

Google Developer Policy - April 16, 2020

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 Program 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.

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.

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 include content that sexualizes minors are subject to immediate removal from the Store. Apps that appeal to children but contain adult themes are not allowed.

If we become aware of content with child sexual abuse imagery, we will report it to the appropriate authorities and delete the Google Accounts of those involved with the distribution.

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

We don't allow apps that contain or promote sexual content, such as pornography, or any content or services intended to be sexually gratifying. Content that contains nudity may be allowed if the primary purpose is educational, documentary, scientific or artistic, and is not gratuitous.

Here are some examples of common violations:

Depictions of nudity in which the subject is nude or minimally clothed, and where the clothing would not be acceptable in an appropriate public context.

Depictions, animations or illustrations of sex acts or sexually suggestive poses.

Content that depicts sexual aids and fetishes.

Content that is lewd or profane.

Content that depicts, describes, or encourages bestiality.

Apps that promote sex-related entertainment, escort services or other services that may be interpreted as providing sexual acts in exchange for compensation.

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, or any other characteristic that is associated with systemic discrimination or marginalization.

Here are examples of common violations:

Compilations of assertions intended to prove that a protected group is inhuman, inferior or worthy of being hated.

Apps that contain theories about a protected group possessing negative characteristics (e.g. malicious, corrupt, evil, etc.), or explicitly or implicitly claims 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.

Violence

We don't allow apps that depict or facilitate gratuitous violence or other dangerous activities.

Here are some examples of common violations:

Graphic depictions or descriptions of realistic violence or violent threats to any person or animal.

Apps that promote self harm, suicide, eating disorders, choking games or other acts where serious injury or death may result.

Terrorist Content

We do not permit terrorist organizations 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 enough information so users understand the context.

Sensitive Events

We don't allow apps that lack reasonable sensitivity towards or capitalize on a natural disaster, atrocity, conflict, death, or other tragic event.

Here are examples of common violations:

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

Bullying and Harassment

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

Here are examples of common violations:

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

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 (e.g. 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.

Here are some examples of common violations:

- Allowing users to order marijuana through an in-app shopping cart feature.
- Assisting users in arranging delivery or pick up of marijuana.
- Facilitating the sale of products containing THC.

Tobacco and Alcohol

We don't allow apps that facilitate the sale of tobacco (including e-cigarettes) or encourage the irresponsible use of alcohol or tobacco.

Here are examples of common violations:

Depicting or encouraging the use or sale of alcohol or tobacco to minors.
Implying that consuming tobacco can improve social, sexual, professional, intellectual, or athletic standing.
Portraying excessive drinking favorably, including the favorable portrayal of excessive, binge or competition drinking.

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 personalized advice.

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

Binary Options

We do not allow apps that provide users with the ability to trade binary options.

Cryptocurrencies

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

Personal loans

We define personal loans as lending money from one individual, organization, or entity to an individual consumer on a nonrecurring basis, not for the purpose of financing purchase of a fixed asset or education. Personal loan consumers require information about the quality, features, fees, 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

Not included: Mortgages, car loans, student loans, revolving lines of credit (such as credit cards, personal lines of credit)

Apps for personal loans must 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 all applicable fees

We do not allow apps that promote personal loans which require repayment in full in 60 days or less from the date the loan is issued (we refer to these as "short-term personal loans"). This policy applies to apps which offer loans directly, lead generators, and those who connect consumers with third-party lenders.

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.

Gambling

We allow content, services, and ads that facilitate online gambling, as long as they meet certain requirements. We also allow daily fantasy sports apps that meet certain requirements.

Gambling Apps

(Currently permitted in the UK, Ireland, and France only)

We allow content and services that facilitate online gambling, as long as they meet the following requirements:

- Developer must successfully [complete the application process](#) in order to distribute the app on Play;
- App must comply with all applicable laws and industry standards for any country in which it is distributed;
- Developer must have a valid gambling license for each country in which the app is distributed;
- App must prevent under-age users from gambling in the app;
- App must prevent use from countries not covered by the developer-provided gambling license;
- 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; and
- App and its app listing must clearly display information about responsible gambling.

For all other locations, we don't allow content or services that facilitate online gambling, including, but not limited to, online casinos, sports betting and lotteries, and games of skill that offer prizes of cash or other real world value.

Gambling Ads within Play-distributed Apps

We allow ads that facilitate online gambling, as long as they meet the following requirements:

- App and ad (including gambling advertisers) must comply with all applicable laws and industry standards for any location where the gambling ad is displayed;
- Ad must meet local 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 program;

App must not target individuals under the age of 18;
Ad must clearly display information about responsible gambling on the landing page, the advertised app listing itself or within the app; and
App that is advertising a gambling ad must not be a simulated gambling app (an entertainment game without real money gambling).

Here are some examples of common violations:

'KIDS 123' app having an ad promoting gambling services

Daily Fantasy Sports (DFS) Apps

We allow daily fantasy sports (DFS) apps, as long as they meet following requirements:

App must only allow access and be distributed in the United States; DFS apps targeting jurisdictions outside the US must establish eligibility through the Real Money Gambling Apps process;
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 any US state or US territory in which it is distributed;
Developer must have a valid license for each US state or US territory in which a license is required for daily fantasy sports apps;
App must prevent under-age users from wagering or conducting monetary transactions within the app;
App must prevent use from US States or US territories in which the developer does not hold a license required for daily fantasy sports apps;
App must prevent use from US States or US territories where daily fantasy sports apps are not legal;
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; and
App and its app listing must clearly display information about responsible gambling.

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

Here are some examples of common violations:

Facilitating the sale or purchase of illegal drugs or prescription drugs without a prescription.
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. Objectionable content is content that violates our policies.

Apps that contain or feature UGC must:

- require that users accept the app's terms of use and/or user policy before users can create or upload UGC;
- define, in a manner consistent with the spirit of Google Play's Developer Program Policies, UGC that is objectionable, and prohibit that UGC via the app's terms of use and/or user policy;
- implement robust, effective and ongoing UGC moderation, as is reasonable and consistent with the type(s) of UGC hosted by the app;
- provide a user-friendly, in-app system for reporting and removal of objectionable UGC;
 - In the case of live-streaming apps, problematic UGC must be removed in as close to real-time as reasonably possible; and
- remove or block abusive users who violate the app's terms of use and/or user policy;
- provide safeguards to prevent in-app monetization from encouraging objectionable user behavior.

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.

Here are some examples of common violations:

- Promoting sexually explicit user-generated content, including implementing 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.

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

- 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

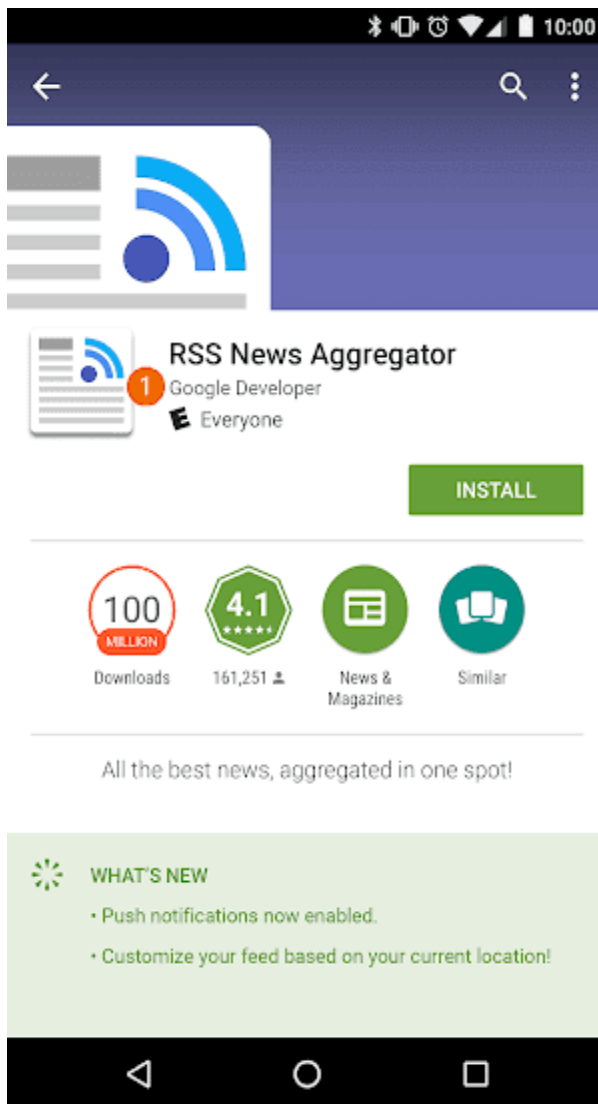
Products with names that are confusingly similar to an unapproved pharmaceutical or supplement or controlled substance

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

We don't allow apps that use another app or entity's brand, title, logo, or name in a manner that may result in misleading users. Don't try to imply an endorsement or relationship with another entity where none exists. Impersonation can occur even if there isn't an intent to deceive, so please be careful when referencing any brands that do not belong to you. This applies even if that brand doesn't yet have a presence on Google Play.

