Developer Programme Policy

(effective as of 6 March 2024, unless otherwise stated)

Let's build the world's most trusted source for apps and games

Your innovation is what drives our shared success, but with it comes responsibility. These Developer Programme Policies, along with the Developer Distribution Agreement, ensure that together we continue to deliver the world's most innovative and trusted apps to over a billion people through Google Play. We invite you to explore our policies below.

Restricted content

People from all over the world use Google Play to access apps and games every day. Before submitting an app, ask yourself if your app is appropriate for Google Play and compliant with local laws.

Child endangerment

Apps that do not prohibit users from creating, uploading or distributing content that facilitates the exploitation or abuse of children will be subject to immediate removal from Google Play. This includes all child sexual abuse material. To report content on a Google product that may exploit a child, click **Report abuse** . If you find content elsewhere on the Internet, please contact the appropriate agency in your country directly.

We prohibit the use of apps to endanger children. This includes, but is not limited to the use of apps to promote predatory behaviour towards children, such as:

- Inappropriate interaction targeted at a child (for example, groping or caressing).
- Child grooming (for example, befriending a child online to facilitate, either online or offline, sexual contact and/or exchanging sexual imagery with that child).
- Sexualisation of a minor (for example, imagery that depicts, encourages or promotes the sexual abuse of children or the portrayal of children in a manner that could result in the sexual exploitation of children).
- Sextortion (for example, threatening or blackmailing a child by using real or alleged access to a child's intimate images).
- Trafficking of a child (for example, advertising or solicitation of a child for commercial sexual exploitation).

We will take appropriate action, which may include reporting to the National Centre for Missing and Exploited Children, if we become aware of content with child sexual abuse material. If you believe that a child is in danger of or has been subject to abuse, exploitation or trafficking, please contact your local law enforcement and contact a child safety organisation listed here .

In addition, apps that appeal to children but contain adult themes are not allowed, including, but not limited to:

- Apps with excessive violence, blood and gore.
- Apps that depict or encourage harmful and dangerous activities.

We also don't allow apps that promote negative body or self-image, including apps that depict for entertainment purposes plastic surgery, weight loss and other cosmetic adjustments to a person's physical appearance.

Inappropriate Content

To ensure that Google Play remains a safe and respectful platform, we've created standards defining and prohibiting content that is harmful or inappropriate for our users.

Sexual content and profanity

We don't allow apps that contain or promote sexual content or profanity, including pornography, or any content or services intended to be sexually gratifying. We don’t allow apps or app content that appear to promote or solicit a sexual act in exchange for compensation. We don’t allow apps that contain or promote content associated with sexually predatory behaviour, or distribute non-consensual sexual content. Content that contains nudity may be allowed if the primary purpose is educational, documentary, scientific or artistic, and is not gratuitous.

If an app contains content that violates this policy but that content is deemed appropriate in a particular region, the app may be available to users in that region, but will remain unavailable to users in other regions.

To ensure that Google Play remains a safe and respectful platform, we've created standards defining and prohibiting content that is harmful or inappropriate for our users.

- Depictions of sexual nudity, or sexually suggestive poses in which the subject is nude, blurred or minimally clothed, and/or where the clothing would not be acceptable in an appropriate public context.
- Depictions, animations or illustrations of sex acts, or sexually suggestive poses or the sexual depiction of body parts.
- Content that depicts or are functionally sexual aids, sex guides, illegal sexual themes and fetishes.
- Content that is lewd or profane – including but not limited to content which may contain profanity, slurs, explicit text or adult/sexual keywords in the store listing or in-app.
- Content that depicts, describes or encourages bestiality.
- Apps that promote sex-related entertainment, escort services or other services that may be interpreted as providing or soliciting sexual acts in exchange for compensation, including, but not limited to compensated dating or sexual arrangements where one participant is expected or implied to provide money, gifts or financial support to another participant ('sugar dating').
- Apps that degrade or objectify people, such as apps that claim to undress people or see through clothing, even if labelled as prank or entertainment apps.
- Content or behaviour that attempts to threaten or exploit people in a sexual manner, such as creepshots, hidden camera, non-consensual sexual content created via deepfake or similar technology or assault content.

Hate speech

We don't allow apps that promote violence or incite hatred against individuals or groups based on race or ethnic origin, religion, disability, age, nationality, veteran status, sexual orientation, gender, gender identity, caste, immigration status or any other characteristic that is associated with systemic discrimination or marginalisation.

Apps that contain EDSA (educational, documentary, scientific or artistic) content related to Nazis may be blocked in certain countries, in accordance with local laws and regulations.

To ensure that Google Play remains a safe and respectful platform, we've created standards defining and prohibiting content that is harmful or inappropriate for our users.

- Content or speech asserting that a protected group is inhuman, inferior or worthy of being hated.
- Apps that contain hateful slurs, stereotypes or theories about a protected group possessing negative characteristics (for example, malicious, corrupt, evil, etc.), or that explicitly or implicitly claim that the group is a threat.

- Content or speech trying to encourage others to believe that people should be hated or discriminated against because they are a member of a protected group.
- Content that promotes hate symbols such as flags, symbols, insignias, paraphernalia or behaviours associated with hate groups.

Violence

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

To ensure that Google Play remains a safe and respectful platform, we've created standards defining and prohibiting content that is harmful or inappropriate for our users.

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

Terrorist content

We don't permit terrorist organisations to publish apps on Google Play for any purpose, including recruitment.

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

Dangerous organisations and movements

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

We don’t allow apps with content related to planning, preparing or glorifying violence against civilians. If your app includes such content for an EDSA purpose, that content must be provided alongside the relevant EDSA context.

Sensitive events

We don't allow apps that capitalise on or are insensitive towards a sensitive event with significant social, cultural or political impact, such as civil emergencies, natural disasters, public health emergencies, conflicts, deaths or other tragic events. Apps with content related to a sensitive event are generally allowed if that content has EDSA (educational, documentary, scientific or artistic) value or intends to alert users to or raise awareness for the sensitive event.

To ensure that Google Play remains a safe and respectful platform, we've created standards defining and prohibiting content that is harmful or inappropriate for our users.

- Lacking sensitivity regarding the death of a real person or group of people due to suicide, overdose, natural causes, etc.
- Denying the occurrence of a well-documented, major tragic event.
- Appearing to profit from a sensitive event with no discernible benefit to the victims.

Bullying and harassment

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

To ensure that Google Play remains a safe and respectful platform, we've created standards defining and prohibiting content that is harmful or inappropriate for our users.

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

Dangerous products

We don't allow apps that facilitate the sale of explosives, firearms, ammunition or certain firearms accessories.

- Restricted accessories include those that enable a firearm to simulate automatic fire or convert a firearm to automatic fire (for example, bump stocks, gatling triggers, drop-in auto sears, conversion kits), and magazines or belts carrying more than 30 rounds.

We don't allow apps that provide instructions for the manufacture of explosives, firearms, ammunition, restricted firearm accessories or other weapons. This includes instructions on how to convert a firearm to automatic, or simulated automatic, firing capabilities.

Marijuana

We don't allow apps that facilitate the sale of marijuana or marijuana products, regardless of legality.

To ensure that Google Play remains a safe and respectful platform, we've created standards defining and prohibiting content that is harmful or inappropriate for our users.

- Allowing users to order marijuana through an in-app shopping basket feature.
- Assisting users in arranging delivery or collection of marijuana.
- Facilitating the sale of products containing THC (tetrahydrocannabinol), including products such as CBD oils containing THC.

Tobacco and alcohol

We don't allow apps that facilitate the sale of tobacco (including e-cigarettes and vape pens) or encourage the illegal or inappropriate use of alcohol or tobacco.

Additional information

- Depicting or encouraging the use or sale of alcohol or tobacco to minors is not allowed.
- Implying that consuming tobacco can improve social, sexual, professional, intellectual or athletic standing is not allowed.
- Portraying excessive drinking favourably, including the favourable portrayal of excessive, binge or competition drinking is not allowed.
- Advertisements, promotions or the prominent feature of tobacco products (including ads, banners, categories and links to tobacco-selling sites) are not allowed.
- We may allow the limited sale of tobacco products in food/grocery delivery apps, in certain regions, and subject to age-gating safeguards (such as ID check at delivery).

Financial services

We don't allow apps that expose users to deceptive or harmful financial products and services.

For the purposes of this policy, we consider financial products and services to be those related to the management or investment of money and cryptocurrencies, including personalised advice.

If your app contains or promotes financial products and services, you must comply with regional and local regulations for any region or country that your app targets—for example, include specific disclosures required by local law.

Any app that contains any financial features must complete the Financial features declaration form within Play Console.

Binary options

We don't allow apps that provide users with the ability to trade binary options.

Personal loans

We define personal loans as lending money from one individual, organisation or entity to an individual consumer on a non-recurring basis, not for the purpose of financing the purchase of a fixed asset or education. Personal loan consumers require information about the quality, features, fees, repayment schedule, risks and benefits of loan products in order to make informed decisions about whether to undertake the loan.

- Examples: Personal loans, payday loans, peer-to-peer loans, title loans
- Examples not included: Mortgages, car loans, revolving lines of credit (such as credit cards, personal lines of credit)

Apps that provide personal loans, including but not limited to apps which offer loans directly, lead generators and those who connect consumers with third-party lenders, must have the app category set to 'Finance' in Play Console and disclose the following information in the app metadata:

- Minimum and maximum period for repayment
- Maximum annual percentage rate (APR), which generally includes interest rate plus fees and other costs for a year, or similar other rate calculated consistently with local law
- A representative example of the total cost of the loan, including the principal and all applicable fees
- A privacy policy that comprehensively discloses the access, collection, use and sharing of personal and sensitive user data, subject to the restrictions outlined in this policy

We do not allow apps that promote personal loans which require repayment in full in 60 days or less from the date that the loan is issued (we refer to these as 'short-term personal loans').

We must be able to establish a connection between your developer account and any provided licences or documentation proving your ability to service personal loans. Additional information or documents may be requested to confirm your account is in compliance with all local laws and regulations.

Personal loan apps or apps with the primary purpose of facilitating access to personal loans (for example, lead generators or facilitators) are prohibited from accessing sensitive data, such as photos and contacts. The following permissions are prohibited:

- Read_external_storage
- Read_media_images
- Read_contacts
- Access_fine_location
- Read_phone_numbers
- Read_media_videos
- Query_all_packages
- Write_external_storage

Apps that utilise sensitive information or APIs are subject to additional restrictions and requirements. Please see the Permissions policy for additional information.

High APR personal loans

In the United States, we do not allow apps for personal loans where the Annual Percentage Rate (APR) is 36% or higher. Apps for personal loans in the United States must display their maximum APR, calculated consistently with the Truth in Lending Act (TILA) .

This policy applies to apps which offer loans directly, lead generators, and those who connect consumers with third-party lenders.

Country-specific requirements

Personal loan apps targeting the listed countries must comply with additional requirements and provide supplementary documentation as part of the financial features declaration within Play Console. You must, upon Google Play's request, provide additional information or documents relating to your compliance with the applicable regulatory and licensing requirements.

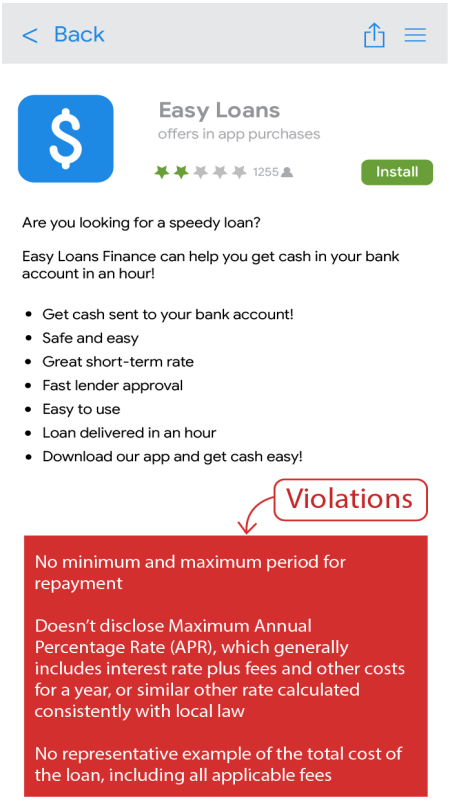
1. **India**
   - If you are licensed by the Reserve Bank of India (RBI) to provide personal loans, you must submit a copy of your licence for our review.
   - If you are not directly engaged in money lending activities and are only providing a platform to facilitate money lending by registered non-banking financial companies (NBFCs) or banks to users, you will need to accurately reflect this in the declaration.
     - In addition, the names of all registered NBFCs and banks must be prominently disclosed in your app's description.
2. **Indonesia**
   - If your app is engaged in the activity of information technology-based money lending services in accordance with OJK regulation no. 77/POJK.01/2016 (as may be amended from time to time), you must submit a copy of your valid licence for our review.
3. **Philippines**
   - All financing and lending companies offering loans via online lending platforms (OLP) must obtain an SEC registration number and a certificate of authority (CA) number from the Philippines Securities and Exchanges Commission (PSEC).
     - In addition, you must disclose your corporate name, business name, PSEC registration number and certificate of authority to operate a financing/lending company (CA) in your app's description.
   - Apps engaged in lending-based crowdfunding activities, such as peer-to-peer (P2P) lending, or as defined under the rules and regulations governing crowdfunding (CF rules), must process transactions through PSEC-registered CF intermediaries.
4. **Nigeria**
   - Digital money lenders (DML) must adhere to and complete the LIMITED INTERIM REGULATORY/REGISTRATION FRAMEWORK AND GUIDELINES FOR DIGITAL LENDING, 2022 (as may be amended from time to time) by the Federal Competition and Consumer Protection Commission (FCCPC) of Nigeria and obtain a verifiable approval letter from the FCCPC.
   - Loan aggregators must provide documentation and/or certification for digital lending services and contact details for every partnered DML.
5. **Kenya**
   - Digital credit providers (DCP) should complete the DCP registration process and obtain a licence from the Central Bank of Kenya (CBK). You must provide a copy of your licence from the CBK as part of your declaration.
   - If you are not directly engaged in money lending activities and are only providing a platform to facilitate money lending by registered DCP(s) to users, you will need to accurately reflect this in the declaration and provide a copy of the DCP licence of your respective partner(s).
   - Currently, we only accept declarations and licences from entities published under the Directory of Digital Credit Providers on the official website of the CBK.
6. **Pakistan**
   - Each non-banking finance company (NBFC) lender can only publish one digital lending app (DLA). Developers who attempt to publish more than one DLA per NBFC risk the termination of

their developer account and any other associated accounts.

- You must submit proof of approval from the SECP to offer or facilitate digital lending services in Pakistan.

7. **Thailand**
   - Personal loan apps targeting Thailand, with interest rates at or above 15%, must obtain a valid licence from the Bank of Thailand (BoT) or the Ministry of Finance (MoF). Developers must provide documentation that proves their ability to provide or facilitate personal loans in Thailand. This documentation should include:
     - A copy of their licence issued by the Bank of Thailand to operate as a personal loan provider or nano finance organisation.
     - A copy of their Pico-finance business licence issued by the Ministry of Finance to operate as a Pico or Pico-plus lender.

To ensure that Google Play remains a safe and respectful platform, we've created standards defining and prohibiting content that is harmful or inappropriate for our users.



Real money gambling, games and contests

We allow real money gambling apps, ads related to real money gambling, loyalty programmes with gamified outcomes and daily fantasy sports apps that meet certain requirements.

Gambling apps

Subject to restrictions and compliance with all Google Play policies, we allow apps that enable or facilitate online gambling in select countries, as long as the developer completes the application process for gambling apps being distributed on Google Play, is an approved governmental operator and/or is registered as a licensed operator with the appropriate governmental gambling authority in the specified country, and provides a valid operating licence in the specified country for the type of online gambling product that they want to offer.

We only allow valid licensed or authorised gambling apps that have the following types of online gambling products

- Online casino games
- Sports betting
- Horse racing (where regulated and licensed separately from sports betting)
- Lotteries
- Daily fantasy sports

Eligible apps must meet the following requirements:

- Developer must successfully complete the application process in order to distribute the app on Google Play;
- App must comply with all applicable laws and industry standards for each country in which it is distributed;
- Developer must have a valid gambling licence for each country or state/territory in which the app is distributed;
- Developer must not offer a type of gambling product that exceeds the scope of its gambling licence;
- App must prevent under-age users from using the app;
- App must prevent access and use from countries, states/territories or the geographic areas not covered by the developer-provided gambling licence;
- App must NOT be purchasable as a paid app on Google Play, nor use Google Play In-App Billing;
- App must be free to download and install from the Google Play Store;
- App must be rated AO (Adult Only) or IARC equivalent; and
- App and its app listing must clearly display information about responsible gambling.

Other real-money games, contests and tournament apps

For all other apps that do not meet the eligibility requirements for gambling apps noted above and are not included in the 'other real-money game pilots' noted below, we don't allow content or services that enable or facilitate users' ability to wager, stake or participate using real money (including in-app items purchased with money) to obtain a prize of real world monetary value. This includes, but is not limited to, online casinos, sports betting, lotteries and games that accept money and offer prizes of cash or other real-world value (except programmes permitted under the gamified loyalty programmes requirements described below).

Examples of violations

- Games that accept money in exchange for an opportunity to win a physical or monetary prize
- Apps that have navigational elements or features (for example, menu items, tabs, buttons, WebViews, etc.) that provide a 'call to action' to wager, stake or participate in real-money games, contests or tournaments using real money, such as apps that invite users to 'BET!' or 'REGISTER!' or 'COMPETE!' in a tournament for a chance to win a cash prize.
- Apps that accept or manage wagers, in-app currencies, winnings or deposits in order to gamble for, or obtain a physical or monetary prize.

Other real-money game pilots

We may occasionally conduct limited-time pilots for certain types of real-money gaming in selected regions. For details, refer to this Help Centre page. The online crane games pilot in Japan ended on 11 July 2023. Effective 12 July 2023, online crane game apps may be listed on Google Play globally subject to applicable law and certain requirements.

Gamified loyalty programmes

Where permitted by law and not subject to additional gambling or gaming licensing requirements, we allow loyalty programmes that reward users with real-world prizes or monetary equivalent, subject to the following Play Store eligibility requirements:

For all apps (games and non-games):

- Loyalty programme benefits, perks or rewards must be clearly supplementary and subordinate to any qualifying monetary transaction within the app (where the qualifying monetary transaction must be a genuine separate transaction to provide goods or services independent of the loyalty programme) and may not be subject to purchase nor tied to any mode of exchange otherwise in violation of the Real-money gambling, games and contests policy restrictions.
  - For example, no portion of the qualifying monetary transaction may represent a fee or wager to participate in the loyalty programme, and the qualifying monetary transaction must not result in the purchase of goods or services above its usual price.

For Game apps:

- Loyalty points or rewards with benefits, perks or rewards associated with a qualifying monetary transaction may only be awarded and redeemed on a fixed ratio basis, where the ratio is documented conspicuously in the app and also within the publicly available official rules for the programme, and the earning of benefits or redemptive value may **not** be wagered, awarded or exponentiated by game performance or chance-based outcomes.

For non-game apps:

- Loyalty points or rewards may be tied to a contest or chance-based outcomes if they fulfil the requirements noted below. Loyalty programmes with benefits, perks or rewards associated with a qualifying monetary transaction must:
  - Publish official rules for the programme within the app.
  - For programmes involving variable, chance-based or randomised reward systems, disclose within the official terms for the programme: 1) the odds for any reward programmes which use fixed odds to determine rewards; and 2) the selection method (for example, variables used to determine the reward) for all other such programmes.
  - Specify a fixed number of winners, fixed entry deadline and prize award date, per promotion, within the official terms of a programme offering drawings, sweepstakes or other similar style promotions.
  - Document any fixed ratio for loyalty point or loyalty reward accrual and redemption conspicuously in the app and also within the official terms of the programme.

Type of app with loyalty programme	**Loyalty gamification and variable rewards**	**Loyalty rewards based upon a fixed ratio/schedule**	**Terms and Conditions of loyalty programme required**	**T&Cs must disclose odds or selection method of any chance-based loyalty programme**
Game	Not allowed	Allowed	Required	N/A (game apps not allowed to have chance-based elements in loyalty programmes)
Non-game	Allowed	Allowed	Required	Required

Ads for gambling or real-money games, contests and tournaments within Play-distributed apps

We allow apps that have ads which promote gambling, real-money games, contests and tournaments if they meet the following requirements:

- The app and ad (including advertisers) must comply with all applicable laws and industry standards for any location where the ad is displayed;
- Ad must meet all applicable local ad licensing requirements for all gambling-related products and services being promoted;
- App must not display a gambling ad to individuals known to be under the age of 18;
- App must not be enrolled in the Designed for Families programme;
- App must not target individuals under the age of 18;
- If advertising a gambling app (as defined above), the ad must clearly display information about responsible gambling on its landing page, the advertised app listing itself or within the app;
- App must not provide simulated gambling content (for example, social casino apps, apps with virtual slot machines);
- App must not provide gambling or real-money game, lottery or tournament support or companion functionality (for example, functionality that assists with wagering, payouts, sports score/odds/performance tracking or management of participation funds);
- App content must not promote or direct users to gambling or real-money games, lotteries or tournament services

Only apps that meet all of these requirements in the section listed (above) may include ads for gambling or real-money games, lotteries or tournaments. Accepted gambling apps (as defined above), or accepted daily fantasy sports apps (as defined below) which meet requirements 1–6 above, may include ads for gambling or real-money games, lotteries or tournaments.

Examples of violations

- An app that's designed for under-age users and shows an ad promoting gambling services
- A simulated casino game that promotes or directs users to real-money casinos
- A dedicated sports odds tracker app containing integrated gambling ads linking to a sports betting site
- Apps that have gambling ads that violate our deceptive ads policy, such as ads that appear to users as buttons, icons or other interactive in-app elements

Daily fantasy sport (DFS) apps

We only allow daily fantasy sports (DFS) apps, as defined by applicable local law, if they meet the following requirements:

- App is either 1) only distributed in the United States, or 2) eligible under the gambling apps requirements and application process noted above for non-US-based countries;
- Developer must successfully complete the DFS application process and be accepted in order to distribute the app on Play;
- App must comply with all applicable laws and industry standards for the countries in which it is distributed;
- App must prevent under-age users from wagering or conducting monetary transactions within the app;
- App must NOT be purchasable as a paid app on Google Play, nor use Google Play In-App Billing;
- App must be free to download and install from the Store;
- App must be rated AO (Adult Only) or IARC equivalent;
- App and its app listing must clearly display information about responsible gambling;
- App must comply with all applicable laws and industry standards for any US state or US territory in which it is distributed;
- Developer must have a valid licence for each US state or US territory in which a licence is required for daily fantasy sport apps;

- App must prevent use from US states or US territories in which the developer does not hold a licence required for daily fantasy sport apps; and
- App must prevent use from US states or US territories where daily fantasy sport apps are not legal.

Illegal activities

We don’t allow apps that facilitate or promote illegal activities.

To ensure that Google Play remains a safe and respectful platform, we've created standards defining and prohibiting content that is harmful or inappropriate for our users.

- Facilitating the sale or purchase of illegal drugs.
- Depicting or encouraging the use or sale of drugs, alcohol or tobacco by minors.
- Instructions for growing or manufacturing illegal drugs.

