Developer Policy Center - November 2017

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 through the interactive tiles below or in a print view.

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.

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

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.
- Apps that promote self harm.

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

- **Gambling Apps (Currently permitted in the UK, Ireland, and France only)**
  - 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 use Google payments services, including 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 value.

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

- **Gambling Ads within Play-distributed apps**

    - 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

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.

User Generated Content

Apps that contain or feature user-generated content (UGC) must take additional precautions in order to provide a policy compliant app experience.

A policy compliant app must:

- Define content that is objectionable and prohibit it via a terms of use or policy document
- Require users to agree to your product’s terms of use before submitting content
- Implement a user-friendly system for reporting abuse that effectively removes content in violation of your terms
- Remove or block abusive users of your service
- Provide correct categorization and IARC rating for your App

Impersonation and Intellectual Property

When developers copy someone else’s work or deceive users, it hurts users and the developer community. Don't rely on misleading or unfair use of other people’s work.

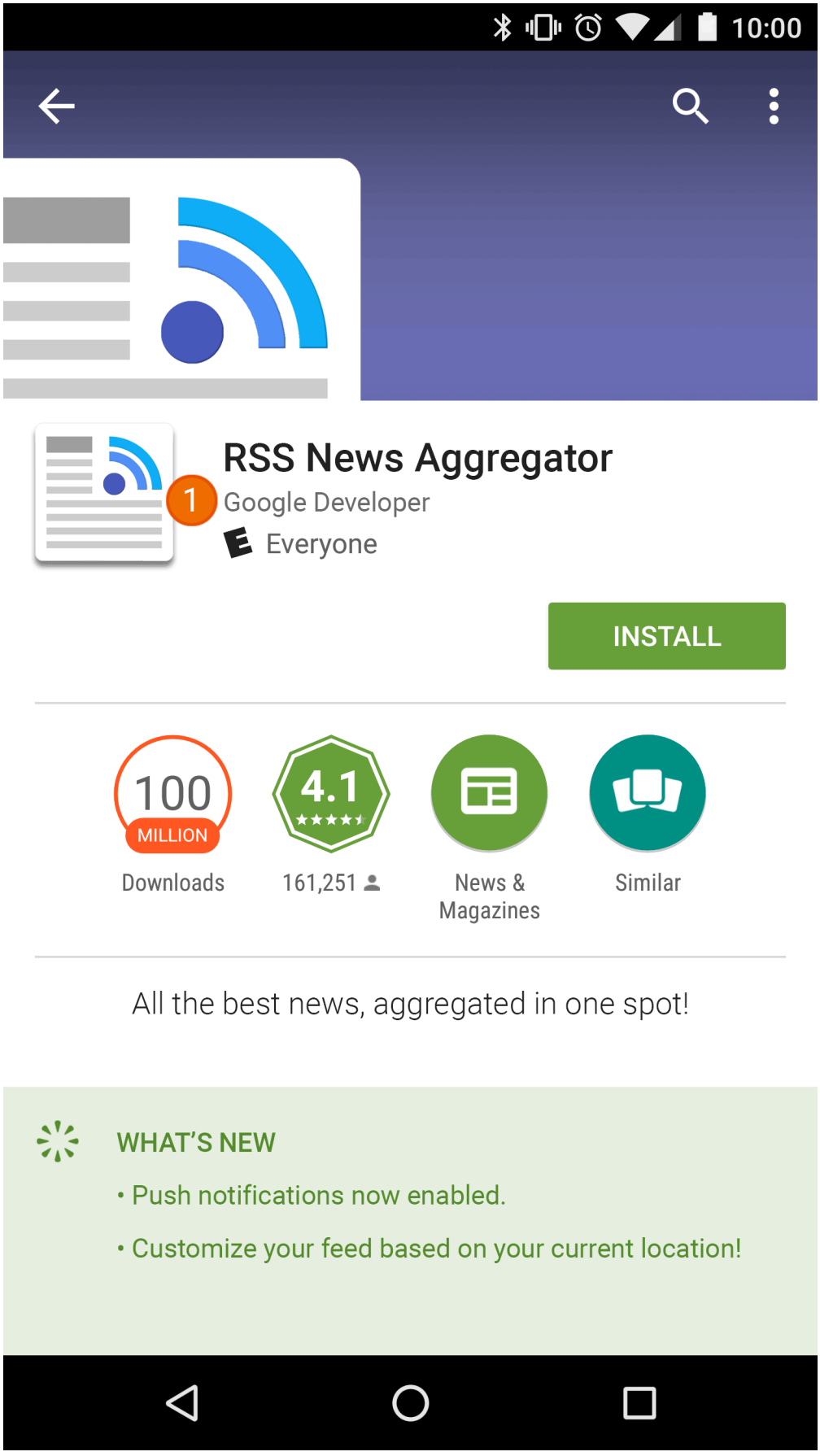
Impersonation

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:



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.

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.

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.

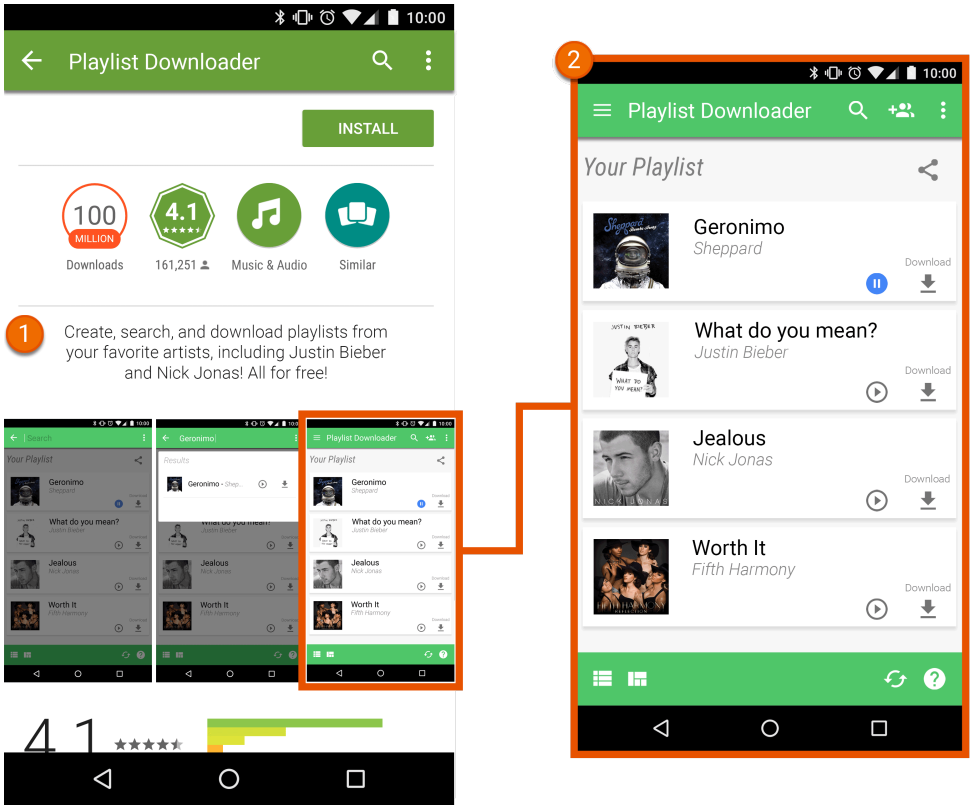
- Artwork or images from comic books, cartoons, movies, music videos, or television.
- College and professional sports team logos.
- Photos taken from a public figure's social media account.
- Professional images of public figures.
- Reproductions or "fan art" indistinguishable from the original work 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.

Privacy, Security, and Deception

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

User Data

You must be transparent in how you handle user data (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

Privacy Policy & Secure Transmission

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

- Post a privacy policy in both the designated field in the Play Console and from within the Play distributed app itself.
- Handle the user data securely, including transmitting it using modern cryptography (for example, over HTTPS).

The privacy policy must, together with any in-app disclosures, comprehensively disclose how your app collects, uses and shares user data, including the types of parties with whom it’s shared.

Prominent Disclosure Requirement

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.

Your in-app disclosure:

- Must be within the app itself, not only in the Play listing or 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 type of data being collected;
- Must explain how the data will be used;
- **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 app's request for consent:

- Must present the consent dialog in a clear and unambiguous way;
- Must require affirmative user action (e.g. tap to accept, tick a check-box, a verbal command, etc.) in order to accept;
- **Must not** begin personal or sensitive data collection prior to obtaining affirmative consent;
- **Must not** consider 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 doesn't treat a user's inventory of installed apps as personal or sensitive user data and doesn't comply with the Privacy Policy, Secure Transmission, and Prominent Disclosure requirements.
- An app that doesn't treat a user's phone or contact book data as personal or sensitive user data and doesn't comply with the Privacy Policy, Secure Transmission, and Prominent Disclosure requirements.

EU-U.S. Privacy Shield

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.

Additional Requirements

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

Activity	Requirement

Activity	Requirement
If your app handles financial or payment information or government identification numbers	Then it must never publicly disclose any personal or sensitive user data related to financial or payment activities or any government identification numbers.
If your app handles non-public phonebook or contact information	We don't allow unauthorized publishing or disclosure of people's non-public contacts.
If your app contains anti-virus or security functionality, such as anti-virus, anti-malware, or security-related features	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.

