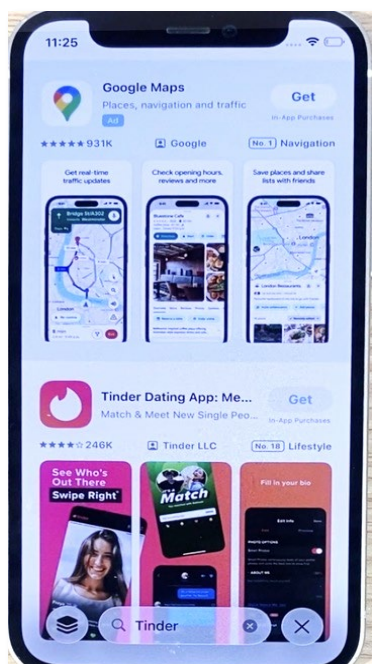
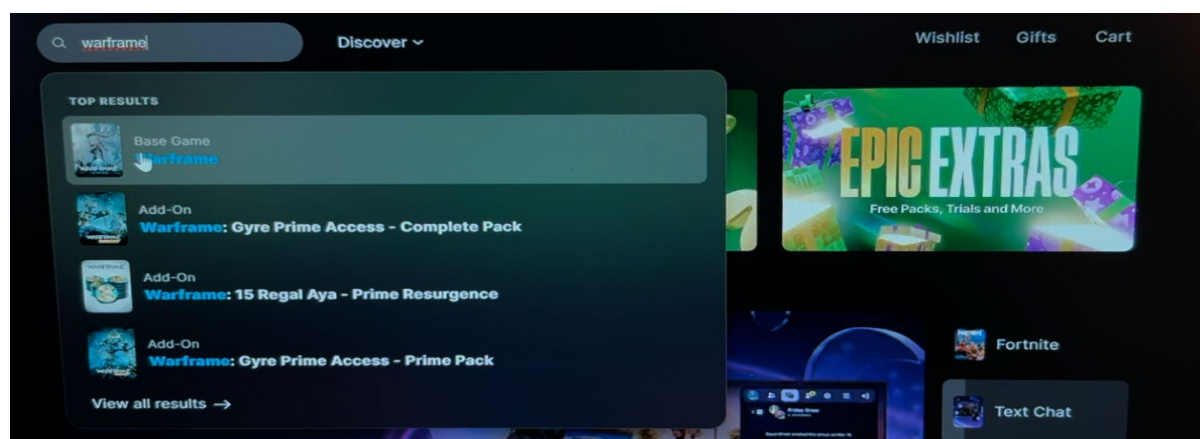


Exhibit 26: Epic Store, 14-year-old user account results for searching “Warframe”
[Testing conducted 18-12-2025]



Recommendations and promotions: How this works

Most of the app stores reviewed surfaced recommendations and promotions of apps at various places during a typical user journey, most commonly when browsing or searching for apps. User journey testing identified the following formats:

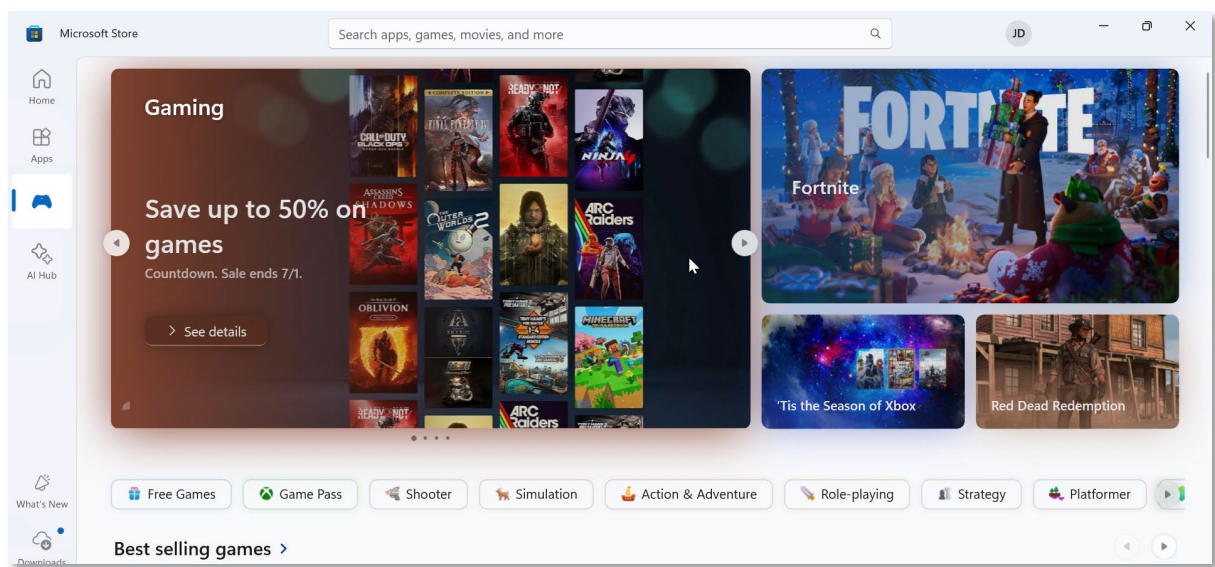
- Suggested apps surfaced during account set up
- Featured apps surfaced at the top of a page in an app store
- Sponsored apps surfaced while browsing
- Suggested apps surfaced against search results
- Suggested apps surfaced on app store listing

Of these, most app stores recommended or promoted apps with a higher age rating than the child’s age at some point in the journey i.e. Apple App Store, Google Play, Samsung Galaxy Store, Microsoft Store, Xbox Store, Steam, Nintendo eShop, Uptodown Market and Aptoide. For example:

- Apple App Store promoted Hinge (17+)³⁶ to a 16-year-old user account in search results
- Microsoft Store promoted Red Dead Redemption (PEGI 18) on games homepage to a 5-year-old user account

³⁶ Hinge rated 17+ on Apple App Store at time of testing [18-12-2025].

Exhibit 27: Microsoft Store, 5-year-old user account exploring games homepage [Testing conducted 19-12-2025]



A few app stores only recommended or promoted apps that were age appropriate. For example, PlayStation Store promoted the same, age appropriate featured games to children, but promoted different, PEGI 18 rated games to adults. Across the Amazon Appstore and the dedicated Kids Store, advertisements were age appropriate for both children and adults.

App Store listing: How this works

The final stage in the discovery journey is opening the app store listing, which provides information about the app including a description, sometimes a trailer, age rating and user reviews. The user journey testing looked at whether a child user could access app store listings for 18+ rated apps and reviewed whether age-ratings and warnings were included in app store listings in general.

Of the app stores reviewed, half did allow child users to access the app store listing for these 18+ apps i.e. Apple App Store, Samsung Galaxy Store, Nintendo eShop, Microsoft Store, Steam and Uptodown Market. The other app stores blocked child users from navigating to, or seeing the content, on the app store listings (see Exhibit 29: Google Play Store, 5-year-old user account attempting to access Tinder app store listing).

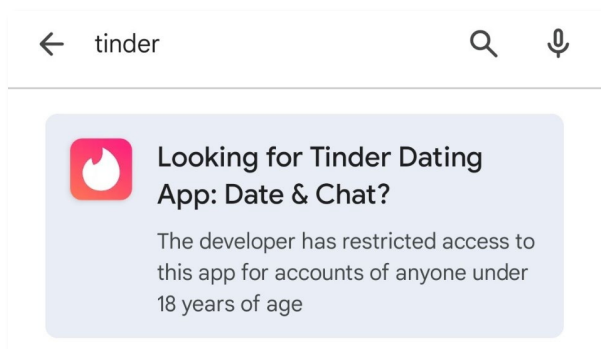
Exhibit 28: Approach to restricting access to app store listing, based on user journey testing

Approach to restricting access to app store listing	Relevant app stores
Allowed child user accounts to access an app store listing for apps with an age rating higher than the account age	Apple App Store: Child user accounts could view the description, screenshots & previews, and user reviews for Tinder (rated 17+).
	Samsung Galaxy Store: Child user accounts could view the description, screenshots & previews, and user reviews for

	Tinder (rated 18+).
	Nintendo eShop: Child user accounts could view the app store listing for Warframe (rated PEGI 18).
	Microsoft Store: Child user accounts could view the description and screenshots for Reddit (rated PEGI 18).
	Steam: Child user accounts aged 13+ could view the trailer, description, and in-game footage for Call of Duty: Warzone (rated PEGI 18).
	Uptodown Market: Child user accounts could view the description and screenshots for Dating (rated 18+).
Prevented child user accounts from accessing an app store listing for apps with an age rating higher than the account age	Google Play: Blocked child user accounts from accessing the app store listing for Tinder with a warning that the app was unavailable (rated PEGI 18).
	Amazon Appstore (Kids Store): Blocked child user accounts from finding Sexy Girls (rated Adult).
	PlayStation Store: Blocked child user accounts from accessing the Call of Duty (rated PEGI 18) with a warning “only adults can view this game”.
	Epic Games Store: Blocked child user accounts from accessing Warframe (rated PEGI 18) with a warning “Warframe may contain content not suitable for all ages. Sorry, you may not access this content.”
	Xbox Store: Blocked the Call of Duty (PEGI 18) tile for child user accounts browsing the app store and required parental permission to view the app store listing.
	Aptoide: Blocked users from finding Kik (rated PEGI 18) when adult content toggle was off by default.

Exhibit 29: Google Play Store, 5-year-old user account attempting to access Tinder store listing

[Testing conducted 18-12-2025]



All the app stores reviewed displayed age ratings on the app store listing. Most stores also displayed warnings for certain types of content and features within apps (see section ‘5.2 Content Policies’ for more details).

Protection offered and limitations across app discovery stages

Where app stores use age-based restrictions on the apps surfaced in the discovery journey, this may reduce the likelihood that child users discover regulated apps where they may encounter content harmful to children (though this depends on the age-ratings of regulated apps). Where users can see the app store listing, age ratings and content warnings may help users or parents and guardians better understand the nature of the content within regulated apps. This could then help them make a more informed choice about whether to use an app or to approve use for their children.

In practice however, a significant proportion of the app stores did surface regulated apps with age ratings higher than account ages, including 18+ apps, in user journey testing. This may risk raising children’s awareness of regulated apps, even if those users are still blocked from accessing the apps (see next section).

5.6 App access

Overview

Age restrictions on app purchases and downloads blocked child accounts from accessing certain apps (e.g. where the age rating is 18+). These restrictions may be applied by default to child accounts or turned on by parents or guardians (see section ‘5.4 Parental Controls’ for more details).

How this works

The majority of the app stores reviewed during user journey testing blocked child accounts from accessing 18+ apps by default. Approaches here included:

- blocking 18+ apps for all child accounts by default;
- blocking 18+ apps for child users aged under 13 but not those aged 13-17;
- giving parents or guardians the option to restrict access for child accounts but not blocking by default;
- prompting users to self-declare as an 18+ user; or,
- not blocking for any users with no restrictions available.

Exhibit 30: Approach in blocking users from accessing 18+ apps, based on user journey testing

Approach to blocking users from accessing 18+ apps	Relevant app stores
Blocked all child accounts by default (age established in account setup)	PlayStation Store Google Play Epic Games Store Microsoft Store Xbox Store (users could download but not use) Amazon Appstore (for optional child accounts)
Blocked under 13 accounts by default, but not child users aged 13-17 who were able to download (age established in account setup)	Apple App Store (see note in section '5.4 Parental Controls' about age-based restrictions on by default to all child accounts).
Gave parents or guardians the option to apply restrictions but did not block access for child users by default (age established in account setup)	Nintendo eShop
Prompted users to self-declare their age as 18+ (age established in account setup)	Samsung Galaxy Store (users had to self-declare they were over 18 to download 18+ apps – this was in addition to self-declaring during account setup). Aptoide (users had to self-declare they were over 21 to discover and download 18+ apps).
Not blocked for any users: no restrictions on accessing 18+ apps	Uptodown Market (note: no child accounts) Steam (note: no under 13 accounts)

When blocked, in some cases child users had the option to request approval from parents or guardians, e.g. Apple App Store, Microsoft Store, Xbox Store. For example:

- Apple App Store: children could click “Ask for Exception” on the restricted app, sending a notification to parents or guardians. Parents or guardians could approve or deny requests on their own devices.
- Microsoft Store: children had to “Ask now” for permission to download a restricted game. Parents or guardians received a notification via email and could approve or deny the request.
- Xbox Store: children had to “Ask a Parent” for permission to download a restricted game. Parents or guardians received a notification via email and could approve or deny the request.