User-generated content

User-generated content (UGC) is content that users contribute to an app, and which is visible to or accessible by at least a subset of the app's users.

Apps that contain or feature UGC, including apps which are specialised browsers or clients to direct users to a UGC platform, must implement robust, effective and ongoing UGC moderation that:

- Requires that users accept the app's Terms of Use and/or user policy before users can create or upload UGC;
- Defines objectionable content and behaviours (in a way that complies with Google Play Developer Programme Policies), and prohibits them in the app’s Terms of Use or user policies;
- Conducts UGC moderation, as is reasonable and consistent with the type of UGC hosted by the app. This includes providing an in-app system for reporting and blocking objectionable UGC and users, and taking action against UGC or users where appropriate. Different UGC experiences may require different moderation efforts. For example:
  - Apps featuring UGC that identify a specified set of users through means such as user verification or offline registration (for example, apps exclusively used within a specific school or company, etc.) must provide in-app functionality to report content and users.
  - UGC features that enable 1:1 user interaction with specific users (for example, direct messaging, tagging, mentioning, etc.) must provide an in-app functionality for blocking users.
  - Apps that provide access to publicly accessible UGC, such as social networking apps and blogger apps, must implement in-app functionality to report users and content and to block users.
  - In the case of augmented reality (AR) apps, UGC moderation (including the in-app reporting system) must account for both objectionable AR UGC (for example, a sexually explicit AR image) and sensitive AR anchoring location (for example, AR content anchored to a restricted area, such as a military base, or a private property where AR anchoring may cause issues for the property owner).
- Provides safeguards to prevent in-app monetisation from encouraging objectionable user behaviour.

Incidental sexual content

Sexual content is considered 'incidental' if it appears in a UGC app that (1) provides access to primarily non-sexual content, and (2) does not actively promote or recommend sexual content. Sexual content defined as illegal by applicable law and child endangerment content is not considered 'incidental' and is not permitted.

UGC apps may contain incidental sexual content if all of the following requirements are met:

- Such content is hidden by default behind filters that require at least two user actions in order to completely disable (for example, behind an obfuscating interstitial or precluded from view by default unless 'safe search' is disabled).
- Children, as defined in the families policy, are explicitly prohibited from accessing your app using age screening systems, such as a neutral age screen or an appropriate system as defined by applicable law.
- Your app provides accurate responses to the content rating questionnaire regarding UGC, as required by the content ratings policy.

Apps whose primary purpose is featuring objectionable UGC will be removed from Google Play. Similarly, apps that end up being used primarily for hosting objectionable UGC, or that develop a reputation among users of being a place where such content thrives, will also be removed from Google Play.

To ensure that Google Play remains a safe and respectful platform, we've created standards defining and prohibiting content that is harmful or inappropriate for our users.

- Promoting sexually explicit user-generated content, including implementing or permitting paid features that principally encourage the sharing of objectionable content.
- Apps with user-generated content (UGC) that lack sufficient safeguards against threats, harassment or bullying, particularly toward minors.
- Posts, comments or photos within an app that are primarily intended to harass or single out another person for abuse, malicious attack or ridicule.
- Apps that continually fail to address user complaints about objectionable content.

Health content and services

We don't allow apps that expose users to harmful health content and services.

If your app contains or promotes health content and services, you must ensure that your app is compliant with any applicable laws and regulations.

Prescription drugs

We do not allow apps that facilitate the sale or purchase of prescription drugs without a prescription.

Unapproved substances

Google Play doesn't allow apps that promote or sell unapproved substances, irrespective of any claims of legality.

To ensure that Google Play remains a safe and respectful platform, we've created standards defining and prohibiting content that is harmful or inappropriate for our users.

- All items on this non-exhaustive list of prohibited pharmaceuticals and supplements .
- Products that contain ephedra.
- Products containing human chorionic gonadotropin (hCG) in relation to weight loss or weight control, or when promoted in conjunction with anabolic steroids.
- Herbal and dietary supplements with active pharmaceutical or dangerous ingredients.
- False or misleading health claims, including claims implying that a product is as effective as prescription drugs or controlled substances.
- Non-government-approved products that are marketed in a way that implies that they're safe or effective for use in preventing, curing or treating a particular disease or ailment.
- Products that have been subject to any government or regulatory action or warning.

- Products with names that are confusingly similar to an unapproved pharmaceutical or supplement or controlled substance.

For additional information on the unapproved or misleading pharmaceuticals and supplements that we monitor, please visit www.legitscript.com .

Health misinformation

We don't allow apps containing misleading health claims that contradict existing medical consensus or can cause harm to users.

To ensure that Google Play remains a safe and respectful platform, we've created standards defining and prohibiting content that is harmful or inappropriate for our users.

- Misleading claims about vaccines, such as 'vaccines can alter one's DNA'.
- Advocacy of harmful, unapproved treatments.
- Advocacy of other harmful health practices, such as conversion therapy.

COVID-19 restrictions

Apps must follow the Requirements for coronavirus disease 2019 (COVID-19) apps article .

Medical functionalities

We don't allow apps that feature medical or health-related functionalities that are misleading or potentially harmful. For example, we do not allow apps that claim to have oximetry functionality that is solely app-based. Oximeter apps must be supported by external hardware, wearable or dedicated smartphone sensors designed to support oximetry functionality. These supported apps must also contain disclaimers in the metadata stating that they are not intended for medical use, are only designed for general fitness and wellness purposes, are not a medical device, and must properly disclose the compatible hardware model/device model.

Payments – clinical services

Transactions involving regulated clinical services should not use Google Play's billing system. For more information, see Understanding Google Play's payments policy .

Health Connect data

Data accessed through Health Connect permissions is regarded as personal and sensitive user data subject to the User data policy, and is subjected to additional requirements .

Blockchain-based content

As blockchain technology continues to rapidly evolve, we aim to provide a platform for developers to thrive with innovation and build more enriched, immersive experiences for users.

For the purposes of this policy, we consider blockchain-based content to be tokenised digital assets secured on a blockchain. If your app contains blockchain-based content, you must comply with these requirements.

Cryptocurrency exchanges and software wallets

The purchase, holding or exchange of cryptocurrencies should be conducted through certified services in regulated jurisdictions.

You must also comply with applicable regulations for any region or country that your app targets and avoid publishing your app where your products and services are prohibited. Google Play may request you to provide additional information or documents regarding your compliance with any applicable regulatory or licensing requirements.

Cryptomining

We don't allow apps that mine cryptocurrency on devices. We permit apps that remotely manage the mining of cryptocurrency.

Transparency requirements for distributing tokenised digital assets

If your app sells or enables users to earn tokenised digital assets, you must declare this via the Financial features declaration form on the app content page in Play Console.

When creating an in-app product, you must indicate in the product details that it represents a tokenised digital asset. For additional guidance, see Create an in-app product.

You may not promote or glamourise any potential earnings from playing or trading activities.

Additional requirements for NFT gamification

As required by Google Play's Real-money gambling, games and contests policy, gambling apps that integrate tokenised digital assets, such as NFTs, should complete the application process.

For all other apps which do not meet the eligibility requirements for gambling apps and are not included in Other real-money game pilots, anything of monetary value should not be accepted in exchange for a chance to obtain an NFT of unknown value. NFTs bought by users should be consumed or used in the game to enhance a user's experience or aid users in advancing the game. NFTs must not be used to wager or stake in exchange for the opportunity to win prizes of real-world monetary value (including other NFTs).

To ensure that Google Play remains a safe and respectful platform, we've created standards defining and prohibiting content that is harmful or inappropriate for our users.

- Apps that sell bundles of NFTs without disclosing the specific contents and values of the NFTs.
- Pay-to-play social casino games, such as slot machines, that reward NFTs.

AI-generated content

As generative AI models become more widely available to developers, you may be incorporating these models into your apps to increase engagement and improve user experience. Google Play wants to help ensure that AI-generated content is safe for all users and that user feedback is incorporated to enable responsible innovation.

AI-generated content

AI-generated content is content that is created by generative AI models based on user prompts. Examples of AI-generated content include:

- Text-to-text conversational generative AI chatbots, in which interacting with the chatbot is a central feature of the app
- Image generated by AI based on text, image or voice prompts

To ensure user safety and in accordance with Google Play's policy coverage, apps that generate content using AI must comply with existing Google Play developer policies, including by prohibiting and preventing the generation of restricted content, such as content that facilitates the exploitation or abuse of children, and content that enables deceptive behaviour.

Apps that generate content using AI must contain in-app user reporting or flagging features that allow users to report or flag offensive content to developers without needing to exit the app. Developers should utilise user reports to inform content filtering and moderation in their apps.

Intellectual property

We don’t allow apps or developer accounts that infringe on the intellectual property rights of others (including trademark, copyright, patent, trade secret and other proprietary rights). We also don’t allow apps that encourage or induce infringement of intellectual property rights.

We will respond to clear notices of alleged copyright infringement. For more information or to file a DMCA request, please visit our copyright procedures .

To submit a complaint regarding the sale or promotion for sale of counterfeit goods within an app, please submit a counterfeit notice .

If you are a trademark owner and you believe that there is an app on Google Play that infringes on your trademark rights, we encourage you to get in touch with the developer directly to resolve your concern. If you are unable to reach a resolution with the developer, please submit a trademark complaint through this form .

If you have written documentation proving that you have permission to use a third- party's intellectual property in your app or Store Listing (such as brand names, logos and graphic assets), contact the Google Play team in advance of your submission to ensure that your app is not rejected for an intellectual property violation.

Unauthorised use of copyrighted content

We don’t allow apps that infringe copyright. Modifying copyrighted content may still lead to a violation. Developers may be required to provide evidence of their rights to use copyrighted content.

Please be careful when using copyrighted content to demonstrate the functionality of your app. In general, the safest approach is to create something that’s original.

To ensure that Google Play remains a safe and respectful platform, we've created standards defining and prohibiting content that is harmful or inappropriate for our users.

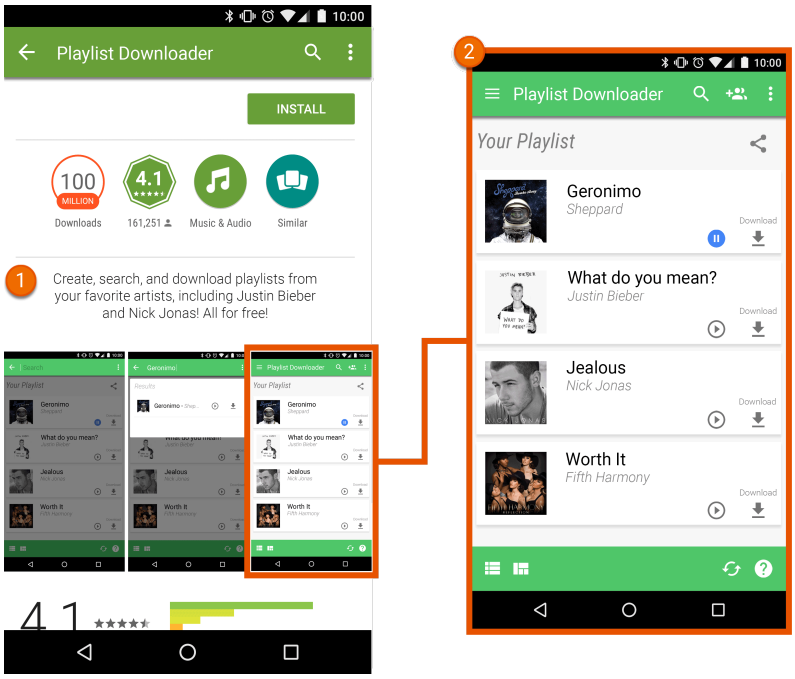
- Cover art for music albums, video games and books.
- Marketing images from films, television or video games.
- Artwork or images from comic books, cartoons, films, music videos or television.
- College and professional sports team logos.
- Photos taken from a public figure’s social media account.
- Professional images of public figures.
- Reproductions or “fan art” indistinguishable from the original work under copyright.
- Apps that have soundboards that play audio clips from copyrighted content.
- Full reproductions or translations of books that are not in the public domain.

Encouraging infringement of copyright

We don’t allow apps that induce or encourage copyright infringement. Before you publish your app, look for ways that your app may be encouraging copyright infringement and seek legal advice if necessary.

To ensure that Google Play remains a safe and respectful platform, we've created standards defining and prohibiting content that is harmful or inappropriate for our users.

- Streaming apps that allow users to download a local copy of copyrighted content without authorisation.
- Apps that encourage users to stream and download copyrighted works, including music and video, in violation of applicable copyright law:



① The description in this app listing encourages users to download copyrighted content without authorisation.
② The screenshot in the app listing encourages users to download copyrighted content without authorisation.

Trademark infringement

We don't allow apps that infringe on others' trademarks. A trademark is a word, symbol or combination that identifies the source of a good or service. Once acquired, a trademark gives the owner exclusive rights to the trademark usage with respect to certain goods or services.

Trademark infringement is improper or unauthorised use of an identical or similar trademark in a way that is likely to cause confusion as to the source of that product. If your app uses another party's trademarks in a way that is likely to cause confusion, your app may be suspended.

Counterfeit

We don't allow apps that sell counterfeit goods or promote them for sale. Counterfeit goods contain a trademark or logo that is identical to or substantially indistinguishable from the trademark of another. They mimic the brand features of the product in an attempt to pass themselves off as a genuine product of the brand owner.

Privacy, deception and device abuse

We're committed to protecting user privacy and providing a safe and secure environment for our users. Apps that are deceptive, malicious, or intended to abuse or misuse any network, device or personal data are strictly prohibited.

User data

You must be transparent in how you handle user data (for example, information collected from or about a user, including device information). That means disclosing the access, collection, use, handling and sharing of user data from your app, and limiting the use of the data to the policy-compliant purposes disclosed. Please be aware that any handling of personal and sensitive user data is also subject to additional requirements in the 'Personal and sensitive user data' section below.

These Google Play requirements are in addition to any requirements prescribed by applicable privacy and data protection laws.

If you include third-party code (for example, an SDK) in your app, you must ensure that the third-party code used in your app, and that third party's practices with respect to user data from your app, are compliant with Google Play Developer Programme Policies, which include use and disclosure requirements. For example, you must ensure that your SDK providers do not sell personal and sensitive user data from your app. This requirement applies regardless of whether user data is transferred after being sent to a server, or by embedding third-party code in your app.

Personal and sensitive user data

Personal and sensitive user data includes, but isn't limited to, personally identifiable information, financial and payment information, authentication information, phonebook, contacts, device location , SMS and call-related data, health data , Health Connect data, inventory of other apps on the device, microphone, camera, and other sensitive device or usage data. If your app handles personal and sensitive user data, then you must:

- Limit the access, collection, use and sharing of personal and sensitive user data acquired through the app to app and service functionality and policy-conforming purposes reasonably expected by the user:
  - Apps that extend usage of personal and sensitive user data for serving advertising must comply with Google Play's ads policy .
  - You may also transfer data as necessary to service providers or for legal reasons such as to comply with a valid governmental request, applicable law, or as part of a merger or acquisition with legally adequate notice to users.
- Handle all personal and sensitive user data securely, including transmitting it using modern cryptography (for example, over HTTPS).
- Use a runtime permissions request whenever available, prior to accessing data gated by Android permissions .
- Not sell personal and sensitive user data.
  - 'Sale' means the exchange or transfer of personal and sensitive user data to a third party for monetary consideration.
    - User-initiated transfer of personal and sensitive user data (for example, when the user is using a feature of the app to transfer a file to a third party, or when the user chooses to use a dedicated purpose research study app), is not regarded as sale.

Prominent disclosure and consent requirement

In cases where your app's access, collection, use or sharing of personal and sensitive user data may not be within the reasonable expectation of the user of the product or feature in question (for example, if data collection occurs in the background when the user is not engaging with your app), you must meet the following requirements:

Prominent disclosure: you must provide an in-app disclosure of your data access, collection, use and sharing. The in-app disclosure:

- Must be within the app itself, not only in the app description or on a website;
- Must be displayed in the normal usage of the app and not require the user to navigate into a menu or settings;
- Must describe the data being accessed or collected;
- Must explain how the data will be used and/or shared;
- Cannot only be placed in a privacy policy or Terms of Service; and
- Cannot be included with other disclosures unrelated to personal and sensitive user data collection.

Consent and runtime permissions: requests for in-app user consent and runtime permission requests must be immediately preceded by an in-app disclosure that meets the requirement of

this policy. The app's request for consent:

- Must present the consent dialogue clearly and unambiguously;
- Must require affirmative user action (for example, tap to accept, tick a tick box);
- Must not interpret navigation away from the disclosure (including tapping away or pressing the back or home button) as consent;
- Must not use auto-dismissing or expiring messages as a means of obtaining user consent; and
- Must be granted by the user before your app can begin to collect or access the personal and sensitive user data.

Apps that rely on other legal bases to process personal and sensitive user data without consent, such as a legitimate interest under the EU GDPR, must comply with all applicable legal requirements and provide appropriate disclosures to the users, including in-app disclosures as required under this policy.

To meet policy requirements, it's recommended that you reference the following example format for prominent disclosure when it's required:

- '[This app] collects/transmits/syncs/stores [type of data] to enable ["feature"], [in what scenario].'
- *Example: 'Fitness Funds collects location data to enable fitness tracking even when the app is closed or not in use and is also used to support advertising'.*
- *Example: 'Call buddy collects read and write call log data to enable contact organisation even when the app is not in use'.*

If your app integrates third-party code (for example, an SDK) that is designed to collect personal and sensitive user data by default, you must, within two weeks of receipt of a request from Google Play (or, if Google Play's request provides for a longer time period, within that time period), provide sufficient evidence demonstrating that your app meets the prominent disclosure and consent requirements of this policy, including with regard to the data access, collection, use or sharing via the third-party code.

To ensure that Google Play remains a safe and respectful platform, we've created standards defining and prohibiting content that is harmful or inappropriate for our users.

- An app collects device location but does not have a prominent disclosure explaining which feature uses this data and/or indicates the app's usage in the background.
- An app has a runtime permission requesting access to data before the prominent disclosure which specifies what the data is used for.
- An app that accesses a user's inventory of installed apps and doesn't treat this data as personal or sensitive data subject to the above privacy policy, data handling, and prominent disclosure and consent requirements.
- An app that accesses a user's phone or contact book data and doesn't treat this data as personal or sensitive data subject to the above privacy policy, data handling, and prominent disclosure and consent requirements.
- An app that records a user's screen and doesn't treat this data as personal or sensitive data subject to this policy.
- An app that collects device location and does not comprehensively disclose its use and obtain consent in accordance with the above requirements.
- An app that uses restricted permissions in the background of the app including for tracking, research or marketing purposes, and does not comprehensively disclose its use and obtain consent in accordance with the above requirements.
- An app with an SDK that collects personal and sensitive user data and doesn't treat this data as subject to this user data policy, access, data handling (including disallowed sale), and prominent disclosure and consent requirements.

Refer to this article for more information on the prominent disclosure and consent requirement.

Restrictions for personal and sensitive data access

In addition to the requirements above, the table below describes requirements for specific activities.

Activity	Requirement
Your app handles financial or payment information or government identification numbers	Your app must never publicly disclose any personal and sensitive user data related to financial or payment activities or any government identification numbers.
Your app handles non-public phone book or contact information	We don't allow unauthorised publishing or disclosure of people's non-public contacts.
Your app contains anti-virus or security functionality, such as anti-virus, anti-malware or security-related features	Your app must post a privacy policy that, together with any in-app disclosures, explain what user data your app collects and transmits, how it's used and the type of parties with whom it's shared.
Your app targets children	Your app must not include an SDK that is not approved for use in child-directed services. See Designing apps for children and families for full policy language and requirements.
Your app collects or links persistent device identifiers (for example, IMEI, IMSI, SIM Serial #, etc.)	Persistent device identifiers may not be linked to other personal and sensitive user data or resettable device identifiers except for the purposes of • Telephony linked to a SIM identity (for example, Wi-Fi calling linked to an operator account) and • Enterprise device management apps using device owner mode. These uses must be prominently disclosed to users as specified in the user data policy . Please consult this resource for alternative unique identifiers. Please read the ads policy for additional guidelines for Android advertising ID.

Data safety section

All developers must complete a clear and accurate Data safety section for every app detailing collection, use and sharing of user data. The developer is responsible for the accuracy of the label and keeping this information up to date. Where relevant, the section must be consistent with the disclosures made in the app's privacy policy.

Please refer to this article for additional information on completing the Data safety section.

Privacy policy

All apps must post a privacy policy link in the designated field within Play Console, and a privacy policy link or text within the app itself. The privacy policy must, together with any in-app disclosures, comprehensively disclose how your app accesses, collects, uses and shares user data, not limited by the data disclosed in the Data Safety section. This must include:

- Developer information and a privacy point of contact or a mechanism to submit enquiries.
- Disclosing the types of personal and sensitive user data that your app accesses, collects, uses and shares; and any parties with which any personal or sensitive user data is shared.
- Secure data handling procedures for personal and sensitive user data.
- The developer's data retention and deletion policy.
- Clear labelling as a privacy policy (for example, listed as 'privacy policy' in title).

The entity (for example, developer, company) named in the app's Google Play Store Listing must appear in the privacy policy or the app must be named in the privacy policy. Apps that do not access any personal and sensitive user data must still submit a privacy policy.

Please make sure that your privacy policy is available on an active, publicly accessible and non-geo-fenced URL (no PDFs) and is non-editable.

Account deletion requirement

If your app allows users to create an account from within your app, then it must also allow users to request for their account to be deleted. Users must have a readily discoverable option to initiate app account deletion from within your app and outside of your app (for example, by visiting your website). A link to this web resource must be entered in the designated URL form field within Play Console.

When you delete an app account based on a user's request, you must also delete the user data associated with that app account. Temporary account deactivation, disabling or 'freezing' the app account does not qualify as account deletion. If you need to retain certain data for legitimate reasons such as security, fraud prevention or regulatory compliance, you must clearly inform users about your data retention practices (for example, within your privacy policy).

To learn more about account deletion policy requirements, please review this Help Centre article. For additional information on updating your Data safety form, visit this article.

Usage of app set ID

Android will introduce a new ID to support essential use cases such as analytics and fraud prevention. Terms for the use of this ID are below.

- **Usage**: App set ID must not be used for ads personalisation and ads measurement.
- **Association with personally identifiable information or other identifiers:** App set ID may not be connected to any Android identifiers (for example, AAID) or any personal and sensitive data for advertising purposes.
- **Transparency and consent:** The collection and use of the app set ID and commitment to these terms must be disclosed to users in a legally adequate privacy notification, including your privacy policy. You must obtain users' legally valid consent where required. To learn more about our privacy standards, please review our User data policy .

EU-U.S. Swiss Privacy Shield

If you access, use or process personal information made available by Google that directly or indirectly identifies an individual, and that originated in the European Union or Switzerland ('EU Personal Information'), then you must:

- Comply with all applicable privacy, data security and data protection laws, directives, regulations and rules;
- Access, use or process EU Personal Information only for purposes that are consistent with the consent obtained from the individual to whom the EU Personal Information relates;
- Implement appropriate organisational and technical measures to protect EU personal information against loss, misuse and unauthorised or unlawful access, disclosure, alteration and destruction; and
- Provide the same level of protection as is required by the Privacy Shield principles .