Permissions

Permission requests should make sense to users, and should be limited to the critical information necessary to implement your app.

Don't request access to information that you don't need. You may only request access to the user data that is necessary to implement existing features or services in your application. Don't attempt to "future proof" your access to user data by requesting access to information that might benefit services or features that have not yet been implemented.

Request permissions in context where possible. Request access to user data in context (via incremental auth) whenever you can, so that users understand why you need the data.

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.

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).

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 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 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.

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.

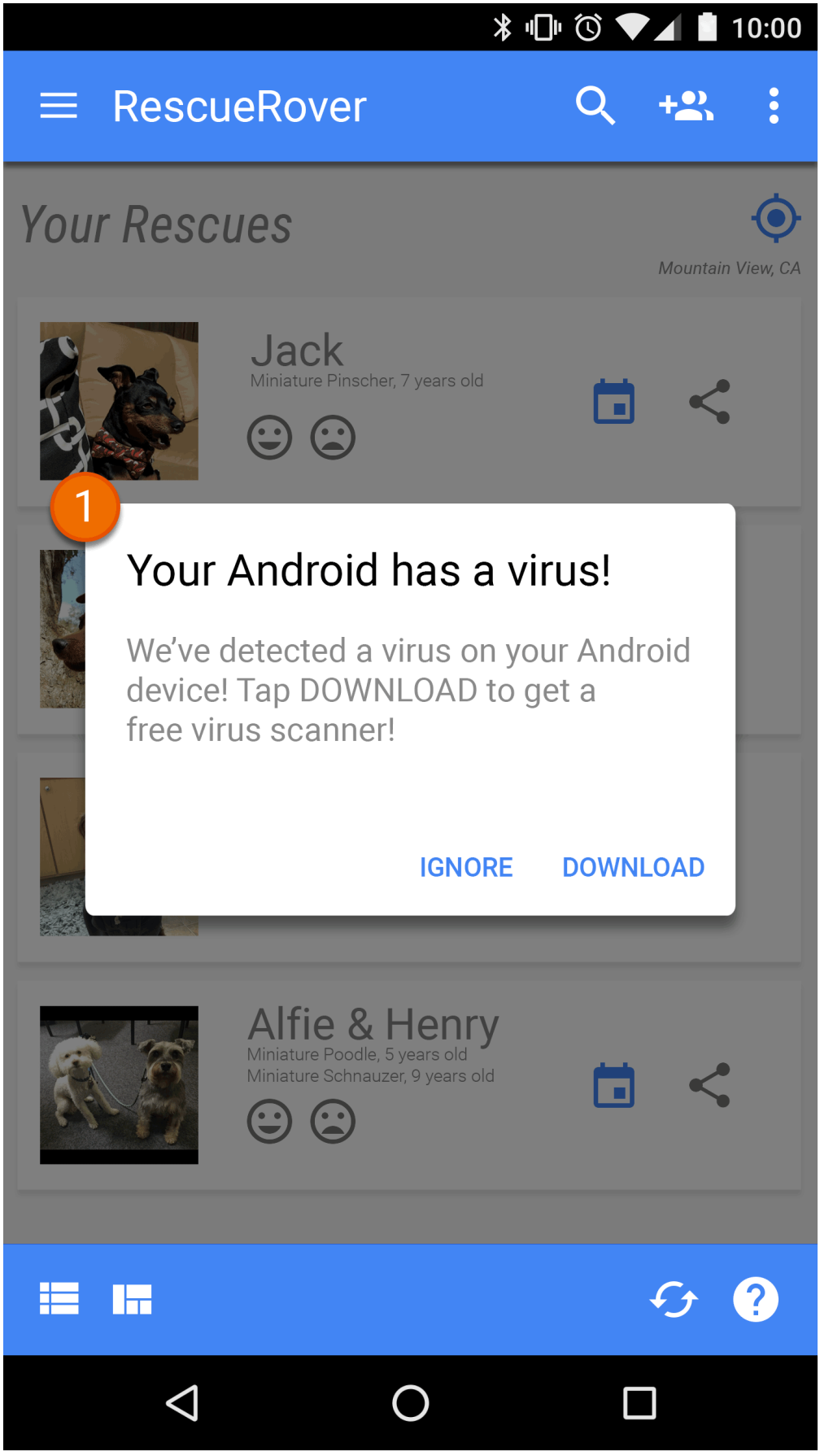
- Developer or app names that misrepresent their current status or performance on Play. (E.g. “Editor’s Choice,” “Number 1 App,” “Top Paid”).
- Apps that feature medical or health-related functionalities that are misleading or potentially harmful.
- Apps that claim functionalities that are not possible 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.

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.

Note that in some markets, we offer Android Pay for apps selling physical products and services. For more information, please visit our Android Pay developer page for details and brand usage requirements.

Subscriptions and Cancellations

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 refund policies and ensure that the policies comply with applicable law.

Ads

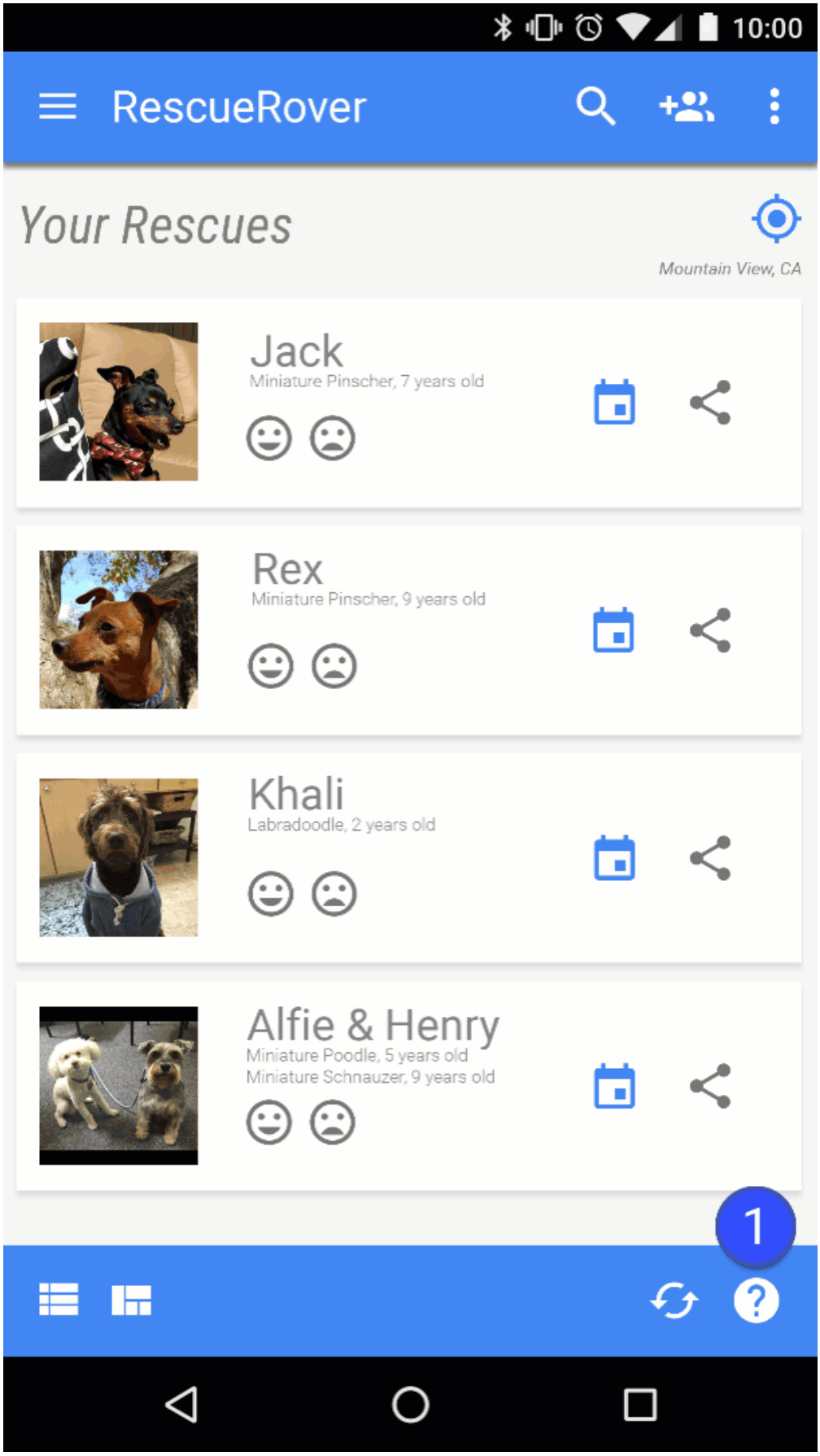
We don’t allow apps that contain deceptive or disruptive ads. Ads must only be displayed within the app serving them. We consider ads served in your app as part of your app. The ads shown in your app must be compliant with all our policies. For policies on gambling ads, please click here.

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.