Here are some examples of common violations:

Developers that falsely suggest an affiliation with another entity:



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

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

	 Google Maps	 Google+	 YouTube	 Twitter
	 Google Maps Navigator	 Google+ Sharfy	 YouTube Aggregator	 TwitterPro

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](#).

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 there is an app on Google Play that infringes on your trademark rights, we encourage you to reach out to 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.

Unauthorized 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.

Here are some examples of copyrighted content that is often used without authorization or a legally valid reason:

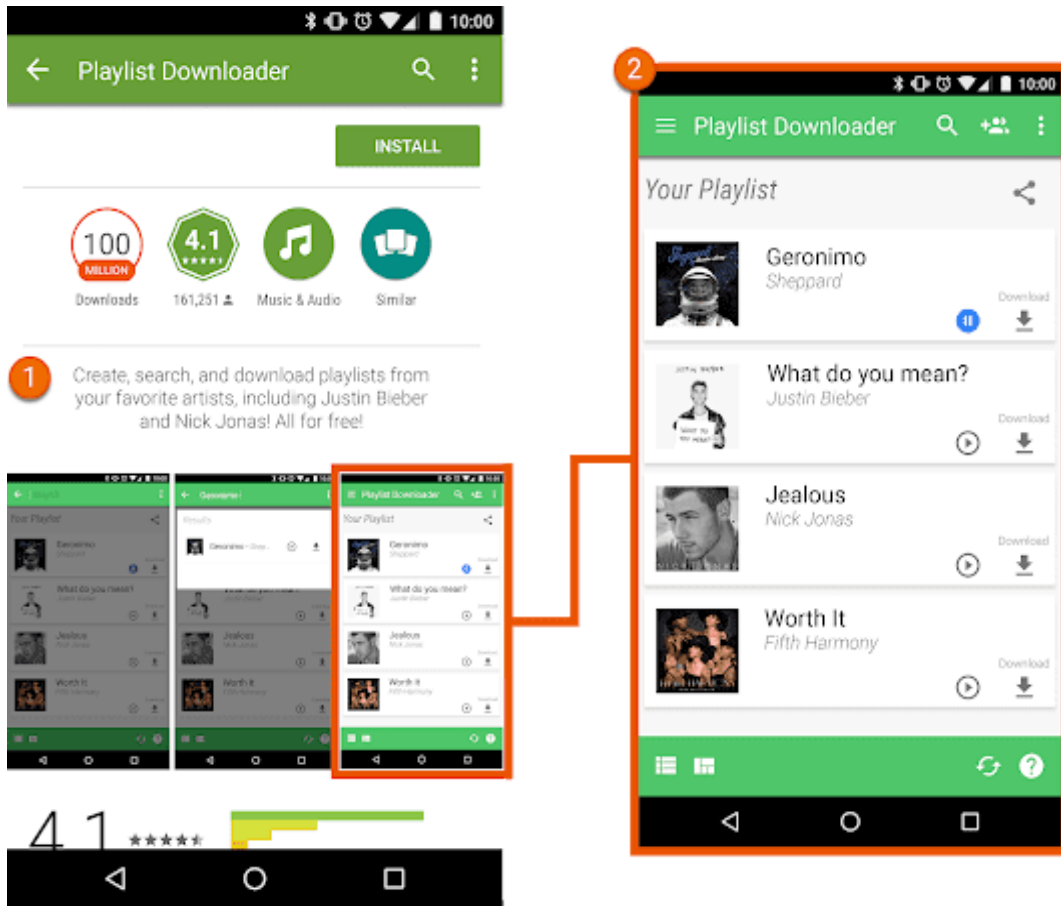
- Cover art for music albums, video games, and books.
- Marketing images from movies, television, or video games.
- Artwork or images from comic books, cartoons, movies, music videos, or television.
- College and professional sports team logos.
- Photos taken from a public figure's social media account.
- 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 your app may be encouraging copyright infringement and get legal advice if necessary.

Here are some examples of common violations:

- Streaming apps that allow users to download a local copy of copyrighted content without authorization.
- 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 authorization.
- ② The screenshot in the app listing encourages users to download copyrighted content without authorization.

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 unauthorized 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 or promote for sale counterfeit goods. 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.

You must be transparent in how you handle user data (e.g., information collected from or about a user, including device information). That means disclosing your app's access, collection, use, and sharing of the data, and limiting the use of the data to the purposes disclosed. In addition, if your app handles personal or sensitive user data, please also refer to the additional requirements in the "Personal and Sensitive Information" section below. These Google Play requirements are in addition to any requirements prescribed by applicable privacy and data protection laws.

Personal and Sensitive Information

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, microphone, camera, and other sensitive device or usage data. If your app handles sensitive user data, then you must:

- Limit your access, collection, use, and sharing of personal or sensitive data acquired through the app to purposes directly related to providing and improving the features of the app (e.g., user anticipated functionality that is documented and promoted in the app's description in the Play Store). Apps that extend usage of this data for serving advertising must be in compliance with our [Ads Policy](#).

- Post a privacy policy in both the designated field in the Play Console and 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. Your privacy policy must disclose the types of personal and sensitive data your app accesses, collects, uses, and shares and the types of parties with which any personal or sensitive user data is shared. Handle all personal or 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 or sensitive user data.

Prominent Disclosure & Consent Requirement

In cases where users may not reasonably expect – as determined by Play in its sole discretion – that their personal or sensitive user data will be required to provide or improve the policy compliant features or functionality within your app, you must meet the following requirements:

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 or sensitive data collection.

Your in-app disclosure must accompany and immediately precede a request for user consent and, where available, an associated runtime permission. You may not access or collect any personal or sensitive data until the user consents. The app's request for consent:

- Must present the consent dialog clearly and unambiguously;
- Must require affirmative user action (e.g. tap to accept, tick a check-box);
- Must not interpret navigation away from the disclosure (including tapping away or pressing the back or home button) as consent; and
- Must not utilize auto-dismissing or expiring messages.

Here are some examples of common violations:

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 Privacy Policy, Secure Transmission, and Prominent Disclosure 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 Privacy Policy, Secure Transmission, and Prominent Disclosure 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 in accordance with the above requirements

Restrictions for 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 or sensitive user data related to financial or payment activities or any government identification numbers.
Your app handles non-public phonebook or contact information	We don't allow unauthorized 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.

EU-U.S. 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 organizational and technical measures to protect EU Personal Information against loss, misuse, and unauthorized 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.

Permission requests should make sense to users. You may only request permissions that are necessary to implement current features or services in your app that are promoted in your Play Store listing. You may not use permissions that give access to user or device data for undisclosed, unimplemented, or disallowed features or purposes. Personal or sensitive data accessed through permissions may never be sold.

Request permissions to access data in context (via incremental auth), 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 they affirmatively agree to the additional uses.

Restricted Permissions

In addition to the above, restricted permissions are permissions that are designated as [Signature](#) or [Dangerous](#) in our developer documentation, and are subject to the following additional requirements and restrictions:

- Sensitive user or device data accessed through Restricted Permissions may only be transferred to third parties if necessary to provide or improve current features or services in the app from which the data was collected. You may also transfer data as necessary to comply with applicable law or as part of a merger, acquisition, or sale of assets with legally adequate notice to users. All other transfers or sales of the user data are prohibited.
- 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 (e.g., allowing a user to manually enter a phone number if they’ve restricted access to Call Logs).

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 (e.g. 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 (e.g. 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 Center 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 (e.g., 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

April 16, 2020 update: We realize that compliance with the Location policy may require substantial work for some developers, so we are offering an extended timeline to make any necessary changes. To view timelines and other updates, please visit our [Help Center](#).

[Device location](#) is regarded as personal and sensitive user data subject to the [Personal and Sensitive Information](#) policy and the following requirements:

Apps may not access data protected by location permissions (e.g., 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 (i.e., 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 e.g.: "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.