You must monitor your compliance with these conditions on a regular basis. If, at any time, you cannot meet these conditions (or if there is a significant risk that you will not be able to meet them), you must immediately notify us by email to data-protection-office@google.com and immediately either stop processing EU personal information or take reasonable and appropriate steps to restore an adequate level of protection.

As of 16 July 2020, Google no longer relies on the EU-U.S. Privacy Shield to transfer personal data that originated in the European Economic Area or the UK to the United States. (Learn more.) More information is set forth in Section 9 of the DDA.

Permissions and APIs that Access Sensitive Information

Requests for permission and APIs that access sensitive information should make sense to users. You may only request permissions and APIs that access sensitive information that are necessary to implement current features or services in your app that are promoted in your Google Play listing. You may not use permissions or APIs that access sensitive information that give access to user or device data for undisclosed, unimplemented, or disallowed features or purposes. Personal or sensitive data accessed through permissions or APIs that access sensitive information may never be sold nor shared for a purpose facilitating sale.

Request permissions and APIs that access sensitive information to access data in context (via incremental requests), so that users understand why your app is requesting the permission. Use the data only for purposes that the user has consented to. If you later wish to use the data for other purposes, you must ask users and make sure that they affirmatively agree to the additional uses.

Restricted permissions

In addition to the above, restricted permissions are permissions that are designated as Dangerous , Special , Signature or as documented below. These permissions are subject to the following additional requirements and restrictions:

- User or device data accessed through restricted permissions is considered as personal and sensitive user data. The requirements of the user data policy apply.
- Respect users' decisions if they decline a request for a restricted permission, and users may not be manipulated or forced into consenting to any non-critical permission. You must make a reasonable effort to accommodate users who do not grant access to sensitive permissions (for example, allowing a user to manually enter a phone number if they've restricted access to call logs).
- Use of permissions in violation of Google Play malware policies (including elevated privilege abuse) is expressly prohibited.

Certain restricted permissions may be subject to additional requirements as detailed below. The objective of these restrictions is to safeguard user privacy. We may make limited exceptions to the requirements below in very rare cases where apps provide a highly compelling or critical feature, and where there is no alternative method available to provide the feature. We evaluate proposed exceptions against the potential privacy or security impacts on users.

SMS and call log permissions

SMS and call log permissions are regarded as personal and sensitive user data subject to the personal and sensitive Information policy, and the following restrictions:

Restricted permission	Requirement
Call log permission group (for example, READ_CALL_LOG, WRITE_CALL_LOG, PROCESS_OUTGOING_CALLS)	It must be actively registered as the default Phone or Assistant handler on the device.
SMS permission group (for example, READ_SMS, SEND_SMS, WRITE_SMS, RECEIVE_SMS, RECEIVE_WAP_PUSH, RECEIVE_MMS)	It must be actively registered as the default SMS or Assistant handler on the device.

Apps lacking default SMS, Phone or Assistant handler capability may not declare use of the above permissions in the manifest. This includes placeholder text in the manifest. Additionally, apps must be actively registered as the default SMS, phone or Assistant handler before prompting users to accept any of the above permissions, and must immediately stop using the permission when they're no longer the default handler. The permitted uses and exceptions are available on this Help Centre page .

Apps may only use the permission (and any data derived from the permission) to provide approved core app functionality. Core functionality is defined as the main purpose of the app. This may include a

set of core features, which must all be prominently documented and promoted in the app's description. Without the core feature(s), the app is 'broken' or rendered unusable. The transfer, sharing or licensed use of this data must only be for providing core features or services within the app, and its use may not be extended for any other purpose (for example, improving other apps or services, advertising or marketing purposes). You may not use alternative methods (including other permissions, APIs or third-party sources) to derive data attributed to call log- or SMS-related permissions.

Location permissions

Device location is regarded as personal and sensitive user data subject to the Personal and sensitive information policy and the Background location policy, and the following requirements:

- Apps may not access data protected by location permissions (for example, ACCESS_FINE_LOCATION, ACCESS_COARSE_LOCATION, ACCESS_BACKGROUND_LOCATION) after it is no longer necessary to deliver current features or services in your app.
- You should never request location permissions from users for the sole purpose of advertising or analytics. Apps that extend permitted usage of this data for serving advertising must be in compliance with our ads policy .
- Apps should request the minimum scope necessary (for example, coarse instead of fine, and foreground instead of background) to provide the current feature or service requiring location, and users should reasonably expect that the feature or service needs the level of location requested. For example, we may reject apps that request or access background location without compelling justification.
- Background location may only be used to provide features beneficial to the user and relevant to the core functionality of the app.

Apps are allowed to access location using foreground service (when the app only has foreground access for example, 'while in use') permission if the use:

- has been initiated as a continuation of an in-app user-initiated action, and
- is terminated immediately after the intended use case of the user-initiated action is completed by the application.

Apps designed specifically for children must comply with the Designed for Families policy.

For more information on the policy requirements, please see this help article .

All files access permission

Files and directory attributes on a user's device are regarded as personal and sensitive user data subject to the personal and sensitive information policy and the following requirements:

- Apps should only request access to device storage that is critical for the app to function, and may not request access to device storage on behalf of any third-party for any purpose that is unrelated to critical user-facing app functionality.
- Android devices running R or later will require the MANAGE_EXTERNAL_STORAGE permission in order to manage access in shared storage. All apps that target R and request broad access to shared storage ('all files access') must successfully pass an appropriate access review prior to publishing. Apps allowed to use this permission must clearly prompt users to enable 'All files access' for their app under 'Special app access' settings. For more information on the R requirements, please see this help article .

Package (app) visibility permission

The inventory of installed apps queried from a device are regarded as personal and sensitive user data subject to the personal and sensitive information policy, and the following requirements:

Apps that have a core purpose to launch, search or interoperate with other apps on the device, may obtain scope-appropriate visibility to other installed apps on the device as outlined below:

- **Broad app visibility:** Broad visibility is the capability of an app to have extensive (or 'broad') visibility of the installed apps ('packages') on a device.
  - For apps targeting API level 30 or later , broad visibility to installed apps via the QUERY_ALL_PACKAGES permission is restricted to specific use cases where awareness of and/or interoperability with any and all apps on the device are required for the app to function.
    - You may not use QUERY_ALL_PACKAGES if your app can operate with a more targeted scoped package visibility declaration (for example, querying and interacting with specific packages instead of requesting broad visibility).
  - Use of alternative methods to approximate the broad visibility level associated with QUERY_ALL_PACKAGES permission are also restricted to user-facing core app functionality and interoperability with any apps discovered via this method.
  - Please see this Help Centre article for allowable use cases for the QUERY_ALL_PACKAGES permission.
- **Limited app visibility**: Limited visibility is when an app minimises access to data by querying for specific apps using more targeted (instead of 'broad') methods(for example, querying for specific apps that satisfy your app's manifest declaration). You may use this method to query for apps in cases where your app has policy-compliant interoperability, or management of these apps.
- Visibility to the inventory of installed apps on a device must be directly related to the core purpose or core functionality that users access within your app.

App inventory data queried from Play-distributed apps may never be sold nor shared for analytics or ads monetisation purposes.

Accessibility API

The Accessibility API cannot be used to:

- Change user settings without their permission or prevent the ability for users to disable or uninstall any app or service unless authorised by a parent or guardian through a parental control app or by authorised administrators through enterprise management software;
- Work around Android built-in privacy controls and notifications; or
- Change or leverage the user interface in a way that is deceptive or otherwise violates Google Play developer policies.

The Accessibility API is not designed and cannot be requested for remote call audio recording.

The use of the Accessibility API must be documented in the Google Play listing.

Guidelines for IsAccessibilityTool

Apps with a core functionality intended to directly support people with disabilities are eligible to use the **IsAccessibilityTool** to appropriately publicly designate themselves as an accessibility app.

Apps not eligible for **IsAccessibilityTool** may not use the flag and must meet prominent disclosure and consent requirements as outlined in the user data policy as the accessibility-related functionality is not obvious to the user. Please refer to the AccessibilityService API Help Centre article for more information.

Apps must use more narrowly scoped APIs and permissions in lieu of the Accessibility API when possible to achieve the desired functionality.

Request install packages permission

The REQUEST_INSTALL_PACKAGES permission allows an application to request the installation of app packages. To use this permission, your app's core functionality must include:

- Sending or receiving app packages; and
- Enabling user-initiated installation of app packages.

Permitted functionalities include:

- Web browsing or search
- Communication services that support attachments
- File sharing, transfer or management
- Enterprise device management
- Backup and restore
- Device migration/Phone transfer
- Companion app to sync phone to wearable or IoT device (for example, smart watch or smart TV)

Core functionality is defined as the main purpose of the app. The core functionality, as well as any core features that comprise this core functionality, must all be prominently documented and promoted in the app's description.

The REQUEST_INSTALL_PACKAGES permission may not be used to perform self updates, modifications or the bundling of other APKs in the asset file unless for device management purposes. All updates or installing of packages must abide by Google Play's device and network abuse policy and must be initiated and driven by the user.

Health Connect by Android Permissions

Data accessed through Health Connect Permissions is regarded as personal and sensitive user data subject to the User data policy, and the following additional requirements:

Appropriate access to and use of Health Connect

Requests to access data through Health Connect must be clear and understandable. Health Connect may only be used in accordance with the applicable policies, Terms and Conditions and for approved use cases as set forth in this policy. This means that you may only request access to permissions when your application or service meets one of the approved use cases.

Approved use cases for access to Health Connect Permissions are:

- Applications or services with one or more features to benefit users' health and fitness via a user interface allowing users to directly **journal, report, monitor and/or analyse** their physical activity, sleep, mental well-being, nutrition, health measurements, physical descriptions and/or other health or fitness-related descriptions and measurements.
- Applications or services with one or more features to benefit users' health and fitness via a user interface allowing users to **store** their physical activity, sleep, mental well-being, nutrition, health measurements, physical descriptions and/or other health or fitness-related descriptions and measurements on their phone and/or wearable, and share their data with other on-device apps that satisfy these use cases.

Health Connect is a general-purpose data storage and sharing platform that allows users to aggregate health and fitness data from various sources on their Android device and share it with third parties at their election. The data may originate from various sources as determined by the users. Developers must assess whether Health Connect is appropriate for their intended use and investigate and vet the source and quality of any data from Health Connect in connection with any purpose and, in particular, for research, health or medical uses.

- Apps conducting health-related human subject research using data obtained through Health Connect must obtain consent from participants or, in the case of minors, their parent or guardian. Such consent must include the (a) nature, purpose and duration of the research; (b) procedures, risks and benefits to the participant; (c) information about confidentiality and handling of data (including any sharing with third parties); (d) a point of contact for participant questions; and (e) the withdrawal process. Apps conducting health-related human subject research using data obtained

through Health Connect must receive approval from an independent board whose aim is 1) to protect the rights, safety and well-being of participants and 2) with the authority to scrutinise, modify and approve human subjects research. Proof of such approval must be provided upon request.

- It is also your responsibility for ensuring compliance with any regulatory or legal requirements that may apply based on your intended use of Health Connect and any data from Health Connect. Except as explicitly noted in the labelling or information provided by Google for specific Google products or services, Google does not endorse the use of or warrant the accuracy of any data contained in Health Connect for any use or purpose and, in particular, for research, health or medical uses. Google disclaims all liability associated with use of data obtained through Health Connect.

Limited use

Upon using Health Connect for an appropriate use, your use of the data accessed through Health Connect must also comply with the below requirements. These requirements apply to the raw data obtained from Health Connect, and data aggregated, de-identified or derived from the raw data.

- Limit your use of Health Connect data to providing or improving your appropriate use case or features that are visible and prominent in the requesting application's user interface.
- Only transfer user data to third parties:
  - To provide or improve your appropriate use case or features that are clear from the requesting application's user interface and only with the user's consent;
  - If necessary for security purposes (for example, investigating abuse);
  - To comply with applicable laws and/or regulations; or,
  - As part of a merger, acquisition or sale of assets of the developer after obtaining explicit prior consent from the user.
- Do not allow humans to read user data, unless:
  - The user's explicit consent to read specific data is obtained;
  - It's necessary for security purposes (for example, investigating abuse);
  - To comply with applicable laws; or,
  - The data (including derivations) is aggregated and used for internal operations in accordance with applicable privacy and other jurisdictional legal requirements.

All other transfers, uses or sale of Health Connect data is prohibited, including:

- Transferring or selling user data to third parties, like advertising platforms, data brokers or any information resellers.
- Transferring, selling or using user data for serving ads, including personalised or interest-based advertising.
- Transferring, selling or using user data to determine creditworthiness or for lending purposes.
- Transferring, selling or using the user data with any product or service that may qualify as a medical device pursuant to Section 201(h) of the United States Federal Food, Drug and Cosmetic Act if the user data will be used by the medical device to perform its regulated function.
- Transferring, selling or using user data for any purpose or in any manner involving Protected Health Information (as defined by HIPAA) unless you receive prior written approval to such use from Google.

Access to Health Connect may not be used in violation of this policy or other applicable Health Connect Terms and Conditions or policies, including for the following purposes:

- Do not use Health Connect in developing, or for incorporation into, applications, environments or activities where the use or failure of Health Connect could reasonably be expected to lead to death, personal injury or environmental or property damage (such as the creation or operation of nuclear facilities, air traffic control, life-support systems or weaponry).

- Do not access data obtained through Health Connect using headless apps. Apps must display a clearly identifiable icon in the app tray, device app settings, notification icons, etc.
- Do not use Health Connect with apps that sync data between incompatible devices or platforms.
- Health Connect cannot connect to applications, services or features that solely target children. Health Connect is not approved for use in primarily child-directed services.

An affirmative statement that your use of Health Connect data complies with limited use restrictions must be disclosed in your application or on a website belonging to your web service or application; for example, a link on a homepage to a dedicated page or privacy policy noting: 'The use of information received from Health Connect will adhere to the Health Connect Permissions policy, including the Limited use requirements'.

Minimum scope

You may only request access to permissions that are critical to implementing your application or service's functionality.

This means:

- Don't request access to information that you don't need. Only request access to the permissions necessary to implement your product's features or services. If your product does not require access to specific permissions, then you must not request access to these permissions.

Transparent and accurate notice and control

Health Connect handles health and fitness data, which includes personal and sensitive information. All applications and services must contain a privacy policy, which must comprehensively disclose how your application or service collects, uses and shares user data. This includes the types of parties to which any user data is shared, how you use the data, how you store and secure the data, and what happens to the data when an account is deactivated and/or deleted.

In addition to the requirements under applicable law, you must also adhere to the following requirements:

- You must provide a disclosure of your data access, collection, use and sharing. The disclosure:
  - Must accurately represent the identity of the application or service that seeks access to user data;
  - Must provide clear and accurate information explaining the types of data being accessed, requested and/or collected;
  - Must explain how the data will be used and/or shared: if you request data for one reason, but the data will also be utilised for a secondary purpose, you must notify users of both use cases.
- You must provide user help documentation that explains how users can manage and delete their data from your app.

Secure data handling

You must handle all user data securely. Take reasonable and appropriate steps to protect all applications or systems that make use of Health Connect against unauthorised or unlawful access, use, destruction, loss, alteration or disclosure.

Recommended security practices include implementing and maintaining an information security management system such as outlined in ISO/IEC 27001 and ensuring that your application or web service is robust and free from common security issues as set out by the OWASP Top 10.

Depending on the API being accessed and the number of user grants or users, we will require that your application or service undergo a periodic security assessment and obtain a letter of assessment from a designated third party if your product transfers data off the user's own device.

For more information on requirements for apps connecting to Health Connect, please see this help article.

VPN service

The VpnService is a base class for applications to extend and build their own VPN solutions. Only apps that use the VpnService and have VPN as their core functionality can create a secure device-level tunnel to a remote server. Exceptions include apps that require a remote server for core functionality, such as:

- Parental control and enterprise management apps.
- App usage tracking.
- Device security apps (for example, anti-virus, mobile device management, firewall).
- Network-related tools (for example, remote access).
- Web browsing apps.
- Operator apps that require the use of VPN functionality to provide telephony or connectivity services.

The VpnService cannot be used to:

- Collect personal and sensitive user data without prominent disclosure and consent.
- Redirect or manipulate user traffic from other apps on a device for monetisation purposes (for example, redirecting ad traffic through a country different to that of the user).

Apps that use the VpnService must:

- Document use of the VpnService in the Google Play listing, and
- Must encrypt the data from the device to VPN tunnel end point, and
- Abide by all Developer Programme Policies, including the Ad fraud, Permissions and Malware policies.

Exact alarm permission

A new permission, USE_EXACT_ALARM, will be introduced that will grant access to exact alarm functionality in apps starting with Android 13 (API target level 33).

USE_EXACT_ALARM is a restricted permission and apps must only declare this permission if their core functionality supports the need for an exact alarm. Apps that request this restricted permission are subject to review, and those that do not meet the acceptable use case criteria will be disallowed from publishing on Google Play.

Acceptable use cases for using the exact alarm permission

Your app must use the USE_EXACT_ALARM functionality only when your app's core, user-facing functionality requires precisely timed actions, such as:

- The app is an alarm or timer app.
- The app is a calendar app that shows event notifications.

If you have a use case for exact alarm functionality that's not covered above, you should evaluate if using SCHEDULE_EXACT_ALARM as an alternative is an option.

For more information on exact alarm functionality, please see this developer guidance.

Device and network abuse

We don't allow apps that interfere with, disrupt, damage or access in an unauthorised manner the user's device, other devices or computers, servers, networks, application programming interfaces (APIs) or services, including but not limited to other apps on the device, any Google service or an authorised operator network.

Apps on Google Play must comply with the default Android system optimisation requirements documented in the Core app quality guidelines for Google Play.

An app distributed via Google Play may not modify, replace or update itself using any method other than Google Play's update mechanism. Likewise, an app may not download executable code (such as dex, JAR, .so files) from a source other than Google Play. This restriction does not apply to code that runs in a virtual machine or an interpreter where either provides indirect access to Android APIs (such as JavaScript in a WebView or browser).

Apps or third-party code, like SDKs, with interpreted languages (JavaScript, Python, Lua, etc.) loaded at run time (for example, not packaged with the app) must not allow potential violations of Google Play policies.

We don't allow code that introduces or exploits security vulnerabilities. Review the App security improvement programme to find out about the most recent security issues flagged to developers.

To ensure that Google Play remains a safe and respectful platform, we've created standards defining and prohibiting content that is harmful or inappropriate for our users.

- Apps that block or interfere with another app displaying ads.
- Game cheating apps that affect the gameplay of other apps.
- Apps that facilitate or provide instructions on how to hack services, software or hardware, or circumvent security protections.
- Apps that access or use a service or API in a manner that violates its Terms of Service.
- Apps that are not eligible for allowlisting and attempt to bypass system power management .
- Apps that facilitate proxy services to third parties may only do so in apps where that is the primary, user-facing core purpose of the app.
- Apps or third-party code (for example, SDKs) that download executable code, such as DEX files or native code, from a source other than Google Play.
- Apps that install other apps on a device without the user's prior consent.
- Apps that link to or facilitate the distribution or installation of malicious software.
- Apps or third-party code (for example, SDKs) containing a WebView with added JavaScript interface that loads untrusted web content (for example, http:// URL) or unverified URLs obtained from untrusted sources (for example, URLs obtained with untrusted intents)

Foreground service use

The foreground service permission ensures the appropriate use of user-facing foreground services. For apps targeting Android 14 and above, you must specify a valid foreground service type for each foreground service used in your app and declare the foreground service permission that is appropriate for that type. For example, if your app's use case requires map geolocation, you must declare the FOREGROUND_SERVICE_LOCATION permission in your app's manifest.

With the exceptions of systemExempted and shortService foreground service types, apps are only allowed to declare a foreground service permission if the use:

- provides a feature that is beneficial to the user and relevant to the core functionality of the app
- is initiated by the user or is user perceptible (for example, audio from playing a song, cast media to another device, accurate and clear user notification, user request to upload a photo to the cloud)
- can be terminated or stopped by the user
- can't be interrupted or deferred by the system without causing a negative user experience or causing the user anticipated feature to not work as intended (for example, a phone call needs to start immediately and can't be deferred by the system)
- runs only for as long as necessary to complete the task

The use of foreground service is further explained here.

User-initiated data transfer jobs

Apps are only allowed to use the user-initiated data transfer jobs API if the use is:

- initiated by the user
- for network data transfer tasks
- runs only for as long as necessary to complete the data transfer

The usage of user-initiated data transfer APIs is further explained here.

Flag secure requirements

FLAG_SECURE is a display flag declared in an app's code to indicate that its UI contains sensitive data intended to be limited to a secure surface while using the app. This flag is designed to prevent the data from appearing in screenshots or from being viewed on non-secure displays. Developers declare this flag when the app's content should not be broadcast, viewed or otherwise transmitted outside of the app or users' device.

For security and privacy purposes, all apps distributed on Google Play are required to respect the FLAG_SECURE declaration of other apps. Meaning, apps must not facilitate or create workarounds to bypass the FLAG_SECURE settings in other apps.

Apps that qualify as an accessibility tool are exempt from this requirement, as long as they do not transmit, save or cache FLAG_SECURE protected content for access outside of the user's device.

Apps that run on-device Android containers

On-device Android container apps provide environments that simulate whole or portions of an underlying Android OS. The experience within these environments may not reflect the full suite of Android security features, which is why developers can choose to add a secure environment manifest flag to communicate to on-device Android containers that they must not operate in their simulated Android environment.

Secure environment manifest flag

REQUIRE_SECURE_ENV is a flag that can be declared in an app's manifest to indicate that this app must not run in on-device Android container apps. For security and privacy purposes, apps that provide on-device Android containers must respect all apps that declare this flag and:

- Review the manifests of apps that they intend to load in their on-device Android container for this flag.
- Not load the apps that declared this flag into their on-device Android container.
- Not function as a proxy by intercepting or calling APIs on the device so that they appear to be installed in the container.
- Not facilitate, or create workarounds to bypass the flag (such as loading an older version of an app to bypass the current app's REQUIRE_SECURE_ENV flag).

Learn more about this policy in our Help Centre.

Deceptive behaviour

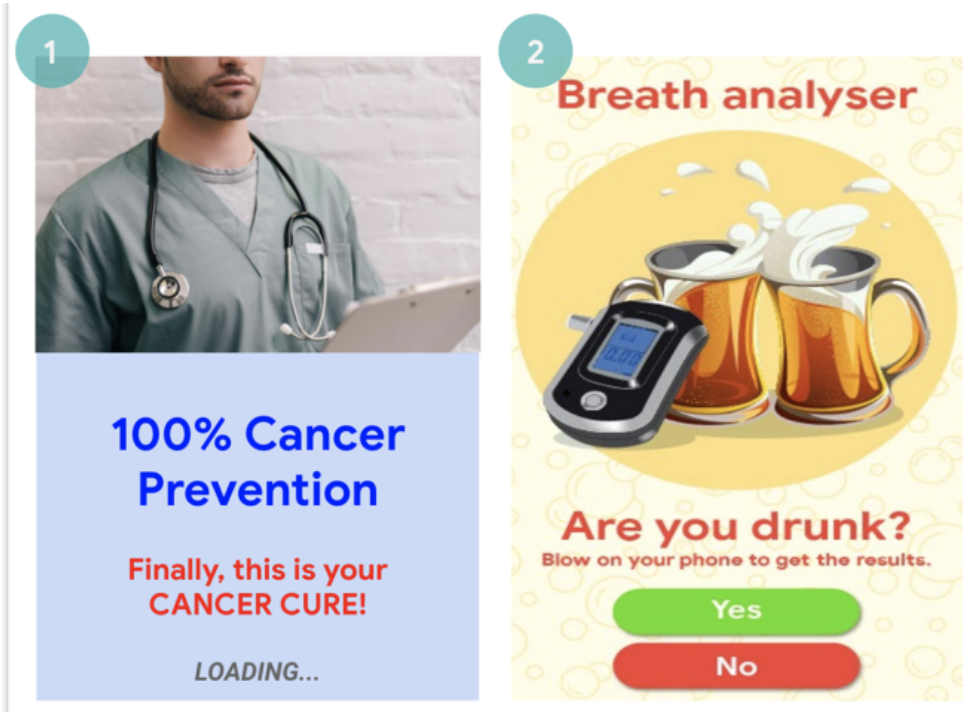
We don't allow apps that attempt to deceive users or enable dishonest behaviour, including but not limited to apps which are determined to be functionally impossible. Apps must provide an accurate disclosure, description and images/video of their functionality in all parts of the metadata. Apps must not attempt to mimic functionality or warnings from the operating system or other apps. Any changes to device settings must be made with the user's knowledge and consent and be reversible by the user.

