# **Developer Policy Center - March 2016**

# Let's build the world's most trusted store 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 through the interactive tiles below or in a print view.

# **Restricted Content**

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

# **Sexually Explicit Content**

We don't allow apps that contain or promote sexually explicit content, such as pornography. In general, we don't allow content intended to be sexually gratifying.

#### Here are some examples of common violations:

- Depictions of sex acts or sexually suggestive poses.
- · Promotional images of sex toys.
- Promoting sexually explicit user-generated content.
- Content that depicts, describes, or encourages bestiality.

# **Child Endangerment**

Google has a zero-tolerance policy against child sexual abuse imagery. 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.

#### **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.
- Terrorist groups documenting their attacks.
- Instructions for engaging in violent activities, including bomb- or weapon-making.
- Instructions on how to commit suicide.

### **Bullying and Harassment**

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

#### Here are some examples of common violations:

- 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.

## **Hate Speech**

We don't allow apps that advocate against groups of people based on their race or ethnic origin, religion, disability, gender, age, nationality, veteran status, sexual orientation, or gender identity.

#### 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.

# **Gambling**

We don't allow content or services that facilitate online gambling, including but not limited to, online casinos, sports betting, lotteries, or games of skill that offer prizes of cash or other value.

#### Here are some examples of common violations:

- Apps that allow a user to wager in order to earn real money.
- Redirecting users to a gambling or betting website where users can earn real money. This
  includes ad SDKs that redirect users to gambling websites that facilitate real gambling.

# **Illegal Activities**

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.

# Intellectual Property, Deception, and Spam

When developers copy someone else's work or deceive users, it hurts users and the developer community. Don't rely on deceptive, spammy tactics or unfairly use other people's work.

# Impersonation and Intellectual Property

We don't allow apps or developer accounts that impersonate other entities, brands, or otherwise infringe on 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.

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 Impersonation or Intellectual Property violation.

#### **Impersonation**

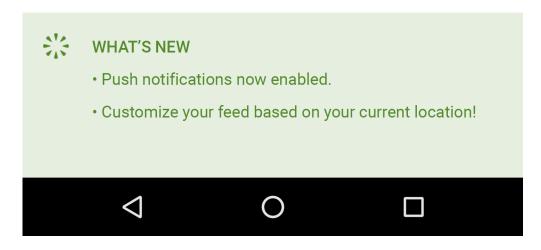
We don't allow apps that use another app or entity's brand, title, logo, or name in a manner that may result in misleading users. Don't try to imply an endorsement or relationship with another entity where none exists. Impersonation can occur even if there isn't an intent to deceive, so please be careful 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:



All the best news, aggregated in one spot!



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:



- 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.

#### **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:

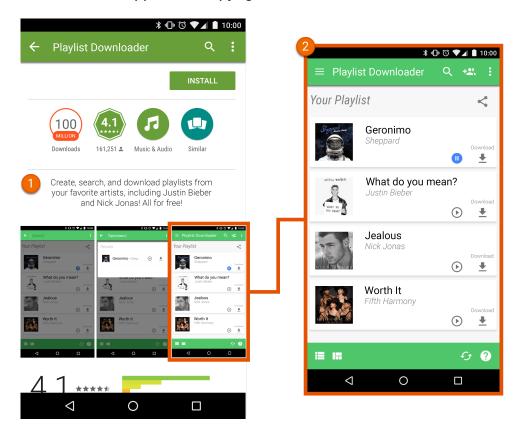
- Cover art for music albums, video games, and books.
- Marketing images from movies, television, or video games.
- Artwork or images from comic books, cartoons, movies, music videos, or television.
- · College and professional sports team logos.
- Photos taken from a public figure's social media account.
- · 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.