Note: User journey testing focused on the ability to purchase or download apps but did not test the ability to access apps that were already available on a user's device (e.g. pre-installed, installed by another user).

Protection offered and limitations

When used, these restrictions may block child access to certain regulated apps where they may encounter content harmful to children.

Limitations included where age assurance was not used to establish the child user's age (e.g. relying on self-declaration instead), where age restrictions were not applied by default, or where restrictions were not used at all.

5.7 Reporting

Overview

Where available, user reporting enables all users to report issues with a given app to the app store. Developers are required to address significant issues raised or face their app being removed from the app store.

How this works

Several app stores offered multiple methods for filing reports. This included reporting within the app store, which was most common, and reporting features via another online method, e.g. on store websites or via email.

Exhibit 31: Reporting mechanisms for app stores reviewed, based on user journey testing

Relevant app store	Reporting mechanism		
	Reporting available within the app store (e.g. users could flag apps as inappropriate on app store listings)	Reporting available via an online method outside of the app store (e.g. on the app store company website or via email)	Developers required to offer a reporting function within the app (e.g. games with UGC must include an in-game reporting function)
PlayStation Store	✓*	✓ ³⁷	✓
Xbox Store	✓*	✓	✓

³⁷The PlayStation Store does not publicly document a way to report harmful or inappropriate game content. Their Contact Support page is available, but it has no category for reporting harmful content. <https://www.playstation.com/en-gb/support/contact-us/>. [Accessed on 26/01/2026]

Google Play	✓		✓
Apple App Store		✓	✓
Nintendo eShop	✓*	✓	
Microsoft Store	✓		✓
Amazon Appstore	✓		✓
Samsung Galaxy Store	✓		
Steam	✓		
Epic Games Store	✓		
Uptodown Market		✓	
Aptoide	✓		

*Reporting was only available for player behaviour and messages, not for app store content

Several app stores required developers to include in-app reporting tools when apps enabled features such as user-generated content or live-generated AI content. For example:

- The Apple App Store required that apps containing user-generated content must include an in-app reporting mechanism.³⁸
- The Google Play store required that apps targeted towards children or apps containing user-generated content must include an in-app reporting mechanism.³⁹
- The Microsoft Store required that apps containing user-generated content or live generative AI content must provide an in-product reporting mechanism.⁴⁰

App stores tended to provide users with prompts within a reporting feature, including the different reasons why a user may have wanted to report an issue. These prompts varied across app stores but generally included options such as inappropriate content, illegal content, and technical issues. App stores generally did not define what constitutes each of these categories, and did not provide opportunities for users to add more detail in their report.

However, there were some exceptions. Several app stores provided users with open-ended text boxes to provide more detail when reporting. For example:

- The Xbox Store allowed users to report offensive content using open-ended text fields, where they could describe the content and specify where it was found.

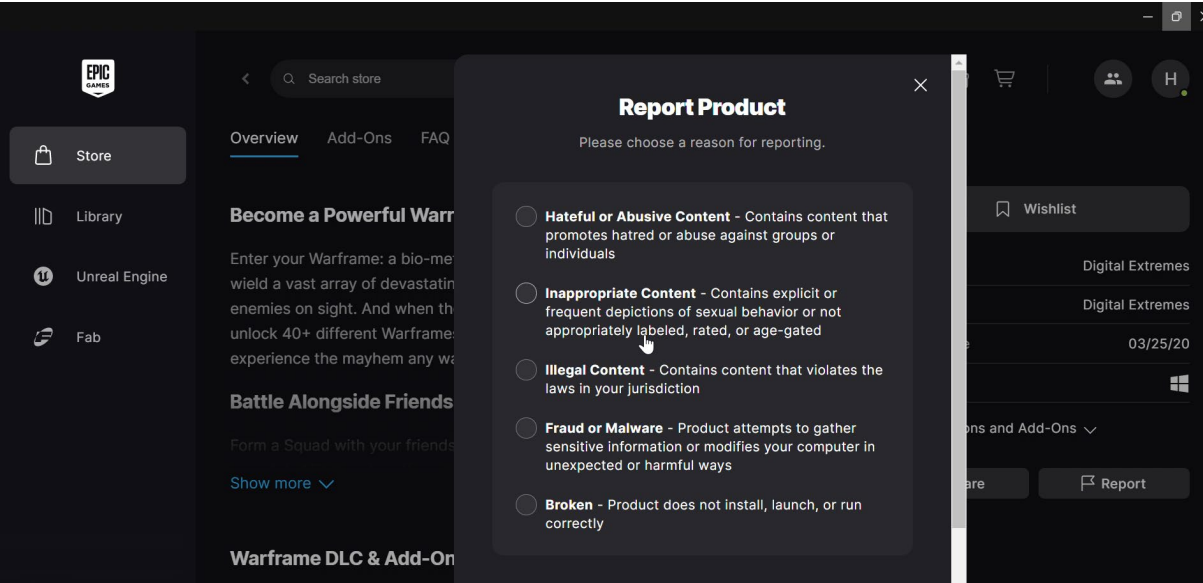
³⁸ <https://developer.apple.com/app-store/review/guidelines/>. [Accessed on 10/04/2026]

³⁹ <https://support.google.com/googleplay/android-developer/answer/9876937?hl=en-GB>. [Accessed on 10/04/2026]

⁴⁰ <https://learn.microsoft.com/en-us/windows/apps/publish/store-policies#1112-user-generated-content>. [Accessed on 10/04/2026]

- The Steam store allowed users to enter additional, relevant information after selecting a reason for reporting a game.

Exhibit 32: Epic Games Store, 18-year-old user account investigating how to report a game [Testing conducted 15-01-2026]



User reports fed into a process between the app store and developers, where developers were required to address significant issues or face consequences that included their app being removed from the app store (see section ‘5.8 Developer processes’ for further details).

Protection offered and limitations

Reporting tools helped app stores identify regulated apps which may have contained content harmful to children. This information could then be used as part of app moderation and enforcement (see section ‘5.8 Developer policies and processes’ for more details) to make developers aware of issues.

5.8 Developer processes

Overview

There are a set of developer policies and processes that govern how apps are reviewed, published, and then moderated on app stores. This involves four main stages:

Exhibit 33: Developer policies and processes governing app review, publication, and moderation

Stages	App creation and setup	Pre-publication review	App reporting	Moderation and enforcement
Typical	Set up a developer	Submission of app	App stores	App stores

steps	account, including an agreement with the app store (if required), and set up of an app store listing, providing information on the app to be published.	for approval, including a review of the app and app information provided by the developer (including details to determine age rating).	collecting user reports on apps and sharing them with developers.	moderating apps, ensuring developers address issues or face action, e.g. take down of app.
--------------	---	--	---	--

How this works

All app stores reviewed had an approval process for developers and their apps to go through before being published. This was lighter touch in some cases, for example with Uptodown Market encouraging but not requiring age ratings.

Apps were rated in line with content policies and were subject to technical reviews. Content policies (see section ‘5.2 Content Policies’ above) played an important role here in setting the criteria that apps were rated against: including determining an appropriate age rating, identifying potentially harmful content to highlight to users, and prohibiting some content entirely.

Most of the app stores enabled user reporting (see section ‘5.7 Reporting’ above) and hold developers to account with the threat of app removal and, in some cases, termination of the developer’s account.

- The Google Play Store may have rejected a new app submission or update, removed an app from the app store, limited the visibility of an app (e.g. only accessible by a direct link), and suspended and/or terminated a Google Play Developer account following content violations.⁴¹
- The Epic Games Store reserved the right to remove a game or permanently ban a developer account depending on the severity of the issue and whether this issue had occurred before.⁴²

Protection offered and limitations

Developer policies and processes offer protection to children by helping ensure that regulated apps meet content policy requirements, e.g. apps displaying appropriate age ratings and warnings. App stores managed user safety both proactively, by assessing apps before they appear on app stores, and reactively, by monitoring apps once on the app store for issues and taking corrective action when issues are discovered. This ranged from contacting the developer to removing the app from the store, depending on the severity.

This protection was dependent on policies and processes being sufficiently robust, e.g. in the assessment of apps before they were added to the app store and in the monitoring and enforcement of content policies after apps were available on the app store.

⁴¹<https://support.google.com/googleplay/android-developer/answer/9899234?hl=en-GB#:~:text=Play%20Developer%20accounts.,Enforcement%20actions,be%20unavailable%20in%20all%20regions.> [Accessed on 18/11/2025]

⁴²<https://dev.epicgames.com/docs/epic-games-store/requirements-guidelines/content-ratings/content-guidelines#consequences>. [Accessed on 27/01/2026]

5.9 Overall analysis of app stores

The review of app store measures to protect children from content harmful to children demonstrated that approaches varied across app stores.

The app stores reviewed could be categorised into four general archetypes. This was based on a set of key factors including whether accounts were required, whether parents or guardians were required to set up child accounts and to approve downloads, whether restrictions on accessing 18+ apps were applied automatically based on age in account set up, and whether age checks on 18+ users involved age assurance or self-declaration of age. An important caveat was that this did not consider all measures used by app stores⁴³ and that there were some variations between app stores within the four general archetypes.

Exhibit 34: App store archetypes with details on key factors (plus variations below)

App store archetype	A: Automatic restrictions supported by age assurance	B. Automatic restrictions based on self-declared age	C. Manually enabled restrictions based on self-declared age	D. Access without account-based age restrictions
Accounts	Account required			No account required
Parent or guardian role	Parent or guardian required to set up child account and/or to give approval to download 18+ apps			Not required
Age check for 18+ users	Age assurance used	Age self-declared	Age self-declared	Not applicable
Age-based restrictions	Restrictions on accessing 18+ apps set automatically	Restrictions on accessing 18+ apps set automatically	Restrictions on 18+ apps available, requiring manual setup to turn on	Not applicable
Which app stores (note variations*)	PlayStation Store Google Play Epic Games Store	Microsoft Store Xbox Store Apple App Store Amazon Appstore Samsung Galaxy Store	Nintendo eShop Steam	Uptodown Market Aptoide

Variations*

Google Play	Archetype A	Required users to verify as 18+ when accessing 18+ apps for the first time. Also required parents or guardians to verify their own age when setting up child accounts for children under 13.
Epic Games Store	Archetype A	Parent or guardian required for children under 13, but not for children aged 13–17. Note age verification only required for 18+ accounts in order to set up under 13 accounts.

⁴³ For example, while the review of app store measures also covered app discovery, the differences between app stores were less clear cut. The majority of app stores surfaced apps with a higher age rating than the child's age, including 18+ apps, as they browsed, searched or saw ads, and so were not factored into the archetypes.

Xbox Store	Archetype B	Age self-declared with the exception of where age verification was used to access Communications features in Xbox Live.
Apple App Store	Archetype B	Parent or guardian required for under 13 accounts, but not for aged 13-17 accounts; Age restrictions on access to 18+ apps applied by default for under 13, but not 13-17 (based on user testing results).
Amazon Appstore	Archetype B	Child accounts required a parent or guardian for setup. However, child accounts were optional, with no age checks or any restrictions on app access applying to adult accounts.
Samsung Galaxy Store	Archetype B	Minimum age of 13 for accounts and a parent or guardian was not required for aged 13-17 accounts. Optional family accounts were also available.
Steam	Archetype C	Minimum age of 13 for accounts. Age verification was required to access 'mature content games' or their associated community hubs. Steam did not define what themes constituted 'mature content.' The 18+ rated game selected for user testing did not fall under the 'mature content' category.
Aptoide	Archetype D	Users self-declared their age as over 18 to access 18+ apps

The protection offered to children varied across app store archetypes. To demonstrate this, we considered the ability of a child user to access 18+ rated apps under different scenarios, and the findings were based on the user journey testing. The scenarios described different ways the child may have accessed the app store:

1. No account created
2. A child attempts to create an account without parent or guardian involvement if that is possible, and if they are asked to declare their age at any point, they do so accurately
3. A child attempts to create an adult (18+) account without parent or guardian involvement if that is possible, and if they are asked to self-declare age, they falsely declare their age as 18+ (but are not able to verify age if required);
4. A parent or guardian sets up an account and leaves parental controls on default settings.