We don't allow apps that interfere with, disrupt, damage, or access in an unauthorized 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 authorized carrier's network.

Apps on Google Play must comply with the default Android system optimization requirements documented in the [Core App Quality guidelines for Google Play](#).

Here are examples of common violations:

- 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 attempt to bypass [system power management](#) that are not [eligible for whitelisting](#).

- 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.

We don't allow apps that steal data, secretly monitor or harm users, or are otherwise malicious.

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 (e.g. dex, JAR, .so files) from a source other than Google Play. This restriction does not apply to code that

runs in a virtual machine and has limited access to Android APIs (such as JavaScript in a webview or browser).

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.

Surveillance and Commercial Spyware apps are explicitly prohibited on Google Play. Only policy compliant apps exclusively designed and marketed for parental (including family) monitoring or enterprise management may distribute on the Store with tracking and reporting features, provided they fully comply with the requirements described below.

The following are explicitly prohibited:

- Viruses, trojan horses, malware, spyware or any other malicious software.

- Apps that link to or facilitate the distribution or installation of malicious software.

- Apps or SDKs that download executable code, such as dex files or native code, from a source other than Google Play.

- Apps that introduce or exploit security vulnerabilities.

- Apps that steal a user's authentication information (such as usernames or passwords) or that mimic other apps or websites to trick users into disclosing personal or authentication information.

- Apps may not depict unverified or real world phone numbers, contacts, addresses, or personally identifiable information of non-consenting individuals or entities.

- Apps that install other apps on a device without the user's prior consent.

- Apps with content delivery network (CDN) facilitated downloads that fail to prompt the user and disclose the download size prior to downloading.

- Apps designed to secretly collect device usage, such as commercial spyware apps.

Apps that monitor or track a user's behavior on a device must comply with these requirements:

- Apps must not present themselves as a spying or secret surveillance solution.

- Apps must not hide or cloak tracking behavior or attempt to mislead users about such functionality.

- Present users with a persistent notification and unique icon that clearly identifies the app.

- Apps and app listings on Google Play must not provide any means to activate or access functionality that violate these terms, such as linking to a non-compliant APK hosted outside Google Play.

- You are solely responsible for determining the legality of your app in its targeted locale. Apps determined to be unlawful in locations where they are published will be removed.

Check out our [App Security Improvement Program](#) to find out about the most recent security issues flagged to developers on Google Play. Vulnerability and remediation details are available in each campaign's support page link.

We don't allow apps that attempt to deceive users or enable dishonest behavior 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 and should perform as reasonably expected by the user. 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 easily 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.

Here are some examples of common violations:

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.

Developer or app names that misrepresent their current status or performance on Play. (E.g. "Editor's Choice," "Number 1 App," "Top Paid").

Apps that feature medical or health-related content or functionalities that are misleading or potentially harmful.

Apps that claim functionalities that are not possible to implement.

Apps that are improperly categorized.

Demonstrably deceptive content that may interfere with voting processes.

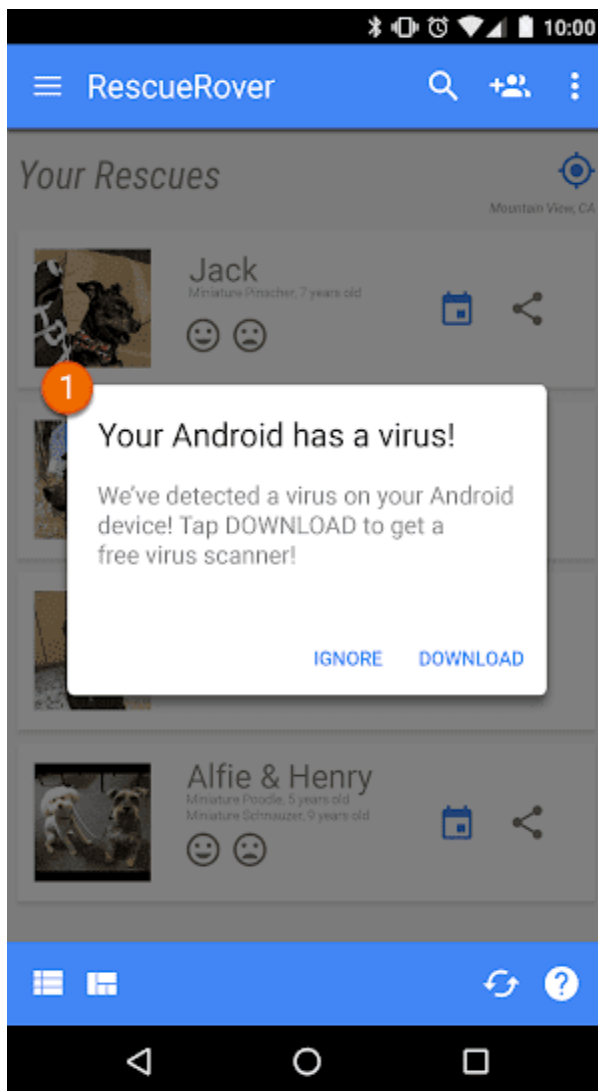
Apps that falsely claim affiliation with a government entity or to provide or facilitate government services for which they are not properly authorized.

Unauthorized 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.

Here are some examples of common violations:

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](#).

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 homescreen.

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 incentivize 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 Behavior

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 and driver's licenses. 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.

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

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.

Here are some examples of common violations:

- 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.

We do not allow apps or developer accounts that impersonate any person or organization, or that misrepresent or conceal their ownership or primary purpose. We do not allow apps or developer accounts 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.

Our Malware policy is simple, the Android ecosystem including the Google Play Store, and user devices should be free from malicious behaviors (i.e. 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 therefore can generate malicious behavior, even if 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 behavior 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 behavior 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 they technically disclose SMS sending behavior, introduce additional behavior 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 carrier 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 to click 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.

Commercial Spyware

Code that transmits personal information off the device without adequate notice or consent and doesn't display a persistent notification that this is happening.

Commercial spyware apps transmit data to a party other than the PHA provider. Legitimate forms of these apps can be used by parents to track their children. However, these apps cannot be used to track a person (a spouse, for example) without their knowledge or permission if a persistent notification is not displayed while the data is being transmitted.

Denial of Service (DoS)

Code that, without the knowledge of the user, executes a denial-of-service (DoS) attack or is a 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 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 intercept 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 subsidized device management may be excluded from the ransomware category provided they successfully meet requirements for secure lock and management, and 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.

Behaviors 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 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 behavior 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 then the app will be treated as having a vulnerability, rather than being backdoor malware, and the developer will be asked to patch it.

Monetization and Ads

Google Play supports a variety of monetization 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

Apps that employ in-store or in-app purchases must comply with the following guidelines:

In-store purchases: Developers charging for apps and downloads from Google Play must use Google Play's payment system.

In-app purchases:

- Developers offering products within a game downloaded on Google Play or providing access to game content must use [Google Play In-app Billing](#) as the method of payment.

- Developers offering products within another category of app downloaded on Google Play must use [Google Play In-app Billing](#) as the method of payment, except for the following cases:

 - Payment is solely for physical products

 - Payment is for digital content that may be consumed outside of the app itself (e.g. songs that can be played on other music players).

- In-app virtual currencies must only be used within the app or game title for which they were purchased.

- Developers must not mislead users about the apps they are selling nor about any in-app services, goods, content, or functionality offered for purchase. If your product description on

Google Play refers to in-app features that may require a specific or additional charge, your description must clearly notify users that payment is required to access those features. Apps offering mechanisms to receive randomized virtual items from a purchase (i.e. "loot boxes") must clearly disclose the odds of receiving those items in advance of purchase.

Subscriptions

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

In your app: 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.

Here are some examples of common violations:

- Monthly subscriptions that do not inform users 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 localized.

- 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 Trial" for a subscription with an auto-recurring charge.

1 Get AnalyzeAPP Premium

16 issues found in your data!
Subscribe to see how we can help

2	12 months	6 months	1 month
	\$9.16/mo Save 35%	\$12.50/mo Save 11%	\$14.00/mo
		MOST POPULAR PLAN	

3 Try for \$12.50!

4 Cancele su suscripción en cualquier momento. Por favor, consulte nuestra política de privacidad para más información.

- 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 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 localized in the same language as the terms and conditions so that users can understand the entire offer.

Free Trials & 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. Be sure

to 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.

Here are some examples of common violations:

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 localized.



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 emphasizes 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 localized in the same language as the terms and conditions so that users can understand the entire offer.