Misleading claims

We don't allow apps that contain false or misleading information or claims, including in the description, title, icon and screenshots.

To ensure that Google Play remains a safe and respectful platform, we've created standards defining and prohibiting content that is harmful or inappropriate for our users.

- Apps that misrepresent or do not accurately and clearly describe their functionality:
  - An app that claims to be a racing game in its description and screenshots, but is actually a puzzle block game using a picture of a car.
  - An app that claims to be an antivirus app, but only contains a text guide explaining how to remove viruses.
- Apps that claim functionalities that are not possible to implement, such as insect repellent apps, even if it is represented as a prank, fake, joke, etc.
- Apps that are improperly categorised, including, but not limited to, the app rating or app category.
- Demonstrably deceptive or false content that may interfere with voting processes, or about the outcome of elections.
- Apps that falsely claim affiliation with a government entity or offer to provide or facilitate government services for which they are not properly authorised.
- Apps that falsely claim to be the official app of an established entity. Titles like 'Justin Bieber Official' are not allowed without the necessary permissions or rights.



(1) This app features medical or health-related claims (cures cancer) that are misleading.
(2) This app claims functionality that is not possible to implement (using your phone) as a breathalyser.

Deceptive device settings changes

We don't allow apps that make changes to the user's device settings or features outside of the app without the user's knowledge and consent. Device settings and features include system and browser settings, bookmarks, shortcuts, icons, widgets and the presentation of apps on the Home screen.

Additionally, we do not allow:

- Apps that modify device settings or features with the user's consent but do so in a way that is not easily reversible.
- Apps or ads that modify device settings or features as a service to third parties or for advertising purposes.
- Apps that mislead users into removing or disabling third-party apps or modifying device settings or features.

- Apps that encourage or incentivise users into removing or disabling third-party apps or modifying device settings or features unless it is part of a verifiable security service.

Enabling dishonest behaviour

We don't allow apps that help users to mislead others or are functionally deceptive in any way, including, but not limited to: apps that generate or facilitate the generation of ID cards, social security numbers, passports, diplomas, credit cards, bank accounts and driving licences. Apps must provide accurate disclosures, titles, descriptions and images/video regarding the app's functionality and/or content and should perform as reasonably and accurately expected by the user.

Additional app resources (for example, game assets) may only be downloaded if they are necessary for the users' use of the app. Downloaded resources must be compliant with all Google Play policies, and before beginning the download, the app should prompt users and clearly disclose the download size.

Any claim that an app is a 'prank' or 'for entertainment purposes' (or other synonym) does not exempt an app from application of our policies.

To ensure that Google Play remains a safe and respectful platform, we've created standards defining and prohibiting content that is harmful or inappropriate for our users.

- Apps that mimic other apps or websites to trick users into disclosing personal or authentication information.
- Apps that depict or display unverified or real-world phone numbers, contacts, addresses or personally identifiable information of non-consenting individuals or entities.
- Apps with different core functionality based on a user's geography, device parameters or other user-dependent data where those differences are not prominently advertised to the user in the Store Listing.
- Apps that change significantly between versions without alerting the user (for example, 'what's new' section) and updating the Store Listing.
- Apps that attempt to modify or obfuscate behaviour during review.
- Apps with Content Delivery Network (CDN) facilitated downloads that fail to prompt the user and disclose the download size prior to downloading.

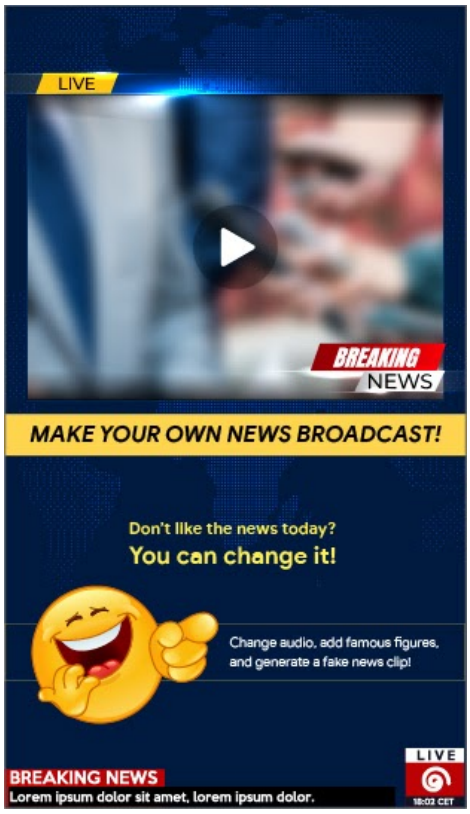
Manipulated media

We don't allow apps that promote or help create false or misleading information or claims conveyed through imagery, videos and/or text. We disallow apps determined to promote or perpetuate demonstrably misleading or deceptive imagery, videos and/or text, which may cause harm pertaining to a sensitive event, politics, social issues or other matters of public concern.

Apps that manipulate or alter media, beyond conventional and editorially acceptable adjustments for clarity or quality, must prominently disclose or watermark altered media when it may not be clear to the average person that the media has been altered. Exceptions may be provided for public interest, or obvious satire or parody.

To ensure that Google Play remains a safe and respectful platform, we've created standards defining and prohibiting content that is harmful or inappropriate for our users.

- Apps adding a public figure to a demonstration during a politically sensitive event.
- Apps using public figures or media from a sensitive event to advertise media altering capability within an app's Store Listing.
- Apps that alter media clips to mimic a news broadcast.



(1) This app provides functionality to alter media clips to mimic a news broadcast, and add famous or public figures to the clip without a watermark.

Behaviour transparency

Your app's functionality should be reasonably clear to users; don't include any hidden, dormant or undocumented features within your app. Techniques to evade app reviews are not allowed. Apps may be required to provide additional details to ensure user safety, system integrity and policy compliance.

Misrepresentation

We do not allow apps or developer accounts that:

- impersonate any person or organisation, or that misrepresent or conceal their ownership or primary purpose.
- that engage in coordinated activity to mislead users. This includes, but isn't limited to, apps or developer accounts that misrepresent or conceal their country of origin and that direct content at users in another country.
- coordinate with other apps, sites, developers or other accounts to conceal or misrepresent developer or app identity or other material details, where app content relates to politics, social issues or matters of public concern.

Google Play's target API level policy

To provide users with a safe and secure experience, Google Play requires the following target API levels for **all apps**:

New apps and app updates MUST target an Android API level within one year of the latest major Android version release. New apps and app updates that fail to meet this requirement will be prevented from app submission in Play Console.

Existing Google Play apps that are not updated and that do not target an API level within two years of the latest major Android version release, will not be available to new users with devices running newer versions of Android OS. Users who have previously installed the app from Google Play will continue to be able to discover, re-install and use the app on any Android OS version that the app supports.

For technical advice on how to meet the target API level requirement, please consult the migration guide .

For exact timelines and exceptions, please refer to this Help Centre article .

SDK requirements

App developers often rely on third-party code (for example, an SDK) to integrate key functionality and services for their apps. When including an SDK in your app, you want to make sure that you can keep your users safe and your app secure from any vulnerabilities. In this section, we demonstrate how some of our existing privacy and security requirements apply in the SDK context and are designed to help developers safely and securely integrate SDKs into their apps.

If you include an SDK in your app, you are responsible for ensuring that their third-party code and practices do not cause your app to violate Google Play Developer Programme Policies. It is important to be aware of how the SDKs in your app handle user data and to ensure that you know what permissions they use, what data they collect, and why. Remember, an SDK's collection and handling of user data must align with your app's policy-compliant use of said data.

To help ensure that your use of an SDK does not violate policy requirements, read and understand the following policies in their entirety and note some of their existing requirements pertaining to SDKs below:

User data policy

You must be transparent in how you handle user data (for example, information collected from or about a user, including device information). That means disclosing the access, collection, use, handling and sharing of user data from your app, and limiting the use of the data to the policy-compliant purposes disclosed.

If you include third-party code (for example, an SDK) in your app, you must ensure that the third-party code used in your app, and that third party's practices with respect to user data from your app, are compliant with Google Play Developer Programme Policies, which include use and disclosure requirements. For example, you must ensure that your SDK providers do not sell personal and sensitive user data from your app. This requirement applies regardless of whether user data is transferred after being sent to a server, or by embedding third-party code in your app.

Personal and sensitive user data

- Limit the access, collection, use and sharing of personal and sensitive user data acquired through the app to app and service functionality and policy-conforming purposes reasonably expected by the user:
  - Apps that extend usage of personal and sensitive user data for serving advertising must comply with Google Play's ads policy.
- Handle all personal and sensitive user data securely, including transmitting it using modern cryptography (for example, over HTTPS).
- Use a runtime permissions request whenever available, prior to accessing data gated by Android permissions

Sale of personal and sensitive user data

Do not sell personal and sensitive user data.

- 'Sale' means the exchange or transfer of personal and sensitive user data to a third party for monetary consideration.

- User-initiated transfer of personal and sensitive user data (for example, when the user is using a feature of the app to transfer a file to a third party, or when the user chooses to use a dedicated purpose research study app), is not regarded as sale.

Prominent disclosure and consent requirements

In cases where your app's access, collection, use or sharing of personal and sensitive user data may not be within the reasonable expectation of the user of the product or feature in question, you must meet the prominent disclosure and consent requirements of the user data policy.

If your app integrates third-party code (for example, an SDK) that is designed to collect personal and sensitive user data by default, you must, within two weeks of receipt of a request from Google Play (or, if Google Play's request provides for a longer time period, within that time period), provide sufficient evidence demonstrating that your app meets the prominent disclosure and consent requirements of this policy, including with regard to the data access, collection, use or sharing via the third-party code.

Remember to ensure that your use of third-party code (for example, an SDK) does not cause your app to violate the user data policy.

Refer to this Help Centre article for more information on the prominent disclosure and consent requirement.

Examples of SDK-caused violations

- An app with an SDK that collects personal and sensitive user data and doesn't treat this data as subject to this user data policy, access, data handling (including disallowed sale), and prominent disclosure and consent requirements.
- An app integrates an SDK that collects personal and sensitive user data by default in violation of this policy's requirements regarding user consent and prominent disclosure.
- An app with an SDK that claims to collect personal and sensitive user data only to provide anti-fraud and anti-abuse functionality for the app, but the SDK also shares the data that it collects with third parties for advertising or analytics.
- An app includes an SDK that transmits users' installed packages information without meeting the prominent disclosure guidelines and/or privacy policy guidelines.
  - Also refer to the mobile unwanted software policy.

Additional requirements for personal and sensitive data access

The table below describes requirements for specific activities.

Activity	Requirement
Your app collects or links persistent device identifiers (for example, IMEI, IMSI, SIM Serial No., etc.)	Persistent device identifiers may not be linked to other personal and sensitive user data or resettable device identifiers except for the purposes of: • Telephony linked to a SIM identity (for example, Wi-Fi calling linked to an operator account) and • Enterprise device management apps using device owner mode. These uses must be prominently disclosed to users as specified in the user data policy. Please consult this resource for alternative unique identifiers. Please read the ads policy for additional guidelines for Android advertising ID.
Your app targets children	Your app may only include SDKs that have self-certified for use in child-directed services. See Families Self-Certified Ads SDK Programme for full policy language and requirements.

Examples of SDK-caused violations

- An app using an SDK which links Android ID and location
- An app with an SDK which connects AAID to persistent device identifiers for any advertising purpose or analytics purpose.

- An app using an SDK that connects AAID and email address for analytics purposes.

Data safety section

All developers must complete a clear and accurate Data safety section for every app detailing collection, use and sharing of user data. This includes data collected and handled through any third-party libraries or SDKs used in their apps. The developer is responsible for the accuracy of the label and keeping this information up to date. Where relevant, the section must be consistent with the disclosures made in the app's privacy policy.

Please refer to this Help Centre article for additional information on completing the Data safety section.

See the full user data policy.

Permissions and APIs that access sensitive information policy

Requests for permission and APIs that access sensitive information should make sense to users. You may only request permissions and APIs that access sensitive information that are necessary to implement current features or services in your app that are promoted in your Google Play listing. You may not use permissions or APIs that access sensitive information that give access to user or device data for undisclosed, unimplemented, or disallowed features or purposes. Personal or sensitive data accessed through permissions or APIs that access sensitive information may never be sold nor shared for a purpose facilitating sale.

See the full Permissions and APIs that access sensitive information policy.

Examples of SDK-caused violations

- Your app includes an SDK which requests location in the background for an unallowed or undisclosed purpose.
- Your app includes an SDK which transmits IMEI derived from the read_phone_state Android permission without user consent.

Malware policy

Our malware policy is simple: the Android ecosystem including the Google Play Store and user devices should be free from malicious behaviours (for example, malware). Through this fundamental principle we strive to provide a safe Android ecosystem for our users and their Android devices.

Malware is any code that could put a user, a user's data or a device at risk. Malware includes, but is not limited to, potentially harmful applications (PHAs), binaries or framework modifications, consisting of categories such as trojans, phishing and spyware apps, and we are continuously updating and adding new categories.

See the full malware policy.

Examples of SDK-caused violations

- An app that violates the Android permissions model, or steals credentials (such as OAuth tokens) from other apps.
- Apps that abuse features to prevent them from being uninstalled or stopped.
- An app that disables SELinux.
- Your app includes an SDK that violates the Android permissions model by gaining elevated privileges through the access of device data for an undisclosed purpose
- Your app includes an SDK with code that tricks users into subscribing to or purchasing content via their mobile phone bill.

Privilege escalation apps that root devices without user permission are classified as rooting apps.

Mobile unwanted software policy

Transparent behaviour and clear disclosures

All code should deliver on promises made to the user. Apps should provide all communicated functionality. Apps should not confuse users.

Example violations:

- Ad fraud
- Social engineering

Protect user data

Be clear and transparent about the access, use, collection and sharing of personal and sensitive user data. Uses of user data must adhere to all relevant user data policies, where applicable, and take all precautions to protect the data.

Example violations:

- Data collection (cf spyware)
- Restricted permissions abuse

See the full mobile unwanted software policy

Device and network abuse policy

We don't allow apps that interfere with, disrupt, damage or access in an unauthorised manner the user's device, other devices or computers, servers, networks, application programming interfaces (APIs) or services, including but not limited to other apps on the device, any Google service or an authorised operator network.

Apps or third-party code (for example, SDKs) with interpreted languages (JavaScript, Python, Lua, etc.) loaded at run time (for example, not packaged with the app) must not allow potential violations of Google Play policies.

We don't allow code that introduces or exploits security vulnerabilities. Review the App security improvement programme to find out about the most recent security issues flagged to developers.

See the full device and network abuse policy.

Examples of SDK-caused violations

- Apps that facilitate proxy services to third parties may only do so in apps where that is the primary, user-facing core purpose of the app.
- Your app includes an SDK that downloads executable code, such as dex files or native code, from a source other than Google Play.
- Your app includes an SDK containing a webview with added JavaScript Interface that loads untrusted web content (for example, http:// URL) or unverified URLs obtained from untrusted sources (for example, URLs obtained with untrusted intents)
- Your app includes an SDK that contains code used for updating its own APK
- Your app includes an SDK that exposes users to a security vulnerability by downloading files over an insecure connection.
- Your app is using an SDK which contains code to download or install applications from unknown sources outside Google Play.

Deceptive behaviour policy

We don't allow apps that attempt to deceive users or enable dishonest behaviour, including but not limited to apps which are determined to be functionally impossible. Apps must provide an accurate disclosure, description and images/video of their functionality in all parts of the metadata. Apps must not attempt to mimic functionality or warnings from the operating system or other apps. Any changes to device settings must be made with the user's knowledge and consent and be reversible by the user.

See the full Deceptive behaviour policy.

Behaviour transparency

Your app's functionality should be reasonably clear to users; don't include any hidden, dormant or undocumented features within your app. Techniques to evade app reviews are not allowed. Apps may be required to provide additional details to ensure user safety, system integrity and policy compliance.

Example of an SDK-caused violation

- Your app includes an SDK that uses techniques to evade app reviews.

What Google Play developer policies are commonly associated with SDK-caused violations?

To help you ensure that any third-party code that your app is using complies with Google Play's Developer Programme Policies, please refer to the following policies in their entirety:

- User data policy
- Permissions and APIs that access sensitive information
- Device and network abuse policy
- Malware
- Mobile unwanted software
- Families Self-Certified Ads SDK Programme
- Ads policy
- Deceptive behaviour
- Google Play Developer Programme Policies

While these policies are more commonly at issue, it is important to remember that bad SDK code could cause your app to violate a different policy not referenced above. Remember to review and stay up to date with all policies in their entirety, as it is your responsibility as an app developer to ensure that your SDKs handle your app data in a policy-compliant manner.

To find out more, please visit our Help Centre.

Malware

Our malware policy is simple: the Android ecosystem including the Google Play Store, and user devices should be free from malicious behaviours (for example, malware). Through this fundamental principle we strive to provide a safe Android ecosystem for our users and their Android devices.

Malware is any code that could put a user, a user's data or a device at risk. Malware includes, but is not limited to, potentially harmful applications (PHAs), binaries or framework modifications, consisting of categories such as trojans, phishing and spyware apps, and we are continuously updating and adding new categories.

Though varied in type and capabilities, malware usually has one of the following objectives:

- Compromise the integrity of the user's device.
- Gain control over a user's device.
- Enable remote-controlled operations for an attacker to access, use or otherwise exploit an infected device.
- Transmit personal data or credentials off the device without adequate disclosure and consent.
- Disseminate spam or commands from the infected device to affect other devices or networks.
- Defraud the user.

An app, binary or framework modification can be potentially harmful, and can therefore generate malicious behaviour, even if it wasn't intended to be harmful. This is because apps, binaries or

framework modifications can function differently depending on a variety of variables. Therefore, what is harmful to one Android device might not pose a risk at all to another Android device. For example, a device running the latest version of Android is not affected by harmful apps which use deprecated APIs to perform malicious behaviour, but a device that is still running a very early version of Android might be at risk. Apps, binaries or framework modifications are flagged as malware or PHA if they clearly pose a risk to some or all Android devices and users.

The malware categories below reflect our foundational belief that users should understand how their device is being leveraged and promote a secure ecosystem that enables robust innovation and a trusted user experience.

Visit Google Play Protect for more information.

Backdoors

Code that allows the execution of unwanted, potentially harmful, remote-controlled operations on a device.

These operations may include behaviour that would place the app, binary or framework modification into one of the other malware categories if executed automatically. In general, backdoor is a description of how a potentially harmful operation can occur on a device and is therefore not completely aligned with categories like billing fraud or commercial spyware. As a result, a subset of backdoors, under some circumstances, are treated by Google Play Protect as a vulnerability.

Billing fraud

Code that automatically charges the user in an intentionally deceptive way.

Mobile billing fraud is divided into SMS fraud, call fraud, and toll fraud.

SMS fraud
Code that charges users to send premium SMS without consent, or tries to disguise its SMS activities by hiding disclosure agreements or SMS messages from the mobile operator notifying the user of charges or confirming subscriptions.

Some code, even though it technically discloses SMS sending behaviour, introduces additional behaviour that accommodates SMS fraud. Examples include hiding parts of a disclosure agreement from the user, making them unreadable, and conditionally suppressing SMS messages from the mobile operator informing the user of charges or confirming a subscription.

Call fraud
Code that charges users by making calls to premium numbers without user consent.

Toll fraud
Code that tricks users into subscribing to or purchasing content via their mobile phone bill.

Toll fraud includes any type of billing except premium SMS and premium calls. Examples of this include direct operator billing, wireless access point (WAP) and mobile airtime transfer. WAP fraud is one of the most prevalent types of toll fraud. WAP fraud can include tricking users into clicking a button on a silently loaded, transparent WebView. Upon performing the action, a recurring subscription is initiated, and the confirmation SMS or email is often hijacked to prevent users from noticing the financial transaction.

Stalkerware

Code that collects personal or sensitive user data from a device and transmits the data to a third party (enterprise or another individual) for monitoring purposes.

Apps must provide adequate prominent disclosure and obtain consent as required by the user data policy .

Guidelines for monitoring applications

Apps exclusively designed and marketed for monitoring another individual, for example, parents to monitor their children or enterprise management for the monitoring of individual employees, provided that they fully comply with the requirements described below are the only acceptable monitoring apps. These apps cannot be used to track anyone else (a spouse, for example) even with their knowledge and permission, regardless if persistent notification is displayed. These apps must use the IsMonitoringTool metadata flag in their manifest file to appropriately designate themselves as monitoring apps.

Monitoring apps must comply with these requirements:

- Apps must not present themselves as a spying or secret surveillance solution.
- Apps must not hide or cloak tracking behaviour or attempt to mislead users about such functionality.
- Apps must present users with a persistent notification at all times when the app is running and a unique icon that clearly identifies the app.
- Apps must disclose monitoring or tracking functionality in the Google Play Store description.
- Apps and app listings on Google Play must not provide any means to activate or access functionality that violates these terms, such as linking to a non-compliant APK hosted outside Google Play.
- Apps must comply with any applicable laws. You are solely responsible for determining the legality of your app in its targeted locale.

Please reference the Use of the isMonitoringTool flag Help Centre article for more information.

Denial of service (DoS)

Code that, without the knowledge of the user, executes a denial-of-service (DoS) attack or is part of a distributed DoS attack against other systems and resources.

For example, this can happen by sending a high volume of HTTP requests to produce excessive load on remote servers.

Hostile downloaders

Code that isn't in itself potentially harmful, but downloads other PHAs.

Code may be a hostile downloader if:

- There is reason to believe that it was created to spread PHAs and it has downloaded PHAs or contains code that could download and install apps; or
- At least 5% of apps downloaded by it are PHAs with a minimum threshold of 500 observed app downloads (25 observed PHA downloads).

Major browsers and file-sharing apps aren't considered hostile downloaders as long as:

- They don't drive downloads without user interaction; and
- All PHA downloads are initiated by consenting users.

Non-Android threat

Code that contains non-Android threats.

These apps can't cause harm to the Android user or device, but contain components that are potentially harmful to other platforms.