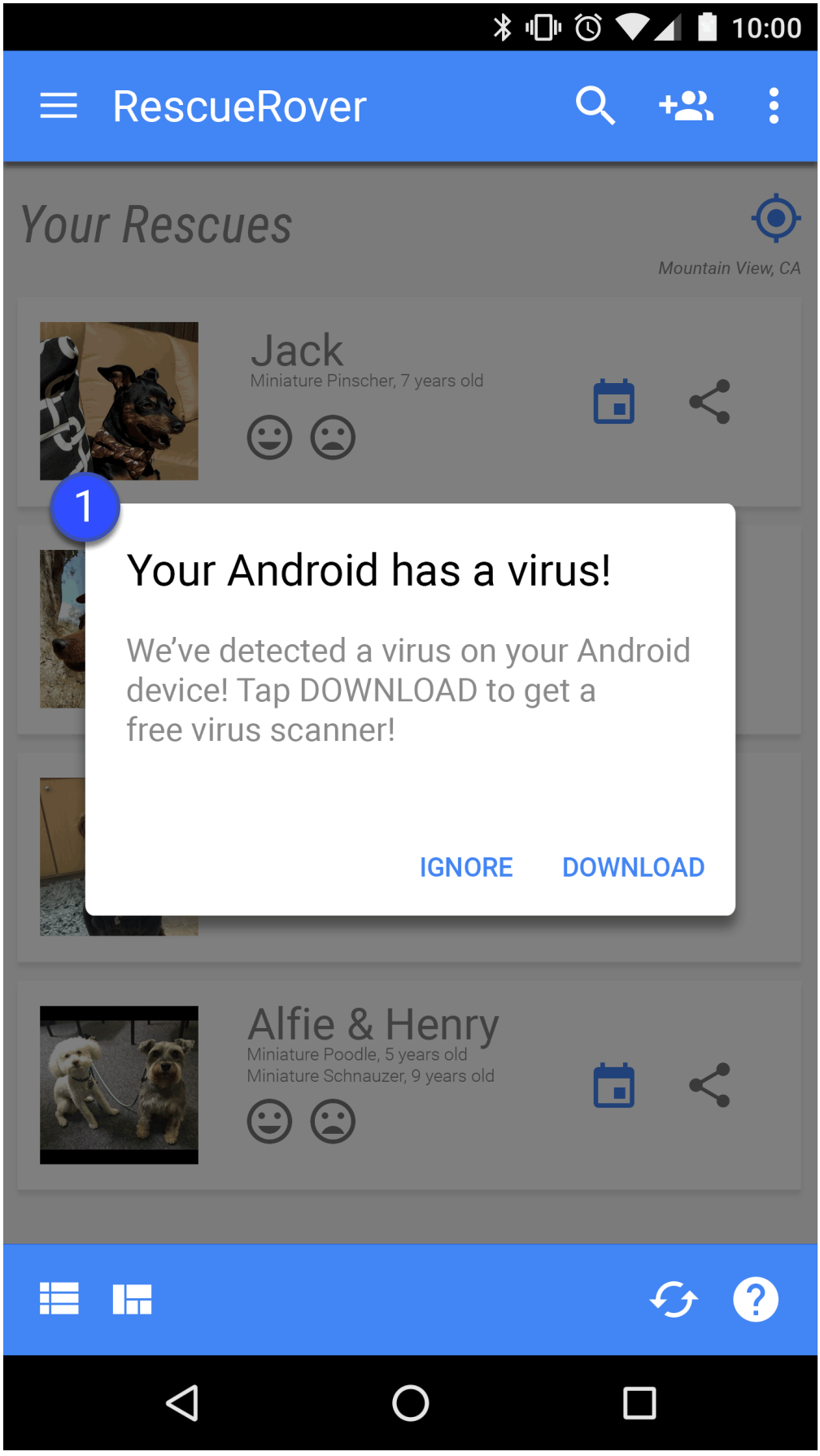
Here are some examples of common violations:

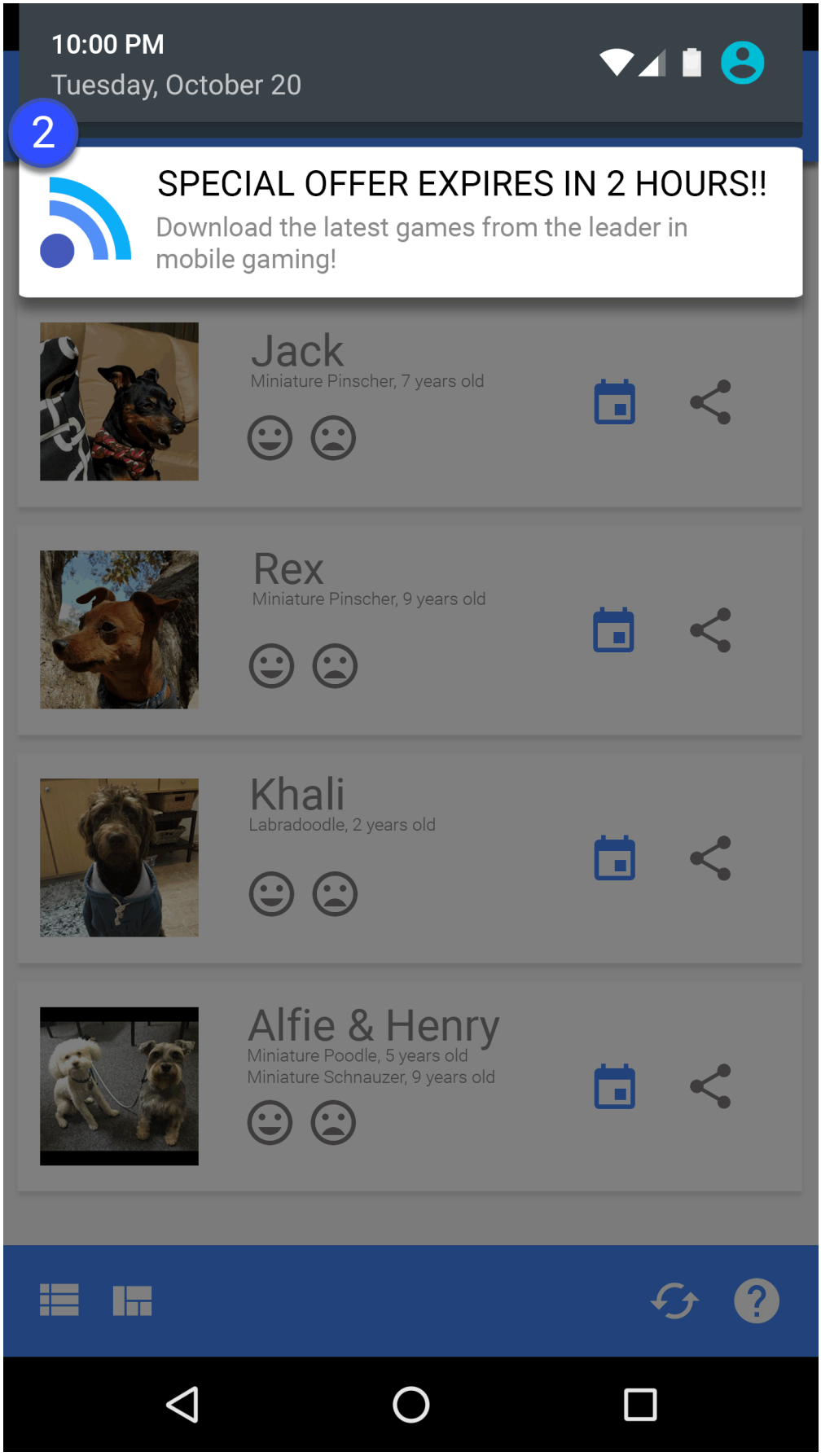
- Ads that mimic an app's UI:



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:


10:00
RescueRover
Your Rescues
Mountain View, CA
Jack
Miniature Pinscher, 7 years old
1
Your Android has a virus!
We've detected a virus on your Android device! Tap DOWNLOAD to get a free virus scanner!
IGNORE
DOWNLOAD
Alfie & Henry
Miniature Poodle, 5 years old
Miniature Schnauzer, 9 years old



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 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:

