# Google play policy

**1.Child Endangerment**

Apps that include content that sexualizes minors are subject to immediate removal from the Store. Apps that appeal to children but contain adult themes are not allowed. If we become aware of content with child sexual abuse imagery, we will report it to the appropriate authorities and delete the Google Accounts of those involved with the distribution.

**2.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.

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.

**3.Hate Speech**

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

**4.Violence**

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

Here are some examples of common violations:

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

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

Terrorist Content

We do not permit terrorist organizations to publish apps on Google Play for any purpose, including recruitment. We don't allow apps with content related to terrorism, such as content that promotes terrorist acts, incites violence, or celebrates terrorist attacks. If posting content related to terrorism for an educational, documentary, scientific, or artistic purpose, be mindful to provide enough information so users understand the context.

**5.Sensitive Events**

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

Here are examples of common violations:

Lacking sensitivity regarding the death of a real person or group of people due to suicide, overdose, natural causes, etc.

Denying a major tragic event.

Appearing to profit from a tragic event with no discernible benefit to the victims.

**6.Bullying and Harassment**

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

Here are examples of common violations:

Bullying victims of international or religious conflicts.

Content that seeks to exploit others, including extortion, blackmail, etc.

Posting content in order to humiliate someone publicly.

Harassing victims, or their friends and families, of a tragic even

**7.Dangerous Products**

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

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

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

**8.Binary Options**

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

**9.Cryptocurrencies**

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

**10.Gambling Apps**

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

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

Developer must successfully complete the application process in order to distribute the app on Play;

App must comply with all applicable laws and industry standards for any country in which it is distributed;

Developer must have a valid gambling license for each country in which the app is distributed;

App must prevent under-age users from gambling in the app;

App must prevent use from countries not covered by the developer-provided gambling license;

App must NOT be purchasable as a paid app on Google Play, nor use Google Play In-app Billing;

App must be free to download and install from the Store;

App must be rated AO (Adult Only) or IARC equivalent; and

App and its app listing must clearly display information about responsible gambling.

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

**11.Gambling Ads within Play-distributed Apps**

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

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

Ad must meet local licensing requirements for all gambling-related products and services being promoted;

App must not display a gambling ad to individuals known to be under the age of 18;

App must not be enrolled in the Designed for Families program;

App must not target individuals under the age of 18;

Ad must clearly display information about responsible gambling on the landing page, the advertised app listing itself or within the app; and

App that is advertising a gambling ad must not be a simulated gambling app (an entertainment game without real money gambling).

**12.Daily Fantasy Sports (DFS) Apps**

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

App must only allow access and be distributed in the United States; DFS apps targeting jurisdictions outside the US must establish eligibility through the Real Money Gambling Apps process;

Developer must successfully complete the DFS application process and be accepted in order to distribute the app on Play;

App must comply with all applicable laws and industry standards for any US state or US territory in which it is distributed;

Developer must have a valid license for each US state or US territory in which a license is required for daily fantasy sports apps;

App must prevent under-age users from wagering or conducting monetary transactions within the app;

App must prevent use from US States or US territories in which the developer does not hold a license required for daily fantasy sports apps;

App must prevent use from US States or US territories where daily fantasy sports apps are not legal;

App must NOT be purchasable as a paid app on Google Play, nor use Google Play In-app Billing;

App must be free to download and install from the Store;

App must be rated AO (Adult Only) or IARC equivalent; and

App and its app listing must clearly display information about responsible gambling.

**13.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.

**14.User Generated Content**

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

Apps that contain or feature UGC must:

require that users accept the app's terms of use and/or user policy before users can create or upload UGC;

define, in a manner consistent with the spirit of Google Play's Developer Program Policies, UGC that is objectionable, and prohibit that UGC via the app’s terms of use and/or user policy;

implement robust, effective and ongoing UGC moderation, as is reasonable and consistent with the type(s) of UGC hosted by the app;

provide a user-friendly, in-app system for reporting and removal of objectionable UGC;

In the case of live-streaming apps, problematic UGC must be removed in as close to real-time as reasonably possible; and remove or block abusive users who violate the app's terms of use and/or user policy.