## **Deceptive Behavior**

We don't allow apps that attempt to deceive users. Apps must provide accurate disclosure of their functionality 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:

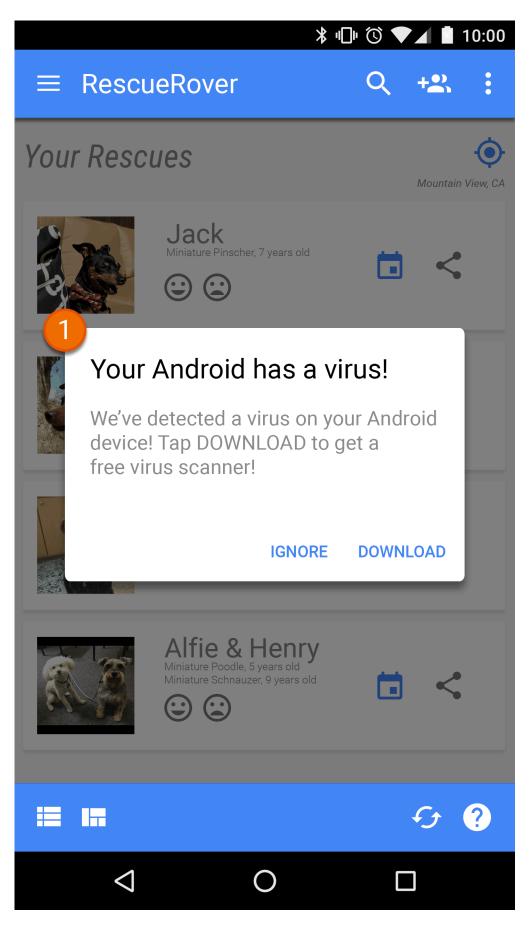
- Apps that misrepresent or do not accurately and clearly describe their functionality:
  - An app that claims to be a racing game in its description and screenshots, but is actually a
    puzzle block game using a picture of a car.
  - An app that claims to be an antivirus app, but only contains a text guide explaining how to remove viruses.
- Apps that feature medical or health-related functionalities that are misleading or potentially harmful.
- Apps that claim functionalities that are not possible to implement.
- Apps that are improperly categorized.

#### **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.

## **Spam**

We don't allow apps that spam users or the Store, such as apps that send users unsolicited messages or apps that are duplicative and low-quality.

#### **Message Spam**

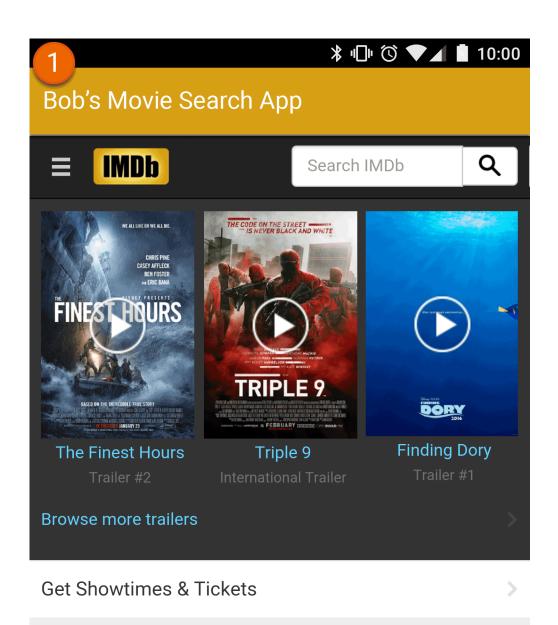
We don't allow apps that send SMS, email, or other messages on behalf of the user without giving the user the ability to confirm the content and intended recipients.

#### Webviews and Affiliate Spam

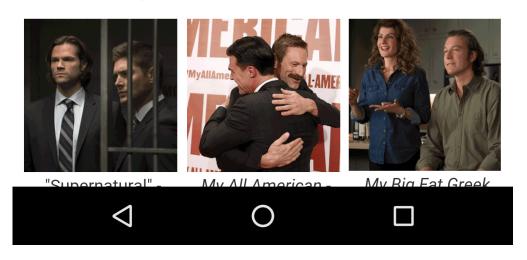
We don't allow apps whose primary purpose is to drive affiliate traffic to a website or provide a webview of a website without permission from the website owner or administrator.

#### 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:



# **IMDb** Snapshot



1) This app is called "Bob's Movie Search App" and it simply provides a webview of IMDb.

We don't allow apps that are created by an automated tool or wizard service and submitted to Google Play by the operator of that service on behalf of other persons. 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.