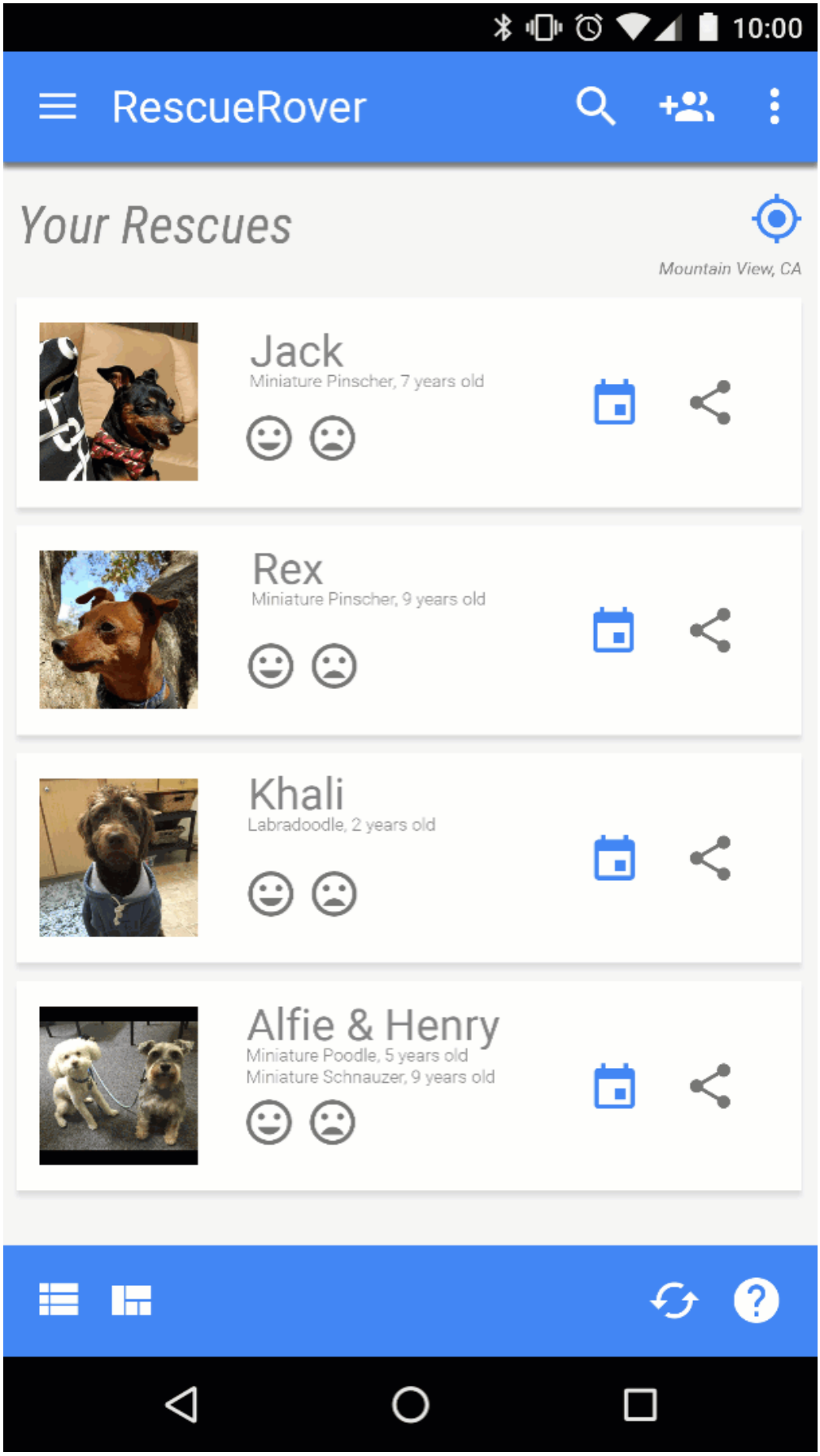
① This ad does not have a dismiss button.

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

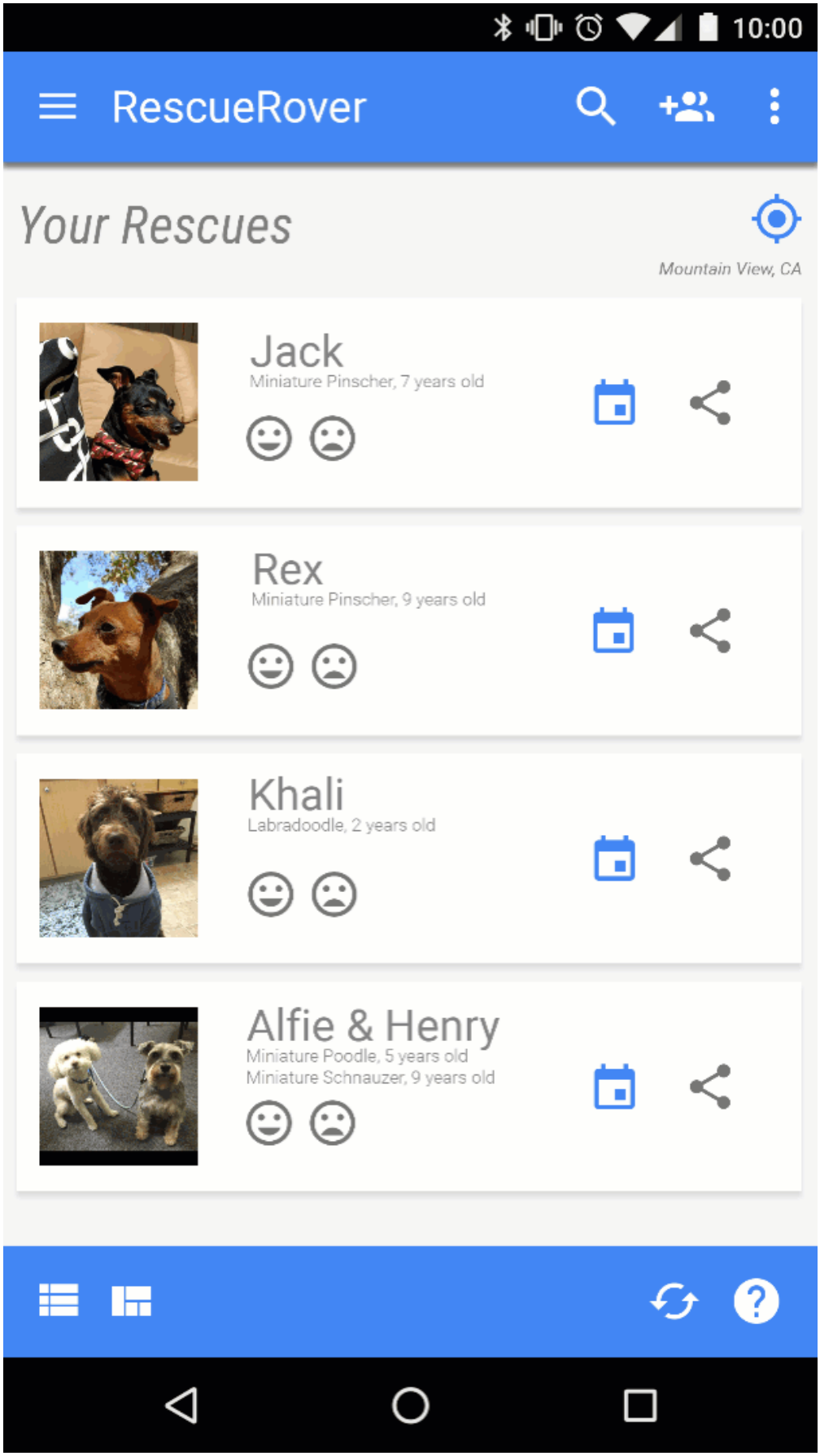
Here are some examples of common violations:

- 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:

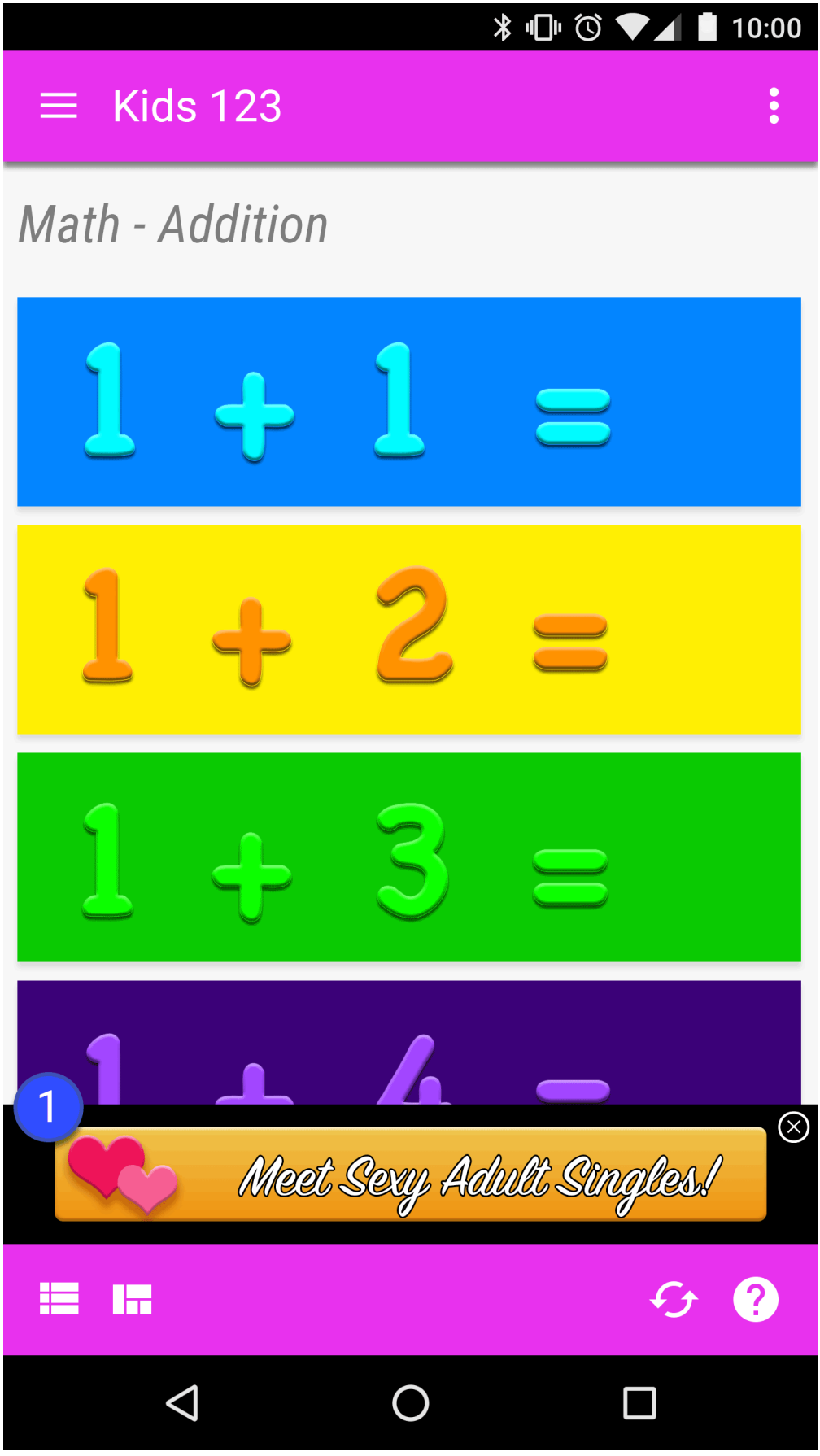


Description: The user attempts to exit the app and navigate to the home screen, but instead, the expected flow is interrupted by an ad.