Exhibit 35: Ability of child user to download an 18+ app under different scenarios, by app store category

Scenario	Can a child user download an 18+ app?				Commentary
	A: Automatic restrictions supported by age assurance	B. Automatic restrictions based on self-declared age	C. Manually enabled restrictions based on self-declared age	D. Access without account-based age restrictions	
1. No account	No	No	No	Varies	A, B and C required accounts; for D, no account

					needed but one app store required users to self-declare they were 18+.
2. Child attempts to create account (accurate age)	No	Generally no (yes for 13-17 in some cases)	Generally no (yes for 13-17 in some cases)	Varies	A, B and C required parent involvement in account set up, with some exceptions for child users aged 13-17; Did not require accounts, but one app store required users to self-declare they are 18+.
3. Child attempts to create account (falsely claims age as 18+)	No	Yes	Yes	Yes	A required age-verification; B and C relied on self-declared age, bypassed with false age; D relied on self-declared age or didn't have age check.
4. Parent or guardian sets up child account with default settings	No	Generally no (yes for 13-17 in some cases)	Generally yes	Varies	A and generally B blocked access by default; C did not block by default (one app store had a minimum age of 13); For D, one app store did not block access, whereas the other did.

In summary:

- Archetype A (Automatic restrictions supported by age assurance): Blocked child access to the 18+ apps in all these scenarios;
- Archetype B (Automatic restrictions based on self-declared age): Blocked child access by relying on self-declaration. Vulnerable to child users falsely claiming they were over 18;
- Archetype C (Manually enabled restrictions based on self-declared age): Blocked child access in terms of setting up accounts but, as with Archetype B relied on self-declaration and users entering age correctly. Vulnerable to users falsely claiming they were over 18. Also, where a parent or guardian had set up an account, it relied on them turning on parental age restrictions for access to content;
- Archetype D (Access without account-based age restrictions): Either did not block child access to 18+ apps or relied on self-declaration. Subject to child users falsely claiming their age.

Across the app stores, there were a range of differences based on child users' age. Age-based distinctions for child users were most pronounced between those under 13 and those aged 13-17, with relatively few differences within each age group. Examples of these differences included:

- Account setup and parental controls: Certain app stores gave more freedom to users aged 13-17 than under 13s, including not requiring parents or guardians to set up accounts or giving users aged 13-17 the option to turn off parental controls.
- Content policies: App stores tended to categorise apps by relatively narrow age bands (e.g. for PEGI these include 3+, 7+, 12+, 16+ and 18+) which could be used for age-based restrictions.
- Age-based restrictions on app access: App stores tended to imply that parents or guardians could restrict their child's access to age-appropriate apps (not covered in full in user journey testing).
- Age-based restrictions on app discovery: Certain app stores tailored what apps surfaced when browsing or searching for apps by age, although a significant proportion did not appear to do this based on user journey testing.

6. Digital ecosystem overview

Phase 1 of this research explored the role app stores played in child users accessing regulated apps. This included the role app stores played in providing a way for users to discover and access regulated apps, as well as a range of protective measures for child users.

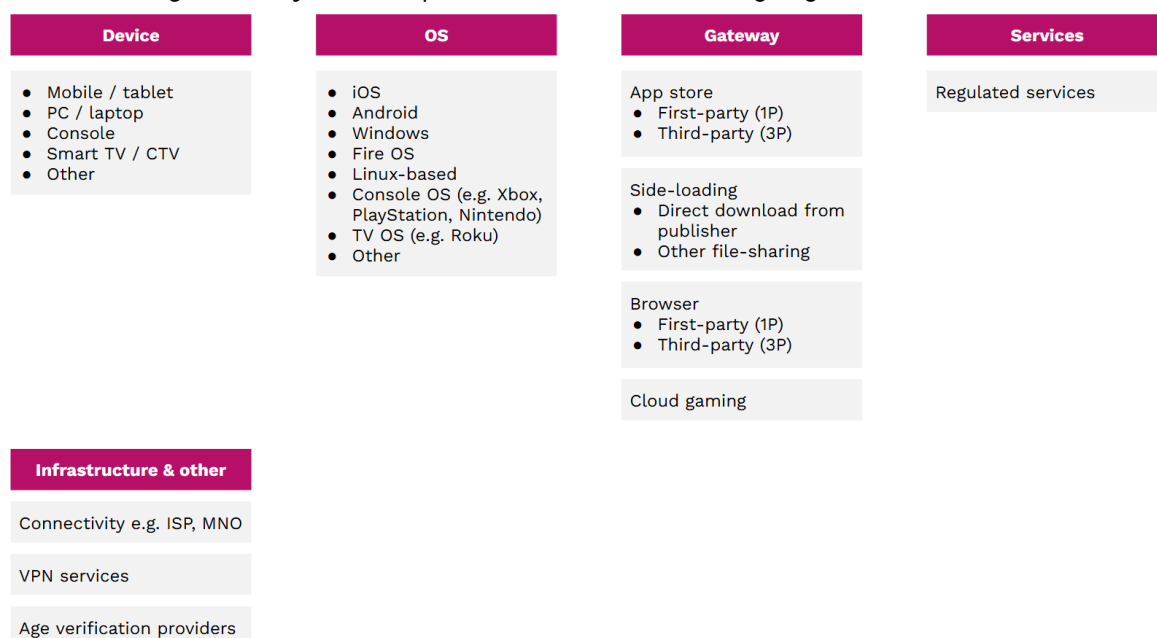
This section puts the app stores reviewed in phase 1 in the context of the wider digital ecosystem.

6.1 Digital ecosystem map

Stepping back from app stores and considering the wider digital ecosystem, there are a range of different actors that may also play a role in child users accessing regulated services:

- **Devices:** such as mobile, tablet, PC, laptop, console and smart TV, connected TV;
- **Operating system (OS):** system-level software powering these devices and enabling them to run software applications;
- **Gateway:** Various gateways through which users can access regulated services, e.g. app stores, sideloading, web browsers, cloud gaming services;
- **Services:** Including regulated services and apps;
- **Infrastructure:** Connectivity providers, virtual private network (VPN) services that may be used to mask the country the user is accessing services from, and age assurance providers used for age assurance when users are accessing services.

Exhibit 36: Digital ecosystem map for child users accessing regulated services



6.2 Role of key actors

Actors in the digital ecosystem may play a role in child users accessing regulated services by:

- 1) providing a gateway to regulated services for child users,
- 2) applying protective measures for child users, or
- 3) being involved in the sharing of age signals about child users:

Exhibit 37: Key actors and their roles in child users accessing regulated services⁴⁴

Actor type	Role in accessing regulated services	Example practices ⁴⁵ (not exhaustive, may not apply to all providers)
Operating system (OS)	- Provide system-level software that gateways that regulated services run on - Manage protective measures for child users that may apply across gateways and services - May share age signals with gateways and regulated services	- Account management - Age assurance including age verification - Federated sign-on for regulated services to authenticate users⁴⁶ - Sharing of age signals, e.g. via APIs - Parental controls or age-based restrictions including family and child account models and restrictions, e.g. on app access, comms features, web filters - Digital wallets, enabling online payments - Managing methods of app installation
App store	- Provide a gateway to regulated apps - May offer or apply protective measures for child users - May inherit account or age signal from OS or capture during app store account setup	- Moderation of apps and associated age ratings and content warnings - Account management, for accounts set up with app store - Age assurance, including age verification - Parental controls and age-based restrictions, including on app discovery and access - User reporting on apps - Mediating app-related payments
Sideloaded gateway	A gateway enabling download and installation of regulated apps outside of 1P app stores	- Share files required to install and run apps - Options include direct download from app providers and publishers, file-sharing services and other alternative channels
Browser	- Provide a gateway to regulated services through direct web access - May offer or apply protective measures for child users - May inherit age signal from OS or app-store level accounts	- Various sign-on options: Direct, via OS or app-store level accounts, or signed out experience - Parental controls and age-based restrictions, e.g. search filtering, web filtering or blocking
Cloud gaming	- Provide a gateway to regulated services through a streamed version of the service - May offer or apply protective measures for child users - May inherit age signal from OS or app-store level accounts, or capture in direct sign-on process	- Moderation of games and associated age ratings and content warnings - Various sign-on options: Direct, via OS or app-store level accounts - Age checks including age verification - Parental controls and age-based restrictions, e.g. on game access, communication features
Regulated services and	The regulated services themselves	Various sign-on options: Direct, via OS or app-store level accounts

⁴⁴ Refer to Section 7 of this report for sources.

⁴⁵ Examples of the relevant functional, child-safety and technical roles typically exercised by each actor. Not intended to be exhaustive and practices may not apply to all providers of these services.

⁴⁶ The federated sign-on allows a provider to use an existing account from another service to verify a user's identity.

apps	• May offer or apply protective measures for child users • May inherit age signal from OS or app-store level accounts, or capture in direct sign-on process	• Age checks including age verification • Parental controls and age-based restrictions, e.g. on content and communication features within the service
Connectivity providers	• Enable web access to gateways and regulated services • Apply protective measures	• Web access, e.g. for gateways and regulated services • Parental controls and age-based restrictions, e.g. web filtering

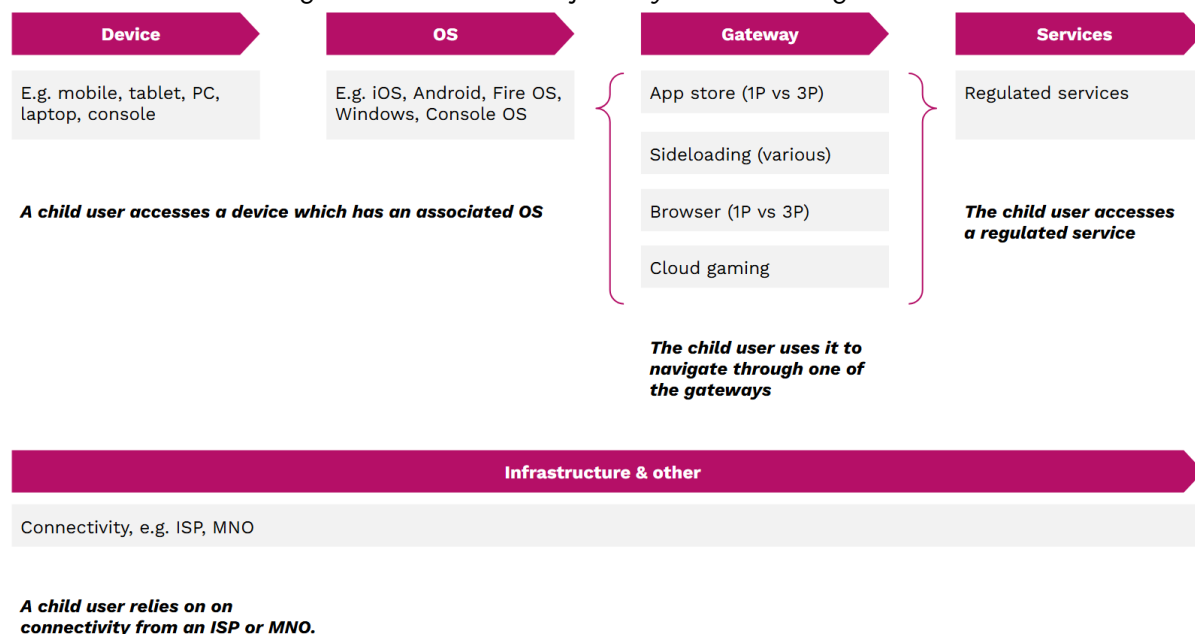
7. App stores in context

This section explores the different ways child users may access regulated services and where the different actors fit in. This desk research was conducted in February and March 2026 and the findings below reflect our observations during this time.

7.1 Overview of the different ways child users may access regulated services

Starting at a general level this typically involves the child user accessing a **device**, with an associated **OS**, and using this device to navigate through a **gateway** and access a regulated service, relying on connectivity from an **infrastructure provider**.