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

Here are some examples of common violations:

Promoting sexually explicit user-generated content.

Apps with user generated content (UGC) that lack sufficient safeguards against threats, harassment, or bullying, particularly toward minors.

Posts, comments, or photos within an app that are primarily intended to harass or single out another person for abuse, malicious attack, or ridicule.

Apps that continually fail to address user complaints about objectionable content.

**15.Unapproved Substances**

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

All items on this non-exhaustive list of prohibited pharmaceuticals and supplements

Products that contain ephedra

Products containing human chorionic gonadotropin (hCG) in relation to weight loss or weight control, or when promoted in conjunction with anabolic steroids

Herbal and dietary supplements with active pharmaceutical or dangerous ingredients

False or misleading health claims, including claims implying that a product is as effective as prescription drugs or controlled substances

Non-government approved products that are marketed in a way that implies that they're safe or effective for use in preventing, curing, or treating a particular disease or ailment

Products that have been subject to any government or regulatory action or warning

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

## 16.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.

Developers that falsely suggest an affiliation with another entity:

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.

## 17.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.

**18.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:

**19.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.

**20.Personal and Sensitive Information**

Personal and sensitive user data includes, but isn't limited to, personally identifiable information, financial and payment information, authentication information, phonebook, contacts SMS and call related data, microphone and camera sensor data, and sensitive device or usage data. If your app handles sensitive user data, then you must:

Limit your collection and use of this data to purposes directly related to providing and improving the features of the app (e.g. user anticipated functionality that is documented and promoted in the app's description).

Post a privacy policy in both the designated field in the Play Console and within the app itself. The privacy policy must, together with any in-app disclosures, comprehensively disclose how your app collects, uses, and shares user data. Your privacy policy must disclose the type of parties to which any personal or sensitive user data is shared.

Handle all personal or sensitive user data securely, including transmitting it using modern cryptography (for example, over HTTPS).

Prominent Disclosure Requirement

In cases where users may not expect that their personal or sensitive user data will be required to provide or improve the features of your app, you must meet the following requirements:

Your app must provide an in-app disclosure of your data collection and use. The 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 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 in-app disclosure must include a request for user consent. The 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 accesses a user's inventory of installed apps and doesn't treat this data as personal or sensitive data subject to the Privacy Policy, Secure Transmission, and Prominent Disclosure requirements.

An app that accesses a user's phone or contact book data and doesn't treat this data as personal or sensitive data subject to the Privacy Policy, Secure Transmission, and Prominent Disclosure requirements.

Specific Restrictions for Sensitive Data Access

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

21.Activity Requirement

Your app handles financial or payment information or government identification numbers Your app must never publicly disclose any personal or sensitive user data related to financial or payment activities or any government identification numbers.

Your app handles non-public phonebook or contact information  We don't allow unauthorized publishing or disclosure of people's non-public contacts.

Your app contains anti-virus or security functionality, such as anti-virus, anti-malware, or security-related features  Your app must post a privacy policy that, together with any in-app disclosures, explain what user data your app collects and transmits, how it's used, and the type of parties with whom it's shared.

## 22.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.

Permissions

Permission requests should make sense to users. You may only request permissions that are necessary to implement critical current features or services in your application. You may not use permissions that give access to user or device data for undisclosed, unimplemented, or dsallowed features or purposes.

Request permissions access to data in context (via incremental auth), so that users understand why you need the permission or data. Use the data only for purposes that the user has consented to. If you later wish to use the data for other purposes, you must ask users and make sure they affirmatively agree to the additional uses.

Additional requirements for the use of specific permissions:

**23.Activity Requirement**

Your app manifest requests the Call Log permission group (e.g. READ_CALL_LOG, WRITE_CALL_LOG, PROCESS_OUTGOING_CALLS) It must be actively registered as the default Phone or Assistant handler on the device.