Subscription Management & Cancellation

As a developer, you must ensure that your app(s) clearly disclose how a user can manage or cancel their subscription.

If a user cancels a subscription purchased from an app on Google Play, our 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.

Ads

We don't allow apps that contain deceptive or disruptive ads. Ads must only be displayed within the app serving them. We consider ads served in your app as part of your app. The ads shown in your app must be compliant with all our policies. For policies on gambling ads, please click [here](#).

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.

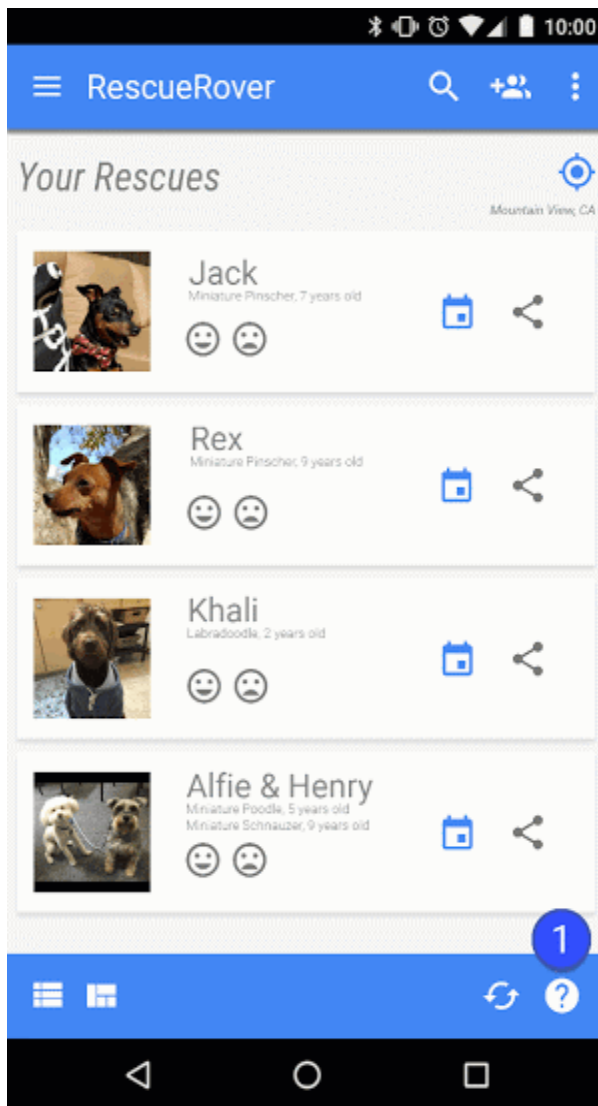
In accordance with [Location Permissions](#) requirements, location permissions may only be requested to implement current features or services within your app, and may not request device location permissions solely for the use of ads.

Deceptive Ads

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

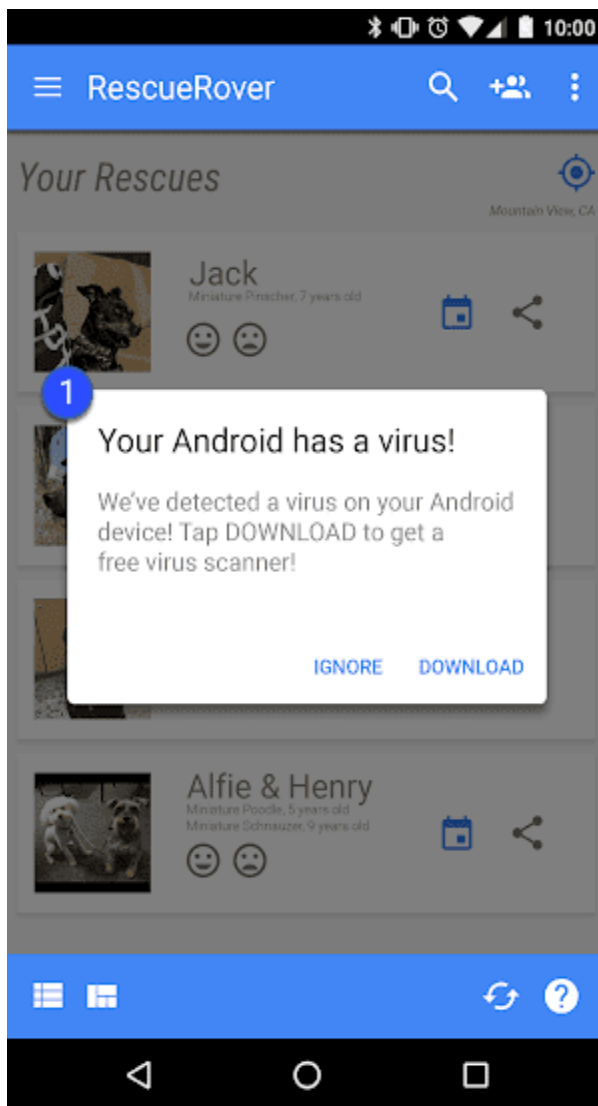
Here are some examples of common violations:

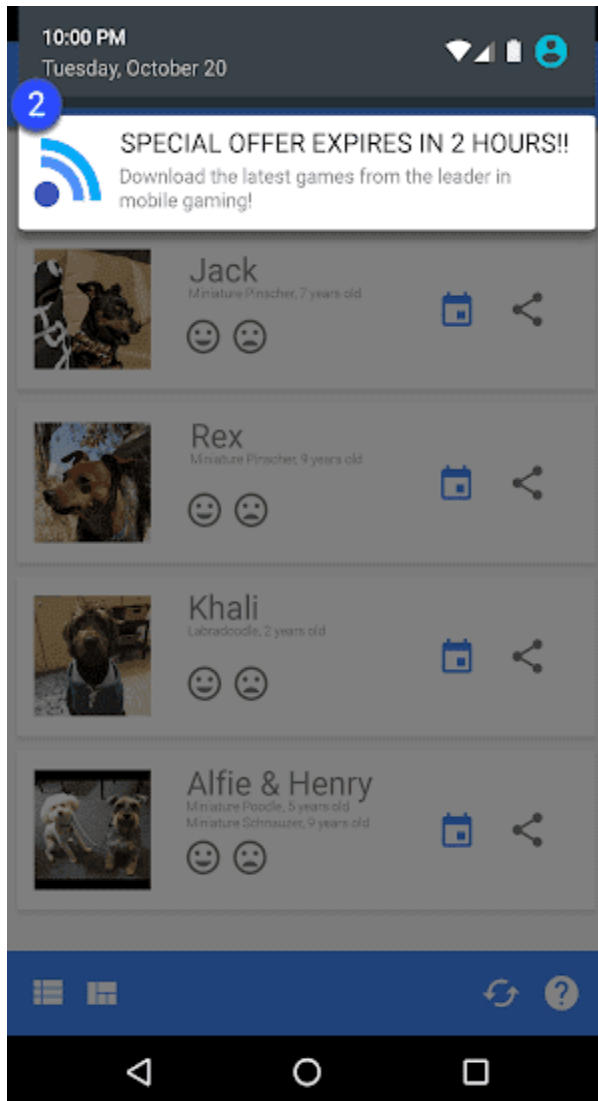
Ads that mimic an app's UI:



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.

Lockscreen Monetization

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

Disruptive Ads

Ads should not be shown in a way that results in inadvertent clicks. Forcing a user to click an ad or submit personal information for advertising purposes before they can fully use an app is prohibited.

Interstitial ads may only be displayed inside of the app serving them. If your app displays interstitial ads or other ads that interfere with normal use, they must be easily dismissible without penalty.