Exhibit 38: General stages in the child user journey to access regulated services



Within this user journey, each gateway offers a different way to access regulated services. **App stores** provide one route to access regulated services but may not be the only one. There is also **sideloading**, which involves downloading apps outside the 1P app store, **browsers**, which can be used to navigate to web versions of regulated services, and **cloud gaming**, which offers streamed versions of regulated services.

There is further variation in how child users may access regulated services, based on:

- **Different OS ecosystems** ranging from more open, allowing more types of gateway and sign-on options, to more closed, with the capability to limit both types of gateways and sign-on options;
- **Different types of actors** and their interaction with the OS, with 1P actors often more closely integrated into the OS ecosystem than 3P equivalents.

In addition to these ecosystem-level differences, the way a child user ultimately accesses a regulated service also depends on choices made by the parent or the child user, for example:

- Which device and associated OS are used, for instance if there are multiple devices available in each household;

- Which gateway users select to navigate through and which specific provider they use, e.g. 1P versus 3P;
- Which regulated service/app users select to use and its relationship to the OS, e.g. 1P versus 3P;
- Whether parents or guardians are involved in creating accounts, if they choose to set up child accounts where possible, and if they enter the child's age correctly;
- Whether parents or guardians configure parental controls where available.

In summary, there are a variety of ways in which child users may be able to access regulated services, with a range of actors that could be involved, and with how this works being partly dependent on the specific providers involved (OS ecosystems, gateways and regulated services) and the choices made by users.

In the following sections we take each actor in turn, exploring their role in child users accessing regulated services and variations based on the different types of providers involved.

7.2 Operating systems

The role of operating systems in child users accessing regulated services

Operating systems provide the system-level software on devices that gateways and regulated services run on, in some cases determining which gateways are available.

They can also play a key role in managing user accounts and associated parental controls and age-based restrictions, including:

- Handling account creation and corresponding age assurance for the 1P app stores and services, e.g. 1P browsers, regulated apps and services⁴⁷;
- Providing managed sign-on⁴⁸, where the OS provider controls user registration for regulated services;
- In some cases, passing account details, age signals (e.g. age, age range or supervised account status) to the regulated services;
- Offering federated sign-on⁴⁹, where the OS provider offers a mechanism to share user credentials with regulated services, potentially including age signals;
- Offering age APIs⁵⁰, where the OS provider offers an interface for regulated services to receive an age signal;
- Managing parental controls and age-based restrictions which apply to 1P app stores and services including family and child account models and various controls on child user activity, e.g. app access, web filters, communication features⁵¹; and,

⁴⁷ E.g. Apple <https://support.apple.com/en-gb/111001?device-type=iphone>. [Accessed 05/03/2026]

⁴⁸ E.g. for gaming platforms, based on Ofcom's Interactive Services Model report (April 2023) <https://www.ofcom.org.uk/siteassets/resources/documents/research-and-data/online-research/interactive-services-model/interactive-services-model?v=329476>. [Accessed 05/03/2026]

⁴⁹ E.g. Sign in with Apple <https://support.apple.com/en-gb/102609> and Sign in with Google <https://support.google.com/accounts/answer/12849458?hl=en>. [Accessed 05/03/2026]

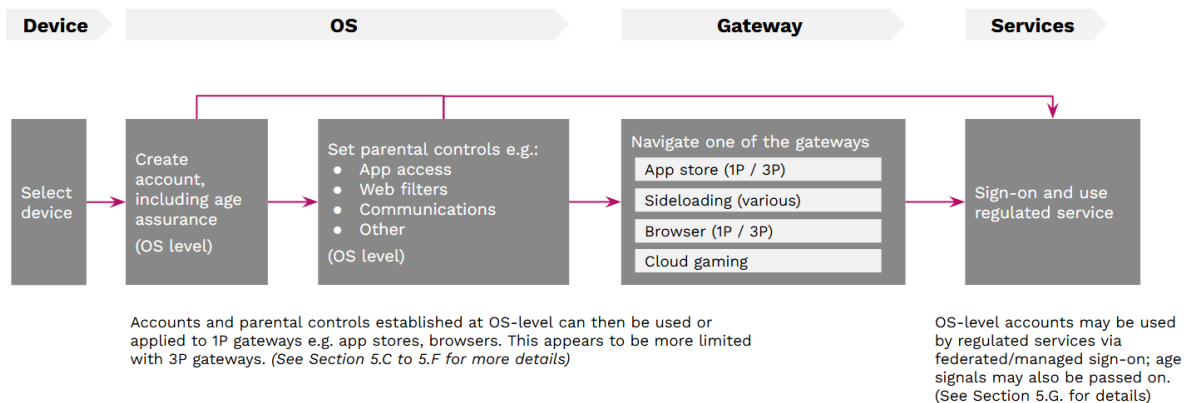
⁵⁰ E.g. Apple's Declared Age Range API <https://developer.apple.com/kids/>. [Accessed 03/03/2026]

⁵¹ E.g. Apple accounts <https://support.apple.com/en-gb/105121>; Google accounts <https://support.google.com/families/answer/9055704?hl=en>; Xbox and associated Microsoft Accounts <https://www.xbox.com/en-GB/apps/family-settings-app>. [Accessed 05/03/2026]

- Facilitating online payments, which in some cases are integrated with parental approval processes, e.g. a parent must approve app purchases⁵².

The following diagram shows how features of the OS, including the accounts, parental controls and age restrictions established at this level, flow through the child user journey, to being used by gateways and regulated services:

Exhibit 39: A diagram showing how the features of an OS flow through the child user journey



What happens in the child user journey, including if and how protective measures and age signals are passed on from the OS level to the gateway and to regulated services, may depend on several factors:

- **Capabilities:** The extent to which the OS provider, gateway, and regulated service support the sharing of accounts, credentials, age signals and protective measures.
- **Parental/guardian involvement:** Whether they are involved in creating OS-level accounts including child accounts, and if they accurately reflect the user's age.
- **User choices:** Which and how many devices and OSs are used, requiring set-up for each one. Whether they choose to use the 1P gateways or seek access to 3P alternatives.
- **Default versus optional protections:** If protective mechanisms and age signals are enabled automatically, or are optional and require setup by the parent or guardian.

Differences between OS types

Operating systems and how they fit into the wider ecosystem vary but we can broadly place them on a spectrum from being more closed to more open. Key distinctions relate to the gateways available for users to access regulated services and how account sign-on is managed:

- For **closed ecosystems** the 1P app store is typically the main or only gateway to regulated services, and the OS-level account may be the only sign-on option for regulated services;
- For **open ecosystems** users may have access to a range of additional gateways, and sign-on options for regulated services can include managed, federated, or direct sign-on;

⁵² E.g. Apple and Google based on CMA's Mobile ecosystems market study <https://www.gov.uk/government/publications/mobile-ecosystems-market-study-final-report> [Accessed 05/03/2026]

- **Mixed ecosystems** sit in-between, for instance with limits on the gateways available similar to more closed ecosystems but often with multiple sign-on options, similar to more open ecosystems.

Exhibit 40: A comparison of the different types of OS ecosystem

Characteristics	Closed OS ecosystems e.g. gaming console OSs	Mixed OS ecosystems e.g. iOS	Open OS ecosystems e.g. Android, Windows
Gateways available	The app store is typically the main gateway to regulated services with: • Browsers are not available or limited to 1P browsers⁵³ • Alternative app stores and sideloading options appear to be unavailable⁵⁴ • Cloud gaming appears limited to 1P services⁵⁵	The app store and 1P browser are the main gateway to regulated services with ⁵⁶ : • A 1P browser is available, while 3P browsers run on 1P web browser technology • Alternative app stores and sideloading options appear to be unavailable • Access to cloud gaming appears limited to browsers	In addition to 1P app stores and browsers, users may have access to additional gateways including: • 3P app stores⁵⁷ • Sideloading, e.g. from direct publisher downloads and other file-sharing services⁵⁸ • 3P browsers⁵⁹
Account management and sign-on options for regulated services	The OS handles account creation and any corresponding age assurance for app stores and other 1P services. Managed sign-on is typically used for regulated services where the user is automatically signed in with an OS-level account.	The OS handles account creation and any corresponding age assurance for their 1P app store and other 1P services. The OS may offer optional federated sign-on for regulated services.	
Age signals (See section '7.7 Regulated Services' for more details)	Age signals may be shared as part of a managed sign-on process to regulated services.	Age signals may be shared with regulated services through federated sign-on or through OS age APIs.	

⁵³ E.g. Xbox has Microsoft Edge but does not appear to offer other browsers, based on web search and searching within web version of Xbox Store <https://www.xbox.com/en-gb/Search/Results?q=browser>; while PlayStation has a browser on PS5 but it is 'hidden' <https://www.cnet.com/tech/gaming/your-ps5-has-a-hidden-web-browser-heres-where-to-find-it/> and Nintendo has a browser with limited functionality that is similarly hidden <https://support.microsoft.com/en-gb/account-billing/filter-websites-and-searches-using-microsoft-family-safety-3034d91e-5efa-9f8e-1384-46009f087ccf?> [Accessed 27/03/2026]

⁵⁴ No evidence found in web-based search.

⁵⁵ No evidence found in web-based search.

⁵⁶ Sources: CMA 'Mobile Browsers and Cloud Gaming: Final Decision Report' (March 2025); CMA 'Mobile Ecosystems: Market Study Final Report' (June 2022).

⁵⁷ Based on Phase 1 of this research.

⁵⁸ E.g. Google, inferred based on availability of parental controls that either allow or block child users from being able to download files outside 1P stores (e.g. from 'unknown sources'). <https://blog.google/products-and-platforms/android/how-android-helps-you-stay-safe-from-mobile-fraud-apps/>. [Accessed 27/03/2026]

⁵⁹ E.g. Firefox browser available on Windows, iOS, Android amongst others https://www.firefox.com/en-GB/?utm_campaign=SET_DEFAULT_BROWSER. [Accessed 27/03/2026]

7.3 App stores

The role of app stores in child users accessing regulated apps

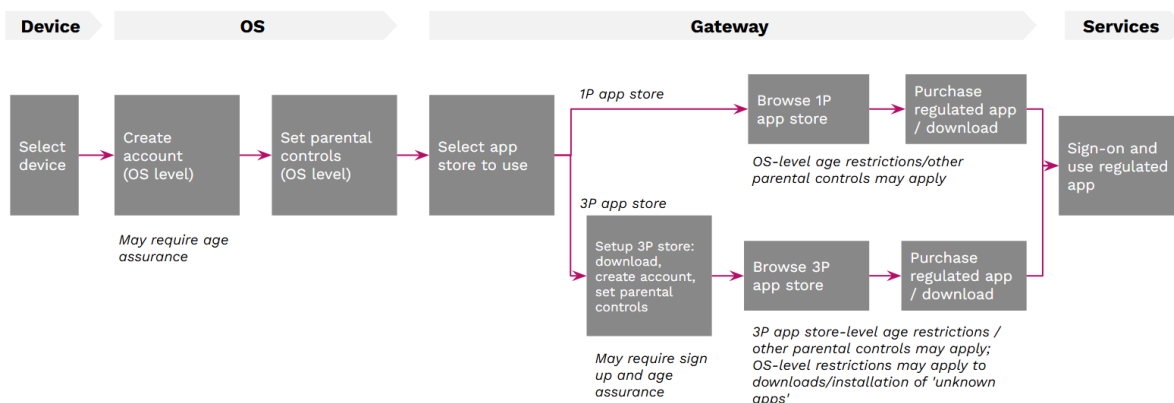
App stores are one of the gateways through which child users can access regulated apps. On a given device and associated OS, users will typically have access to the 1P app store and may also be able to access alternative, 3P app stores, which allow them to discover, purchase and download apps⁶⁰.

As we explored in Phase 1 of the research, these app stores offer a range of protective measures for child users. These vary across app stores but typically include:

- Moderation of apps and associated age ratings and content warnings;
- Parent or guardian and child accounts, and the use of age assurance;
- Parental controls and age-based restrictions on app discovery and app access;
- User-reporting on apps.