Phishing

Code that pretends to come from a trustworthy source, requests a user's authentication credentials or billing information, and sends the data to a third party. This category also applies to code that

intercepts the transmission of user credentials in transit.

Common targets of phishing include banking credentials, credit card numbers and online account credentials for social networks and games.

Elevated privilege abuse

Code that compromises the integrity of the system by breaking the app sandbox, gaining elevated privileges or changing or disabling access to core security-related functions.

Examples include:

- An app that violates the Android permissions model, or steals credentials (such as OAuth tokens) from other apps.
- Apps that abuse features to prevent them from being uninstalled or stopped.
- An app that disables SELinux.

Privilege escalation apps that root devices without user permission are classified as rooting apps.

Ransomware

Code that takes partial or extensive control of a device or data on a device and demands that the user make a payment or perform an action to release control.

Some ransomware encrypts data on the device and demands payment to decrypt the data and/or leverage the device admin features so that it can't be removed by a typical user. Examples include:

- Locking a user out of their device and demanding money to restore user control.
- Encrypting data on the device and demanding payment, ostensibly to decrypt the data.
- Leveraging device policy manager features and blocking removal by the user.

Code distributed with the device whose primary purpose is for subsidised device management may be excluded from the ransomware category provided that they successfully meet requirements for secure lock and management, as well as adequate user disclosure and consent requirements.

Rooting

Code that roots the device.

There's a difference between non-malicious and malicious rooting code. For example, non-malicious rooting apps let the user know in advance that they're going to root the device, and they don't execute other potentially harmful actions that apply to other PHA categories.

Malicious rooting apps don't inform the user that they're going to root the device, or they inform the user about the rooting in advance but also execute other actions that apply to other PHA categories.

Spam

Code that sends unsolicited messages to the user's contacts or uses the device as an email spam relay.

Spyware

Code that transmits personal data off the device without adequate notice or consent.

For example, transmitting any of the following information without disclosures or in a manner that is unexpected to the user is sufficient to be considered spyware:

- Contact list
- Photos or other files from the SD card or that aren’t owned by the app
- Content from user email

- Call log
- SMS log
- Web history or browser bookmarks of the default browser
- Information from the /data/ directories of other apps.

Behaviours that can be considered as spying on the user can also be flagged as spyware. For example, recording audio or recording calls made to the phone, or stealing app data.

Trojan

Code that appears to be benign, such as a game that claims only to be a game, but that performs undesirable actions against the user.

This classification is usually used in combination with other PHA categories. A trojan has an innocuous component and a hidden harmful component. For example, a game that sends premium SMS messages from the user's device in the background and without the user's knowledge.

A note on uncommon apps

New and rare apps can be classified as uncommon if Google Play Protect doesn't have enough information to clear them as safe. This doesn't mean that the app is necessarily harmful, but without further review it can't be cleared as safe either.

A note on the backdoor category

The backdoor malware category classification relies on how the code acts. A necessary condition for any code to be classified as a backdoor is that it enables behaviour that would place the code into one of the other malware categories if executed automatically. For example, if an app allows dynamic code loading and the dynamically loaded code is extracting text messages, it will be classified as a backdoor malware.

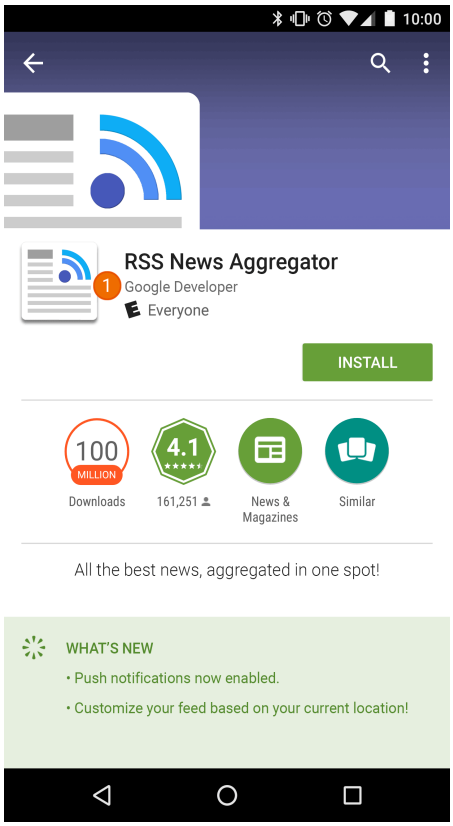
However, if an app allows arbitrary code execution and we don't have any reason to believe that this code execution was added to perform a malicious behaviour, the app will be treated as having a vulnerability, rather than being backdoor malware, and the developer will be asked to patch it.

Impersonation

We don't allow apps that mislead users by impersonating someone else (for example, another developer, company or entity) or another app. Don't imply that your app is related to or authorised by someone when it isn't. Be careful not to use app icons, descriptions, titles or in-app elements that could mislead users about your app's relationship to someone else or another app.

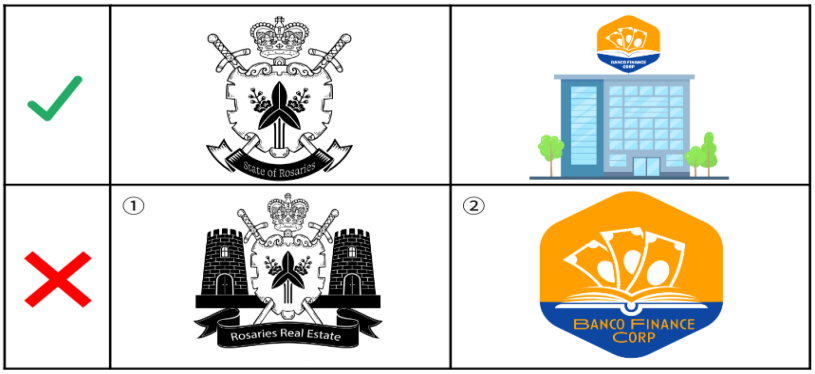
To ensure that Google Play remains a safe and respectful platform, we've created standards defining and prohibiting content that is harmful or inappropriate for our users.

- Developers that falsely imply a relationship to another company/developer/entity/organisation.



① The Developer name listed for this app suggests an official relationship with Google, even though such a relationship doesn't exist.

- Apps whose icons and titles are falsely implying a relationship with another company/developer/entity/organisation.



①The app is using a national emblem and misleads users into believing it is affiliated with the government.
②The app is copying the logo of a business entity to falsely suggest it is an official app of the business.

- App titles and icons that are so similar to those of existing products or services that users may be misled.





①The app is using the logo of a popular cryptocurrency website in its app icon to suggest it is the official website.
②The app is copying the character and title of a famous TV show in its app icon and misleading users to think that it is affiliated with a TV show.

- Apps that falsely claim to be the official app of an established entity. Titles like 'Justin Bieber Official' are not allowed without the necessary permissions or rights.
- Apps that violate the Android brand guidelines .

Mobile unwanted software

At Google, we believe that if we focus on the user, everything else will follow. In our Software principles and the Unwanted software policy, we provide general recommendations for software that delivers a great user experience. This policy builds on the Google unwanted software policy by outlining principles for the Android ecosystem and the Google Play Store. Software that violates these principles is potentially harmful to the user experience, and we will take steps to protect users from it.

As mentioned in the Unwanted software policy, we've found that most unwanted software displays one or more of the same basic characteristics:

- It is deceptive, promising a value proposition that it does not meet.
- It tries to trick users into installing it or it piggybacks on the installation of another program.
- It doesn't tell the user about all of its principal and significant functions.
- It affects the user's system in unexpected ways.
- It collects or transmits private information without the user's knowledge.
- It collects or transmits private information without a secure handling (for example, transmission over HTTPS)
- It is bundled with other software and its presence is not disclosed.

On mobile devices, software is code in the form of an app, binary, framework modification, etc. In order to prevent software that is harmful to the software ecosystem or disruptive to the user experience, we will take action on code that violates these principles.

Below, we build on the unwanted software policy to extend its applicability to mobile software. As with that policy, we will continue to refine this mobile unwanted software policy to address new types of abuse.

Transparent behaviour and clear disclosures

All code should deliver on promises made to the user. Apps should provide all communicated functionality. Apps should not confuse users.

- Apps should be clear about the functionality and objectives.
- Explicitly and clearly explain to the user what system changes will be made by the app. Allow users to review and approve all significant installation options and changes.
- Software should not misrepresent the state of the user's device to the user, for example, by claiming that the system is in a critical security state or infected with viruses.
- Don't use invalid activity designed to increase ad traffic and/or conversions.
- We don't allow apps that mislead users by impersonating someone else (for example, another developer, company or entity) or another app. Don't imply that your app is related to or authorised by someone when it isn't.

Example violations:

- Ad fraud
- Social engineering

Protect user data

Be clear and transparent about the access, use, collection and sharing of personal and sensitive user data. Uses of user data must adhere to all relevant user data policies, where applicable, and take all precautions to protect the data.

- Provide users with an opportunity to agree to the collection of their data before you start collecting and sending it from the device, including data about third-party accounts, email, phone number, installed apps, files, location, and any other personal and sensitive data that the user would not expect to be collected.
- Any personal and sensitive user data collected should be handled securely, including being transmitted using modern cryptography (for example, over HTTPS).
- Software, including mobile apps, must only transmit personal and sensitive user data to servers as it is related to the functionality of the app.

Example violations:

- Data collection (cf. Spyware)
- Restricted permissions abuse

Example user data policies:

- *Google Play User Data policy*
- *GMS requirements user data policy*
- *Google API service user data policy*

Do not harm the mobile experience

The user experience should be straightforward, easy to understand and based on clear choices made by the user. It should present a clear value proposition to the user and not disrupt the advertised or desired user experience.

- Don't show ads that are displayed to users in unexpected ways, including impairing or interfering with the usability of device functions, or displaying outside the triggering app's environment without being easily dismissable or without adequate consent and attribution.
- Apps should not interfere with other apps or the usability of the device

- The uninstall process, where applicable, should be clear.
- Mobile software should not mimic prompts from the device OS or other apps. Do not suppress alerts to the user from other apps or from the operating system, notably those which inform the user of changes to their OS.

Example violations:

- Disruptive ads
- Unauthorised use or imitation of system functionality

Hostile downloaders

Code that isn't in itself unwanted software, but downloads other mobile unwanted software (MUwS).

Code may be a hostile downloader if:

- There is reason to believe it was created to spread MUwS and it has downloaded MUwS or contains code that could download and install apps; or
- At least 5% of apps downloaded by it are MUwS with a minimum threshold of 500 observed app downloads (25 observed MUwS downloads).

Major browsers and file-sharing apps aren't considered hostile downloaders as long as:

- They don't drive downloads without user interaction; and
- All software downloads are initiated by consenting users.

Ad fraud

Ad fraud is strictly prohibited. Ad interactions generated for the purpose of tricking an ad network into believing traffic is from authentic user interest is ad fraud, which is a form of invalid traffic. Ad fraud may be the byproduct of developers implementing ads in disallowed ways, such as showing hidden ads, automatically clicking ads, altering or modifying information and otherwise leveraging non-human actions (spiders, bots, etc.) or human activity designed to produce invalid ad traffic. Invalid traffic and ad fraud is harmful to advertisers, developers and users, and leads to long-term loss of trust in the mobile ads ecosystem.

To ensure that Google Play remains a safe and respectful platform, we've created standards defining and prohibiting content that is harmful or inappropriate for our users.

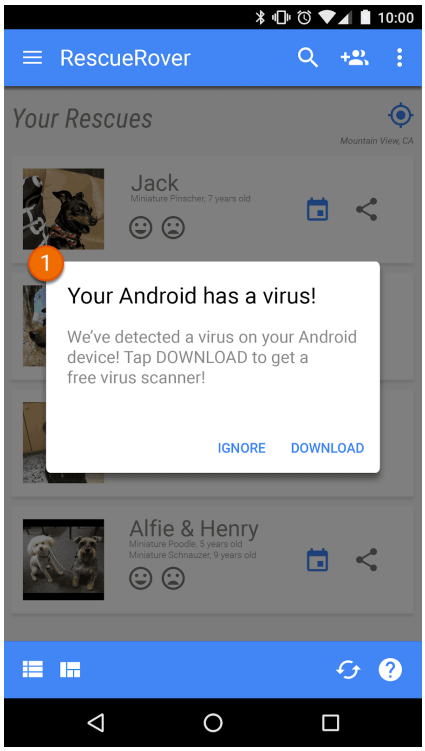
- An app that renders ads that are not visible to the user.
- An app that automatically generates clicks on ads without the user's intention or that produces equivalent network traffic to fraudulently give click credits.
- An app sending fake installation attribution clicks to get paid-for installations that did not originate from the sender’s network.
- An app that makes ads pop up when the user is not within the app interface.
- False representations of the ad inventory by an app, for example, an app that communicates to ad networks that it is running on an iOS device when it is in fact running on an Android device, or an app that misrepresents the package name that is being monetised.

Unauthorised use or imitation of system functionality

We don’t allow apps or ads that mimic or interfere with system functionality, such as notifications or warnings. System level notifications may only be used for an app’s integral features, such as an airline app that notifies users of special deals, or a game that notifies users of in-game promotions.

To ensure that Google Play remains a safe and respectful platform, we've created standards defining and prohibiting content that is harmful or inappropriate for our users.

- Apps or ads that are delivered through a system notification or alert:



① The system notification shown in this app is being used to serve an ad.

For additional examples involving ads, please refer to the Ads policy.

Social engineering

We do not allow apps that pretend to be another app with the intention of deceiving users into performing actions that the user intended for the original trusted app.

Monetisation and ads

Google Play supports a variety of monetisation strategies to benefit developers and users, including paid distribution, in-app products, subscriptions and ad-based models. To ensure the best user experience, we require you to comply with these policies.

Payments

1. Developers charging for app downloads from Google Play must use Google Play's billing system as the method of payment for those transactions.
2. Play-distributed apps requiring or accepting payment for access to in-app features or services, including any app functionality, digital content or goods (collectively, 'in-app purchases'), must use Google Play's billing system for those transactions unless Section 3, Section 8 or Section 9 applies.

> Examples of app features or services requiring use of Google Play's billing system include, but are not limited to, in-app purchases of:

- Items (such as virtual currencies, extra lives, additional playtime, add-on items, characters and avatars);
- subscription services (such as fitness, game, dating, education, music, video, service upgrades and other content subscription services);
- app functionality or content (such as an ad-free version of an app or new features not available in the free version); and
- cloud software and services (such as data storage services, business productivity software and financial management software).

3. Developers charging for app downloads from Google Play must use Google Play's billing system as the method of payment for those transactions.
4. Play-distributed apps requiring or accepting payment for access to in-app features or services, including any app functionality, digital content or goods (collectively 'in-app purchases'), must use Google Play's billing system for those transactions unless Section 3 or Section 8 applies.

   Examples of app features or services requiring use of Google Play's billing system include, but are not limited to, in-app purchases of:

   - Items (such as virtual currencies, extra lives, additional playtime, add-on items, characters and avatars);
   - subscription services (such as fitness, game, dating, education, music, video, service upgrades and other content subscription services);
   - app functionality or content (such as an ad-free version of an app or new features not available in the free version); and
   - cloud software and services (such as data storage services, business productivity software and financial management software).

5. Google Play's billing system must not be used in cases where:
   a. payment is primarily:
      - for the purchase or rental of physical goods (such as groceries, clothing, household goods, electronics);
      - for the purchase of physical services (such as transport services, cleaning services, airfares, gym memberships, food delivery, tickets for live events); or
      - a remittance in respect of a credit card bill or utility bill (such as cable and telecommunications services);

   b. payments include peer-to-peer payments, online auctions and tax-exempt donations;
   c. payment is for content or services that facilitate online gambling, as described in the Gambling apps section of the Real-money gambling, games and contests policy;
   d. payment is in respect of any product category deemed unacceptable under Google's Payments Centre content policies .

      Note: In some markets, we offer Google Pay for apps selling physical goods and/or services. For more information, please visit our Google Pay developer page.

6. Other than the conditions described in Section 3, Section 8 and Section 9, apps may not lead users to a payment method other than Google Play's billing system. This prohibition includes, but is not limited to, leading users to other payment methods via:
   - An app's listing in Google Play;
   - In-app promotions related to purchasable content;
   - In-app webviews, buttons, links, messaging, advertisements or other calls to action; and
   - In-app user interface flows, including account creation or sign-up flows, that lead users from an app to a payment method other than Google Play's billing system as part of those flows.
7. In-app virtual currencies must only be used within the app or game title for which they were purchased.

8. Developers must clearly and accurately inform users about the terms and pricing of their app or any in-app features or subscriptions offered for purchase. In-app pricing must match the pricing displayed in the user-facing Play billing interface. If your product description on Google Play refers to in-app features that may require a specific or additional charge, your app listing must clearly notify users that payment is required to access those features.
9. Apps and games offering mechanisms to receive randomised virtual items from a purchase including, but not limited to, 'loot boxes' must clearly disclose the odds of receiving those items in advance of, and in close and timely proximity to, that purchase.
10. Unless the conditions described in Section 3 apply, developers of Play-distributed apps requiring or accepting payment from users in these markets for access to in-app purchases may offer users an alternative billing system within the app alongside Google Play's billing system for those transactions if they successfully complete the billing declaration form for each respective programme and agree to the additional terms and programme requirements included therein.
11. Developers of Play-distributed apps may lead users in the European Economic Area (EEA) outside the app, including to make a purchase. Unless the conditions described in Section 3 apply, developers who lead EEA users outside the app to make a purchase must successfully complete the declaration form for the programme and agree to the additional terms and programme requirements included therein.

4. Other than the conditions described in Section 3, Section 8 and Section 9, apps may not lead users to a payment method other than Google Play's billing system. This prohibition includes, but is not limited to, leading users to other payment methods via:
   - An app's listing in Google Play;
   - In-app promotions related to purchasable content;
   - In-app webviews, buttons, links, messaging, advertisements or other calls to action; and
   - In-app user interface flows, including account creation or sign-up flows, that lead users from an app to a payment method other than Google Play's billing system as part of those flows.
5. In-app virtual currencies must only be used within the app or game title for which they were purchased.
6. Developers must clearly and accurately inform users about the terms and pricing of their app or any in-app features or subscriptions offered for purchase. In-app pricing must match the pricing displayed in the user-facing Play billing interface. If your product description on Google Play refers to in-app features that may require a specific or additional charge, your app listing must clearly notify users that payment is required to access those features.
7. Apps and games offering mechanisms to receive randomised virtual items from a purchase including, but not limited to, 'loot boxes' must clearly disclose the odds of receiving those items in advance of, and in close and timely proximity to, that purchase.
8. Unless the conditions described in Section 3 apply, developers of Play-distributed apps requiring or accepting payment from users in these countries/regions for access to in-app purchases may offer users an alternative billing system within the app, alongside Google Play's billing system for those transactions if they successfully complete the billing declaration form for each respective programme and agree to the additional terms and programme requirements included therein.
9. Developers of Play-distributed apps may lead users in the European Economic Area (EEA) outside the app, including to promote offers for digital in-app features and services. Developers who lead EEA users outside the app must successfully complete the declaration form for the programme and agree to the additional terms and programme requirements included therein.

Note: To view timelines and frequently asked questions regarding this policy, please visit our Help Centre.

Ads

To maintain a quality experience, we consider your ad's content, audience, user experience, behaviour, security and privacy. We consider ads and associated offers as part of your app; they must also follow all other Google Play policies. We also have additional requirements for ads if you're monetising an app that targets children on Google Play.

You can also read more about our app promotion and store listing policies here, including how we address deceptive promotion practices.

Ad content

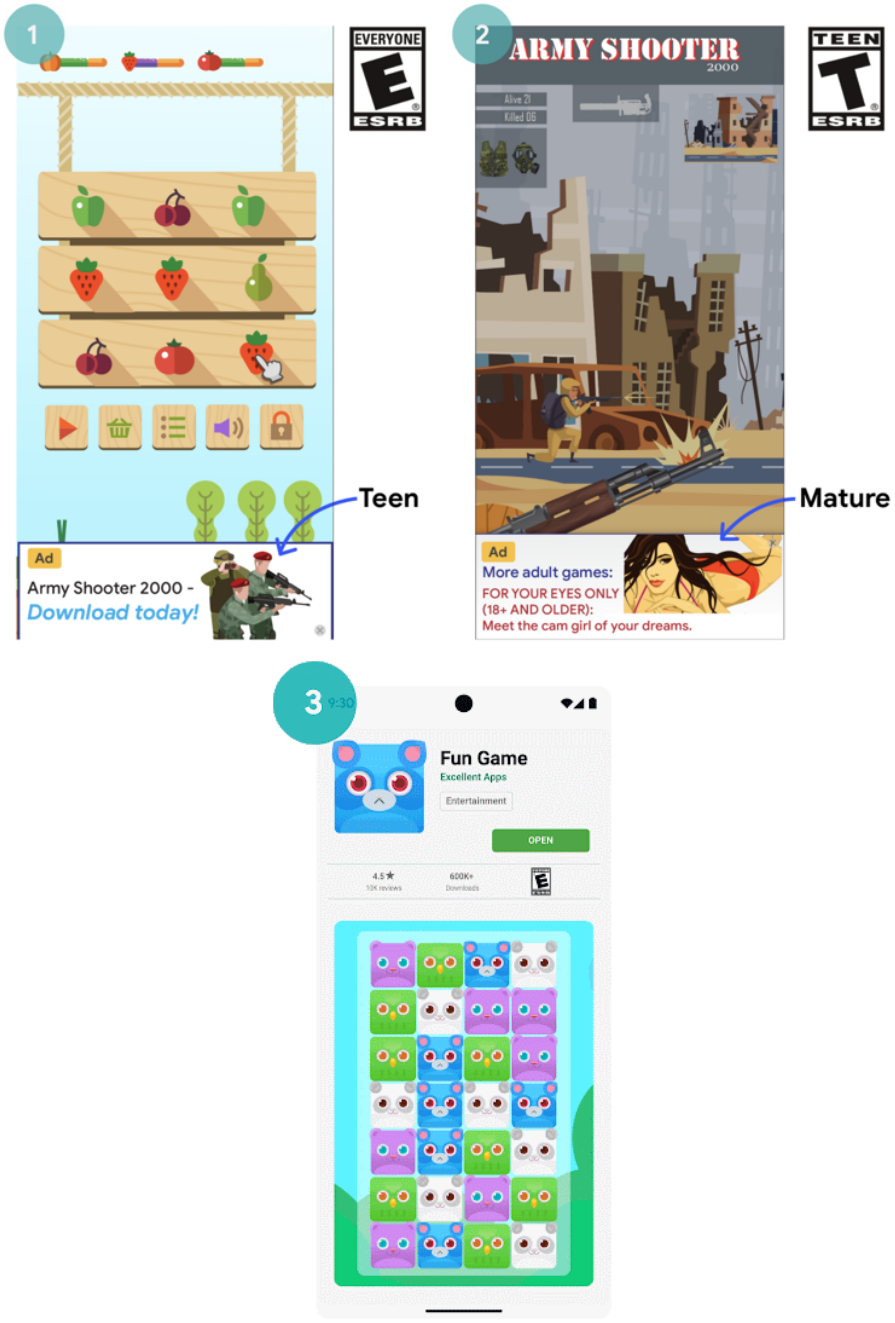
The ads and associated offers are part of your app and must follow our Restricted content policies. Additional requirements apply if your app is a gambling app.