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. Beginning August 1st 2014, all updates and new apps uploaded to Google Play 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 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:

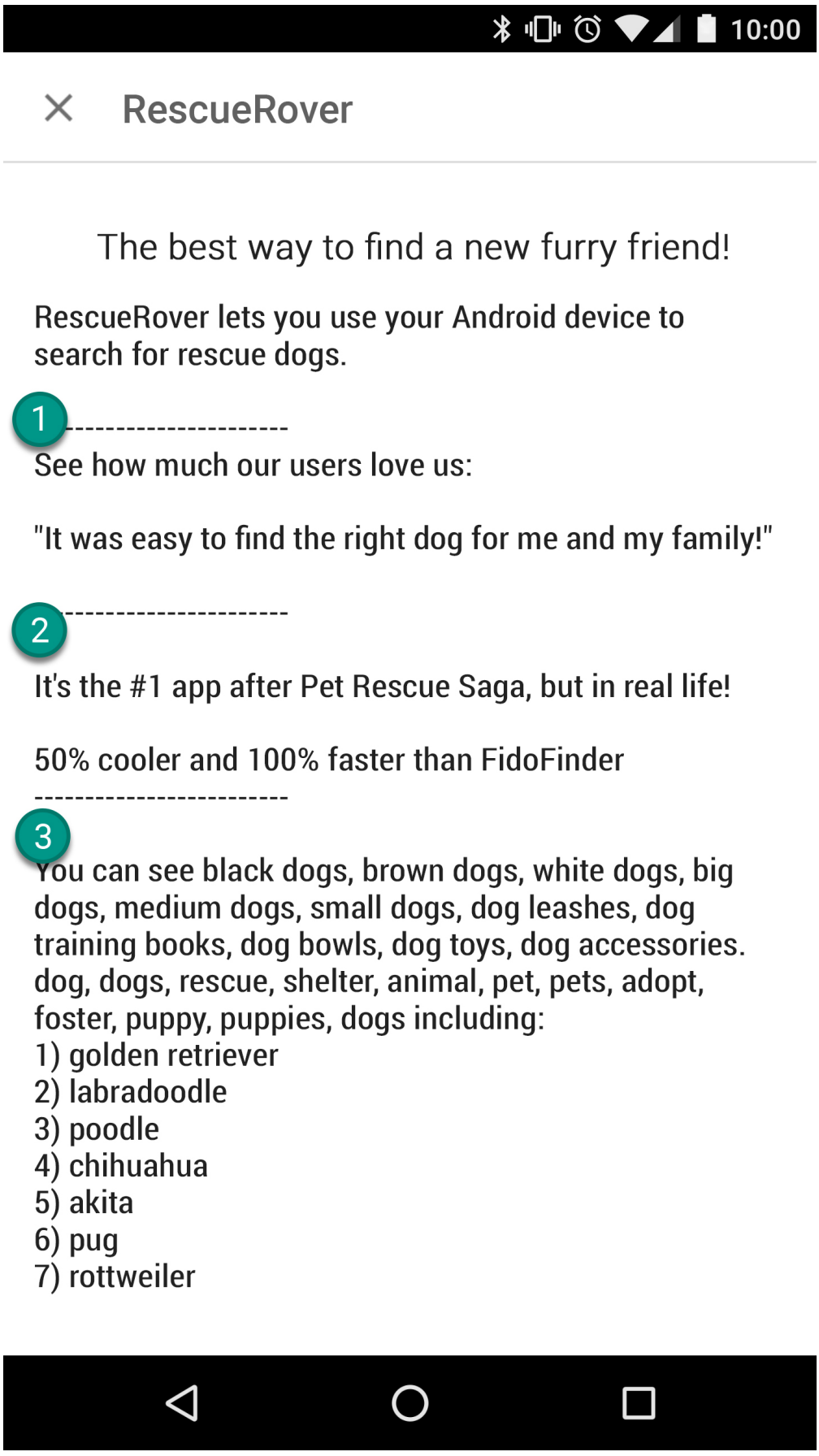
- Using deceptive ads on websites, apps, or other properties, including notifications that are similar to system notifications and alerts.
- Promotion or installation tactics that redirect users to Google Play or download apps without informed user action.
- Unsolicited promotion via SMS services.

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.

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.

Here are some examples of common violations:



① User testimonials

② Excessive details

③ ④ Misleading references to other apps or products

⑤ Repetitive, excessive, or irrelevant keywords

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:

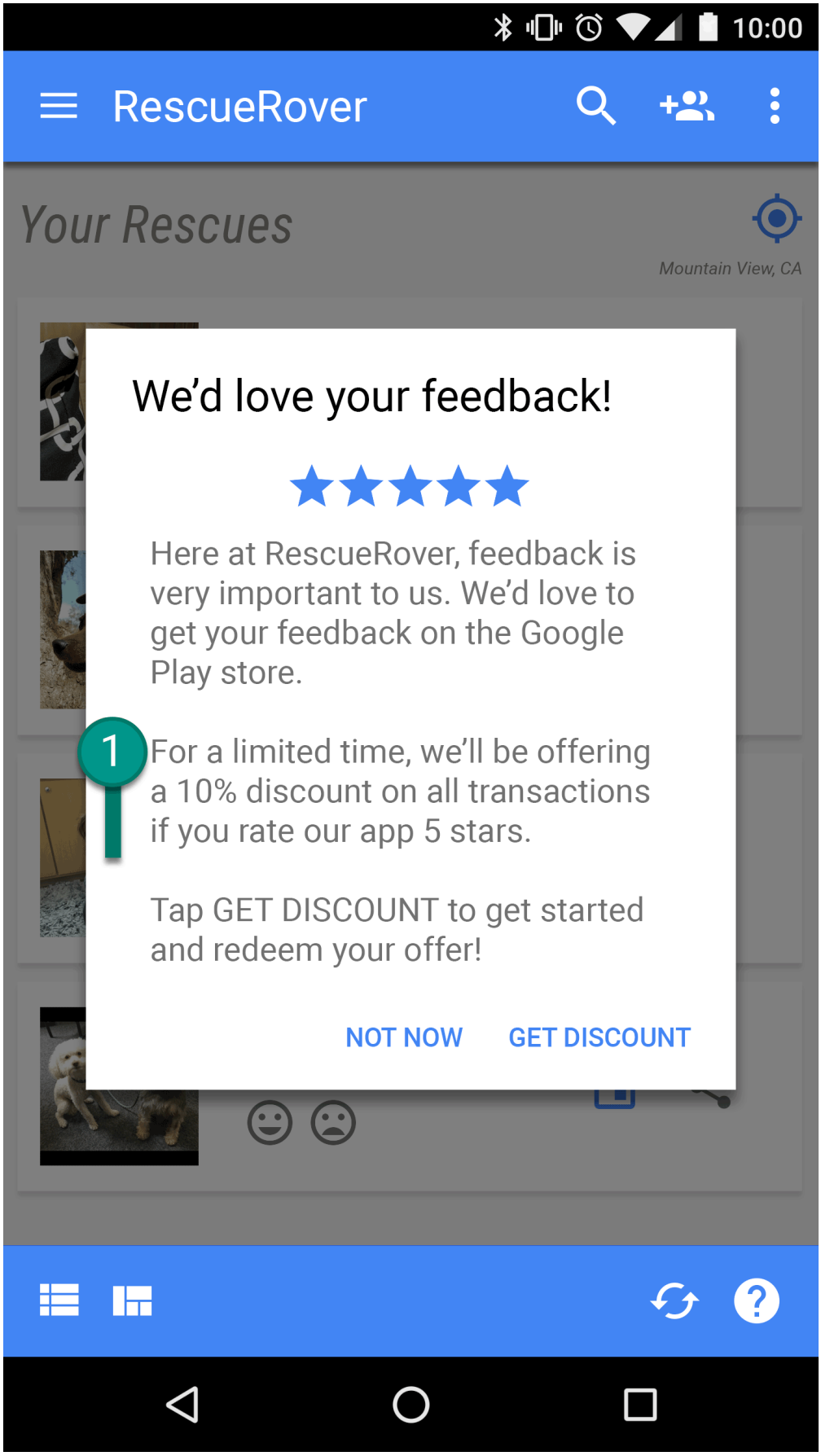
- Highlight what's great about your app. Share interesting and exciting facts about your app to help users understand what makes your app special.
- Make sure that your app’s title and description accurately describe your app’s functionality.
- Avoid using repetitive or unrelated keywords or references.
- 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, 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.