Your app manifest requests the SMS permission group (e.g. READ_SMS, SEND_SMS, WRITE_SMS, RECEIVE_SMS, RECEIVE_WAP_PUSH, RECEIVE_MMS) It must be actively registered as the default SMS or Assistant handler on the device.

The following restrictions also apply to the above permissions:

Apps lacking default SMS, Phone, or Assistant handler capability may not declare use of the above permissions in the manifest. This includes placeholder text in the manifest.

Apps must be actively registered as the default SMS, Phone, or Assistant handler before prompting users to accept any of the above permissions and must immediately stop the use of the permission when it's no longer the default handler.

Apps may only use the permission (and any data derived from the permission) to provide approved critical core app functionality (e.g. critical current features of the app that are documented and promoted in the app's description). You may never sell this data. The transfer, sharing, or licensed use of this data must only be for providing critical core features or services within the app, and its use may not be extended for any other purpose (e.g. improving other apps or services, advertising, or marketing purposes). You may not use alternative methods (including other permissions, APIs, or third-party sources) to derive data attributed to the above permissions.

24.Exceptions to Call Log and SMS Default Handler restrictions

The objective of the above restrictions is to protect user privacy. We may grant limited exceptions to the default handler requirement in cases when an app is not the default handler, but abides by all of the above requirements and clearly and transparently provides a highly compelling or critical feature where there is currently no alternative method to provide the feature. Such features will be evaluated against any potential privacy or security impact on users. These exceptions are rare and will not be extended to all developers. Please see this Help Center page for more information.

## 25.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.

## 26.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).

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

The following are explicitly prohibited:

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

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

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

Apps that introduce or exploit security vulnerabilities.

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

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

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

Apps 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.

**27.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.

**28.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.

**29.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.

**30.Enabling Dishonest Behavior**

We don't allow apps that help users to mislead others, including, but not limited to, apps that generate or facilitate the generation of ID cards, social security numbers, passports, diplomas, credit cards and driver's licenses.

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

**31.Misrepresentation**

We do not allow apps or developer accounts that impersonate any person or organization, or that misrepresent or conceal their ownership or primary purpose. We do not allow apps or developer accounts that engage in coordinated activity to mislead users. This includes, but isn’t limited to, apps or developer accounts that misrepresent or conceal their country of origin and that direct content at users in another country.

**32.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.

**33.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.

**34.Deceptive Ads**

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

Here are some examples of common violations:

Ads that mimic an app's UI:

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

Ads that mimic a system notification:

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

**35.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.

**36.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.

**37.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.

**38.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.

**39.Usage of Android Advertising ID**

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

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

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

Respecting users' selections. If reset, a new advertising identifier must not be connected to a previous advertising identifier or data derived from a previous advertising identifier without the explicit consent of the user. Also, you must abide by a user’s “Opt out of Interest-based Advertising” or “Opt out of Ads Personalization” setting. If a user has enabled this setting, you may not use the advertising identifier for creating user profiles for advertising purposes or for targeting users with personalized advertising. Allowed activities include contextual advertising, frequency capping, conversion tracking, reporting and security and fraud detection.

Transparency to users. The collection and use of the advertising identifier and commitment to these terms must be disclosed to users in a legally adequate privacy notification. To learn more about our privacy standards, please review our User Data policy.

Abiding by the terms of use. The advertising identifier may only be used in accordance with these terms, including by any party that you may share it with in the course of your business. All apps uploaded or published to Google Play must use the advertising ID (when available on a device) in lieu of any other device identifiers for any advertising purposes.

## 40.Usage of Android Advertising ID

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

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

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

Respecting users' selections. If reset, a new advertising identifier must not be connected to a previous advertising identifier or data derived from a previous advertising identifier without the explicit consent of the user. Also, you must abide by a user’s “Opt out of Interest-based Advertising” or “Opt out of Ads Personalization” setting. If a user has enabled this setting, you may not use the advertising identifier for creating user profiles for advertising purposes or for targeting users with personalized advertising. Allowed activities include contextual advertising, frequency capping, conversion tracking, reporting and security and fraud detection.