Inappropriate ads

The ads and their associated offers (for example, the ad is promoting the download of another app) shown within your app must be appropriate for the content rating of your app, even if the content by itself is otherwise compliant with our policies.

To ensure that Google Play remains a safe and respectful platform, we've created standards defining and prohibiting content that is harmful or inappropriate for our users.

- Ads that are inappropriate for the content rating of the app



① This ad is inappropriate (Teenager) for the content rating of the app (Everyone)
② This ad is inappropriate (Mature) for the content rating of the app (Teenager)
③ The offer of the ad (promoting the download of a Mature app) is inappropriate for the content rating of the game app in which the ad was displayed (Everyone)

Families ads requirements

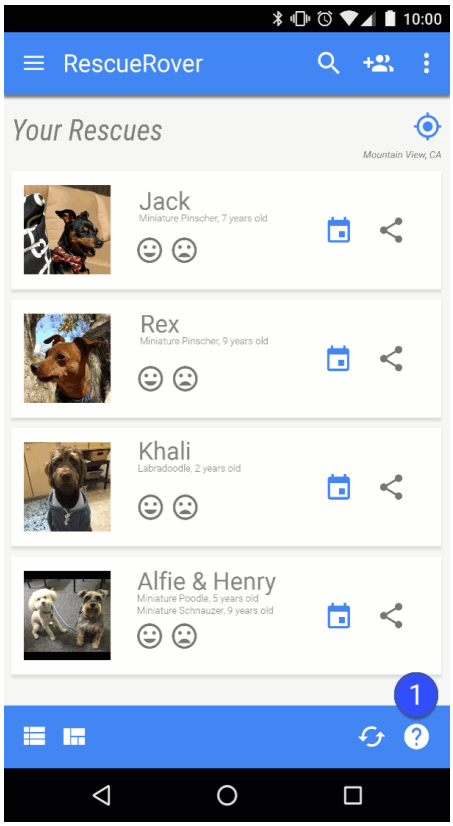
If you're monetising an app that targets children on Google Play, it's important that your app follows the Families Ads and Monetisation policy requirements.

Deceptive ads

Ads must not simulate or impersonate the user interface of any app feature, such as notifications or warning elements of an operating system. It must be clear to the user which app is serving each ad.

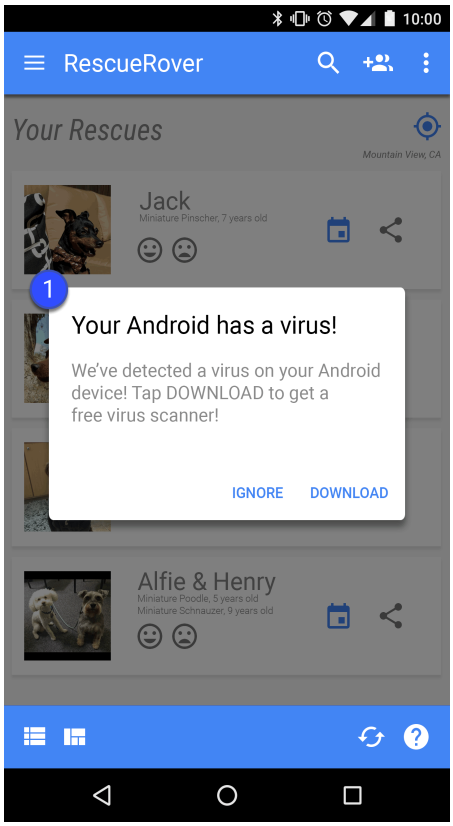
To ensure that Google Play remains a safe and respectful platform, we've created standards defining and prohibiting content that is harmful or inappropriate for our users.

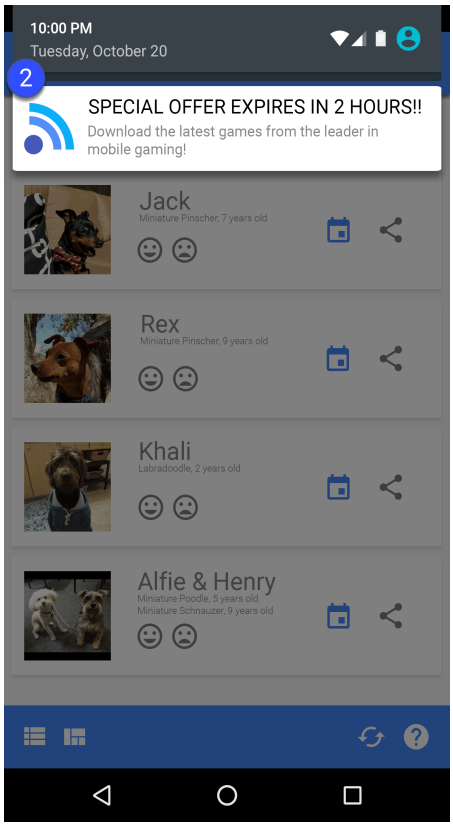
- Ads that mimic an app's UI:



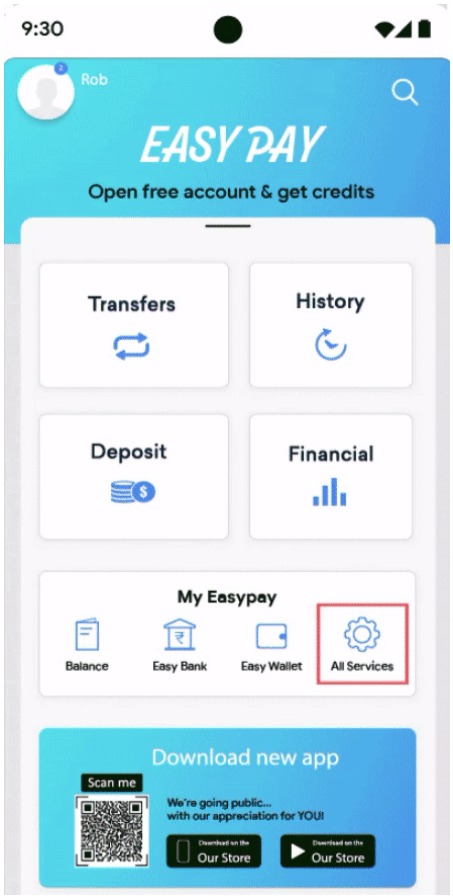
① The question mark icon in this app is an ad that takes the user to an external landing page.

- Ads that mimic a system notification:





① ② The examples above illustrate ads mimicking various system notifications.



① The example above illustrates a feature section that mimics other features but only leads the user to an ad or ads.

Disruptive ads

Disruptive ads are ads that are displayed to users in unexpected ways, that may result in inadvertent clicks, or impairing or interfering with the usability of device functions.

Your app cannot force a user to click an ad or submit personal information for advertising purposes before they can fully use an app. Ads may only be displayed inside of the app serving them and must not interfere with other apps, ads or the operation of the device, including system or device buttons and ports. This includes overlays, companion functionality and widgetised ad units. If your app displays ads or other ads that interfere with normal use, they must be easily dismissible without penalty.

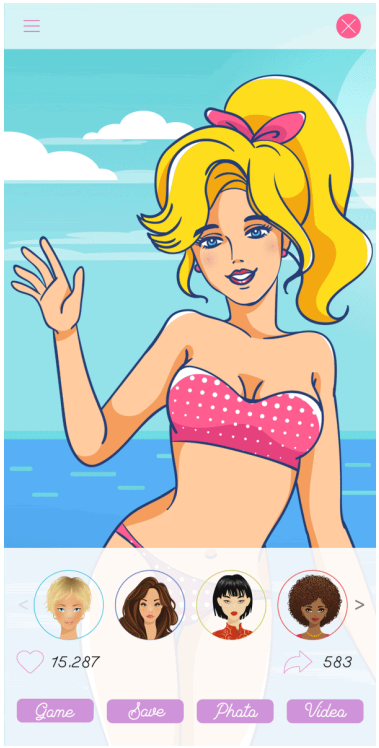
To ensure that Google Play remains a safe and respectful platform, we've created standards defining and prohibiting content that is harmful or inappropriate for our users.

- Ads that take up the entire screen or interfere with normal use and do not provide a clear means to dismiss the ad:

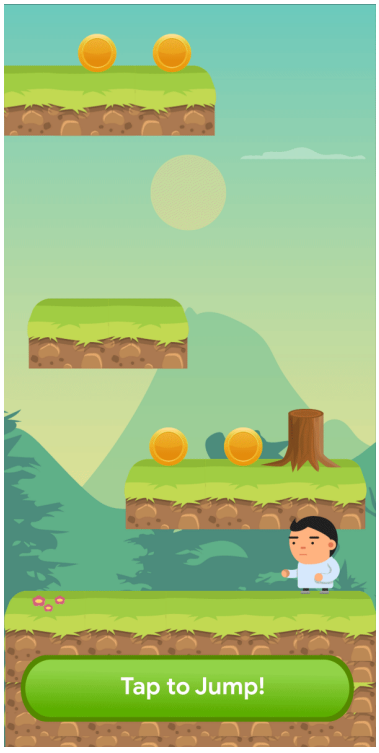


① This ad does not have a dismiss button.

- Ads that force the user to clickthrough by using a false dismiss button, or by making ads suddenly appear in areas of the app whether the user usually taps for another function:

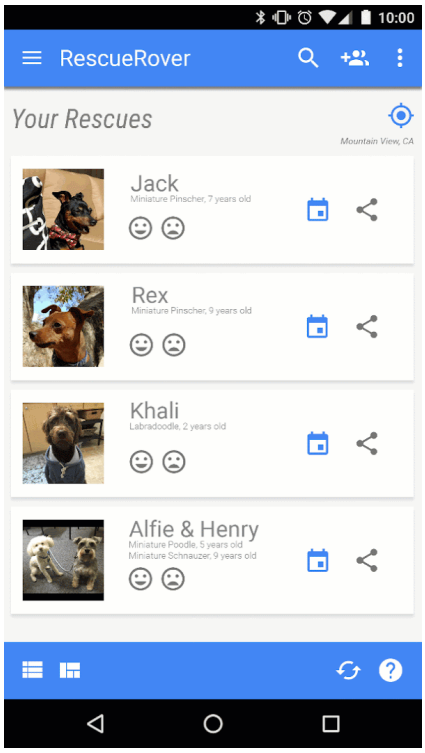


① This ad uses a false dismiss button.



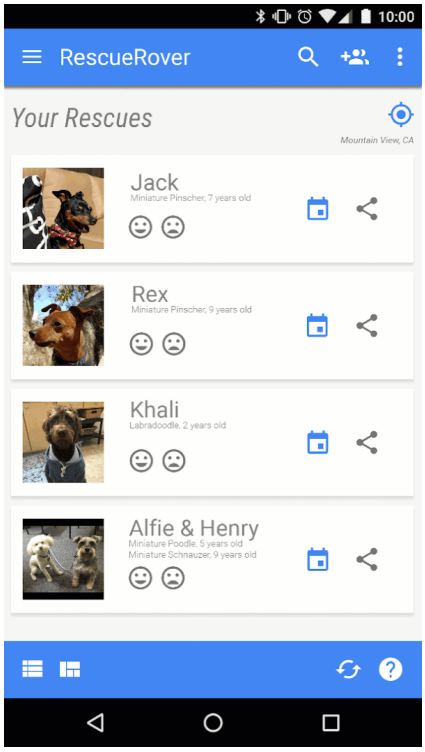
② This ad suddenly appears in an area where the user is used to tapping for in-app functions.

- Ads that display outside of the app serving them:



① The user navigates to the home screen from this app, and suddenly an ad appears on the home screen.

- Ads that are triggered by the home button or other features explicitly designed for exiting the app:



① The user attempts to exit the app and navigate to the home screen, but instead, the expected flow is interrupted by an ad.

Better ad experiences

Developers are required to comply with the following ad guidelines to ensure high-quality experiences for users when they are using Google Play apps. Your ads may not be shown in the following unexpected ways for users:

- Full-screen interstitial ads of all formats (video, GIF, static, etc.) that show unexpectedly, typically when the user has chosen to do something else, are not allowed.
  - Ads that appear during gameplay at the beginning of a level or during the beginning of a content segment are not allowed.
  - Full-screen video interstitial ads that appear before an app's loading screen (splash screen) are not allowed.
- Full-screen interstitial ads of all formats that are not closeable after 15 seconds are not allowed. Opt-in full-screen interstitials or full-screen interstitials that do not interrupt users in their actions (for example, after the score screen in a game app) may persist more than 15 seconds.

This policy does not apply to rewarded ads which are explicitly opted-in by users (for example, an ad that developers explicitly offer a user to watch in exchange for unlocking a specific game feature or a piece of content). This policy also does not apply to monetisation and advertising that does not interfere with normal app use or gameplay (for example, video content with integrated ads, non-fullscreen banner ads).

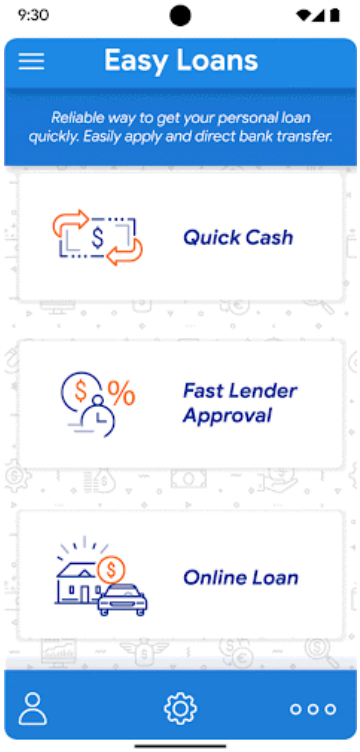
These guidelines are inspired by the Better Ads Standards – mobile apps experience guidelines. For more information on Better Ads Standards, please refer to Coalition of Better Ads .

To ensure that Google Play remains a safe and respectful platform, we've created standards defining and prohibiting content that is harmful or inappropriate for our users.

- Unexpected ads that appear during gameplay or during the beginning of a content segment (for example, after a user has clicked on a button, and before the action intended by the button click has taken effect). These ads are unexpected for users, as users expect to begin a game or engage in content instead.

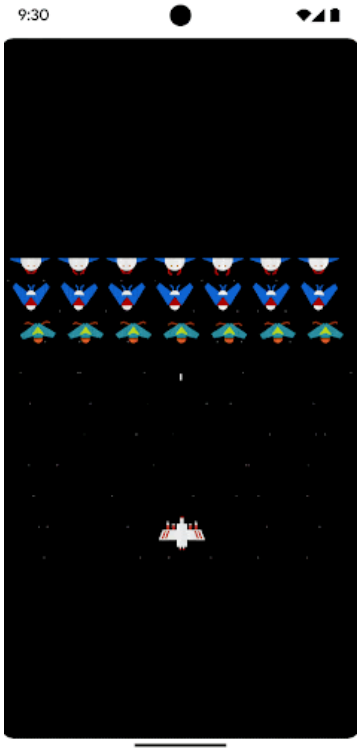


① Unexpected static ad appears during gameplay at the beginning of a level.



② Unexpected video ad appears during the beginning of a content segment.

- A full-screen ad that appears during gameplay and cannot be closed after 15 seconds.



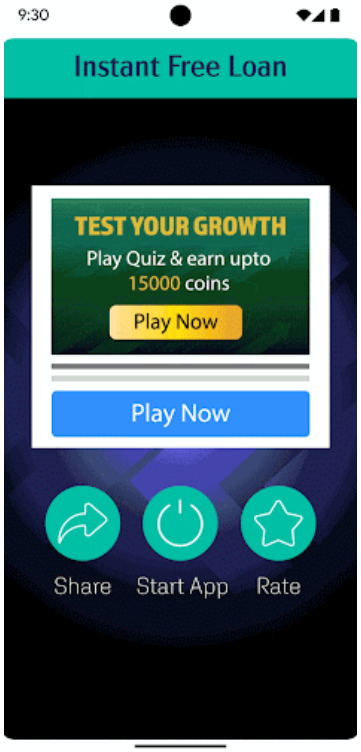
① An interstitial ad appears during gameplay and does not offer users an option to skip within 15 seconds.

Made for ads

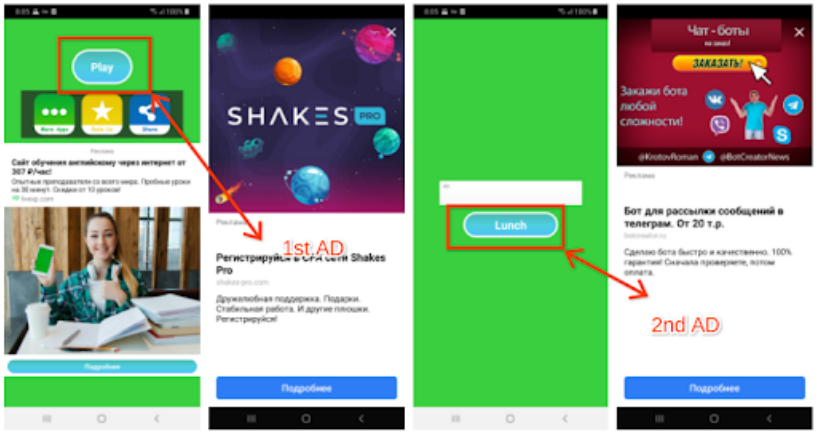
We don’t allow apps that display interstitial ads repeatedly to distract users from interacting with an app and performing in-app tasks.

To ensure that Google Play remains a safe and respectful platform, we've created standards defining and prohibiting content that is harmful or inappropriate for our users.

- Apps where an interstitial ad is placed after a user action (including, but not limited to clicks, swipes, etc.) in a consecutive manner.



① The first in-app page has multiple buttons to interact with. When the user clicks **Start app** to use the app, an interstitial ad pops up. After the ad is closed, the user returns to the app and clicks **Service** to start using the service, but another interstitial ad appears.



② On the first page, the user is led to click **Play** as it is the only button available to use the app. When the user clicks it, an interstitial ad appears. After the ad is closed, the user clicks **Launch** as it is the only button to interact with, and another interstitial ad pops up.

Lock screen monetisation

Unless the exclusive purpose of the app is that of a lock screen, apps may not introduce ads or features that monetise the locked display of a device.

Ad fraud

Ad fraud is strictly prohibited. For more information, refer to our Ad fraud policy.

Use of location data for ads

Apps that extend usage of permission- based device location data for serving ads are subject to the Personal and sensitive information policy, and must also comply with the following requirements:

- Use or collection of permission-based device location data for advertising purposes must be clear to the user and documented in the app's mandatory privacy policy, including linking to any relevant ad network privacy policies addressing location data use.
- In accordance with location permissions requirements, location permissions may only be requested to implement current features or services within your app, and may not request device location permissions solely for the use of ads.

Usage of Android advertising ID

Google Play services version 4.0 introduced new APIs and an ID for use by advertising and analytics providers. Terms for the use of this ID are below.

- **Usage**. The Android advertising identifier (AAID) must only be used for advertising and user analytics. The status of the 'Opt out of interest-based advertising' or 'Opt out of ads personalisation' setting must be verified on each access of the ID.
- **Association with personally identifiable information or other identifiers**.
  - Advertising use: The advertising identifier may not be connected to persistent device identifiers (for example: SSAID, MAC address, IMEI, etc.) for any advertising purpose. The advertising identifier may only be connected to personally identifiable information with the explicit consent of the user.
  - Analytics use: The advertising identifier may not be connected to personally identifiable information or associated with any persistent device identifier (for example: SSAID, MAC address, IMEI, etc.) for any analytics purpose. Please read the User data policy for additional guidelines on persistent device identifiers.
- **Respecting users' selections**.
  - If reset, a new advertising identifier must not be connected to a previous advertising identifier or data derived from a previous advertising identifier without the explicit consent of the user.
  - You must abide by a user's 'Opt out of interest-based advertising' or 'Opt out of ads personalisation' setting. If a user has enabled this setting, you may not use the advertising identifier for creating user profiles for advertising purposes or for targeting users with personalised advertising. Allowed activities include contextual advertising, frequency capping, conversion tracking, reporting and security and fraud detection.
  - On newer devices, when a user deletes the Android advertising identifier, the identifier will be removed. Any attempts to access the identifier will receive a string of zeros. A device without an advertising identifier must not be connected to data linked to or derived from a previous advertising identifier.
- **Transparency to users**. The collection and use of the advertising identifier and commitment to these terms must be disclosed to users in a legally adequate privacy notification. To learn more about our privacy standards, please review our User data policy.
- **Abiding by the Terms of Use**. The advertising identifier may only be used in accordance with the Google Play Developer Programme Policies, including by any party that you may share it with in the course of your business. All apps uploaded or published to Google Play must use the advertising ID (when available on a device) in lieu of any other device identifiers for any advertising purposes.

For more information, refer to our User data policy.

Subscriptions

You, as a developer, must not mislead users about any subscription services or content that you offer within your app. It is critical to communicate clearly in any in-app promotions or splash screens. We do

not allow apps that subject users to deceptive or manipulative purchase experiences (including in-app purchases or subscriptions).

You must be transparent about your offer. This includes being explicit about your offer terms, the cost of your subscription, the frequency of your billing cycle, and whether a subscription is required to use the app. Users should not have to perform any additional action to review the information.

Subscriptions must provide sustained or recurring value to users throughout the life of the subscription, and may not be used to offer what are effectively one-off benefits to users (for example, SKUs that provide lump sum in-app credits/currency or single-use game boosters). Your subscription may offer incentive or promotional bonuses, but these must be complementary to the sustained or recurring value provided throughout the life of the subscription**.** Products that do not offer sustained and recurring value must use an in-app product instead of a subscription product.

You may not disguise or mischaracterise one-off benefits to users as subscriptions. This includes the modification of a subscription to turn it into a one-off offering (for example, cancelling, deprecating or minimising recurring value) after the user has purchased the subscription.

To ensure that Google Play remains a safe and respectful platform, we've created standards defining and prohibiting content that is harmful or inappropriate for our users.

- Monthly subscriptions that do not inform users that they will be automatically renewed and charged every month.
- Annual subscriptions that most prominently display their pricing in terms of monthly cost.
- Subscription pricing and terms that are incompletely localised.
- In-app promotions that do not clearly demonstrate that a user can access content without a subscription (when available).
- SKU names that do not accurately convey the nature of the subscription, such as 'Free of charge trial' or 'Try Premium membership – three days free of charge', for a subscription with an auto-recurring charge.
- Multiple screens in the purchase flow that lead users into accidentally clicking the subscribe button.
- Subscriptions that do not offer sustained or recurring value – for example, offering 1,000 gems for the first month, then reducing the benefit to 1 gem in subsequent months of the subscription.
- Requiring a user to sign up to an auto-renewing subscription to deliver a one-off benefit, and cancelling a user's subscription without their request after the purchase.

Example 1:

① Dismiss button is not clearly visible and users may not understand that they can access functionality without accepting the subscription offer.

② Offer only displays pricing in terms of monthly cost and users may not understand that they will be charged a six-month price at the time that they subscribe.

③ Offer only shows the introductory price and users may not understand what they will automatically be charged at the end of the introductory period.

④ Offer should be localised in the same language as the Terms and Conditions so that users can understand the entire offer.

Example 2:





① Recurring clicks in the same button area causes the user to inadvertently click the final 'continue' button to subscribe.