The following diagram sets out a typical child user journey involving app stores: From getting set up on a device with an OS-level account, to choosing between using the 1P app store or setting up an alternative 3P store, browsing for and downloading a regulated app and signing on and using that app - with potential for age restrictions at various steps.

Exhibit 41: An illustrative child user journey flow for using an app store to access regulated services



The user journey depends to an extent on user choices, with implications from the protective measures applied and how age signals are passed on. Key decision points include:

- **Select device and associated OS:** Whether the OS on a selected device allows 3P app stores or alternative sideloading methods;
- **Create account (OS-level):** Whether a parent or guardian is involved in creating OS-level accounts, including child accounts and if they are accurately reflecting the user's age;

⁶⁰ E.g. based on Phase 1 of this research, iOS and Apple App Store, Android and Google Play, Windows and Microsoft Store and the various console OSs and their respective stores, with 3P stores available on at least Android and Windows.

- **Parental controls (OS level):** Whether settings are enabled by default or require configuring, and what controls are set by parents or guardians, including whether sideloading is permitted;
- **App store:** Whether a 3P app store is pre-installed or otherwise possible to install, and when installed whether the parent or guardian is aware and if so, if they are involved in account setup and apply protections such as parental controls.

Differences between app store types⁶¹

There are differences between using 1P and 3P app stores, which we set out in the table below. Most notably, 1P app stores generally use OS-level accounts and inherit age signals and parental controls set at OS-level. In contrast, 3P app stores appear to require new user accounts and do not inherit age signals or controls from OS levels used on the device in the same way - noting that OS-level restrictions may apply to installation of 'unknown apps'⁶².

Exhibit 42: A comparison of 1P app stores and 3P app stores and how they fit into the wider digital ecosystem⁶³

Characteristics	1P app stores	3P app stores
Availability in different OS ecosystems	OSs typically have their own app stores ⁶⁴	3P app stores are available on more open ecosystems but not on mixed or more closed ecosystems (see Section '7.2 Operating systems' for more details).
Account management and sign-on options	Typically linked to OS level accounts for sign-on ⁶⁵	Appear to rely on direct sign-up to the app store, however may enable federated sign-on that use OS-level accounts. ⁶⁶
Age signals	Appear to inherit age signals, generally from OS level accounts	May capture age during the direct sign-up process and may apply age assurance, however age may also not be captured. For federated sign-on using OS-level accounts, they may inherit age via age APIs.

⁶¹ In Phase 1 of this research, we explored the variety of approaches across app stores and set out four archetypes (see 'Section 5.1 Overview of app store measures' for more details). Here we consider this at a higher level, comparing 1P app stores and 3P app stores and how they fit into the wider digital ecosystem.

⁶² E.g. Google <https://blog.google/products-and-platforms/platforms/android/how-android-helps-you-stay-safe-from-mobile-fraud-apps/>. [Accessed 27/03/2026]

⁶³ The findings here are generally based on Phase 1 of this research and the in-depth review of a set of 1P and 3P app stores.

⁶⁴ For example, based on Phase 1 of this research, iOS and Apple App Store, Android and Google Play, Windows and Microsoft Store and the various console OSs and their respective stores.

⁶⁵ The initial account sign-up to OS level accounts may be initiated through the app store if this is the first service in the OS ecosystem users encounter.

⁶⁶ In the Phase 1 findings, most of the 3P app stores reviewed required creation of new accounts directly with the app store and had their own parental controls, with the exception of Epic Games Store which has federated sign up options <https://www.epicgames.com/id/login>. [Accessed 27/03/2026]

Parental controls and age-based restrictions	Appear to inherit parental controls managed by OS level accounts	Typically have their own app store level parental controls, if any. ⁶⁷ We found no evidence that 3P app stores can inherit parental controls from OS-level accounts.
---	--	---

7.4 Sideloading

The role of sideloading in child users accessing regulated services

Sideloading refers to methods of installing apps, games and other types of software on devices outside of 1P app stores. The 3P app stores covered in section ‘7.3 App stores’ above, could be considered as an example of sideloading. Other methods of sideloading which we will consider here, include direct download from publishers and other file-sharing services.

These sideloading options are another gateway through which child users could access regulated services. On a given device, users may be able to navigate to a publisher website or follow a link to a file on a file-sharing service, that allows them to download and then install the file for a regulated service.

The OSs on devices may have some protective measures for child users or all users. For example^{68,69}:

- Parental controls that block the installation of apps outside of 1P stores
- Displaying warnings when the user is downloading apps outside of 1P stores
- Security checks that are run on downloaded files

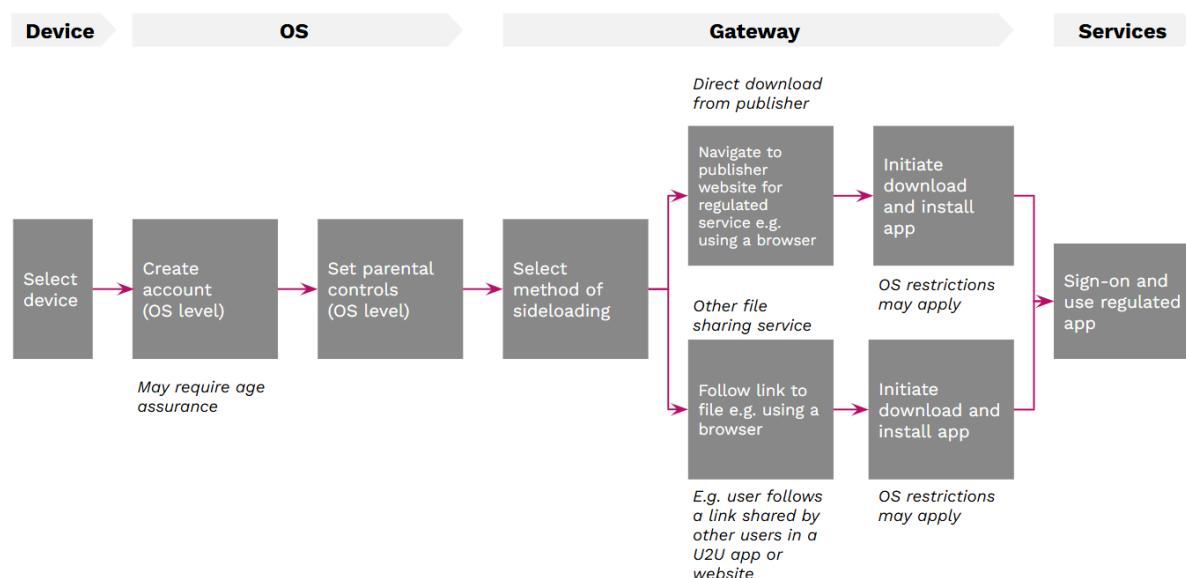
The following diagram sets out a potential child user journey involving these sideloading options: From selecting a method of sideloading, navigating to the publisher website or following the link to a file on a file-sharing service, initiating download and installing the file, and signing on and using the app downloaded - with potential OS-level restrictions on download and installation.

⁶⁷ Based on 3P app stores reviewed in Phase 1 of this research, e.g. Epic, Steam, Aptoide.

⁶⁸ E.g. parental controls on Apple and Google <https://support.apple.com/en-us/118128>; security checks on Microsoft <https://learn.microsoft.com/en-us/windows/security/operating-system-security/virus-and-threat-protection/microsoft-defender-smartscreen/> [Accessed 05/03/2026] <https://blog.google/products-and-platforms/platforms/android/how-android-helps-you-stay-safe-from-mobile-fraud-apps/>. [Accessed 05/03/2026]

⁶⁹ Publishers and file-sharing services may also have protective measures for children or users in general, but were not reviewed in depth as part of this research.

Exhibit 43: An illustrative child user journey flow for using sideloading to access regulated services



Differences between sideloading options

While the services used in these sideloading options vary, there are similarities in how these options interact with other actors in the ecosystem. The following appears to apply across sideloading methods:

- Sideloading is possible across some OS ecosystems but not others, for example console OSs do not allow sideloading on console devices⁷⁰;
- OSs may apply some protective measures on the sideloading of apps, e.g. parental controls blocking downloads from these sources, or more general warnings or security checks;
- Of the more general parental controls and age-based restrictions managed at the OS-level, some may still apply to sideloaded apps, e.g. limits on play time, but others may not, e.g. parental approvals on downloads.⁷¹

7.5 Browsers

The role of browsers in child users accessing regulated services

Browsers are a gateway through which child users can access regulated services. Depending on the device, users generally have access to a 1P browser, often the default browser for a device, and may be able to access or install a 3P browser. Users can access regulated services via these 1P or 3P browsers.

Browsers offer a range of protective measures for child users. Browsers may automatically apply age-based restrictions for child users (e.g. limiting access to adult or mature sites), or provide the controls for parents or guardians to restrict access for their children. Protective measures vary across browsers but can include⁷²:

⁷⁰ No evidence found in web-based search.

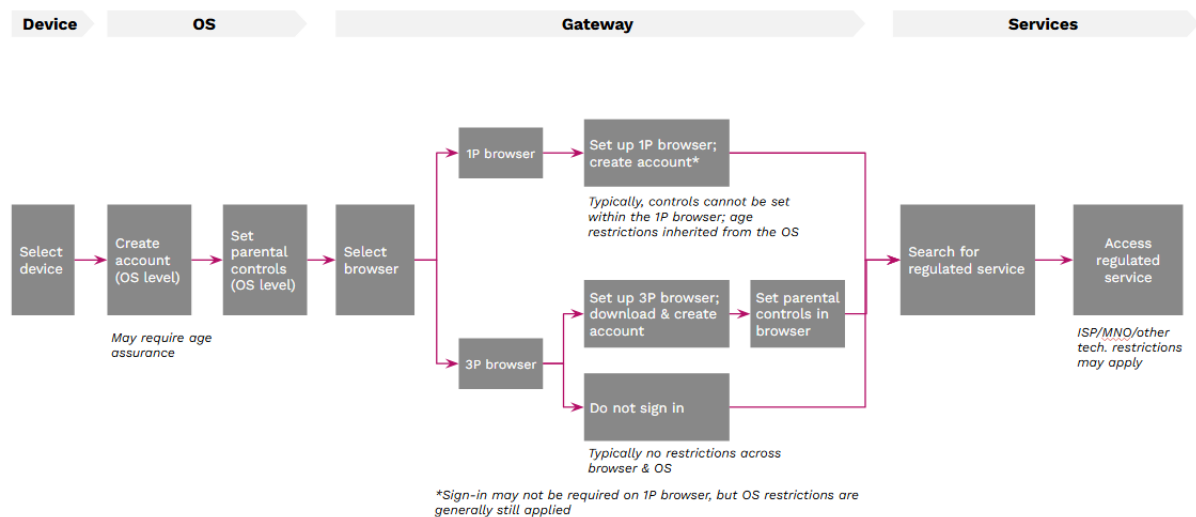
⁷¹ E.g. Apple <https://support.apple.com/en-us/118110>. [Accessed 05/03/2026]

⁷² The findings here are based on Phase 1 of this research and the age-based restrictions captured during device set up.

- **Blocking specific websites** that host adult, unsafe, or inappropriate content for child users; as well as any additional sites that parents or guardians choose to restrict.
- **Enforcing search filtering** which helps restrict access to explicit, inappropriate, or adult material from search engine results.
- **Restricting certain browser features**, such as the ability to use private browsing modes (that do not save history, cookies, etc.), or to sign out of supervised accounts without parental intervention.

The following diagram displays a typical child user journey involving browsers: From setting up a device with an OS-level account, enabling parental restrictions, choosing between a 1P browser or 3P browser, to searching for and accessing a regulated service.

Exhibit 44: Illustrative child user journey flow for using a browser to access regulated services



As the illustrative journey shows, 1P browsers typically inherit parental controls and age restrictions from the OS. In most cases, these controls are set at the OS level, for example through device settings or the OS account, rather than within the browser itself.⁷³ There is also generally no separate “signed out” journey for a 1P browser, since the relevant age restrictions are applied automatically through the OS.

By contrast, 3P browsers generally allow users to proceed without signing in. In those cases, no parental controls or age signals are typically applied, and the browser does not usually inherit these from the OS. Where a user does sign in to a 3P browser, the browser may apply parental controls, either automatically based on age signals captured during sign-up or through settings configured by a parent during account set up.