Here is an example of a common violation:

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



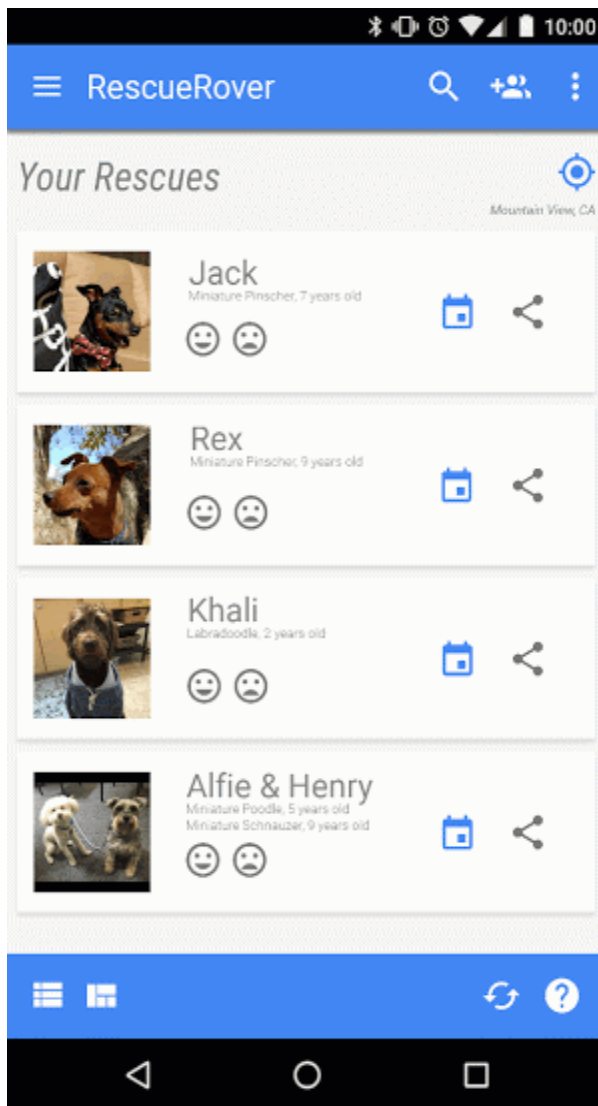
① This ad does not have a dismiss button.

Interfering with Apps, Third-party Ads, or Device Functionality

Ads associated with your app 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 widgetized ad units. Ads must only be displayed within the app serving them.

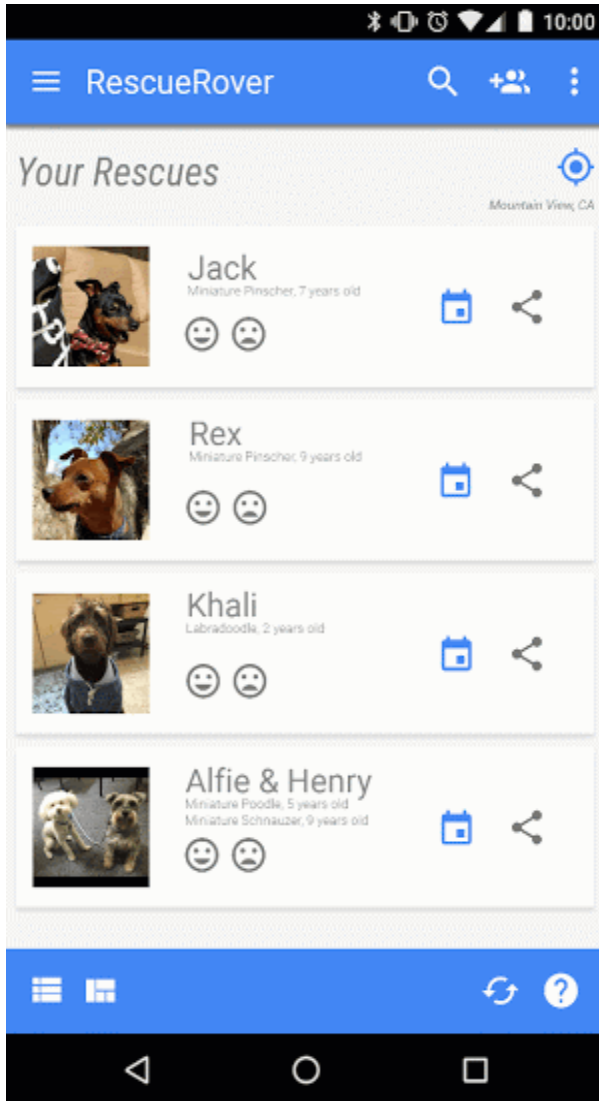
Here are some examples of common violations:

Ads that display outside of the app serving them:



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

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

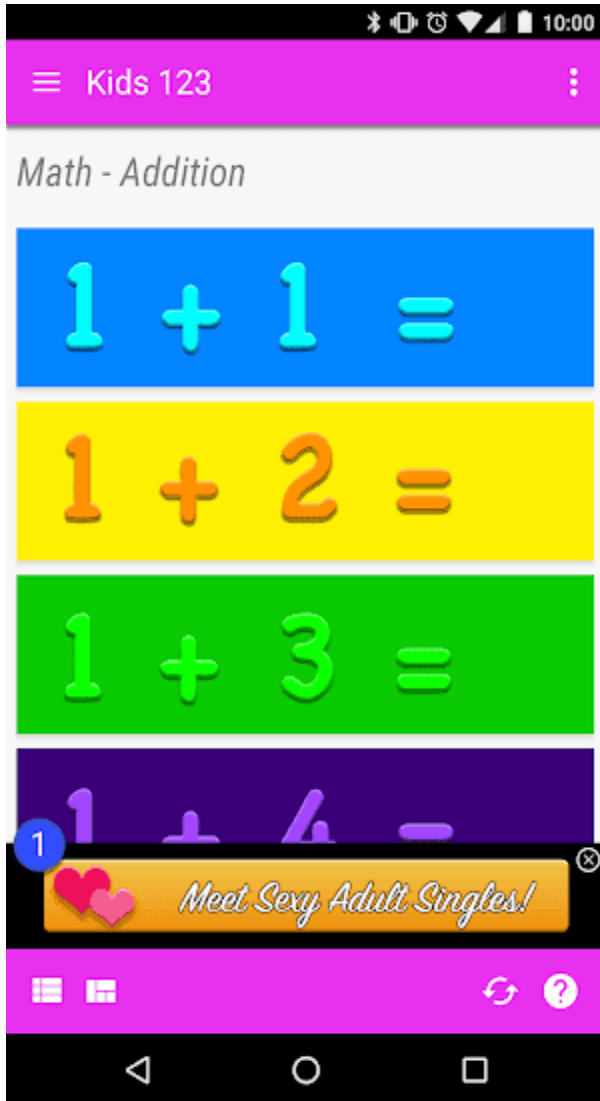


Description: The user attempts to exit the app and navigate to the home screen, but instead, the expected flow is interrupted by an ad.

Inappropriate Ads

The ads shown within your app must be appropriate for the intended audience of your app, even if the content by itself is otherwise compliant with our policies.

Here is an example of a common violation:



① This ad is inappropriate for the intended audience of this app.

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 must only be used for advertising and user analytics. The status of the “Opt out of Interest-based Advertising” or “Opt out of Ads Personalization” setting must be verified on each access of the ID.

Association with personally-identifiable information or other identifiers. The advertising identifier must not be connected to personally-identifiable information or associated with any persistent device identifier (for example: SSAID, MAC address, IMEI, etc.) without explicit consent of the user.

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. Also, you must abide by a user's "Opt out of Interest-based Advertising" or "Opt out of Ads Personalization" 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 personalized advertising. Allowed activities include contextual advertising, frequency capping, conversion tracking, reporting and security and fraud detection.

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 these terms, 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.

Families Ads Program

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 use ad SDKs that have self-certified compliance with Google Play policies, including the Ad SDK certification requirements below. If the target audience for your app includes both children and older users, you must implement age screening measures and make sure that ads shown to children come exclusively from one of these self-certified ad SDKs. Apps in the Designed for Families program are required to only use self-certified ad SDKs.

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

Ad SDK Certification Requirements

- Define what are objectionable ad content and behaviors and prohibit them in the ad SDK's terms or policies. The definitions should not result in non-compliance with Play's Developer Program Policies.

- Create a method to rate your ad creatives according to age appropriate groups, including at least groups for Everyone and Mature. The rating methodology must align with the methodology that Google supplies to SDKs once they have filled out 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 also requires disabling of personalized ads, interest based advertising, and remarketing as part of the child-directed treatment.

- 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 to verify the ad SDK's compliance with all certification requirements, and respond in a timely manner to any subsequent requests for information.

Note: Ad SDKs must support ad serving that complies with all relevant statutes and regulations concerning children that may apply to their publishers.

Mediation requirements for serving platforms when serving ads to children:

only use Play certified ad SDKs or implement safeguards necessary to ensure that all ads served from mediation comply with these requirements; and
pass signals necessary to indicate the ad content rating and any applicable child-directed treatment.

Developers can find a [list of self-certified ad SDKs](#) here.

Also, developers can share this [interest form](#) with ad SDKs who wish to become self-certified.

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 that are deceptive or harmful to users or the developer ecosystem. This includes apps that engage in the following behavior:

Using deceptive ads on websites, apps, or other properties, including notifications that are similar to system notifications and alerts.