# **Privacy and Security**

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

#### **User Data**

You must be transparent in how you handle user data (e.g., information provided by a user, collected about a user, and collected about a user's use of the app or device), including by disclosing the collection, use, and sharing of the data, and you must limit use of the data to the description in the disclosure. If your app handles personal or sensitive user data, there are additional requirements described below. This policy establishes Google Play's minimum privacy requirements; you or your app may need to comply with additional restrictions or procedures if required by an applicable law.

#### **Personal and Sensitive Information**

If your app handles personal or sensitive user data (including personally identifiable information, financial and payment information, authentication information, phonebook or contact data, and sensitive device data) then your app must:

- Post a privacy policy that, together with any in-app disclosures, comprehensively discloses the
  collection, use and sharing of any user data your app handles, how it's used, and the types of
  parties with whom it's shared, and
- Handle the user data securely, including transmitting it using modern cryptography (for example, over HTTPS).

If your app collects and transmits personal or sensitive user data unrelated to functionality described prominently in the app's listing on Google Play or in the app interface, then prior to the collection and transmission, it must prominently highlight how the user data will be used and have the user provide affirmative consent for such use.

#### Here are some examples of common violations:

- An app that collects and transmits the user's inventory of installed apps without adequate disclosure and consent.
- A game that collects and transmits the user's contact book without adequate disclosure and consent.

#### Additional Requirements

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

**Activity** Requirement

#### **Activity**

If your app handles financial or payment information or government identification numbers

If your app handles non-public phonebook or contact information

If your app contains anti-virus or security functionality, such as antivirus, anti-malware, or securityrelated features

#### Requirement

Then it must never publicly disclose any personal or sensitive user data related to financial or payment activities or any government identification numbers.

We don't allow unauthorized publishing or disclosure of people's non-public contacts.

Then it 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 types of parties with whom it's shared.

#### **Device and Network Abuse**

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 some 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.

#### **Malicious Behavior**

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

All apps on Google Play that collect user data must comply with the User Data policy and fully disclose its functions. An app downloaded from Google Play may not modify, replace, or update itself using any method other than Google Play's update mechanism

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

# **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 where they were first 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.

#### Here are some examples of products supported by Google Play In-app Billing:

- **Virtual game products**, including coins, gems, extra lives or turns, special items or equipment, characters or avatars, additional levels or playtime.
- App functionality or content, such as an ad-free version of an app or new features not available in the free version.
- **Subscription services**, such as streaming music, video, book, or other media services; digital publications, including when bundled with a physical edition; and social networking services.
- Cloud software products, including data storage services, business productivity software, and financial management software.

Here are some examples of products not currently supported by Google Play In-app Billing:

- Retail merchandise, such as groceries, clothing, housewares, and electronics.
- Service fees, including taxi and transportation services, cleaning services, food delivery, airfare, and event tickets.
- One-time membership fees or recurring dues, including gym memberships, loyalty programs, or clubs offering accessories, clothing, or other physical products.
- One time-payments, including peer-to-peer payments, online auctions, and donations.
- **Electronic bill payment**, including credit card bills, utilities, and cable or telecommunications services.

# **Subscriptions and Cancellations**

If a user cancels a subscription purchased from an app downloaded 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 refund policies and ensure that the policies comply with applicable law.

#### Ads

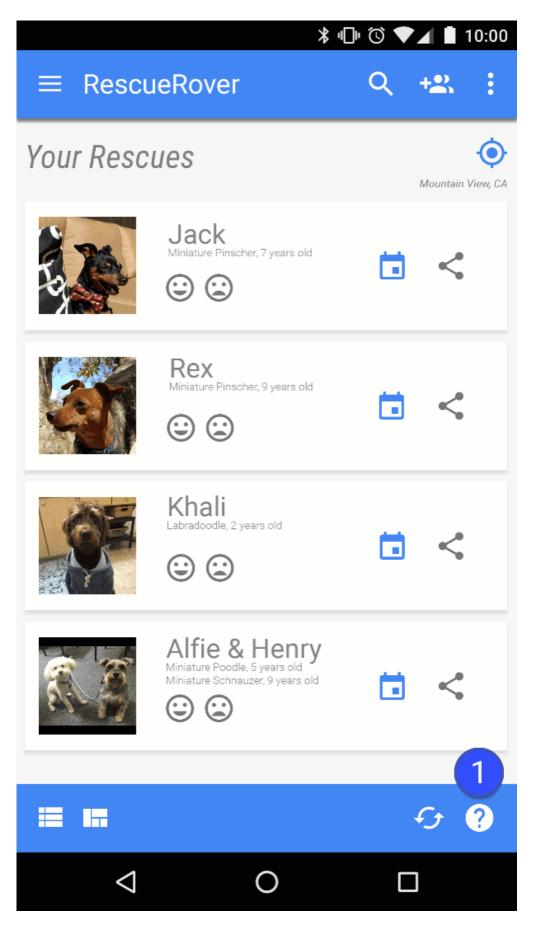
We don't allow apps that contain deceptive or disruptive ads. Ads must only be displayed within the app serving them. We consider ads served in your app as part of your app. The ads shown in your app must be compliant with all our policies.