What happens in this journey, including if and how protective measures and age signals are passed on from OS level to browser, may depend on several factors:

- **Device and OS:** Whether the OS on selected device supports 1P or 3P browsers;

⁷³ The findings here are based on Phase 1 of this research and the parental controls captured during device set up.

- **Create account (OS-level):** Whether a parent or guardian is involved in creating OS-level accounts, including child accounts and if they accurately reflect the user's age;
- **Parental controls (OS level):** Whether the settings are enabled by default or configured, and what controls are set by the parent or guardian relating to web browsers at OS-level, e.g. search filtering, web filtering or blocking;
- **Browser:** Whether a 1P or 3P browser is used and whether the parent or guardian is aware of this;
- **Sign-on and parental controls (browser-level):** Whether the user is signed in or out. If signed in, whether parental controls pass through from OS-level or controls are available at the browser level, and whether they are enabled by default or are configured by the parent or guardian.

Differences between browser types

There are differences between 1P and 3P browsers, detailed in the table below. The biggest difference is that 1P browsers rely on OS-level accounts to inherit age signals and apply parental controls set at OS-level, while 3P browsers generally do not inherit age signals or protections from the OS. Browsers are unique to other gateways in that most do not require user sign in, and 3P browsers may not apply protections until a user is signed in.

Exhibit 45: A comparison of 1P browsers and 3P browsers and how they fit into the wider digital ecosystem

Characteristics	1P Browser	3P Browsers
Availability in different OS ecosystems	It is common for OS ecosystems to have their own browsers ⁷⁴ , with some exceptions, e.g. console OS ecosystems such as PlayStation and Nintendo	Generally, 3P browsers are permitted, with the same exceptions, e.g. console OSs. In some cases, the OS requires a 3P browser to run on a specific 1P engine - controlling the implementation of technical security standards and ensuring that protective measures for child users remain the same across browsers. ⁷⁵
Account management and sign-on	Typically linked to the OS and share a single sign-on with the OS ⁷⁶	Typically, 3P browsers rely on direct sign-up; some browsers enable federated sign-on that uses OS-level accounts. Sign-on may not be required. ⁷⁷
Age signals⁷⁸	Appear to inherit age signals and permissions from OS level accounts and settings	May capture the user's age during the direct sign-up process and may apply age assurance.
Parental controls and age-based	Appear to inherit parental controls managed at OS level accounts ⁷⁹	3P browsers may offer their own parental controls which are not applied automatically but must be configured separately. ⁸⁰

⁷⁴ For example, based on Phase 1 of this research, iOS / Safari, Android / Google Chrome, and Windows / Edge.

⁷⁵ https://assets.publishing.service.gov.uk/media/67d0133cd107f3a16e0287a5/Summary_of_final_decision.pdf. [Accessed on 05/03/26]

⁷⁶ The initial account sign-up to OS level accounts may be initiated through the 1P browser if this is the first service in the OS ecosystem users encounter.

⁷⁷ <https://support.mozilla.org/en-US/kb/sign-in-accounts-using-3rd-party-auth>. [Accessed on 05/03/26]

⁷⁸ In the Phase 1 findings, the 3P app stores reviewed required new accounts, with some checking age and some not. It is possible in the wider market that some 3P app stores allow federated login using OS-level accounts and through OS age APIs can inherit age signals, however, we did not find evidence of this.

⁷⁹ E.g. Apple accounts <https://support.apple.com/en-gb/105121>; Google accounts <https://support.google.com/families/answer/9055704?hl=en>; Xbox and associated Microsoft Accounts <https://www.xbox.com/en-GB/apps/family-settings-app>. [Accessed 05/03/2026]

⁸⁰ E.g. Firefox <https://support.mozilla.org/en-US/kb/block-and-unblock-websites-parental-controls-firefox>. [Accessed 05/03/2026]

restrictions		No evidence found that 3P browsers inherit parental controls from OS-level accounts. Where a 3P browser does not require user sign in or capture user's age, age-based restrictions may not apply. Exceptions include: -where 3P browser runs on 1P engine, automatically enforcing parental controls set at OS level.⁸¹ -parental controls restricting 3P browser download.⁸²
---------------------	--	---

7.6 Cloud gaming

The role of cloud gaming in child users accessing regulated services

Cloud gaming refers to a method of playing video games via remote servers where a game is processed and rendered off-device and streamed to the user over the internet. Cloud gaming services may be accessed via a standalone app, an app that decides to support that capability (e.g. Discord), or a website. Some services are operated by larger gaming consoles (referred to here as 'integrated cloud services'), while other services are standalone ('standalone cloud services'). Cloud gaming services may provide access to a range of regulated services.

Cloud gaming services offer a range of protective measures for child users.

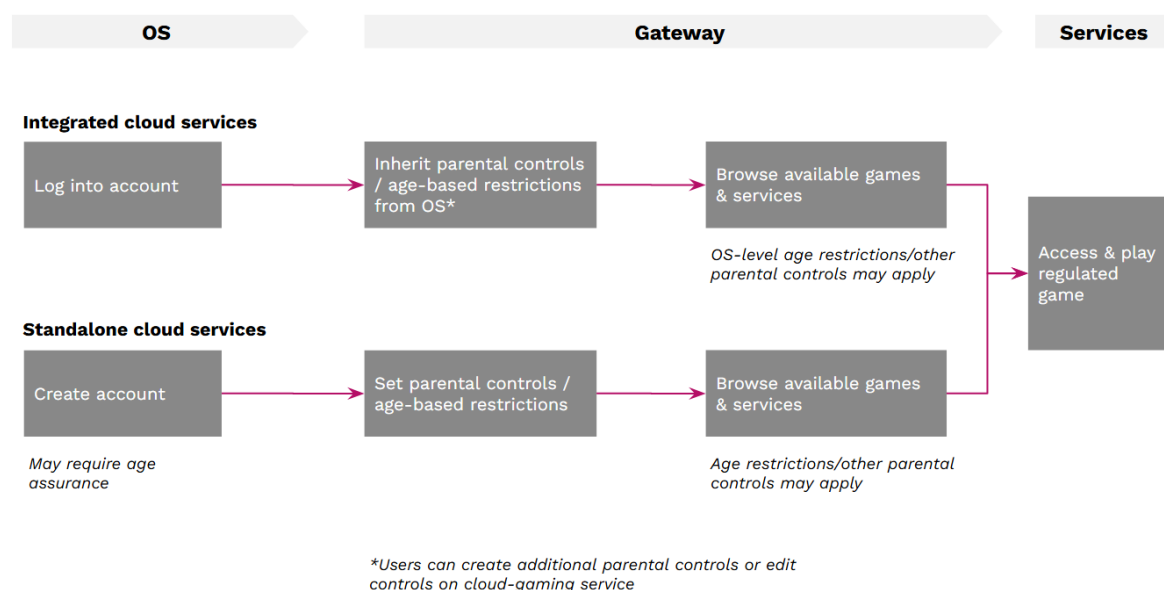
- Parental control or age-based filtering of games based on age rating
- Parental pins to restrict the purchase of age-inappropriate games
- Parental pins to restrict game play
- Parental control over in-game communication capabilities

The diagram below outlines a typical child user journey involving cloud gaming services

⁸¹ Apple specifies that mobile browsers in the UK must use Apple's browser engine WebKit. https://assets.publishing.service.gov.uk/media/67d0133cd107f3a16e0287a5/Summary_of_final_decision.pdf; <https://open-web-advocacy.org/blog/ios-age-restriction-blocks-all-browsers-except-safari-breaks-choice-screen/>. [Accessed on 19/03/26]

⁸² In the Phase 1 findings, some OSs provided parental controls that restricted app downloads, either from the app store or via sideloading.

Exhibit 46: An illustrative child user journey flow for using a cloud gaming service to access regulated services



Generally, users who access integrated cloud services already have a console account. In these cases, the cloud gaming service inherits the parental controls and age-based restrictions set at the console OS level.

Differences between cloud gaming types

Integrated cloud services and standalone services are broadly similar, but there are a few differences detailed in the table below. The biggest difference is that integrated cloud services typically inherit age signals and parental controls or age-based restrictions from the console OS, while standalone services do not. Typically, standalone services rely on age signals captured during the direct sign-on process. Additionally, parental controls or age-based restrictions are configured and applied during account set up, but standalone services do not typically inherit restrictions from the console OS.

Exhibit 47: A comparison of integrated cloud services and standalone cloud gaming services and how they fit into the wider digital ecosystem

Characteristics	Integrated cloud services	Standalone cloud services
Availability in different OS ecosystems	Most cloud gaming services are available across OSs	Most cloud gaming services are available across OSs, except for console OSs which are typically closed environments.
Account management and sign-on options	Users typically sign in using their console OS account details. Accounts are typically created and managed by console OSs. Most console OSs rely on user	Users typically use direct sign up for these cloud gaming services. Some services allow federated sign-on. ⁸⁴

⁸⁴ E.g. NVIDIA GeForce Now <https://www.nvidia.com/en-gb/geforce-now/#product-matrix> [Accessed 06/03/2026]

	managed sign-on capabilities. ⁸³	
Age signals	Appear to inherit age signals generally from OS level accounts. ⁸⁵	Cloud gaming services may have some form of age checks during the direct-sign up process. No evidence was found to show that any OSs share age signals with standalone, 3P cloud gaming services.
Parental controls or age-based restrictions	Parental controls can be added or edited at the console OS account-level.	These services may offer their own parental controls. ⁸⁶ No evidence was found to show that any OSs share parental controls with standalone, 3P cloud gaming services.

7.7 Regulated services

Overview

In this section we consider regulated services, their interactions with other actors in the ecosystem, and where they may have their own protective measures for child users.

In the context of this research, key interactions between regulated services and other actors in the ecosystem relate to sign-on, age signals, parental controls or age-based restrictions, and app moderation (for details on the latter see section ‘5.2 Content policies including age ratings’ in Phase 1 of this research).⁸⁷ Taking these in turn:

Sign-on and age signals

Sign-on options for a regulated service can either be linked to or independent of, OS-level or app store accounts.

Exhibit 48: Sign-on options for regulated services

Sign-on options	Details
Managed sign-on ⁸⁸	The user is automatically signed in with an OS-level account or app store account, which provide credentials to the regulated service. This can

⁸³ In Phase 1 findings several 1P app stores tested on consoles provided managed sign-on capabilities, and did not allow federated sign-on options via 3P.

⁸⁵ Xbox <https://www.xbox.com/en-GB/apps/family-settings-app> and <https://support.xbox.com/en-US/help/account-profile/manage-account/gaming-and-store-accounts#:~:text=The%20Xbox%20app%20on%20PC,account%20you%20use%20for%20Xbox>. [Accessed 05/03/2026]

⁸⁶ E.g. Amazon Luna https://luna.amazon.co.uk/settings?subNav=parental_controls and <https://www.amazon.co.uk/gp/help/customer/display.html?nodeId=GJCN9Z5K9ZVMXQSA>; Blacknut <https://www.blacknut.com/en>. [Accessed 04/03/2026]

⁸⁷ There are a broader set of interactions between regulated services and other actors such as operating systems and app stores, for instance in relation to app development, but that is beyond the scope of this research.

⁸⁸ E.g. for gaming platforms, based on Ofcom’s Interactive Services Model report (April 2023). <https://www.ofcom.org.uk/siteassets/resources/documents/research-and-data/online-research/interactive-services-model/interactive-services-model?v=329476>.

	happen: • Where the regulated service is 1P and native to the device and associated OS; or • With more closed OS ecosystems where this is the preferred approach (see section '7.2 Operating systems' for more details on closed OS ecosystems)
Federated sign-on ⁸⁹	The user uses credentials from an OS-level account or app store account (e.g. Sign in with Apple, Sign in with Google) to sign-up. This is typically optional for both the regulated service to support and the user to use, with alternatives, e.g. direct sign-up, available.
Direct sign-on ⁹⁰	The user registers directly with the regulated service. The regulated service may capture various details about the user, e.g. name, email, phone number, and potentially carries out age checks.