Promotion or installation tactics that redirect users to Google Play or download apps without informed user action.

Unsolicited promotion via SMS services.

It is your responsibility to ensure that any ad networks or affiliates associated with your app comply with these policies and do not employ any prohibited promotion practices.

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. We also don't allow unattributed or anonymous user testimonials in the app's description.

Here are some examples of common violations:



- ① Unattributed or Anonymous User testimonials
- ② Data comparison of apps or brands
- ③ Word blocks and vertical/horizontal word lists

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 fetishized anatomy or content, whether illustrated or real.

Language inappropriate for a general audience. Avoid profane and vulgar language in your app listing. If it is a critical element of your app, you must censor its presentation within the store listing.

Graphic violence prominently depicted in app icons, promotional images, or videos.

Depictions of the illicit usage 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.

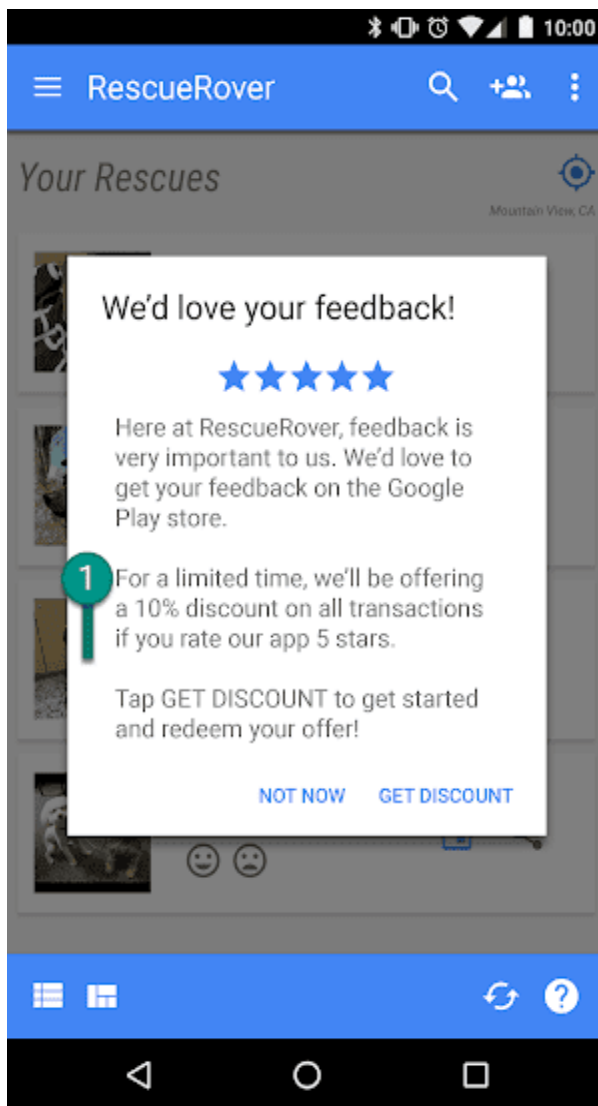
Keep your app's description succinct and straightforward. Shorter descriptions tend to result in a better user experience, especially on devices with smaller displays. Excessive length, detail, improper formatting, or repetition can result in a violation of this policy.

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.

Developers must not attempt to manipulate the placement of any apps in Google Play. This includes, but is not limited to, inflating product ratings, reviews, or install counts by illegitimate means, such as fraudulent or incentivized installs, reviews and ratings.

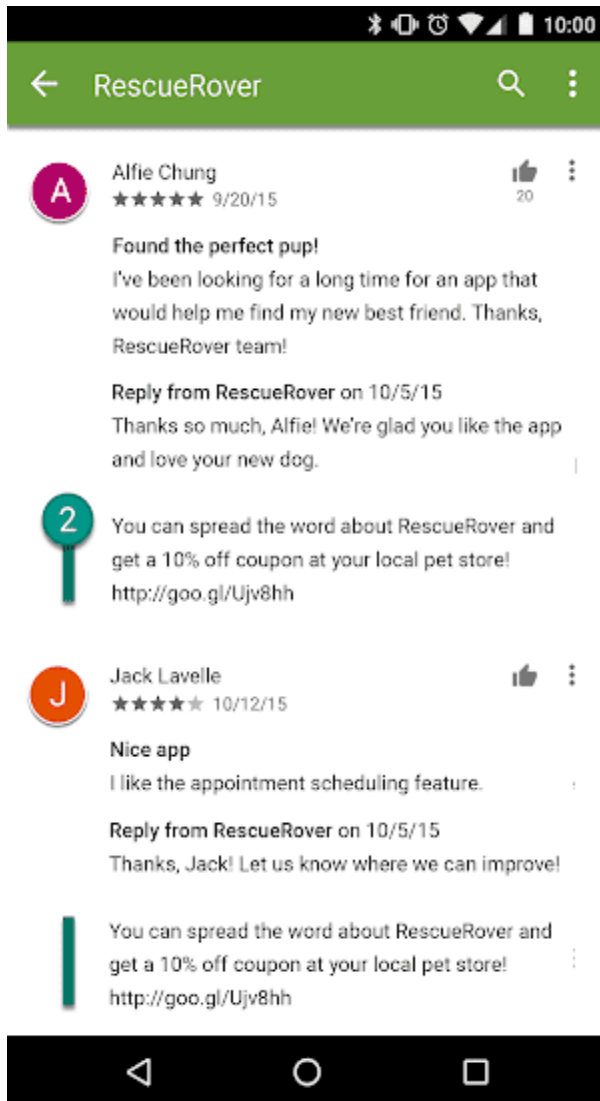
Here are some examples of common violations:

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 to influence the 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 RescueRover 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.

Our content rating system includes official ratings from the [International Age Rating Coalition \(IARC\)](#) and is designed to help developers communicate locally relevant content ratings to users.

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 territories or to

specific users where required by law, and determine your app's eligibility for special developer programs.

How content ratings are assigned

To receive a content rating, you must fill out 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 Center](#) 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.

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.

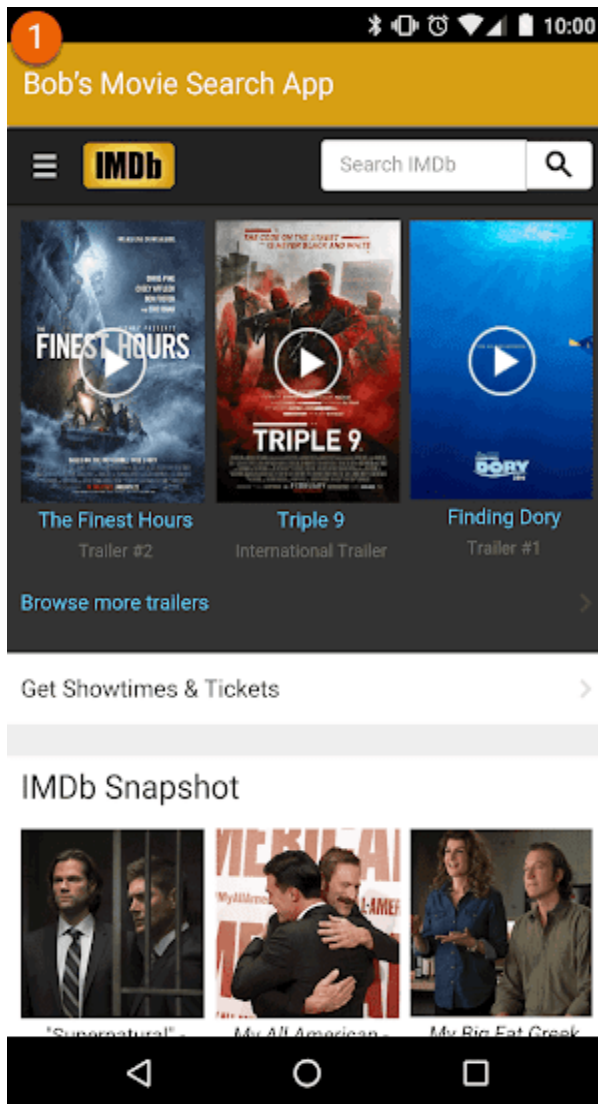
Webviews and Affiliate Spam

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

Here are some examples of common violations:

- 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 webview of a website without permission:



① This app is called “Bob’s Movie Search App” and it simply provides a webview of IMDb.

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.

Here are some examples of common violations:

- 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.