#### **Deceptive Ads**

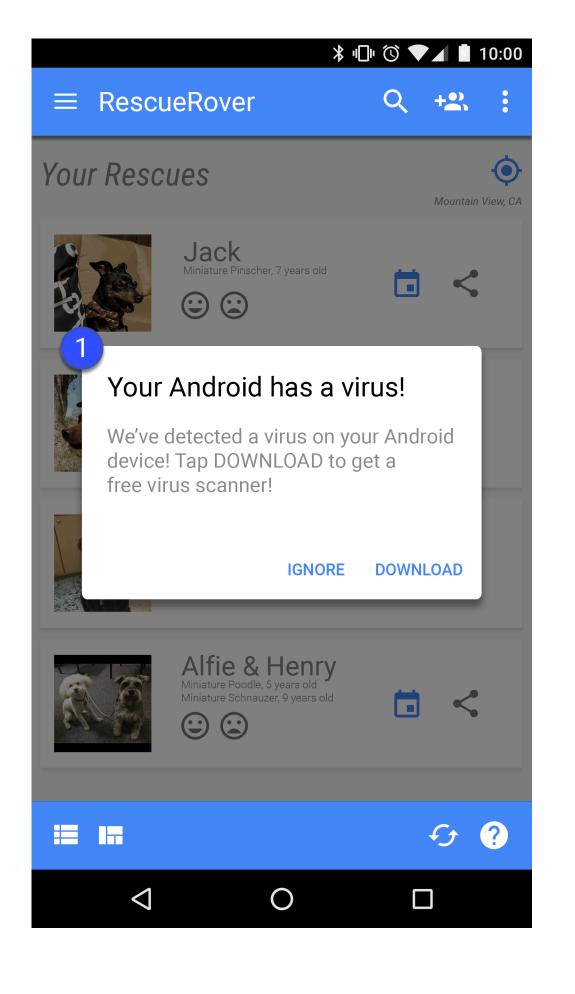
Ads must not simulate or impersonate the user interface of any app, notification, or warning elements of an operating system. It must be clear to the user which app is serving each ad.

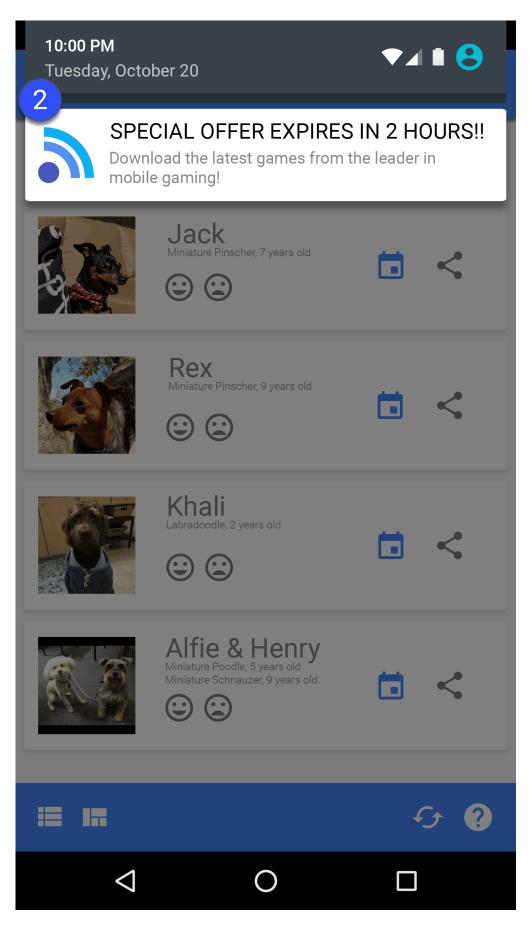
#### Here are some examples of common violations:

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:





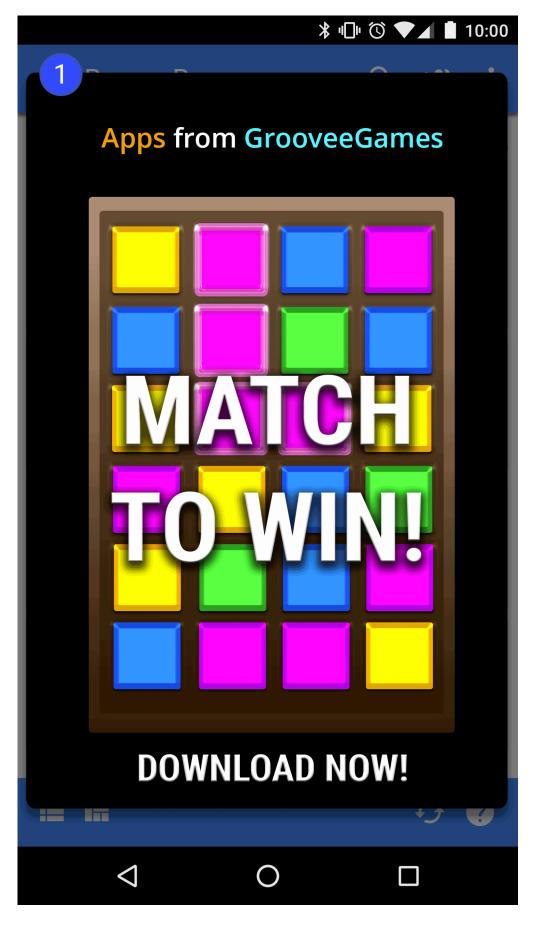
 $\bigcirc$  The examples above illustrate ads mimicking various system notifications.

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 dismissable 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:



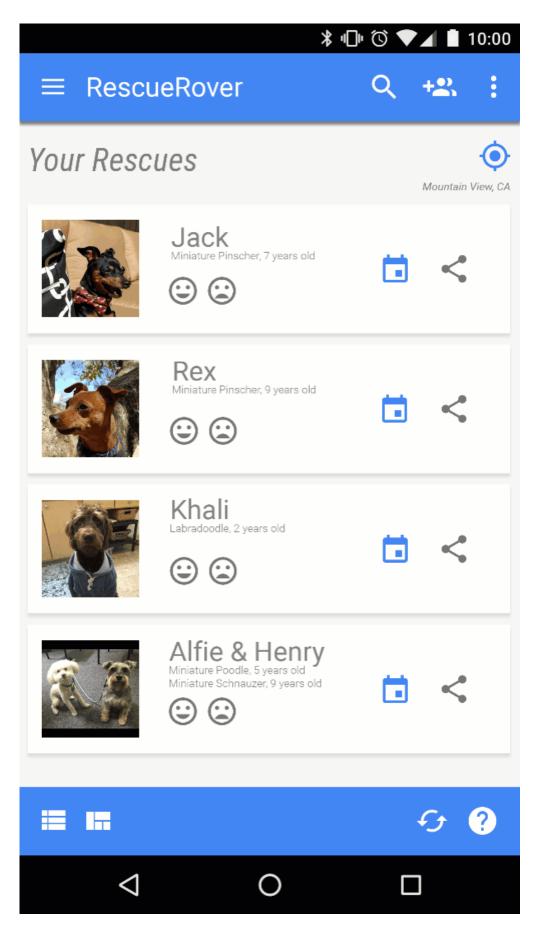
① This ad does not have a dismiss button.

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, or widgetized ad units. Ads must only be displayed within the app serving them.