Age signals, including age, age range and account status (e.g. child) may be shared from OS-level or app-store level accounts, or conducted at a service level. Age signals can be shared through the different sign-on options detailed in the table above. Additionally, in some instances, age-signals can be shared through an age API by an OS provider or age assurance provider. An age API provides an interface that allows a regulated service to receive an age signal, while the regulated service may still manage the rest of the user registration process.⁹¹

Parental controls and age-based restrictions

Parental controls and age-based restrictions set at OS or app store levels may also apply to the regulated services, or the regulated services may also apply their own. For example, restrictions can be:

- Applied at the OS or app store level, e.g. where the user is signed in via a managed sign on, as a 1P service or with more closed ecosystems;
- Applied by the regulated service itself where the service has established the user's age, e.g. during the sign-up process, and restricts some content for child users.

7.8 Other supporting actors

Other actors that play a role in child users accessing regulated services include:

- **Connectivity providers**, used for web-access through the child user journey and which may also apply web filters to restrict content, e.g. for pornographic content⁹²;
- **Third-party age assurance providers** may provide age assurance methods for OS-level accounts and app-store level accounts or when accessing regulated services;
- **VPN services** that may be used to disguise the user's location when accessing the regulated app or service.

⁸⁹ E.g. Sign in with Apple <https://support.apple.com/en-gb/102609> and Sign in with Google <https://support.google.com/accounts/answer/12849458?hl=en>. [Accessed 05/03/2026]

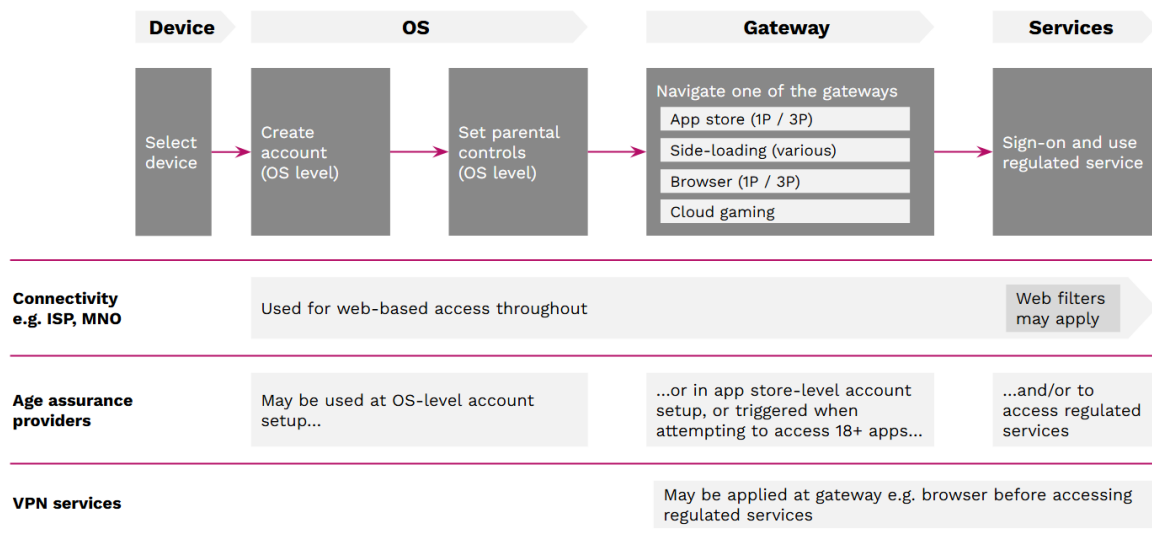
⁹⁰ E.g. Sign in with Apple <https://support.apple.com/en-gb/102609> and Sign in with Google <https://support.google.com/accounts/answer/12849458?hl=en>. [Accessed 05/03/2026]

⁹¹ E.g. Apple's Declared Age Range API <https://developer.apple.com/kids/>. [Accessed 03/03/2026]

⁹² Web filtering by mobile network operators e.g. Three <https://www.three.co.uk/support/internet-and-apps/accessing-and-blocking-adult-content>; and ISPs (e.g. BT <https://www.bt.com/help/security/all-about-parental-controls>). [Accessed 03/03/2026]

The following diagram highlights where these actors may fit into child user journeys:

Exhibit 49: Role of other actors within child user journeys



8. Conclusions

This concluding section summarises our findings on app stores, puts these findings in the context of the wider digital ecosystem, and outlines several considerations for Ofcom.

8.1 Key findings from Phase 1

Many of the app stores available in the UK, and all the app stores reviewed in detail for this research, provided access to regulated apps. This means that children using app stores may have been able to gain access to these regulated apps.

We identified a range of measures in place across the app stores reviewed that were designed to offer some form of protection to children from accessing content that may be harmful to children in regulated apps, for example:

- Prohibition of apps containing certain types of content (e.g. explicit sexual content, extreme violence, hate speech) and pre-publication review of apps by the app store, limiting child users' potential exposure to this content through apps available on the app store.
- Use of age ratings and content warnings intended to help users better understand the nature of content within regulated apps.
- Availability of child accounts which could be used to apply age restrictions within the app store.
- Use of age checks, and in some cases age assurance, to determine if users were over 18.
- Age restrictions on the apps surfaced in the discovery journey (e.g. browsing app store, searching for specific apps) which may reduce the likelihood that child users discovered regulated apps that may contain content harmful to children.
- Age restrictions on the apps a child user could download based on their age-rating, which may block access to certain regulated apps.
- Reporting tools that helped app stores identify regulated apps which may contain content harmful to children, with the potential for this information to have been used in app moderation and enforcement of content policies.

Most of the app stores reviewed deployed at least some of these measures, but the exact combination of measures used and how they were deployed varied across the app stores. The result was that some app stores may have offered different types of protection than others, as described by the following archetypes:

- Archetype A (Automatic restrictions supported by age assurance): required parents or guardians to set up child accounts, used age assurance for 18+ users, automatically applied age restrictions on child users accessing 18+ apps.
- Archetype B (Automatic restrictions based on self-declared age): like Archetype A, but when carrying out an age check 18+ users relied on self-declaration of age rather than age verification.
- Archetype C (Manually enabled restrictions based on self-declared age): like Archetype B but age restrictions required manual setup rather than being applied automatically.
- Archetype D (Access without account-based age restrictions): accounts were optional with a lack of any age check.

There were other potential limitations to the measures used by app stores which included:

- Inconsistent age ratings applied to the same apps across different app stores which suggested that not all app stores had appropriate age ratings.
- A reliance by app stores in general on a one-time setup of accounts with limited or no subsequent age checks, which meant a risk that if an error was made when entering a child's age, or the child gained access to an adult account, this was unlikely to be corrected.
- A significant proportion of the app stores reviewed surfaced regulated apps with age ratings higher than account ages, including 18+ apps in user journey testing. This risked raising children's awareness of these regulated apps, even if those users may still have been blocked from accessing them.

In summary, we found that app stores did provide a means for child users to access regulated apps, and they generally provided some protective measures for child users. However, the combination of measures used, how they were deployed, and the effectiveness of these measures in protecting children from content which is harmful to them varied across app stores.

8.2 Key findings from review of app stores in the context of the wider digital ecosystem (Phase 2)

In the wider digital ecosystem, there were a range of different actors that played a role in child users accessing regulated apps or services. This included devices, operating systems (OS), various gateways, regulated services and the supporting infrastructure.

A key finding was that while app stores may have been the main gateway, or otherwise an important gateway, for child users to access regulated apps or services, users may also have had access through alternative gateways, e.g. with sideloading, browsers, as well as more niche offerings such as cloud gaming providing alternative routes. Other key findings included:

- Account creation and corresponding age assurance may have been carried out by different actors including at OS, app store or regulated service-level;
- Age signals may have passed through the ecosystem, e.g. from OS to app stores or regulated services, but also may have not;
- Parental controls and age-based restrictions could also be implemented by different actors including at the OS, gateway and regulated service levels; and,
- Finally, as with app stores approaches varied across different OS, gateways, and regulated service providers.

8.3 Conclusions

These research findings raise several considerations for Ofcom about the role that app stores could play in protecting children from accessing content that may be harmful to them by means of regulated apps.

Firstly, relating to app store protective measures and the different combinations and ways these may be deployed by app stores, considerations include:

- What combination of measures, if any, offers effective protection for children from encountering content harmful to them?

- How should these measures be applied, e.g. which methods of age check if any should they use?
- When should they be applied, e.g. age checks at account setup or triggered by some action later in the user journey?
- What steps should be taken, if any, to address discrepancies in age ratings across app stores?

Secondly, relating to app stores in the context of the wider digital ecosystem, we saw that, while app stores may have been the main gateway for child users to access regulated services, there may have been alternatives. In addition, we saw that age checks and parental controls could be managed by different actors (e.g. OSs, app stores, regulated services) and that these may pass between actors but they also may not. Based on this, further considerations include:

- What is the role of app stores in child users accessing regulated services compared to other gateways?
- What is the likelihood that protective measures applied at the app store level could be bypassed by child users by using other gateways?
- How would protective measures applied at the app store level interact with protective measures from other actors in the ecosystem?
- What is the ability of parents or guardians to understand, navigate and setup accounts and protective features, and understand where they apply across the devices, OSs, gateways and regulated service their child users may use?

A1. Glossary

Term	Definition
Actor	“Actor” refers to devices, operating systems, app stores, sideloading methods, browsers, cloud gaming, and regulated services.
Age assurance	A collective term for age verification and age estimation.
Age bands	Age ranges used by an app store to distinguish child users and apply different age-based restrictions.
Age check	A collective term for checking a user’s age, including age verification, age estimation, or self-declaration.
Age estimation	Any measure designed to estimate the age or age-range of users of a regulated service. ⁹³
Age ratings	A standardized classification that indicates the minimum recommended age for an app based on its content and features, to help users judge suitability. Standards are typically set by a regional ratings authority (e.g. PEGI) or by the app store.
Age signal	Indicator of an account’s age or age range that can be used to apply age-based restrictions and shared within the app store or with third-party systems.
Age verification	A form of age assurance designed to verify the exact age of the user. ⁹⁴
Age-based restrictions	A collective term for restrictions applied to users under 18 by an app store based on a user’s age.
API (Application Programming Interface)	A standardized set of rules and protocols that governs how distinct software systems communicate, interoperate, and securely exchange data.
Browser engine	Underlying software component of a browser that handles the rendering and display of web content. The browser engine is responsible for processing HTML, CSS, and JavaScript code, and rendering websites into the visual format that users see.
Child	A person under the age of 18.
Child accounts / child user	A user under the age of 18.

⁹³ Section 230(3) of the Act.

⁹⁴ Section 230(2) of the Act.

Cloud-gaming	Consumer-facing services and technologies that allow video games to be streamed over the internet from remote servers to a user's device.
Communications restrictions	Controls that restrict the use of voice, chat, messaging and related services.
Content harmful to children	Primary priority content (PPC), priority content (PC) and non-designated content (NDC). For further details see Ofcom's 'Protecting Children from Harms Online' report. ⁹⁵
Content warnings	Labels shown alongside an app store's listing that flag specific content, themes, features, or access risks a user may encounter within the app (e.g. violence, gambling, weapons).
Metadata	Data that provides users and app stores with context about an app's identity, purpose, functionality, and included content, such as descriptions, screenshots, categories, and age ratings.
First-party (1P)	Where a gateway (e.g. app store) or regulated service is from the same provider as the operating system on the user's device and any Original Equipment Manufacturer (OEM) bundled app stores that come installed with a device.
Neutral age gate	An age assurance mechanism designed to avoid bias or manipulation in the user's response, by using neutral wording and functionality, such as free-form entry of full date of birth, instead of defaults or leading choices.
Non-designated content (NDC)	Content, which is not Primary priority content or Priority content, of a kind which presents a material risk of significant harm to an appreciable number of children in the UK. ⁹⁶
Operating system (OS)	Pre-installed system-level software on devices that enables them to run programs and applications.
Parent account	An account of a user aged 18 and above, that has been designated as a parent or guardian and linked to a child account on an app store.
Parental controls	Parental controls are tools which enable a parent or guardian to exercise control over the types of experiences children are having online, including within an app store.
Primary priority content (PPC)	Pornographic content, and content promoting, encouraging or providing instructions for suicide, self-harm or eating disorders. ⁹⁷
Priority content	Content which is abusive or incites hatred, bullying content, and content which encourages, promotes, or provides instructions for violence, dangerous stunts and challenges, and self-administering harmful substances. ⁹⁸

⁹⁵ <https://www.ofcom.org.uk/siteassets/resources/documents/consultations/category-1-10-weeks/statement-protecting-children-from-harms-online/main-document/guidance-on-content-harmful-to-children.pdf?v=395445>. [Accessed on 31/03/2026]

⁹⁶ Section 60(2)(c) of the Act.