② The amount that users will be charged at the end of the trial is hard to read, such that users may think that the plan is free of charge

Free trials and introductory offers

Before a user is enrolled in your subscription: You must clearly and accurately describe the terms of your offer, including the duration, pricing and description of accessible content or services. Make sure that you let your users know how and when a free trial will convert to a paid subscription, how much the paid subscription will cost, and that a user can cancel if they do not want to convert to a paid subscription.

To ensure that Google Play remains a safe and respectful platform, we've created standards defining and prohibiting content that is harmful or inappropriate for our users.

- Offers that do not clearly explain how long the free trial or introductory pricing will last.
- Offers that do not clearly explain that the user will be automatically enrolled in a paid subscription at the end of the offer period.
- Offers that do not clearly demonstrate that a user can access content without a trial (when available).
- Offer pricing and terms that are incompletely localised.

① Dismiss button is not clearly visible and users may not understand that they can access functionality without signing up for the free trial.

② Offer emphasises the free trial and users may not understand that they will automatically be charged at the end of the trial.

③ Offer does not state a trial period and users may not understand how long their free access to subscription content will last.

④ Offer should be localised in the same language as the Terms and Conditions so that users can understand the entire offer.

Subscription management, cancellation and refunds

If you sell subscriptions in your app(s), you must ensure that your app(s) clearly disclose how a user can manage or cancel their subscription. You must also include in your app access to an easy-to-use, online method to cancel the subscription. In your app's account settings (or equivalent page), you can satisfy this requirement by including:

- A link to Google Play's subscription centre (for apps that use Google Play's billing system); and/or
- direct access to your cancellation process.

If a user cancels a subscription purchased through Google Play's billing system, our general policy is that the user will not receive a refund for the current billing period, but will continue to receive their subscription content for the remainder of the current billing period, regardless of the cancellation date. The user's cancellation goes into effect after the current billing period has passed.

You (as the content or access provider) may implement a more flexible refund policy with your users directly. It is your responsibility to notify your users of any changes to your subscription, cancellation and refund policies, and ensure that the policies comply with applicable law.

Families self-certified ad SDK programme

If you serve ads in your app, and the target audience for your app only includes children as described in the Families policy , then you must only use ads SDK versions that have self-certified compliance with Google Play policies, including the Families Self-Certified Ads SDK requirements below.

If the target audience for your app includes both children and older users, you must make sure that ads shown to children come exclusively from one of these self-certified ads SDK versions (for example, through use of neutral age screening measures).

Note that it is your responsibility to ensure that all SDK versions that you implement in your app, including self-certified ads SDK versions, are compliant with all applicable policies, local laws and regulations. Google does not provide any representations or guarantees as to the accuracy of the information that the ad SDKs provide during the self-certification process.

The use of Families self-certified ad SDKs is only required if you are using ad SDKs to serve ads to children. The following are permitted without an ads SDK's self-certification with Google Play; however, you are still responsible for ensuring that your ad content and data collection practices are compliant with Google Play's user data policy and Families policy :

- In-house advertising whereby you use SDKs to manage cross-promotion of your apps or other owned media and merchandising.
- Entering into direct deals with advertisers whereby you use SDKs for inventory management.

Families self-certified ad SDK requirements

- Define what are objectionable ad content and behaviours and prohibit them in the ad SDK's terms or policies. The definitions should comply with Google Play Developer Programme Policies.
- Create a method to rate your ad creatives according to age-appropriate groups. Age-appropriate groups must at least include groups for 'Everyone' and 'Mature'. The rating methodology must align with the methodology that Google supplies to SDKs once they have filled in the interest form below.
- Allow publishers, on a per-request or per-app basis, to request child-directed treatment for ad serving. Such treatment must be in compliance with applicable laws and regulations, such as the US Children's Online Privacy and Protection Act (COPPA) and the EU General Data Protection Regulation (GDPR) . Google Play requires ad SDKs to disable personalised ads, interest-based advertising and remarketing as part of the child-directed treatment.
- Allow publishers to select ad formats that are compliant with Google Play's Families Ads and Monetisation policy , and meet the requirement of the Expert Approved programme .
- Ensure that when real-time bidding is used to serve ads to children, the creatives have been reviewed and privacy indicators are propagated to the bidders.
- Provide Google with sufficient information, such as submitting a test app and the information indicated in the interest form below, to verify the ads SDK's policy compliance with all self-certification requirements, respond in a timely manner to any subsequent requests for information, such as submitting new version releases to verify the ads SDK version's compliance with all self-certification requirements, and providing a test app.
- Self-certify that all new version releases are compliant with the latest Google Play Developer Programme Policies, including Families policy requirements.

Note: Families Self-Certified Ads SDKs must support ad serving that complies with all relevant statutes and regulations concerning children that may apply to their publishers.

More information on watermarking ad creatives and providing a test app can be found here .

Here are mediation requirements for serving platforms when serving ads to children:

- Only use Families self-certified ad SDKs or implement safeguards necessary to ensure that all ads served from mediation comply with these requirements; and
- Pass the information necessary to mediation platforms to indicate the ad content rating and any applicable child-directed treatment.

Developers can find a list of Families Self-Certified Ads SDKs and can check which specific versions of those ads SDKs are self-certified for use in Families apps here .

Also, developers can share this interest form with ad SDKs who wish to self-certify.

Store Listing and promotion

The promotion and visibility of your app dramatically affects store quality. Avoid spammy Store Listings, low-quality promotion and efforts to artificially boost app visibility on Google Play.

App promotion

We don’t allow apps that directly or indirectly engage in, or benefit from promotion practices (such as ads) that are deceptive or harmful to users or the developer ecosystem. Promotion practices are deceptive or harmful if their behaviour or content violate our Developer Programme Policies.

To ensure that Google Play remains a safe and respectful platform, we've created standards defining and prohibiting content that is harmful or inappropriate for our users.

- Using deceptive ads on websites, apps or other properties, including notifications that are similar to system notifications and alerts.
- Using sexually explicit ads to direct users to your app’s Google Play listing for download.
- Promotion or installation tactics that redirect users to Google Play or download apps without informed user action.
- Unsolicited promotion via SMS services.
- Text or image in the app title, icon or developer name that indicates store performance or ranking, price or promotional information, or that suggests relations to existing Google Play programmes.

It is your responsibility to ensure that any ad networks, affiliates or ads associated with your app comply with these policies.

Metadata

Users depend on descriptions of your app to help them understand its functionality and purpose. We don't allow apps with misleading, improperly formatted, non-descriptive, irrelevant, excessive or inappropriate metadata, including, but not limited to, the app's description, developer name, title, icon, screenshots and promotional images. Developers must provide a clear and well-written description of their app. We also don't allow unattributed or anonymous user testimonials in the app's description.

Your app title, icon and Developer name are particularly helpful for users to find and learn about your app. Don’t use emojis, emoticons or repeated special characters in these metadata elements. Avoid ALL CAPS unless it is part of your brand name. Misleading symbols in app icons are not allowed; for example, new message dot indicator when there are no new messages and download/install symbols when the app is not related to downloading content. Your app title must be 30 characters or fewer. Don’t use text or image in the app title, icon or developer name that indicates store performance or ranking, price or promotional information, or that suggests relations to existing Google Play programmes.

In addition to the requirements noted here, specific Google Play developer policies may require you to provide additional metadata information.

To ensure that Google Play remains a safe and respectful platform, we've created standards defining and prohibiting content that is harmful or inappropriate for our users.

① Unattributed or anonymous user testimonials
② Data comparison of apps or brands
③ Word blocks and vertical/horizontal word lists

① ALL CAPS although not part of brand name
② Special character sequences that are irrelevant to the app
③ Use of emojis, emoticons (including kaomojis) and special characters
④ Misleading symbol
⑤ Misleading text

- Images or text that indicate store performance or ranking, such as 'App of the year', 'No.1', 'Best of Play 20XX', 'Popular', award icons, etc.

- Images or text that indicate price and promotional information, such as '10% off', '£50 cash back', 'free for limited time only', etc.

- Images or text that indicate Google Play programmes, such as 'Editor’s choice', 'New', etc.

Here are some examples of inappropriate text, images or videos within your listing:

- Imagery or videos with sexually suggestive content. Avoid suggestive imagery containing breasts, buttocks, genitalia or other sexual anatomy or content, whether illustrated or real.
- Using profane, vulgar or other language that is inappropriate for a general audience in your app’s Store Listing.
- Graphic violence prominently depicted in app icons, promotional images or videos.
- Depictions of the illicit use of drugs. Even EDSA (Educational, Documentary, Scientific or Artistic) content must be suitable for all audiences within the Store Listing.

Here are a few best practices:

- Highlight what's great about your app. Share interesting and exciting facts about your app to help users understand what makes your app special.
- Make sure that your app's title and description accurately describe your app's functionality.
- Avoid using repetitive or unrelated keywords or references.
- Keep your app's description succinct and straightforward. Shorter descriptions tend to result in a better user experience, especially on devices with smaller displays. Excessive length, detail, improper formatting or repetition can result in a violation of this policy.
- Remember that your listing should be suitable for a general audience. Avoid using inappropriate text, images or videos in your listing and adhere to the guidelines above.

User ratings, reviews and installs

Developers must not attempt to manipulate the placement of any apps on Google Play. This includes, but is not limited to, inflating product ratings, reviews or install counts by illegitimate means, such as fraudulent or incentivised reviews and ratings, or incentivising users to install other apps as the app's main functionality.

To ensure that Google Play remains a safe and respectful platform, we've created standards defining and prohibiting content that is harmful or inappropriate for our users.

- Asking users to rate your app while offering an incentive:

① This notification offers users a discount in exchange for a high rating.

- Repeatedly submitting ratings posing as users to influence an app's placement on Google Play.

- Submitting or encouraging users to submit reviews containing inappropriate content, including affiliates, coupons, game codes, email addresses or links to websites or other apps:

② This review encourages users to promote the Rescue Rover app by making a coupon offer.

Ratings and reviews are benchmarks of app quality. Users depend on them to be authentic and relevant. Here are some best practices when responding to user reviews:

- Keep your reply focused on the issues raised in the user's comments and don't ask for a higher rating.
- Include references to helpful resources such as a support address or FAQ page.

Content ratings

Content ratings on Google Play are provided by the International Age Rating Coalition (IARC) and are designed to help developers communicate locally relevant content ratings to users. Regional IARC authorities maintain guidelines which are used to determine the maturity level of the content in an app. We don't allow apps without a content rating on Google Play.

How content ratings are used

Content ratings are used to inform consumers, especially parents, of potentially objectionable content that exists within an app. They also help filter or block your content in certain regions or to specific users where required by law, and determine your app's eligibility for special developer programmes.

How content ratings are assigned

To receive a content rating, you must fill in a rating questionnaire on the Play Console that asks about the nature of your apps' content. Your app will be assigned a content rating from multiple rating authorities based on your questionnaire responses. Misrepresentation of your app's content may result in removal or suspension, so it is important to provide accurate responses to the content rating questionnaire.

To prevent your app from being listed as 'Unrated', you must complete the content rating questionnaire for each new app submitted to the Play Console, as well as for all existing apps that are

active on Google Play. Apps without a content rating will be removed from the Play Store.

If you make changes to your app content or features that affect the responses to the rating questionnaire, you must submit a new content rating questionnaire in the Play Console.

Visit the Help Centre to find more information on the different rating authorities and how to complete the content rating questionnaire.

Rating appeals

If you do not agree with the rating assigned to your app, you can appeal directly to the IARC rating authority using the link provided in your certificate email.

News

A News app is an app that:

- Declares itself as a 'News' app in the Google Play Console, or
- Lists itself within the 'News and magazine' category on the Google Play Store and describes itself as 'news' in its app title, icon, developer name or description.

Examples of apps within the 'News and magazine' category that qualify as News apps:

- Apps that describe themselves as 'news' in app descriptions, including but not limited to:
  - Latest news
  - Newspaper
  - Breaking news
  - Local news
  - Daily news
- Apps with the word 'News' in app titles, icons or developer name.

However, if apps contain primarily user-generated content (for example, social media apps), they should not declare themselves as News apps, and are not considered to be News apps.

News apps that require a user to purchase a membership must provide an in-app content preview for users prior to purchase.

News apps must:

- Provide ownership information about the app and the source of news articles including, but not limited to, the original publisher or author of each article. In cases where it is not customary to list individual authors for articles, the news app must be the original publisher of the articles. Please note that links to social media accounts are not sufficient forms of author or publisher information.
- Have a dedicated website or in-app page that is clearly labelled as containing contact information, is easy to find (for example, linked at the bottom of the home page or in the site navigation bar), and provides valid contact information for the news publisher, including either a contact email address or a phone number. Please note that links to social media accounts are not sufficient forms of publisher contact information.

News apps must not:

- Contain significant spelling and/or grammatical errors,
- Contain only static content (for example, content that is more than three months old), or
- Have affiliate marketing or ad revenue as its primary purpose.

Please note that News apps *may* use ads and other forms of marketing to monetise as long as the app's primary purpose isn't to sell products and services or generate advertising revenue.

News apps that aggregate content from different publishing sources must be transparent about the publishing source of the content in the app and each of the sources must meet News policy requirements.

Please consult this article for how best to provide required information.

Spam and minimum functionality

At a minimum, apps should provide users with a basic degree of functionality and a respectful user experience. Apps that crash, exhibit other behaviour that is not consistent with a functional user experience, or that serve only to spam users or Google Play are not apps that expand the catalogue in a meaningful way.

Spam

We don't allow apps that spam users or Google Play, such as apps that send users unsolicited messages or apps that are repetitive or low quality.

Message spam

We don’t allow apps that send SMS, email or other messages on behalf of the user without giving the user the ability to confirm the content and intended recipients.

To ensure that Google Play remains a safe and respectful platform, we've created standards defining and prohibiting content that is harmful or inappropriate for our users.

- When the user pressed the ‘Share’ button, the app sent messages on the user’s behalf without giving them the ability to confirm the content and intended recipients:

Web views and affiliate spam

We don’t allow apps whose primary purpose is to drive affiliate traffic to a website or provide a web view of a website without permission from the website owner or administrator.

To ensure that Google Play remains a safe and respectful platform, we've created standards defining and prohibiting content that is harmful or inappropriate for our users.

- An app whose primary purpose is to drive referral traffic to a website to receive credit for user sign-ups or purchases on that website.
- Apps whose primary purpose is to provide a web view of a website without permission:

① This app is called 'Ted's Shopping Deals' and it simply provides a web view of Google Shopping.

Repetitive content

We don't allow apps that merely provide the same experience as other apps already on Google Play. Apps should provide value to users through the creation of unique content or services.

To ensure that Google Play remains a safe and respectful platform, we've created standards defining and prohibiting content that is harmful or inappropriate for our users.

- Copying content from other apps without adding any original content or value.
- Creating multiple apps with highly similar functionality, content and user experience. If these apps are each small in content volume, developers should consider creating a single app that aggregates all the content.

Minimum functionality

Ensure that your app provides a stable, engaging, responsive user experience.

To ensure that Google Play remains a safe and respectful platform, we've created standards defining and prohibiting content that is harmful or inappropriate for our users.

-

Apps that are designed to do nothing or have no function

Broken functionality

We don’t allow apps that crash, force close, freeze or otherwise function abnormally.

To ensure that Google Play remains a safe and respectful platform, we've created standards defining and prohibiting content that is harmful or inappropriate for our users.

- Apps that **don’t install**
-

Apps that install, but **don’t load**

- Apps that load, but are **not responsive**

Other programs

In addition to compliance with the content policies set out elsewhere in this Policy Centre, apps that are designed for other Android experiences and distributed via Google Play may also be subject to program-specific policy requirements. Make sure that you review the list below to determine if any of these policies apply to your app.

Android Instant Apps

Our goal with Android Instant Apps is to create delightful, frictionless user experiences while also adhering to the highest standards of privacy and security. Our policies are designed to support that goal.

Developers choosing to distribute Android Instant Apps through Google Play must adhere to the following policies, in addition to all other Google Play Developer Programme Policies.

Identity

For instant apps that include login functionality, developers must integrate Smart Lock for Passwords

.

Link support

Android Instant Apps developers are required to properly support links for other apps. If the developer's instant app(s) or installed app(s) contains links that have the potential to resolve to an instant app, the developer must send users to that instant app, rather than, for example, capturing the links in a WebView.

Technical specifications

Developers must comply with the Android Instant Apps technical specifications and requirements provided by Google, as may be amended from time to time, including those listed in our public

documentation .

Offering app installation

The instant app may offer the user the installable app, but this must not be the instant app's primary purpose. When offering installation, developers must:

- Use the Material Design 'get app' icon and the label 'install' for the installation button.
- Not have more than 2–3 implicit installation prompts in their instant app.
- Not use a banner or other ad-like technique for presenting an installation prompt to users.

Additional instant app details and UX guidelines can be found in the Best practices for user experience .

Changing device state

Instant apps must not make changes to the user's device that persist longer than the instant app session. For example, instant apps may not change the user's wallpaper or create a home screen widget.

App visibility

Developers must ensure that instant apps are visible to the user, such that the user is aware at all times that the instant app is running on their device.

Device identifiers

Instant apps are prohibited from accessing device identifiers that both (1) persist after the instant app stops running and (2) are not resettable by the user. Examples include, but are not limited to:

- Build Serial
- Mac Addresses of any networking chips
- IMEI, IMSI

Instant apps may access phone numbers if obtained using the runtime permission. The developer must not attempt to fingerprint the user by using these identifiers, or any other means.

Network traffic

Network traffic from inside the instant app must be encrypted using a TLS protocol like HTTPS.

Android emoji policy

Our emoji policy is designed to promote an inclusive and consistent user experience. To accomplish that, all apps must support the latest version of Unicode emoji when running on Android 12+.

Apps that use default Android emoji without any custom implementations already use the latest version of Unicode emoji when running on Android 12+.

Apps with custom emoji implementations, including those provided by third-party libraries, must fully support the latest Unicode version when running on Android 12+ within four months after new Unicode emoji are released.

Consult this guide to learn how to support modern emoji.

Use the emoji examples below to test if your app is compliant with the latest Unicode version:

Examples	Unicode version
🩷 🤳🏾 🦃	15.0

Examples	Unicode version
🫱 🤝 🫲	14.0
👁️ 🧑‍🏫 🧑‍🏫	13.1
🥲 🧑‍🏫 🐨	13.0
🧑‍🦰 🚶 👫	12.1
🦩 🦃 👫	12.0

Families

Google Play offers a rich platform for developers to showcase their high-quality, age-appropriate content for the whole family. Before submitting an app to the Designed for Families programme or submitting an app that targets children to the Google Play Store, you are responsible for ensuring that your app is appropriate for children and compliant with all relevant laws.

Learn about the families process and review the interactive checklist at Academy for App Success.

Google Play Families policies

The use of technology as a tool for enriching families' lives continues to grow, and parents are looking for safe, high-quality content to share with their children. You may be designing your apps specifically for children, or your app may just attract their attention. Google Play wants to help you make sure that your app is safe for all users, including families.

The word 'children' can mean different things in different locales and in different contexts. It is important that you consult with your legal counsel to help determine what obligations and/or age-based restrictions may apply to your app. You know best how your app works, so we are relying on you to help us to make sure that apps on Google Play are safe for families.

All apps that comply with Google Play Families policies can opt in to be rated for the Expert Approved programme, but we cannot guarantee that your app will be included in the Expert Approved programme.

Play Console requirements

Target audience and content

In the Target audience and content section of the Google Play Console you must indicate the target audience for your app, prior to publishing, by selecting from the list of age groups provided. Regardless of what you identify in the Google Play Console, if you choose to include imagery and terminology in your app that could be considered as targeting children, this may impact Google Play's assessment of your declared target audience. Google Play reserves the right to conduct its own review of the app information that you provide to determine whether the target audience that you disclose is accurate.

If you select a target audience that only includes adults, but Google determines that this is inaccurate because your app is targeting both children and adults, you will have the option to make clear to users that your app is not targeting children by agreeing to carry a warning label.

You should only select more than one age group for your app's target audience if you have designed your app for and ensured that your app is appropriate for users within the selected age group(s). For example, apps designed for babies, toddlers and pre-school children should only have the age group 'Ages 5 and under' selected as the age group target for those apps. If your app is designed for a specific level of school, choose the age group that best represents that school level. You should only select age groups that include both adults and children if you have truly designed your app for all ages.

Updates to target audience and content section

You can always update your app's information in the Target audience and Content section in the Google Play Console. An app update is required before this information will be reflected on the Google Play store. However, any changes that you make in this section of the Google Play Console may be reviewed for policy compliance even before an app update is submitted.

We strongly recommend that you let your existing users know if you change the target age group for your app or start using ads or in-app purchases, either by using the 'What's New' section of your app's store listing page or through in-app notifications.

Misrepresentation in Play Console

Misrepresentation of any information about your app in the Play Console, including in the target audience and content section, may result in removal or suspension of your app, so it is important to provide accurate information.

Families policy requirements

If one of the target audiences for your app is children, you must comply with the following requirements. Failure to satisfy these requirements may result in app removal or suspension.

1. **App content:** Your app's content that is accessible to children must be appropriate for children. If your app contains content that is not globally appropriate, but that content is deemed appropriate for child users in a particular region, the app may be available in that region (limited regions) but will remain unavailable in other regions.
2. **App functionality:** Your app must not merely provide a web view of a website or have a primary purpose of driving affiliate traffic to a website without permission from the website owner or administrator.
3. **Play Console answers:** You must accurately answer the questions in the Play Console regarding your app and update those answers to accurately reflect any changes to your app. This includes, but is not limited to, providing accurate responses about your app in the target audience and content section, Data safety section and IARC content rating questionnaire.
4. **Data practices:** You must disclose the collection of any personal and sensitive information from children in your app, including through APIs and SDKs called or used in your app. Sensitive information from children includes, but is not limited to, authentication information, microphone and camera sensor data, device data, Android ID and ad usage data. You must also ensure that your app follows the data practices below:
   - Apps that solely target children must not transmit Android advertising identifier (AAID), SIM serial, build serial, BSSID, MAC, SSID, IMEI and/or IMSI.
     - Apps solely targeted to children should not request AD_ID permission when targeting Android API 33 or higher.
   - Apps that target both children and older audiences must not transmit AAID, SIM serial, build serial, BSSID, MAC, SSID, IMEI and/or IMSI from children or users of unknown age.
   - Device phone number must not be requested from TelephonyManager of the Android API.
   - Apps that solely target children may not request location permission, or collect, use and transmit precise location.
   - Apps must use the Companion Device Manager (CDM) when requesting Bluetooth, unless your app is only targeting device operating system (OS) versions that are not compatible with CDM.
5. **APIs and SDKs:** You must ensure that your app properly implements any APIs and SDKs.
   - Apps that solely target children must not contain any APIs or SDKs that are not approved for use in primarily child-directed services.
     - For example, an API service using OAuth technology for authentication and authorisation whose Terms of Service state that it is not approved for use in child-directed services.
   - Apps that target both children and older audiences must not implement APIs or SDKs that are not approved for use in child-directed services unless they are used behind a neutral age screen or

implemented in a way that does not result in the collection of data from children. Apps that target both children and older audiences must not require users to access app content through an API or SDK that is not approved for use in child-directed services.