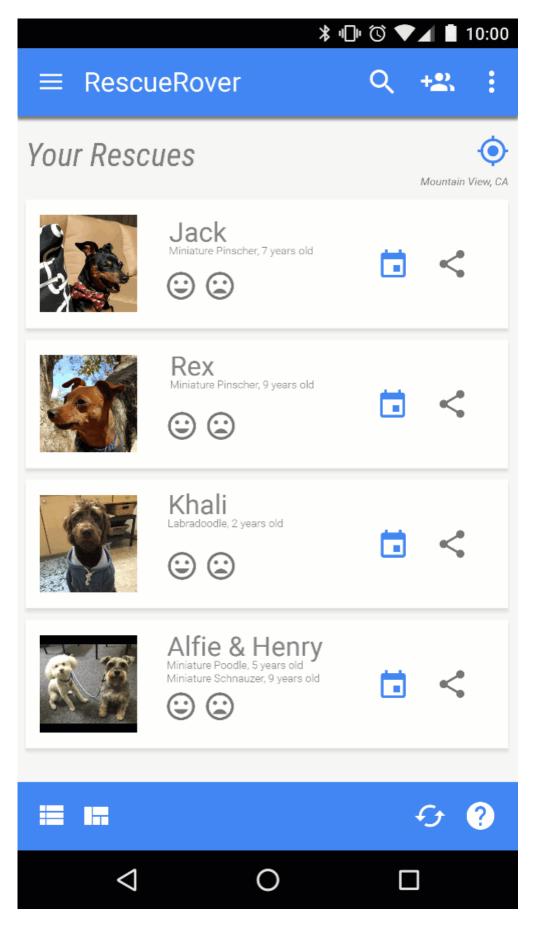
#### Here are some examples of common violations:

• 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:

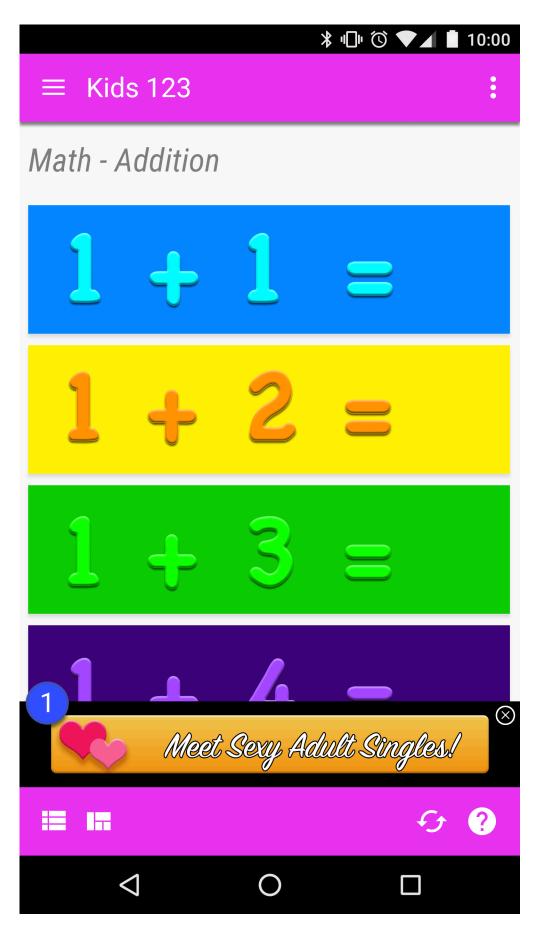


Description: The user attempts to exit the app and navigate to the home screen, but instead, the expected flow is interrupted by an ad.

#### **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.

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" 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" 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 interest-based
  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. Beginning August 1st 2014, all updates and new apps uploaded to the Play Store must use the advertising ID (when available on a device) in lieu of any other device identifiers for any advertising purposes.

# **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 the Store.

## **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.

#### Metadata

We don't allow apps with misleading, irrelevant, excessive, or inappropriate metadata, which include the app's description, title, icon, screenshots, and promotional images. We also don't allow user testimonials in the app's description.

The best way to find a new furry friend!

RescueRover lets you use your Android device to search for rescue dogs.

See how much our users love us:

"It was easy to find the right dog for me and my family!"

2

It's the #1 app after Pet Rescue Saga, but in real life!