⁹⁷ Section 61 of the Act.

⁹⁸ Section 62 of the Act.

Private browsing	Web browser setting that prevents the user's device from saving browsing history, cookies, site data, and form information.
Recommendations and promotions	Apps / games surfaced to a user at various points during the user journey, based on a variety of factors (including store algorithms, a user's paid advertising opportunities). Recommendations and promotions most commonly appear while browsing or searching within an app store.
Regulated apps	Apps that contain a user-to-user service, search service, and / or provide pornographic content as regulated by the Online Safety Act.
Search autocomplete	An algorithmic functionality embedded in the search field of a search service in a store. It operates by anticipating a user's search query and suggesting possible related search requests ('predictive search suggestions'), based on a variety of factors (including a user's past queries and other user queries, locations, and trends) to help users make more relevant searches.
Search filtering	Filtering of certain kinds of content, e.g. explicit images, from search engine results.
Self-declaration of age	A process where the user is asked to provide their own age. This could be in the form of providing a date of birth to gain entry to a service or by ticking a box to confirm a user is over a minimum age threshold.
Sideloaded	Refers to methods of installing apps, games and other types of software on devices outside of 1P app stores. The 3P app stores covered in section '7.3 App stores', could be considered as an example of sideloading. Other methods of sideloading include direct download from publishers and other file-sharing services.
Store listing	The product page for an app or game that a user opens during discovery, which presents key information about the app or game such as description, screenshots, age rating, and user reviews.
Third-party (3P)	Where a gateway (e.g. app store) or regulated service is from a different provider to the operating system on the user's device, excluding any Original Equipment Manufacturer (OEM) bundled app stores that come installed with a device.
User reporting	User reports are a specific type of complaint about a service, store, or content, submitted through a reporting tool.
User-to-user services	An internet service on which users of the service can generate, upload and/or share content, which can then be encountered by other users of the service.
Virtual private network (VPN)	Security technology that establishes an encrypted connection between a user's device and a remote server over the public internet, protecting data privacy and masking the user's origin.
Web app	An application built using common open-web standards designed to operate through a web browser rather than being specific to a particular operating system.

Web filtering or blocking	Filtering or blocking against categories of websites or specific allow / deny lists of websites.
---------------------------	--

A2. Further Details on Methodology: User Journey Testing

A2.1 Devices

MTM conducted user journey testing on one device per store tested. All devices ran the latest available version of their operating system at the time of testing (December 2025). Where device set-up required a user's age (e.g. when configuring a new phone), the device was factory reset before testing each new user profile. All testing was conducted in the UK.

Store	Device	Operating system
Apple App Store	iPhone 12 mini	iOS 26.0.1
Google Play	Samsung Galaxy A17	Android 16
Samsung Galaxy Store	Samsung Galaxy A17	Android 16
PlayStation Store	PS5	25.07-12.20.00.05 [Release date 22/10/25]
Xbox Store	Xbox Series S	10.0.26100.6214 [Release date 12/3/25]
Nintendo eShop	Nintendo Switch	Version 21.1.0
Microsoft Store	Windows 11 Business (PC)	22621.4317
Amazon Appstore	Amazon Fire Tablet	FireOS 8.3.3.8
Steam	Windows 11 Business (PC)	22621.4317
Epic Games Store	Windows 11 Business (PC)	22621.4317
Uptodown Market	Samsung Galaxy A17	Android 16
Aptoide	Samsung Galaxy A17	Android 16

Device details and operating systems:

Account set up

MTM created new accounts for five different age groups: 5, 12, 14, 16, and 18. The same birthdates were used across all app stores:

- Age 5: 15/09/2020
- Age 12: 15/09/2013
- Age 14: 15/09/2011
- Age 16: 15/09/2009
- Age 18: 15/09/2007

Where app stores did not require a date of birth (e.g. Steam), MTM tested only the relevant age groups (e.g. 13+ on Steam).

All accounts were created using pseudonyms. MTM created new email addresses for each age group and, where possible, reused the same age-group email address across multiple app stores. For example, the email address used for the 5-year-old account was used to register accounts on both the Samsung Galaxy Store and Nintendo eShop. Where app stores required an email address within their own domain (e.g. Google Play), MTM created new email accounts for that purpose.

Where phone-number verification was required during device set-up or account creation, MTM used a new phone number for each avatar. Each SIM card was newly purchased and linked to a single avatar (e.g. one number associated with the 5-year-old user).

The 18-year-old user account was used as the parent email address for app stores that required parent or guardian account details.

A2.2 Rationale for the apps covered in User Journey Testing

Our user journeys focus on a single game or app per store, tested across all avatar age groups. Each app has been chosen based on:

- Relevance to store and device: Gaming app stores focused on games, while other mobile and PC stores focused on apps.
- Popularity: Games or apps are chosen based on popularity within the stores themselves (e.g. top downloads, top search result).
- User-to-user functionality: Apps or games with user-to-user functionality were prioritized (applies to all but one of the apps or games tested).
- Age rating: All selected apps or games were rated 18+ which was used as a proxy for regulated apps that may contain content that is potentially harmful to children. (this does not mean that these apps do contain content that is potentially harmful to children in reality). This also ensured we could test the store's age-based restrictions for users under 18.

Store	App or Game to be tested
Apple App Store	Tinder (17+) ⁹⁹
Google Play Store	Tinder (18+)
Samsung Galaxy Store	Tinder (18+)
PlayStation Store	Call of Duty: Warzone (2022 release) (18+)
Xbox Store	Call of Duty: Warzone (2022 release) (18+)
Nintendo eShop	Warframe (18+)
Microsoft Store	Reddit (18+)

⁹⁹ User testing was completed in December 2025, while Apple was rolling out an updated age-rating system. At that time, Apple's highest age rating was 17+. The new system has since launched in the UK (as of 22/02/2026), where the highest rating is now 18+. As of February 2026, Tinder is rated 18+ on the UK Apple App Store. <https://developer.apple.com/news/?id=ks775ehf>. [Accessed on 22/02/2026]

Amazon Appstore	Sexy Girls (Adult)
Steam	Call of Duty: Warzone (2022 release) (18+)
Epic Games Store	Warframe (18+)
Uptodown Market	Dating for Android (18+)
Aptoide	Kik (18+)

Further details on apps:

- Tinder – Includes user-to-user capabilities; Reached 3% (1.5 million) of UK online adults in May 2025.¹⁰⁰
- Call of Duty: Warzone – Includes user-to-user capabilities; historically a popular title in the UK and one of the top streamed titles on Twitch.¹⁰¹
- Reddit – Includes user-to-user capabilities; Estimated audience reach of 4% 231k children in the UK aged 8-14 in a month.¹⁰²
- Warframe – Includes user-to-user capabilities; Free-to-play game with more than 38m users worldwide.¹⁰³
- Sexy Girls – First search result for “porn” on Amazon Appstore; based on review of app store listing appears to include access to PPC.
- Dating for Android – Includes user-to-user capabilities; First search result for “dating app” on Uptodown market; Estimated 36.3k downloads.¹⁰⁴
- Kik – Includes user-to-user capabilities; Top search result for chat-related app on Aptoide; Estimated 100m+ downloads on Aptoide;¹⁰⁵ Flagged as potentially dangerous site for children in the UK by online safety website.¹⁰⁶

A2.3 Rationale for apps covered in metadata analysis

The metadata analysis compared the age ratings and content warnings for eight apps or games across the tested app stores. The apps and games were selected based on:

- Availability across twelve prioritized app stores
- App type (e.g. game, social media, etc.)
- Age rating of the app or game
- User to user and / or search capabilities in the app
- Popularity with children, and where relevant, adults in the UK

App Store	YouTube	Roblox	TikTok	Hinge	GTA V	Apex Legends	Google Search	Bing
Apple App store	✓	✓	✓	✓	X	X	✓	✓
Google Play Store	✓	✓	✓	✓	X	X	✓	✓
Samsung Galaxy Store	X	✓	✓	X	X	X	X	X

¹⁰⁰ Ipsos, Ipsos iris Online Audience Measurement Service, Tinder app, 18+, UK online adults, May 2025.

¹⁰¹ <https://www.uswitch.com/broadband/studies/online-gaming-statistics/> [Accessed on 14/09/2026]

¹⁰² Ofcom, [Children's Passive Online Measurement study](#), wave 1, age: 8-14 internet users, each panellist completed 28 consecutive days of study, 2025. [Accessed on 14/01/2026]

¹⁰³ <https://variety.com/2018/gaming/news/warframe-nintendo-switch-1202868157/> [Accessed on 14/01/2026]

¹⁰⁴ <https://dating.en.uptodown.com/android> [Accessed on 14/01/2026]

¹⁰⁵ https://kik.en.aptoide.com/app?utm_source=aptoide&utm_medium=store_placement&utm_campaign=organic-discovery&utm_content=search [Accessed on 14/01/2026]

¹⁰⁶ <https://www.internetmatters.org/advice/apps-and-platforms/social-media/kik/> [Accessed on 14/01/2026]

PlayStation Store	✓	✓	X	X	✓	✓	X	X
Xbox Store	✓	✓	X	X	✓	✓	X	X
Nintendo eShop	✓	X	X	X	X	✓	X	X
Microsoft Store	X	✓	✓	X	✓	X	X	✓
Amazon Appstore	X	✓	✓	X	X	X	X	X
Steam	X	X	X	X	✓	✓	X	X
Epic Games Store	X	X	X	X	✓	✓	X	X
Uptodown Market	✓	✓	✓	✓	X	✓	✓	✓
Aptoide	✓	✓	✓	X	X	X	X	✓

Further details on apps:

- YouTube - Reaches 81% (estimated 4.6 million) of UK 8-14-year-olds in a month¹⁰⁷
- Roblox - Reaches 60% (estimated 3.4 million) of UK 8-14-year-olds in a month¹⁰⁸
- TikTok - Reaches 47% (estimated 2.7 million) of UK 8-14-year-olds in a month¹⁰⁹
- Hinge - Reached 3% (1.5 million) of UK online adults in May 2025¹¹⁰
- Grand Theft Auto V – A popular game in the UK in Q3 2025;¹¹¹ Reportedly played by underage children in the UK¹¹²
- Apex Legends – A popular game and ranked 8 on Steam in terms of DAU.¹¹³

¹⁰⁷ Ofcom, [Children's Passive Online Measurement study](#), wave 1, age: 8-14 internet users, each panellist completed 28 consecutive days of study, 2025. [Accessed on 06/01/2026]

¹⁰⁸ Ofcom, [Children's Passive Online Measurement study](#), wave 1, age: 8-14 internet users, each panellist completed 28 consecutive days of study, 2025. [Accessed on 06/01/2026]

¹⁰⁹ Ofcom, [Children's Passive Online Measurement study](#), wave 1, age: 8-14 internet users, each panellist completed 28 consecutive days of study, 2025. [Accessed on 06/01/2026]

¹¹⁰ Ipsos, Ipsos iris Online Audience Measurement Service, Hinge app, 18+, UK online adults, May 2025.

¹¹¹ YouGov, The most famous video games (Q3 2025). <https://yougov.co.uk/ratings/technology/fame/video-games/all>. [Accessed on 06/01/2026]

¹¹² YouGov, Seven in ten British GTA gamers first played when they were underage (2023). <https://yougov.com/en-gb/articles/48049-seven-in-ten-gta-gamers-first-played-when-they-were-underage>. [Accessed on 06/01/2026]

¹¹³ SteamDB, Apex Legends. https://steamdb.info/app/1172470/charts/#:~:text=Here's%20some%20information%20about%20the%20number%20of,positive%20reviews%20*%20333%2C146%2032.6%25%20negative%20reviews. [Accessed on 06/01/2026]