User Ratings, Reviews, and Installs

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:

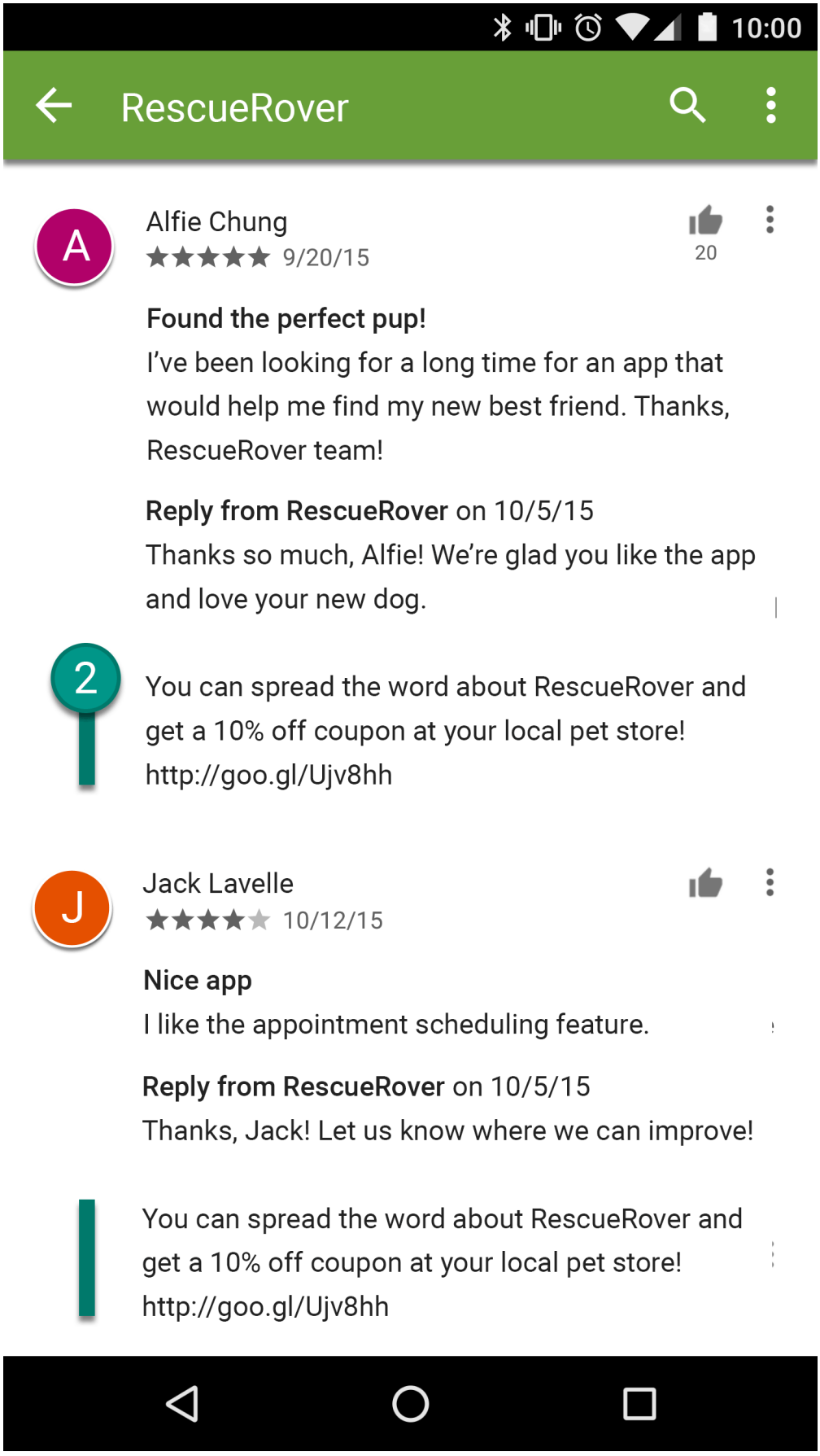
- Asking users to rate your app while offering an incentive:



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.

Content Ratings

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.

Spam and Minimum Functionality

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

Spam

We don’t allow apps that spam users or Google Play, such as apps that send users unsolicited messages or apps that are duplicative and low-quality.

Message Spam

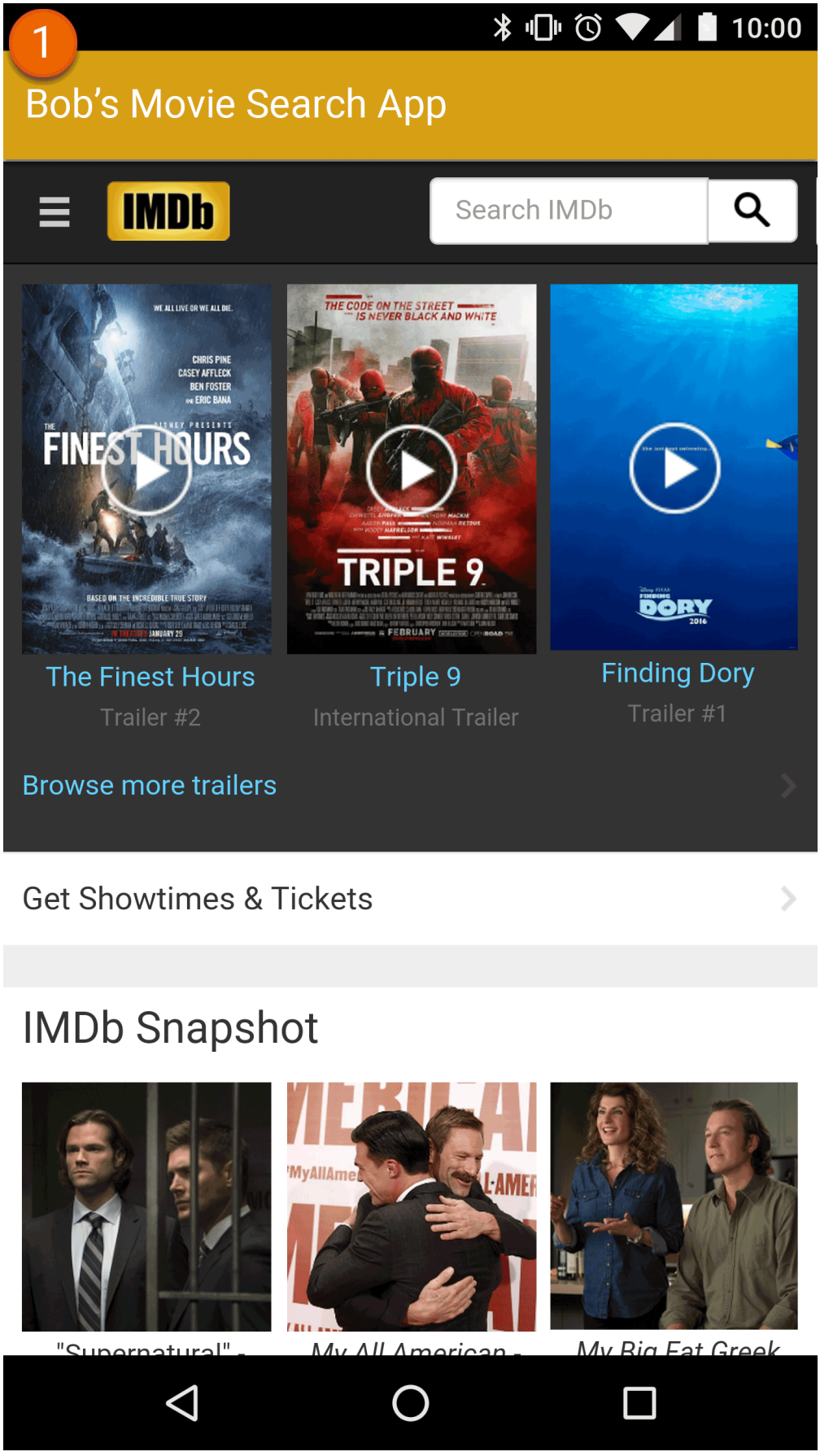
We don’t allow apps that send SMS, email, or other messages on behalf of the user without giving the user the ability to confirm the content and intended recipients.

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:



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

Wizard Spam

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.

Guides

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

Minimum Functionality

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

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**

Other Programs

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

Android Instant Apps

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

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

Payments

Instant app developers must use the Google Payment API for purchases if the developer does not already have the user’s payment information on file. Any new or replacement payment information for a given user must be collected using the Google Payment API.

Developers that have implemented the Google Payment API in their instant app can also offer purely offline payments, like cash on delivery, or store gift cards in their instant app.

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.

Families and COPPA

Google Play offers a rich platform for developers to showcase trusted, high-quality and age appropriate content for the whole family. Before submitting an app to the Designed for Families program, ensure your app is appropriate for children and compliant with COPPA and other relevant laws.

Designed for Families

If you've built great apps designed for kids and/or families - participating in the Designed for Families program on Google Play is a great way to surface your apps to the right users. Read this section to better understand policies and program requirements to take part in the Designed for Families program. For more information on the process of opting into the program, click here.

Before you opt-in, your app must meet all the Designed for Families program requirements, Google Play Developer Program Policies and Developer Distribution Agreement, including the Designed for Families DDA Addendum.