Transparency to users. The collection and use of the advertising identifier and commitment to these terms must be disclosed to users in a legally adequate privacy notification. To learn more about our privacy standards, please review our User Data policy.

Abiding by the terms of use. The advertising identifier may only be used in accordance with these terms, including by any party that you may share it with in the course of your business. All apps uploaded or published to Google Play must use the advertising ID (when available on a device) in lieu of any other device identifiers for any advertising purposes.

## 41.Metadata

We don't allow apps with misleading, irrelevant, excessive, or inappropriate metadata, including but not limited to the app's description, developer name, 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.

**42.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.

**43.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.

**44.Spam**

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

Message Spam

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

Webviews and Affiliate Spam

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

Here are some examples of common violations:

An app whose primary purpose is to drive referral traffic to a website to receive credit for user sign-ups or purchases on that website.

Apps whose primary purpose is to provide a webview of a website without permission:

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

Repetitive Content

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

Here are some examples of common violations:

Copying content from other apps without adding any original content or value.

Creating multiple apps with highly similar content and user experience. If these apps are each small in content volume, developers should consider creating a single app that aggregates all the content.

Apps that are created by an automated tool, wizard service, or based on templates and submitted to Google Play by the operator of that service on behalf of other persons are not allowed. Such apps are only permissible if they are published by an individually registered developer account belonging to the user of the automated tool, not the operator of the service.

Made for Ads

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

Here are some examples of common violations:

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

**45.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

**46.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.

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.

## 47.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. App content must be appropriate for children. Google Play reserves the right to reject or remove any app determined to be inappropriate for the Designed for Families program.

Eligibility Criteria

Apps must be rated as ESRB Everyone or Everyone 10+, or equivalent.

If your Designed for Families app displays ads, you confirm that:

2.1 You comply with applicable legal obligations relating to advertising to children.

2.2 Ads displayed to child audiences do not involve interest-based advertising or remarketing.

2.3 Ads displayed to child audiences present content that is appropriate for children.

2.4 Ads displayed to child audiences follow the Designed for Families ad format requirements.

You must accurately disclose the app's interactive elements on the content rating questionnaire, including:

3.1 Users can interact or exchange information

3.2 Shares user-provided personal information with third parties

3.3 Shares the user's physical location with other users

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.

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.

You must add a link to your app's privacy policy on your app's store listing page.

You represent that apps submitted to Designed for Families are compliant with COPPA (Children's Online Privacy Protection Rule), the EU General Data Protection Regulation 2016/679, and other relevant statutes, including any APIs that your app uses to provide the service.

If your app uses Augmented Reality, you must include a safety warning upon launch of the app that contains the following:

8.1 An appropriate message about the importance of parental supervision

8.2 A reminder to be aware of physical hazards in the real world (e.g., be aware of your surroundings)

Daydream apps are not eligible to participate in the Designed for Families program.

All user-generated content (UGC) apps must be proactively moderated.

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 violence, gore, or shocking content not appropriate for children.

Apps that provide dating services or offer sexual or marital advice.

Age Groups

Misrepresentation of your app’s age group may result in removal or suspension, so it is important to provide accurate declaration.

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 declare, 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.

48.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.

## 49.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. Misrepresentation of your app may result in removal or suspension, so it is important to provide accurate declaration.

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:

**50.Policy Coverage**

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

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

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

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

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

**51.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.

**52.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.

# 360

1、软件中包含反动、色情、暴力信息等违反国家相关法律法规规定的软件。
2、病毒木马类软件。
3、恶意捆绑、静默推广其他软件；释放与软件无关的文件、快捷方式等风险推广行为软件。
4、静默，误导或强制添加开机启动项、修改首页、修改默认搜索项等静默或强制修改行为。
5、恶意弹窗、弹广告行为软件。
6、刷流量骗点，劫持搜索类软件。
7、软件无法或无入口退出，退出后恶意残留进程/服务的行为。
8、难以卸载、恶意卸载；误导或欺骗用户卸载其他软件的行为。
9、私服外挂类、风险辅助类软件。
10、恶意监控、恶意群发、盗取用户隐私信息、恶意收集用户信息行为软件。
11、侵犯用户隐私（涉及输入第三方软件密码）或网银信息等风险行为软件。
12、误导，欺骗用户行为的软件。
13、上传与注册信息不相符，非注册公司研发的软件；涉嫌侵害他人知识产权，商业秘密等合法权利的软件。
14、其他在软件安装，使用和卸载中侵害用户知情权，选择权的恶意行为软件。

| 软件行为 | 软件检测明细参照 |
|---|---|
| **软件安装行为** | 1、软件安装界面必须有“取消”和“关闭按钮”，用户点击后可立即退出安装。<br>2、安装无读取参数（或其他方式）进行静默推广、静默添加开机启动、静默修改首页等行为。<br>3、软件安装界面上需要用户点击的按钮和勾选项有明确显示，推广选项需明确写出推广软件的名称，不允许玩“文字游戏”诱导用户点击。<br>4、软件安装推广不得隐藏和本软件无关的推广软件，推广软件不能过多。 |
| **静默安装行为** | 1、不允许添加开机启动、修改首页等设置。<br>2、必须在桌面释放软件的快捷方式，且在”开始菜单”，“控制面板”中有软件的正规卸载项。<br>3、只允许安装软件产品本身；不允许释放与本产品无关的文件，比如推广模块，广告模块，病毒木马等<br>4、PC 监控类软件不允许静默安装。 |
| **软件退出行为** | 1、软件主程序退出后，其他子进程必须随之退出。<br>2、如软件功能需要有残留进程，必须将残留进程的功能明确告知用户，并由用户主动选择是否允许子进程残留后台。<br>3、残留的子进程不允许在用户机器上进行：侵犯用户隐私，修改浏览器设置、软件更新、弹广告窗、下载或运行其他程序行为。 |
| **软件弹窗行为** | 1、弹出窗体有关闭按钮。<br>2、不允许高频率恶意弹窗，不允许存在文字误导或诱导客户点击行为。 |

| | |
|---|---|
| | 3、软件弹出的所有广告窗体和资讯窗必须在窗体上明确标出软件名称。 |
| **软件卸载行为** | 1、软件必须提供正常的卸载项（开始菜单和控制面板中）。<br>2、用户选择卸载后，必须完全删除软件释放的所有文件，且不允许在对用户机器进行与卸载不相关的动作 |

# 华为

1.1 兼容性要求

第三方应用必须通过在华为终端设备的兼容性要求，若应用未告知兼容性是否达标或出现以下不兼容情况，会在应用下载安装过程中向用户进行风险提示、用户免责声明和华为应用市场已检测版本安装提醒：

1.1.1 应用频繁出现崩溃。

1.1.2 应用无法正常安装、启动、卸载。

1.2 性能要求

1.2.1 应用在冷启动的时候未考虑用户操作的响应速度，若加载时间超过 1000 毫秒，且在屏幕上未向用户提供反馈（进度指示器或类似提示），则不满足性能要求。

1.2.2 应用在进行页面或功能切换的时候未考虑用户操作的响应速度, 若加载时间超过 500 毫秒，则不满足性能要求。

1.2.3 应用未满足良好用户体验，出现使用不流畅等现象。

1.2.4 应用在运行时未充分考虑 CPU 占用是否过高或者异常，导致终端出现卡顿、ANR 现象。

1.2.5 应用在运行时为充分考虑内存占用是否过高或者异常，导致终端出现卡顿、ANR 现象。

1.3 功耗要求

1.3.1 应用转入后台时，有服务处于运行状态（该服务与应用核心功能相关且必要的除外)。

1.3.2 应用转入后台时，未主动释放占用资源。

1.3.3 应用转入后台后，私自启动。

1.3.4 应用转入后台时，有持锁行为。

1.3.5 应用转入后台时，占用系统资源（例如，蓝牙，GPS 等)。

1.4 安全要求

1.4.1 应用含有病毒木马等侵害用户的功能（包括代码等可疑行为)，并限制下载或安装。

1.4.2 应用含有恶意吸费行为，包括但不限于：未经用户二次确认（即用户需要对购买和支付分别进行一次确认）主动扣费、隐形扣费行为，未明确、明显提示用户（例如收费协议嵌套在应用引导页内)，以误导方式实现用户付费等。