Apps that are created by an automated tool, wizard service, or based on templates and submitted to Google Play by the operator of that service on behalf of other persons are not allowed. Such apps

are only permissible if they are published by an individually registered developer account belonging to the user of the automated tool, not the operator of the service.

Made for Ads

We do not allow apps whose primary purpose is to serve ads.

Here are some examples of common violations:

Apps where interstitial ads are placed after every user action, including but not limited to clicks, swipes, etc.

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

Here are some examples of common violations:

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.

Here are some examples of common violations:

Apps that don't install
Apps that install, but don't load
Apps that load, but are not responsive

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 Program 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 homescreen 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 number if obtained using the runtime permission. The developer must not attempt to fingerprint the user 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.

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 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 make sure apps on Google Play are safe for families.

Apps designed specifically for children must participate in the Designed for Families program. However, if your app targets children as only one of its audiences, participating in the Designed for Families program is still a great way to surface your app to the right users. If you decide not to participate in the Designed for Families program, you still must comply with the Google Play Families Policy requirements below, as well as all other [Google Play Developer Program Policies](#) and the [Developer Distribution Agreement](#).

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 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 preschool children should only have the age group "Ages 5 & 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 truly have 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 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.
2. Google Play Console Answers: You must accurately answer the questions in the Google Play Console regarding your app and update those answers to accurately reflect any changes to your app.
3. Ads: If your app displays ads to children or to users of unknown age, you must:
 - only use [Google Play certified ad SDKs](#) to display ads to those users;
 - ensure ads displayed to those users do not involve interest-based advertising or remarketing;
 - ensure ads displayed to those users present content that is appropriate for children;
 - ensure 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.
4. Data Collection: 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, ad usage data, and advertising ID.
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 child-directed services. This includes, Google Sign-In (or any other Google API Service that accesses data associated with a Google Account), Google Play Games Services, and any other API Service using OAuth technology for authentication and authorization.
 - Apps that target both children and older audiences should 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 (e.g., providing Google Sign-in as an optional feature). Note that all users must be able to access your app and a reasonable amount of its functionality.
6. Privacy policy: You must provide a link to your app's privacy policy on your app's store listing page. This link must be maintained at all times while the app is available on the Store, and it

must link to a privacy policy that, among other things, accurately describes your app's data collection and use.

7. Special restrictions:

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 (e.g., be aware of your surroundings).

Your app must not require the usage of a device that is advised not to be used by children. (e.g. Daydream, Oculus)

8. Legal Compliance: You must ensure that your app, including any APIs or SDKs that your app calls or uses, is compliant with the [U.S. Children's Online Privacy and Protection Act \(COPPA\)](#), [E.U. General Data Protection Regulation \(GDPR\)](#), and any other applicable laws or regulations.

Here are some examples of common violations:

Apps that promote play for children in their store-listing but the app content is only appropriate for adults.

Apps that implement APIs that have terms of service that prohibit their use in child-directed apps.

Apps that glamorize 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 show mature ads to children.

Designed for Families Program

Apps designed specifically for children must participate in the Designed for Families program. If your app is designed for everyone, including children and families, you too can apply to participate in the program.

Before being accepted into the program your app must meet all of the Families Policy requirements and Designed for Families eligibility requirements, in addition to those outlined in the [Google Play Developer Program Policies](#) and [Developer Distribution Agreement](#).

For more information on the process for submitting your app for inclusion in the program, click [here](#).

Program Eligibility

All apps participating in the Designed for Families program must have both app and ad content that are relevant and appropriate for children and must satisfy all of the requirements below. Apps accepted into the Designed for Families program must remain compliant with all program requirements. Google Play reserves the right in its sole discretion to reject or remove any app determined to be inappropriate for the Designed for Families program.

Designed for Families Requirements

1. Apps must be rated ESRB Everyone or Everyone 10+, or equivalent.
2. You must accurately disclose the app's interactive elements on the Content Rating Questionnaire in the Google Play Console, including whether:
 - users can interact or exchange information;
 - your app shares user-provided personal information with third parties; and
 - your app shares the user's physical location with other users.
3. If your app uses the [Android Speech API](#), your app's `RecognizerIntent.EXTRA_CALLING_PACKAGE` must be set to its `PackageName`.
4. Apps must only use [Google Play certified ad SDKs](#).
5. Apps designed specifically for children cannot request location permissions.
6. 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.
 - Apps that are rated ESRB Everyone but contain ads for gambling content
 - Apps for parents or care-givers (e.g., breastfeeding tracker, developmental guide)
 - Parent guides or device management apps that are only intended for use by parents or care-givers

Categories

If you are accepted to participate in the Designed for Families program, you can choose a second Families-specific category that describes your app. Here are the categories available for apps participating in the Designed for Families program:

Action & Adventure: Action-oriented apps/games, including everything from simplistic racing games to fairy tale adventures, to other apps and games that are designed to generate excitement.

Brain Games: Games that make the user think, including puzzles, matching games, quizzes, and other games that challenge the memory, intelligence or logic.

Creativity: Apps and games that spur creativity, including drawing apps, painting apps, coding apps, and other apps and games where you can build things.

Education: Apps and games designed with input from learning experts (e.g., educators, learning specialists, researchers) to promote learning, including academic, social-emotional, physical, and creative learning, as well as learning related to basic life skills, critical thinking, and problem solving.

Music and Video: Apps and games with a musical or video component, including everything from instrument simulation apps to apps that provide video and musical audio content.

Pretend Play: Apps and games where the user can pretend to take on a role, for example, pretending to be a chef, care-giver, prince/princess, firefighter, police person or fictional character.

The policies below apply to any advertising (including both for your apps and for third party apps), offers for in-app purchase, or any other commercial content (such as paid product placement) that is served to users of apps that are subject to the Families Policy Requirements and/or the Designed for Families Requirements. All advertising, offers for in-app purchase, and commercial content 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 enforce on apps for overly aggressive commercial tactics.

Ad format requirements

Ads and offers for in-app purchases must not have deceptive content or be designed in a way that will result in inadvertent clicks from child users. The following are prohibited:

Use of [Ad walls](#)

Ads that interfere with normal app use that are not closeable after 5 seconds

Interstitial ads or offers for in-app purchase displayed immediately upon app launch

Multiple ad placements on a page

Ads or offers for in-app purchases that are not clearly distinguishable from your app content

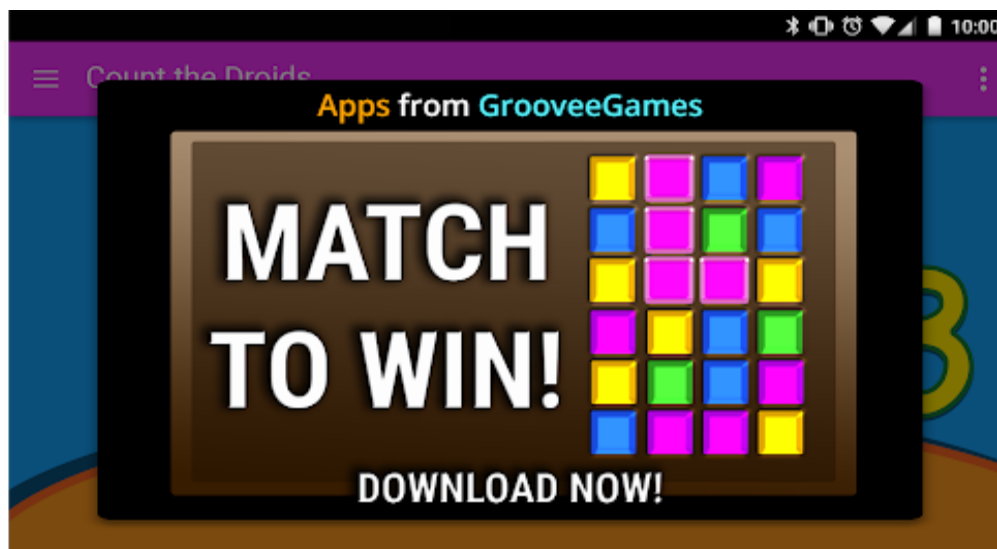
Use of shocking or emotionally manipulative tactics to encourage ads viewing or in-app purchases

Not providing a distinction between the use of virtual game coins versus real-life money to make in-app purchases