6. **Augmented reality (AR):** If your app uses augmented reality, you must include a safety warning immediately upon launch of the AR section. The warning should contain the following:
   - An appropriate message about the importance of parental supervision.
   - A reminder to be aware of physical hazards in the real world (for example, be aware of your surroundings).
   - Your app must not require the usage of a device that is advised not to be used by children (for example, Daydream, Oculus).
7. **Social apps and features:** If your apps allow users to share or exchange information, you must accurately disclose these features in the content rating questionnaire on the Play Console.
   - Social apps: A social app is an app where the main focus is to enable users to share freeform content or communicate with large groups of people. All social apps that include children in their target audience must provide an in-app reminder to be safe online and to be aware of the real-world risk of online interaction before allowing child users to exchange freeform media or information. You must also require adult action before allowing child users to exchange personal information.
   - Social features: A social feature is any additional app functionality that enables users to share freeform content or communicate with large groups of people. Any app that includes children in their target audience and has social features, must provide an in-app reminder to be safe online and to be aware of the real world risk of online interaction before allowing child users to exchange freeform media or information. You must also provide a method for adults to manage social features for child users, including, but not limited to, enabling/disabling the social feature or selecting different levels of functionality. Finally, you must require adult action before enabling features that allow children to exchange personal information.
   - Adult action means a mechanism to verify that the user is not a child and does not encourage children to falsify their age to gain access to areas of your app that are designed for adults (that is, an adult PIN, password, birthdate, email verification, photo ID, credit card or SSN).
   - Social apps where the main focus of the app is to chat with people that they do not know must not target children. Examples include: chat roulette style apps, dating apps, kids-focused open chat rooms, etc.
8. **Legal compliance:** You must ensure that your app, including any APIs or SDKs that your app calls or uses, is compliant with the US Children's Online Privacy and Protection Act (COPPA) , the EU General Data Protection Regulation (GDPR) , and any other applicable laws or regulations.

To ensure that Google Play remains a safe and respectful platform, we've created standards defining and prohibiting content that is harmful or inappropriate for our users.

- Apps that promote play for children in their Store Listing but the app content is only appropriate for adults.
- Apps that implement APIs with Terms of Service that prohibit their use in child-directed apps.
- Apps that glamourise the use of alcohol, tobacco or controlled substances.
- Apps that include real or simulated gambling.
- Apps that include violence, gore or shocking content not appropriate for children.
- Apps that provide dating services or offer sexual or marital advice.
- Apps that contain links to websites that present content that violates Google Play's Developer Programme Policies .
- Apps that show mature ads (for example, violent content, sexual content, gambling content) to children.

Ads and monetisation

If you're monetising an app that targets children on Play, it's important that your app follows the following families ads and monetisation policy requirements.

The policies below apply to all monetisation and advertising in your app, including ads, cross-promotions (for your apps and third party apps), offers for in-app purchases, or any other commercial content (such as paid product placement). All monetisation and advertising in these apps must comply with all applicable laws and regulations (including any relevant self-regulatory or industry guidelines).

Google Play reserves the right to reject, remove or suspend apps for overly aggressive commercial tactics.

Ads requirements

If your app displays ads to children or to users of unknown age, you must:

- Only use Google Play Families self-certified ads SDKs to display ads to those users;
- Ensure that ads displayed to those users do not involve interest-based advertising (advertising targeted at individual users who have certain characteristics based on their online browsing behaviour) or remarketing (advertising targeted at individual users based on previous interaction with an app or website);
- Ensure that ads displayed to those users present content that is appropriate for children;
- Ensure that ads displayed to those users follow the Families ad format requirements; and
- Ensure compliance with all applicable legal regulations and industry standards relating to advertising to children.

Ads format requirements

Monetisation and advertising in your app must not have deceptive content or be designed in a way that will result in inadvertent clicks from child users.

If the sole target audience for your app is children, the following are prohibited. If the target audiences of your app is children and older audiences, the following are prohibited when serving ads to children or users of unknown age:

- Disruptive monetisation and advertising, including monetisation and advertising that takes up the entire screen or interferes with normal use and does not provide a clear means to dismiss the ad (for example, ad walls).
- Monetisation and advertising that interferes with normal app use or gameplay, including rewarded or opt-in ads, that are not closeable after five seconds.
- Monetisation and advertising that do not interfere with normal app use or gameplay may persist for more than five seconds (for example, video content with integrated ads).
- Interstitial monetisation and advertising displayed immediately upon app launch.
- Multiple ad placements on a page (for example, banner ads that show multiple offers in one placement or displaying more than one banner or video ad is not allowed).
- Monetisation and advertising that are not clearly distinguishable from your app content, such as offerwalls and other immersive ad experiences.
- Use of shocking or emotionally manipulative tactics to encourage ad viewing or in-app purchases.
- Deceptive ads that force the user to clickthrough by using a dismiss button to trigger another ad, or by making ads suddenly appear in areas of the app where the user usually taps for another function.
- Not providing a distinction between the use of virtual game coins versus real-life money to make in-app purchases.

To ensure that Google Play remains a safe and respectful platform, we've created standards defining and prohibiting content that is harmful or inappropriate for our users.

- Monetisation and advertising that move away from a user's finger as the user tries to close it

- Monetisation and advertising that do not provide a user with a way to exit the offer after five (5) seconds as depicted in the example below:

- Monetisation and advertising that take up the majority or the device screen without providing the user a clear way to dismiss it, as depicted in the example below:

- Banner ads showing multiple offers, as depicted in the example below:

- Monetisation and advertising that could be mistaken by a user for app content, as depicted in the example below:

- Buttons, ads, or other monetisation that promote your other Google Play store listings but that are indistinguishable from app content, as depicted in the example below:

Here are some examples of inappropriate ad content that should not be displayed to children.

- **Inappropriate media content**: Ads for TV shows, movies, music albums or any other media outlet that is not appropriate for children.
- **Inappropriate video games and downloadable software**: Ads for downloadable software and electronic video games that are not appropriate for children.
- **Controlled or harmful substances**: Ads for alcohol, tobacco, controlled substances or any other harmful substances.
- **Gambling**: Ads for simulated gambling, contests or sweepstakes promotions, even if free to enter.
- **Adult and sexually suggestive content**: Ads with sexual, sexually suggestive and mature content.
- **Dating or relationships**: Ads for dating or adult relationship sites.
- **Violent content**: Ads with violent and graphic content that is not appropriate for children.

Ad SDKs

If you serve ads in your app and your target audience only includes children, then you must use only Families self-certified ads SDK versions. If the target audience for your app includes both children and older users, you must implement age screening measures, such as a neutral age screen , and make sure that ads shown to children come exclusively from Google Play self-certified ads SDK versions.

Please refer to the Families Self-Certified Ads SDK Programme policy page for more details on these requirements and refer here to see the current list of Families Self-Certified ads

SDK versions.

If you use AdMob, refer to the AdMob Help Centre for more details on their products.

It is your responsibility to ensure that your app satisfies all requirements concerning advertisements, in-app purchases and commercial content. Contact your ad SDK provider(s) to learn more about their content policies and advertising practices.

Families self-certified ads SDK policy

Google Play is committed to building a safe experience for children and families. A key part of this is to help ensure that children only see ads that are appropriate for their age and that their data is handled appropriately. To achieve this goal, we require ads SDKs and mediation platforms to self-certify that they are appropriate for children and compliant with Google Play Developer Programme Policies and Google Play Families policies, including Families Self-Certified Ads SDK Programme requirements.

The Google Play Families Self-Certified Ads SDK Programme is an important way for developers to identify which ads SDKs or mediation platforms have self-certified that they are appropriate for use in apps designed specifically for children.

Misrepresentation of any information about your SDK, including in your interest form application, may result in removal or suspension of your SDK from the Families Self-Certified Ads SDK Programme, so it is important to provide accurate information.

Policy requirements

If your SDK or mediation platform serves apps that are part of the Google Play Families programme, you must comply with all Google Play developer policies, including the following requirements. Failure to satisfy any policy requirements may result in removal or suspension from the Families Self-Certified Ads SDK Programme.

It is your responsibility to ensure that your SDK or mediation platform is compliant, so please make sure that you review Google Play Developer Programme Policies, Google Play families policies and Families Self-Certified Ads SDK Programme requirements.

1. **Ad content:** Your ad content that is accessible to children must be appropriate for children.
   - You must (i) define objectionable ad content and behaviours and (ii) prohibit them in your terms or policies. The definitions should comply with Google Play Developer Programme Policies.
   - You must also create a method to rate your ad creatives according to age-appropriate groups. Age-appropriate groups must at least include groups for 'Everyone' and 'Mature'. The rating methodology must align with the methodology that Google supplies to SDKs once they have filled in the interest form.
   - You must ensure that when real-time bidding is used to serve ads to children, the creatives have been reviewed and comply with the above requirements.
   - In addition, you must have a mechanism to visually identify creatives coming from your inventory (for example, watermarking the ad creative with a visual logo of your company or similar functionality).
2. **Ad format:** You must ensure that all ads displayed to child users follow the Families Ad format requirements, and you must allow developers to select ad formats that are compliant with Google Play families policy.
   - Advertising must not have deceptive content or be designed in a way that will result in inadvertent clicks from child users. Deceptive ads that force the user to clickthrough by using a dismiss button to trigger another ad, or by making ads suddenly appear in areas of the app where the user usually taps for another function are not allowed.

- Disruptive advertising, including advertising that takes up the entire screen or interferes with normal use and does not provide a clear means to dismiss the ad (for example, Ad walls), is not allowed.
- Advertising that interferes with normal app use or gameplay, including rewarded or opt-in ads, must be closeable after five seconds.
- Multiple ad placements on a page are not allowed. For example, banner ads that show multiple offers in one placement or displaying more than one banner or video ad is not allowed.
- Advertising must be clearly distinguishable from app content. Offerwalls and immersive ads experiences that are not clearly identifiable as advertising by child users are not allowed.
- Advertising must not use shocking or emotionally manipulative tactics to encourage ads viewing.

3. **IBA/Remarketing:** You must ensure that ads displayed to child users do not involve interest-based advertising (advertising targeted at individual users who have certain characteristics based on their online browsing behaviour) or remarketing (advertising targeted at individual users based on previous interaction with an app or website).
4. **Data practices:** You, the SDK provider, must be transparent in how you handle user data (for example, information collected from or about a user, including device information). That means disclosing your SDK's access, collection, use and sharing of the data, and limiting the use of the data to the purposes disclosed. These Google Play requirements are in addition to any requirements prescribed by applicable privacy and data protection laws. You must disclose the collection of any personal and sensitive information from children including, but not limited to, authentication information, microphone and camera sensor data, device data, Android ID and ad usage data.
   - You must allow developers, on a per-request or per-app basis, to request child-directed treatment for ad serving. Such treatment must be in compliance with applicable laws and regulations, such as the US Children's Online Privacy and Protection Act (COPPA) and the EU General Data Protection Regulation (GDPR).
     - Google Play requires ads SDKs to disable personalised ads, interest-based advertising and remarketing as part of the child-directed treatment.
   - You must ensure that when real-time bidding is used to serve ads to children, the privacy indicators are propagated to the bidders.
   - You must not transmit AAID, SIM serial, build serial, BSSID, MAC, SSID, IMEI and/or IMSI from children or users of unknown age.
5. **Mediation platforms:** When serving ads to children, you must:
   - Only use Families Self-Certified Ads SDKs or implement safeguards necessary to ensure that all ads served from mediation comply with these requirements; and
   - Pass the information necessary to mediation platforms to indicate the ad content rating and any applicable child-directed treatment.
6. **Self-certification and compliance:** You must provide Google with sufficient information, such as information indicated in the interest form, to verify the ads SDK's policy compliance with all self-certification requirements including, but not limited to:
   - Providing an English language version of your SDK or mediation platform's Terms of Service, privacy policy and publisher integration guide
   - Submitting a sample test app which uses the latest compliant version of the ads SDK. The sample test app should be a fully built and executable Android APK that utilises all the features of the SDK. Test app requirements:
     - Must be submitted as a fully built and executable Android APK meant to run on a phone form factor.
     - Must use the latest released, or soon to be released version of the ads SDK that adheres to Google Play policies.
     - Must use all of the features of your ads SDK including calling your ads SDK to retrieve and display ads.

- Must have full access to all live/serving ad inventories on the network via creatives requested through the test app.
- Must not be restricted by geolocation.
- If your inventory is for a mixed audience, your test app must be capable of differentiating between requests for ad creatives from full inventory and the inventory suitable for children or all age groups.
- Must not be restricted to specific ads within the inventory unless it is controlled by the neutral age screen.

7. You must respond in a timely manner to any subsequent requests for information and self-certify that all new version releases are compliant with the latest Google Play Developer Programme Policies, including Families Policy Requirements.
8. **Legal compliance:** Families Self-Certified Ads SDKs must support ad serving that complies with all relevant statutes and regulations concerning children that may apply to their publishers.
   - You must ensure that your SDK or mediation platform is compliant with the US Children's Online Privacy and Protection Act (COPPA) , EU General Data Protection Regulation (GDPR) and any other applicable laws or regulations.

     Note: The word 'children' can mean different things in different locales and in different contexts. It is important that you consult with your legal counsel to help determine what obligations and/or age-based restrictions may apply to your app. You know best how your app works, so we are relying on you to help us to make sure that apps on Google Play are safe for families.

Please refer to the Families Self-Certified Ads SDK Programme page for more details on programme requirements.

Enforcement

Avoiding a policy violation is always better than managing one, but when violations do occur, we're committed to ensuring that developers understand how they can bring their app into compliance. Please let us know if you see any violations or have any questions about managing a violation .

Policy coverage

Our policies apply to any content your app displays or links to, including any ads it shows to users and any user-generated content it hosts or links to. Furthermore, they apply to any content from your developer account which is publicly displayed in Google Play, including your developer name and the landing page of your listed developer website.

We don't allow apps that let users install other apps to their devices. Apps that provide access to other apps, games or software without installation, including features and experiences provided by third parties, must ensure that all the content they provide access to adheres to all Google Play policies and may also be subject to additional policy reviews.

Defined terms used in these policies have the same meaning as in the Developer Distribution Agreement (DDA). In addition to complying with these policies and the DDA, the content of your app must be rated in accordance with our Content rating guidelines.

We don't allow apps or app content that undermine user trust in the Google Play ecosystem. In assessing whether to include or remove apps from Google Play, we consider a number of factors including, but not limited to, a pattern of harmful behaviour or high risk of abuse. We identify risk of abuse including, but not limited to, items such as app- and developer-specific complaints, news reporting, previous violation history, user feedback, and use of popular brands, characters and other assets.

How Google Play Protect works

Google Play Protect checks apps when you install them. It also periodically scans your device. If it finds a potentially harmful app, it might:

- Send you a notification. To remove the app, tap the notification, then tap Uninstall.
- Disable the app until you uninstall it.
- Remove the app automatically. In most cases, if a harmful app has been detected, you will get a notification saying that the app was removed.

How malware protection works

To protect you against malicious third-party software, URLs and other security issues, Google may receive information about:

- Your device's network connections
- Potentially harmful URLs
- Operating system, and apps installed on your device through Google Play or other sources.

You may get a warning from Google about an app or URL that may be unsafe. The app or URL may be removed or blocked from installation by Google if it is known to be harmful to devices, data or users.

You can choose to disable some of these protections in your device settings. But Google may continue to receive information about apps installed through Google Play, and apps installed on your device from other sources may continue to be checked for security issues without sending information to Google.

How privacy alerts work

Google Play Protect will alert you if an app is removed from the Google Play Store because the app may access your personal information and you'll have an option to uninstall the app.

Enforcement process

When reviewing content or accounts to determine whether they are illegal or violate our policies, we take various information into consideration when making a decision. This includes app metadata (for example, app title, description), in-app experience, account information (for example, past history of policy violations) and other information provided through reporting mechanisms (where applicable) and own-initiative reviews.

If your app or developer account violates any of our policies, we'll take appropriate action as outlined below. In addition, we'll provide you with relevant information about the action that we've taken via email, along with instructions on how to appeal if you believe we've taken action in error.

Please note that removal or administrative notices may not indicate each and every policy violation present in your account, app or broader app catalogue. Developers are responsible for addressing any policy issue and conducting extra due diligence to ensure that the remainder of their app or account is fully policy compliant. Failure to address policy violations in your account and all of your apps may result in additional enforcement actions.

Repeated or serious violations (such as malware, fraud and apps that may cause the user or device harm) of these policies or the Developer Distribution Agreement (DDA) will result in the termination of individual or related Google Play Developer accounts.

Enforcement actions

Different enforcement actions can impact your apps in different ways. We use a combination of human and automated evaluation to review apps and app content to detect and assess content which violates our policies and is harmful to users and the overall Google Play ecosystem. Using automated models helps us detect more violations and evaluate potential issues faster, which helps keep Google Play

safe for everyone. The policy-violating content is either removed by our automated models or, where a more nuanced determination is required, it is flagged for further review by trained operators and analysts who conduct content evaluations, for example, because an understanding of the context of the piece of content is required. The results of these manual reviews are then used to help build training data to further improve our machine-learning models.

The following section describes the various actions that Google Play may take, and the impact on your app and/or your Google Play Developer account.

Unless otherwise noted in an enforcement communication, these actions affect all regions. For example, if your app is suspended, it will be unavailable in all regions. In addition, unless otherwise noted, these actions will remain in effect unless you appeal the action and the appeal is granted.

Rejection

- A new app or app update submitted for review will not be made available on Google Play.
- If an update to an existing app was rejected, the app version published prior to the update will remain available on Google Play.
- Rejections don’t impact your access to a rejected app’s existing user installs, statistics and ratings.
- Rejections don’t impact the standing of your Google Play Developer account.

Note: Do not attempt to resubmit a rejected app until you’ve fixed all the policy violations.

Removal

- The app, along with any previous versions of that app, is removed from Google Play and will no longer be available for users to download.
- Because the app is removed, users will not be able to see the app’s store listing. This information will be restored once you submit a policy-compliant update for the removed app.
- Users may not be able to make any in-app purchases, or utilise any in-app billing features in the app until a policy-compliant version is approved by Google Play.
- Removals don’t immediately impact the standing of your Google Play Developer account, but multiple removals may result in a suspension.

Note: Don't attempt to republish a removed app until you’ve fixed all policy violations.

Suspension

- The app, along with any previous versions of that app, is removed from Google Play and will no longer be available for users to download.
- Suspension can occur as the result of egregious or multiple policy violations, as well as repeated app rejections or removals.
- Because the app is suspended, users will not be able to see the app’s store listing. This information will be restored once you submit a policy-compliant update.
- You can no longer use a suspended app’s APK or app bundle.
- Users will not be able to make any in-app purchases or utilise any in-app billing features in the app until a policy-compliant version is approved by Google Play.
- Suspensions count as strikes against the good standing of your Google Play Developer account. Multiple strikes can result in the termination of individual and related Google Play Developer accounts.

Note: Don't attempt to republish a suspended app unless Google Play has explained that you may do so.

Limited visibility

- Your app's discoverability on Google Play is restricted. Your app will remain available on Google Play and can be accessed by users with a direct link to the app's store listing.
- Having your app placed in a limited visibility state doesn't impact the standing of your Google Play Developer account.
- Having your app placed in a limited visibility state doesn't impact users' ability to see the app's existing store listing.

Limited regions

- Your app can only be downloaded by users through Google Play in certain regions.
- Users from other regions will not be able to find the app on the Play Store.
- Users who previously installed the app can continue to use it on their device but will no longer receive updates.
- Region limiting does not impact the standing of your Google Play Developer account.

Account restricted state

- When your developer account is in a restricted state, all apps in your catalogue will be removed from Google Play and you will no longer be able to publish new apps or republish existing apps. You will still be able to access the Play Console.
- Because all apps are removed, users will not be able to see your app's store listing and your Developer Profile.
- Your current users will not be able to make any in-app purchases or utilise any in-app billing features of your apps.
- You can still use the Play Console to provide more information to Google Play and amend your account information.
- You will be able to republish your apps once you have fixed all policy violations.

Account termination

- When your developer account is terminated, all apps in your catalogue will be removed from Google Play and you will no longer be able to publish new apps. This also means that any related Google Play Developer accounts will also be permanently suspended.
- Multiple suspensions or suspensions for egregious policy violations may also result in the termination of your Play Console account.
- Because the apps within the terminated account are removed, users will not be able to see your apps' store listing and your Developer Profile.
- Your current users will not be able to make any in-app purchases or utilise any in-app billing features of your apps.

Note: Any new account that you try to open will be terminated as well (without a refund of the developer registration fee), so please do not attempt to register for a new Play Console account while one of your other accounts is terminated.

Dormant accounts

Dormant accounts are developer accounts that are inactive or abandoned. Dormant accounts are not in good standing as required by the Developer Distribution Agreement .

Google Play Developer accounts are intended for active developers who publish and actively maintain apps. To prevent abuse, we close accounts that are dormant or not used or otherwise significantly engaged (for example, for publishing and updating apps, accessing statistics or managing Store Listings) on a regular basis.

Dormant account closure will delete your account and any data associated with it. Your registration fee is not refundable and will be forfeited. Before we close your dormant account, we will notify you using

the contact information that you provided for that account.

Closure of a dormant account will not limit your ability to create a new account in the future if you decide to publish on Google Play. You will not be able to reactivate your account and any previous apps or data will not be available on a new account.

Managing and reporting policy violations

Appealing an enforcement action

We will reinstate applications if an error was made, and we find that your application does not violate the Google Play programme policies and Developer Distribution Agreement. If you've reviewed the policies carefully and feel that our decision may have been in error, please follow the instructions provided to you in the enforcement email notification or click here to appeal our decision.

Additional resources

If you need more information regarding an enforcement action or a rating/comment from a user, you may refer to some of the resources below or contact us through the Google Play Help Centre. We cannot, however, offer you legal advice. If you need legal advice, please consult your legal counsel.

- App verification
- Report a policy violation
- Contact Google Play about an account termination or app removal
- Fair warnings
- Report inappropriate apps and comments
- My app has been removed from Google Play
- Understanding Google Play Developer account terminations

Play Console requirements

Google Play wants to provide safe and wonderful app experiences for our users and a great opportunity for all our developers to be successful. We strive to ensure that the process of making your app available to users goes as smoothly as possible.

To help you avoid common violations, make sure that you do the following when submitting information through Play Console and any profiles that are linked to your Play Console developer account.

Before you submit your app, you must:

- Accurately provide your developer account information, including the following details:
  - Legal name and address
  - D-U-N-S number , if registering as an organisation
  - Contact email address and phone number
  - Developer email address and phone number shown on Google Play where applicable
  - Payment methods where applicable
  - Google payments profile linked to your developer account
- If registering as an organisation, ensure that your developer account information is up to date and consistent with the details stored on your Dun & Bradstreet profile
- Accurately provide all app information and metadata
- Upload your app's privacy policy and fill out your Data safety section requirements
- Provide an active demo account, login information and all other resources needed for Google Play to review your app (specifically, login credentials, QR code, etc.)

As always, you should make sure that your app provides a stable, engaging, responsive user experience: Double-check that everything in your app, including ad networks, analytics services and third-party SDKs, complies with Google Play Developer Programme Policies; and if your app target audience includes children, make sure that you comply with our Families policy.

Remember, it is your responsibility to review the Developer Distribution Agreement and all Developer Programme Policies to ensure that your app fully complies.

Developer Distribution Agreement

Need more help?

Try these next steps:

Post to the Help Community

Get answers from community members

Contact us

Tell us more and we'll help you get there