50% cooler and 100% faster than FidoFinder

You can see black dogs, brown dogs, white dogs, big dogs, medium dogs, small dogs, dog leashes, dog training books, dog bowls, dog toys, dog accessories. dog, dogs, rescue, shelter, animal, pet, pets, adopt, foster, puppy, puppies, dogs including:

- 1) golden retriever
- 2) labradoodle
- 3) poodle
- 4) chihuahua
- 5) akita
- 6) pug
- 7) rottweiler



- 1 User testimonials
- ② Excessive details
- 3 4 Misleading references to other apps or products
- (5) Repetitive, excessive, or irrelevant keywords

#### Here are a few best practices:

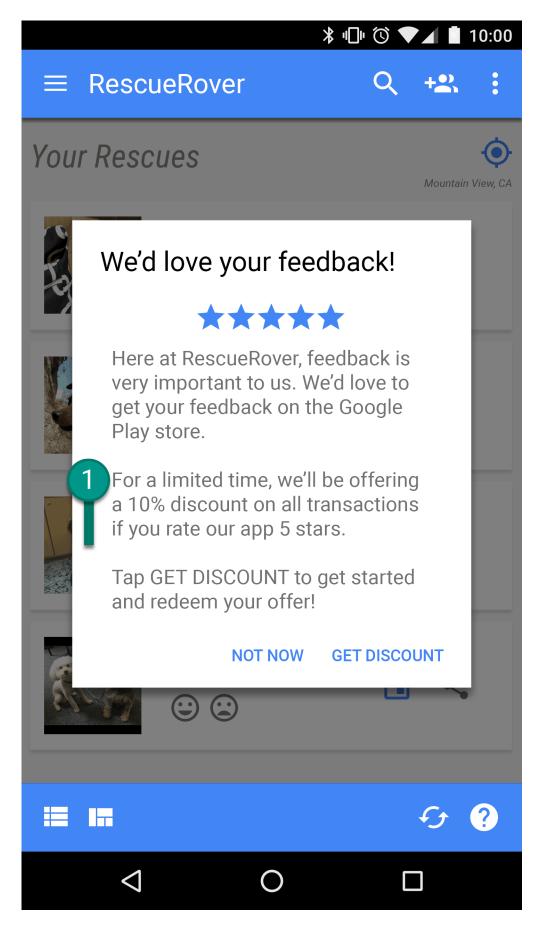
- Highlight what's great about your app. Share interesting and exciting facts about your app to help users understand what makes your app special.
- Make sure that your app's title and description accurately describe your app's functionality.
- Avoid using repetitive or unrelated keywords or references.
- 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, or
  repetition can result in a violation of this policy.

## Ratings, Reviews, and Installs

Developers must not attempt to manipulate the placement of any apps in the Store. This includes inflating product ratings or reviews by illegitimate means, such as fraudulent installs and incentivized, paid, or fake reviews and ratings.

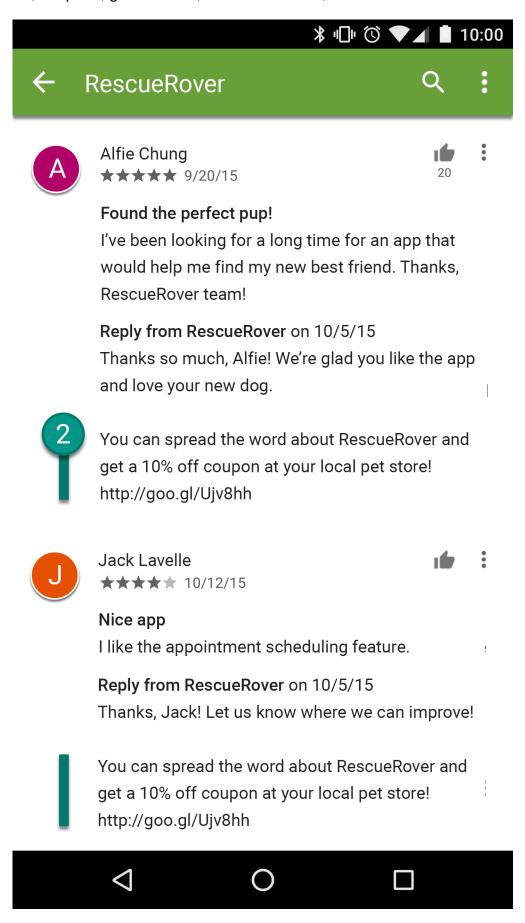
#### Here are some examples of common violations:

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 the Google Play Storefront.

• 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.

# **Enforcement**

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.

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.

#### **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**