Program Requirements

Eligibility

All apps participating in the Designed for Families program must be relevant for children under the age of 13 and comply with the eligibility criteria below. Google Play reserves the right to reject or remove any app determined to be inappropriate for the Designed for Families program.

Eligibility Criteria

1. Apps must be rated as ESRB Everyone or Everyone 10+, or equivalent.
2. If your Designed for Families app displays ads, you confirm that:
    - You comply with applicable legal obligations relating to advertising to children.
    - Ads displayed to child audiences do not involve interest-based advertising or remarketing.
    - Ads displayed to child audiences present content that is appropriate for children.
    - Ads displayed to child audiences follow the Designed for Families ad format requirements.
3. You must accurately disclose the app's interactive elements on the content rating questionnaire, including:
    - Users can interact or exchange information
    - Shares user-provided personal information with third parties
    - Shares the user's physical location with other users
4. Apps that target child audiences may not use Google Sign-In or any other Google API Service that accesses data associated with a Google Account. This restriction includes Google Play Games Services and any other Google API Service using the OAuth technology for authentication and authorization. Apps that target both children and older audiences (mixed audience), should not require users to sign in to a Google Account, but can offer, for example, Google Sign-In or Google Play Games Services as an optional feature. In these cases, users must be able to access the application in its entirety without signing into a Google Account.
5. If your app targets child audiences and uses the Android Speech API, your app's RecognizerIntent.EXTRA_CALLING_PACKAGE must be set to its PackageName.
6. You must add a link to your app's privacy policy on your app's store listing page.

7. You represent that apps submitted to Designed for Families are compliant with COPPA (Children's Online Privacy Protection Rule) and other relevant statutes, including any APIs that your app uses to provide the service.
8. If your app uses Augmented Reality, you must include a safety warning upon launch of the app that contains 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)
9. Daydream apps are not eligible to participate in the Designed for Families program.

Apps accepted to the Designed for Families program need to stay compliant with the program's eligibility requirements at all times.

Here are some examples of common violations:

- General utility/productivity apps that are not marketed towards a child audience (e.g., calculator, ringtones, flashlight, apps intended for parents).
- Apps that glamorize the use of alcohol or tobacco in a non-educational manner.
- Apps that include simulated gambling.
- Apps that include violent and graphic content not appropriate for children.
- Apps that provide dating services or offer sexual or marital advice.

Age Groups

Primarily Child-Directed Apps

Here are the age groups available for apps primarily directed to children in the Designed for Families program:

- Ages 5 & Under
- Ages 6-8
- Ages 9-12

Apps declared as primarily child-directed may not choose Mixed Audience as an age group.

When you opt-in, select an age group based on your app's primary target audience. If you include an age group in your app's title or description, this is considered your app's primary age target during review.You should only select two age groups if you've designed your app for users in both age groups. Your app's content needs to be appropriate for children in each age group. For example: Apps designed for babies, toddlers, and preschool children should only select “Ages 5 & Under.” If your app is designed for a specific grade level, choose the age range the best represents the grade.

Mixed Audience

If your app is designed for both children under the age of 13 as well as teens or adults, you must select the mixed audience category. Mixed audience apps will display a family star badge that indicates they're family-friendly, without specifying an age group.

If your app is not designed for audiences that include children under the age of 13, it won't be accepted into the Designed for Families program. For example: Calculator apps, maps, wallpapers, recipe books, and games that aren't specifically designed for children shouldn't be opted-in to the program.

Updates to Age

After you've been accepted to the Designed for Families program, if you need to update your app's age group, you can update your information using the Play Console.

We strongly recommend you let your existing users know if you change the target age level of your app or start using ads or in-app purchases using the "What's New" section of your app's store listing page.

Categories

When you opt-in to the Designed for Families program, you can choose a category. Your app will also be available on Google Play in the general app category you select on your app's store listing page.

Here are the categories available for Designed for Families:

Action & Adventure: Action-oriented apps/games, including everything from racing games, fairy tale adventures, and more.

Brain Games: Games that make the user think, including puzzles, matching games, and similar games.

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

Education: Apps and games that are primarily education-focused, including math, science, learning the alphabet, learning to count, geography, history, and other types of educational content.

Music and Video: Apps and games with a musical element or video component, including everything from playing the piano to watching videos and more.

Pretend Play: Apps and games where the user can pretend to take on a role, like pretending to be a cook or a doctor.

Ads & Monetization

All apps participating in the Designed for Families program must comply with the following policy and quality requirements for ads as well as Play's general policy guidelines and practices. This policy applies to any advertising or commercial content (such as paid product placement or offers to make in-app purchases) served to the user for the benefit of a sponsor. Additionally, advertising and commercial content must comply with applicable laws and regulations (including any relevant self-regulatory or industry guidelines).

Ad format requirements

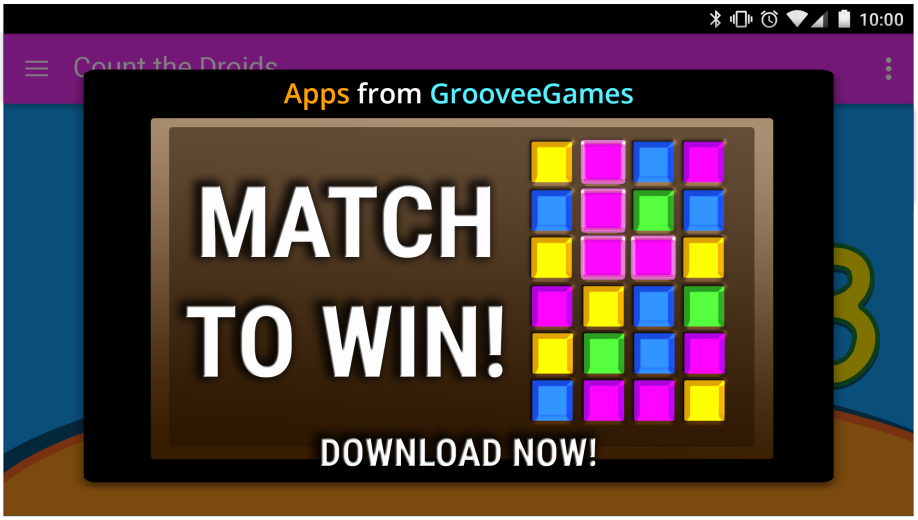
Ads in apps participating in Designed for Families must not have deceptive content or be designed in a way that will result in inadvertent clicks from child users. For example:

- Ad walls must not be used
- Interstitial ads must not display immediately upon app launch
- A maximum of one ad placement per page
- Ads must be clearly distinguishable from app content

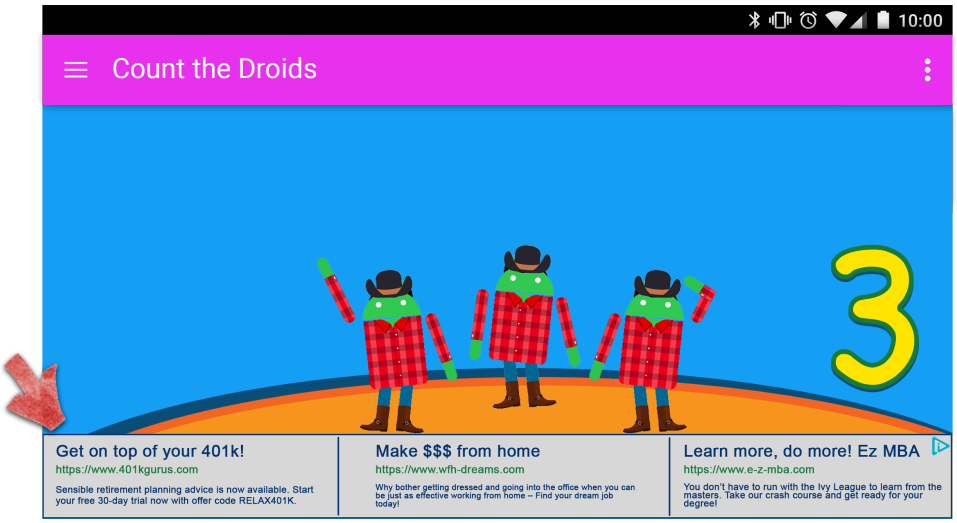
Here are some examples of common violations:

- Ad that moves away from your finger as you try to close it

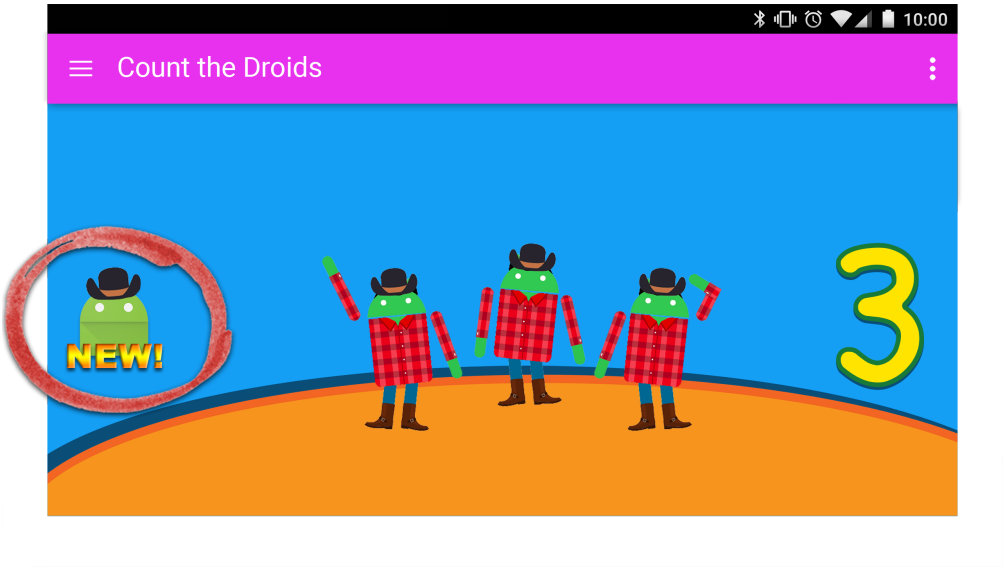
- More than one ad placement per page.
- Ad that takes up the majority or the entire screen without providing the user a clear way to dismiss it, as depicted in the example below:



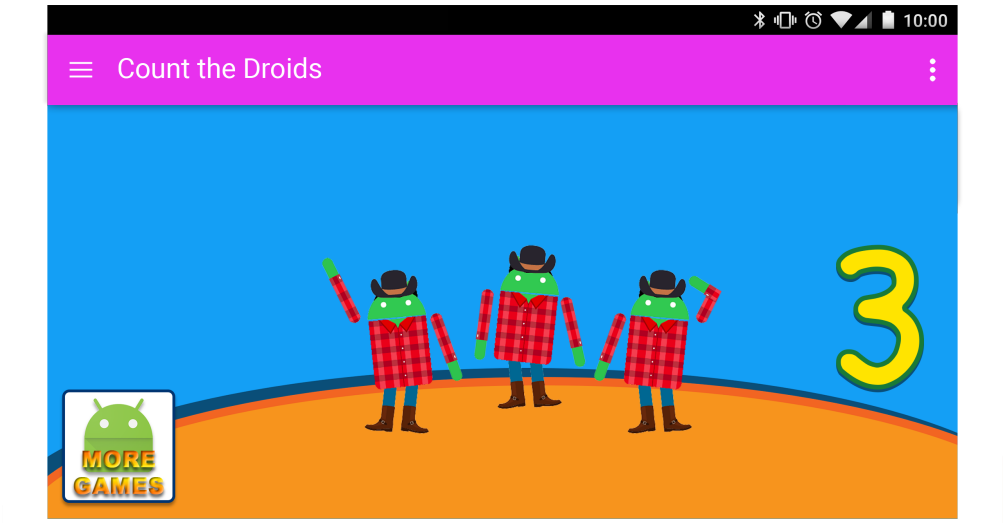
- Banner ad showing multiple offers in one placement:



- Ads that could be mistaken by the user for app content:



Note: Developers are **allowed** to promote their other Play store listings with buttons or ads that are distinguishable from app content:



Ad targeting and data collection

Ads displayed to child audiences must comply with laws relating to advertising to kids. For example, your app must disable interest-based advertising and remarketing, and should comply with child relevant regulations and industry standards for all countries where the app is distributed.

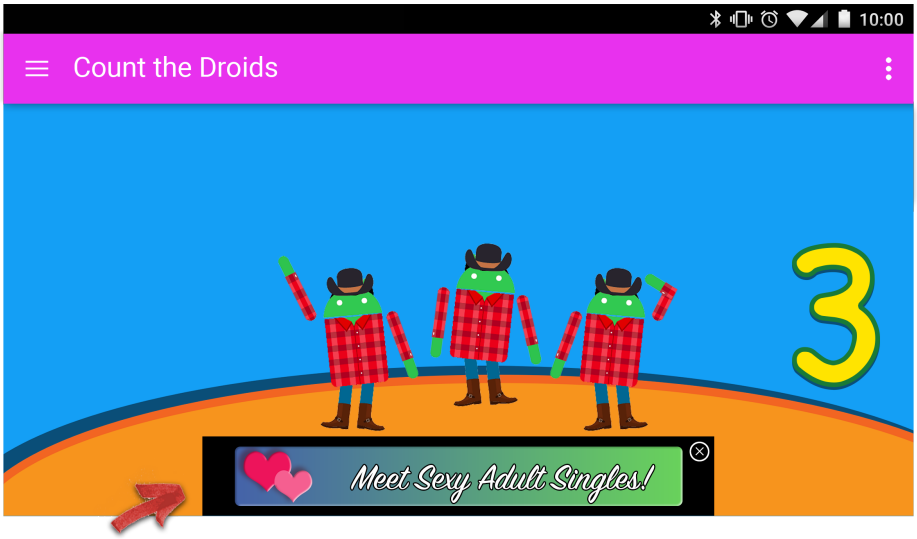
Appropriate ad content

Apps that participate in the Designed for Families program must present ad content that is appropriate for children.

The following are examples of ads not allowed in the Designed for Families program. Please note this is not an exhaustive list.

- **Media Content**: Ads for TV shows, movies, music albums, or any other media outlet not appropriate for children.
- **Video Games & Downloadable Software**: Ads for downloadable software and electronic video games that are not appropriate for children.

- **Controlled or Uncontrolled Substances**: Ads for alcohol, tobacco, controlled or uncontrolled substances.
- **Gambling**: Ads for simulated gambling, contests or sweepstakes promotions, even if free to enter.
- **Adult and Sexually Suggestive Content**: Ads with sexual and mature content.
- **Dating or Relationships**: Ads for dating sites:



- **Violent Content**: Ads with violent and graphic content not appropriate for children.

Ad networks

To find out if your ad network is compliant with Designed for Families ads policies, contact your ad network to ask them about their content policies and advertising practices.

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

It is your responsibility to ensure your app's overall experience with in-app advertising meets the Designed for Families program requirements.

Using ads

Apps and games in the Designed for Families program can have ads as long as they follow the ads policy for Designed for Families. Before opting-in, make sure to review the ads policy to make sure your app comply with all requirements.

In-app purchases & other commercial content

There are no specific restrictions relating to in-app purchases (IAP) in apps participating in the Designed for Families program.

Google Play reserves the right to reject apps for overly aggressive commercial tactics. Google Play will enforce IAP password protection on all apps participating in the Designed for Families program that primarily target child audiences to ensure that parents, not children, are approving purchases.

Note: *This treatment does not extend to apps targeting mixed audiences.*

Authentication

As stated in the Eligibility Requirements, apps that target primarily child audiences should not use Google Sign-In or any other Google API Service that accesses data associated with a Google Account.

Apps that target both children and older audiences (mixed audience), shouldn't require users to sign in to a Google Account, but can use, for example, Google sign-in or Google Play Games Services as an optional feature. In these cases, users must be able to access the app or game in its entirety without signing into a Google Account.

Google Play for Education users

If your app is part of the Google Play for Education program and uses Google Sign-In or any other Google API Service that accesses data associated with a Google Account so that students can use their school accounts with your app, your app can use these services as long as it isn't a blocking requirement for all app users.

Google Play Games Services

If your app appeals to a mixed audience, and you wish to provide a sign-in option in your game, follow section 1.1.2 of this checklist**.**

COPPA Compliance and Child-Directed Apps

Understanding the nuances of integrating Google services and being COPPA compliant is important when distributing child-directed apps. The Children's Online Privacy Protection Act, or COPPA, applies to websites, apps, and services directed to children under the age of 13 and general audience apps, websites, or services with users known to be under the age of 13.

About child-directed apps

If your app is child-directed, you'll find information about integrating Google services below. There are two types of child-directed apps:

- Apps that are directed primarily to children
- Apps that have a mixed audience (meaning they don't target children as their primary audience)

You can find more information about the differences between mixed audience apps and apps directed primarily to children on the FTC's website.

Note: While child-directed apps may use some Google services, developers are responsible for using these services according to their obligations under the law. Please review the FTC's guidance on COPPA and consult with your own legal counsel.

Primarily Child-Directed Declaration

You must declare in the Play Console whether your app is primarily directed to children under the age of 13 as defined by COPPA. Apps that are primarily child-directed must opt-in to the Designed for Families program.

How to integrate with Google services

Select a Google service below to learn how to integrate it in child-directed apps.

Google Mobile Ads

If you're using Google's mobile advertising services, you must indicate that you want Google to treat ad requests from your app as child-directed, as applicable.

If you tag the ad requests from your app for child-directed treatment, we will take steps to disable interest-based advertising and remarketing ads for such requests.

To learn how to correctly set up your ads, visit the following resources:

- Tag an ad request from an app for child-directed treatment
- Targeting: child-directed setting

Google sign-in or Google Play Games Services

If your app is directed primarily to children, it should not use Google sign-in or Google Play Game Services.

Apps that are mixed audience shouldn't require Google sign-in or Google Play Game Services but can offer these as optional features. In these cases, users must be able to access the app or game in its entirety without signing into Google or Google Play Game Services.

If your app appeals to a mixed audience and you use Google Play Games Services, follow section 1.1 of this checklist.

Android Speech API

Child-directed apps shouldn't use the Android Speech API if they don't participate in the Designed for Families program. Apps in the Designed for Families program should follow these instructions when using the Android Speech API:

RecognizerIntent.EXTRA_CALLING_PACKAGE must be set to its PackageName.

Related content

If you've built great apps designed for kids and/or families, consider participating in the Designed for Families program on Google Play to surface your app to parents.

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