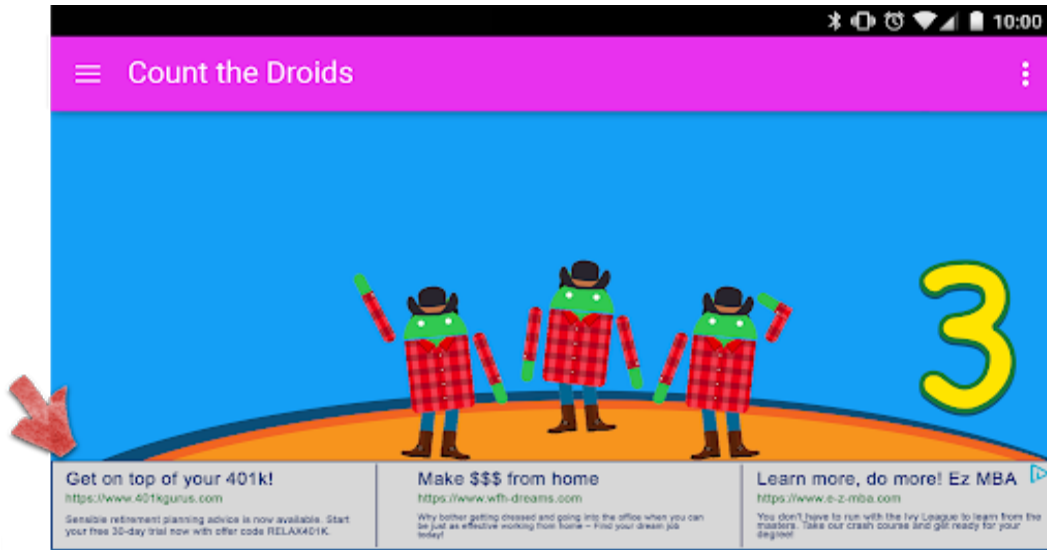
Here are some examples of common ad format violations

Ads that move away from a user's finger as the user tries to close it

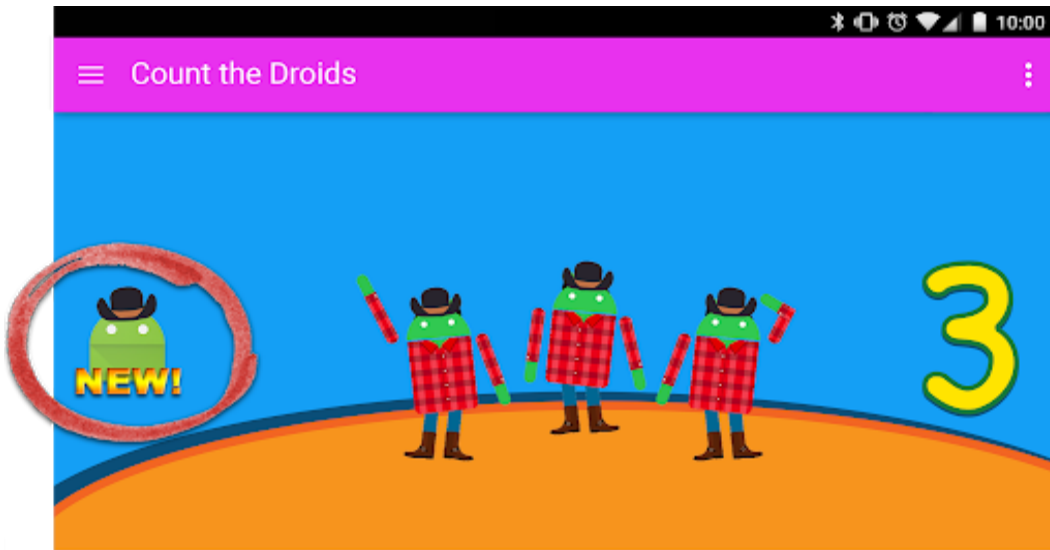
Ads that take up the majority or the device screen without providing the user a clear way to dismiss it, as depicted in the example below:



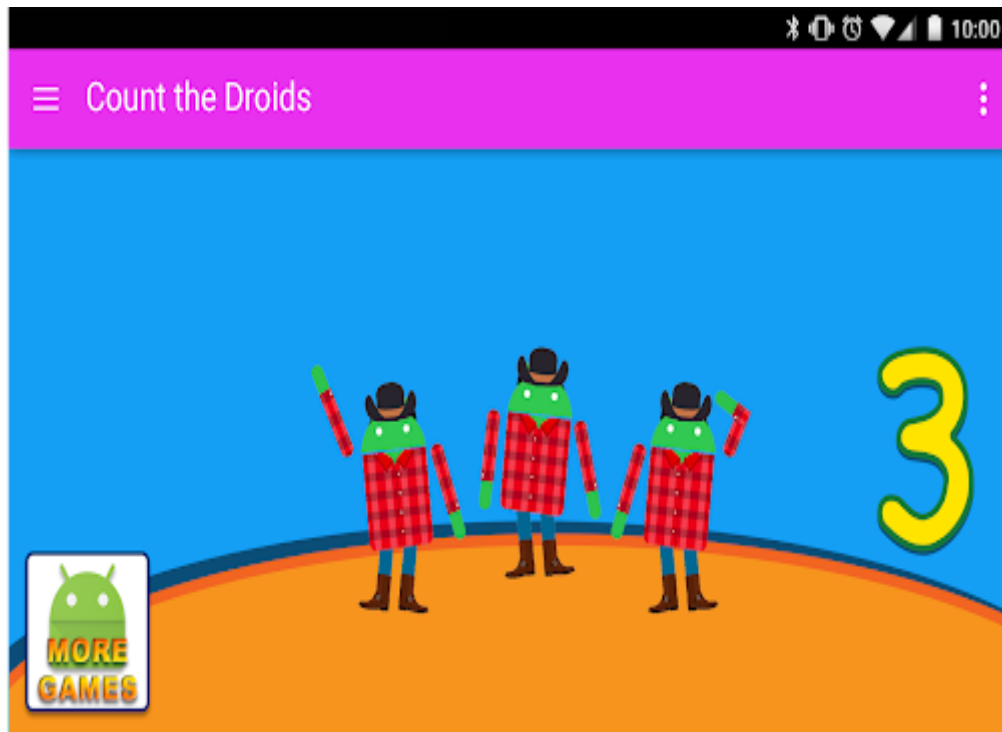
Banner ads showing multiple offers, as depicted in the example below:



Ads that could be mistaken by a user for app content, as depicted in the example below:



Buttons or ads 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 are not appropriate for children.

Inappropriate Video Games & 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

Only [Google Play certified ad SDKs](#) can be used to serve ads to children. Apps in the Designed for Families program are required to only use Google Play certified ad SDKs. For apps that also target adult users, non-certified ad SDKs may be used if a [neutral age screen](#) is present in the app and non-certified ad SDKs are only used to serve ads to known adult users.

Please refer to the [Families Ads Program policy](#) page for more details on these requirements and to see the current list of approved ad SDKs.

If you use AdMob, refer to the [AdMob Help Center](#) for more details on their products.

It is your responsibility to ensure 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.

In-app purchases

Google Play will re-authenticate all users prior to any in-app purchases in apps participating in the Designed for Families program. This measure is to help ensure that the financially responsible party, and not children, are approving purchases.

Avoiding a policy violation is always better than managing one, but when violations do occur, we're committed to ensuring 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. Further, 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](#).

Apps that may be inappropriate for a broad audience or result in a low quality experience for our end users may not be eligible for promotion on Google Play. Such apps will, however, remain available on Google Play so long as they are in compliance with these policies and the DDA.

Google reserves the discretion to include or remove apps from Google Play. We may take action based on a number of factors including, but not limited to, a pattern of harmful behavior or high risk of abuse. We identify risk of abuse using various items such as previous violation history, user feedback, and use of popular brands, characters, and other assets.

Enforcement Process

If your app violates any of our policies, it will be removed from Google Play, and you will receive an email notification with the specific reason for removal. Repeated or serious violations (such as

malware, fraud, and apps that may cause user or device harm) of these policies or the [Developer Distribution Agreement](#) (DDA) will result in termination of individual or related accounts.

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

Managing and Reporting Policy Violations

If you have any questions or concerns regarding a removal or a rating/comment from a user, you may refer to the resources below or contact us through the [Google Play Help Center](#). We cannot, however, offer you legal advice. If you need legal advice, please consult legal counsel.

[App verification & appeals](#)

[Report a policy violation](#)

[Contact Google Play about an account termination or app removal](#)

[Fair warnings](#)

[Report inappropriate apps & comments](#)

[My app has been removed from Google Play](#)

[Understanding Google Play developer account terminations](#)

[Developer Distribution Agreement](#)