1.4.3 除支持核心功能而需要的最低级别权限外，应用擅自申请其他无关的权限。

1.4.4 应用请求访问与核心功能不相关的敏感数据（例如通讯录或系统日志）或访问用户付费服务（例如：拨号器、短信或频繁自动联网）的权限。

1.4.5 应用影响手机功能，包括但不限于：安装后自动修改系统默认配置且用户无法修改，功能键失灵等。

1.4.6 应用的签名与华为应用市场货架上检测过的同包名应用不一致。

1.4.7 同名应用因含有的支付、推送等SDK不同，或被第三方加固、重新打包或添加渠道号等差异化处理后，未在华为应用市场进行过安全检测。

2. 第三方移动智能终端应用软件下载渠道的质量检测与安全审查标准

2.1 隐私保护

2.1.1 具有明确的规定用户个人信息收集和使用的目的、方式和范围的规章制度。

2.1.2 具有完善的用户个人信息保护制度和用户数据监控与风险上报机制。

2.2.3 用户个人信息三方传递保密与评估制度。

# 联想

应用本身不得出现以下行为，否则将无法通过审核：

1.1.2.1 应用功能与简介描述不一致；

1.1.2.2 应用存在功能问题，基本功能不可用，不能解决用户某方面的需求；

1.1.2.3 应用无法正常安装或安装时提示解析失败；

1.1.2.4 应用无法正常卸载或卸载报错；

1.1.2.5 应用要求登录，但没有提供注册入口；

1.1.2.6 应用在大部分机型上启动时崩溃；

1.1.2.7 应用在大部分机型上运行时崩溃；

1.1.2.8 应用中内容无法正常显示或无法获取；

1.1.2.10 应用存在病毒；

1.1.2.11 应用存在恶意扣费行为（包括但不限于：未经用户二次确认主动、隐形扣费行为）；

1.1.2.12 应用升级时，升级为毫无关联的其他应用或游戏；

1.1.2.13 应用需要下载其他应用才能运行；

1.1.3 应用内容

应用不得包含或涉及以下内容，否则将无法通过审核：

1.1.3.3 过于令人反感、低俗或激怒用户的内容；

1.1.3.4 存在非法金钱交易或内容；

1.1.3.5 存在虚假、欺诈行为。

1.1.4 广告、推送

应用中的广告和推送不得出现以下行为，否则应用将无法通过审核：

1.1.4.1 应用存在强制积分墙，在启动、使用时强制要求下载积分墙里面的其他应用，否则不能继续使用；

1.1.4.2 应用迫使用户必须下载积分墙广告内容方能使用程序的主要功能；

1.1.4.3 故意造成用户误点，以下载积分墙广告的内容等；

1.1.4.4 通知栏广告有匿名push广告，有无法关闭的常驻通知栏，推送与应用自身无关的内容；

1.1.4.5 桌面悬浮窗广告在应用使用过程中频繁弹出，中断用户操作，影响用户体验；

1.1.4.6 悬浮窗广告、弹窗广告、侧边栏广告不可关闭，影响应用正常使用；

1.1.4.7 插屏广告退出应用后，在应用外或桌面显示，干扰其他应用以及其中的广告；

1.1.4.8 插屏广告超过屏幕50%；

1.1.4.9 应用广告banner上有3个及以上的应用推荐；

1.1.4.10 应用在使用的过程中弹出广告，强制要求点击广告，否则不能正常使用；
1.1.4.11 在用户不知情或不通知用户的情况下，在后台进行任何与用户所使用的功能无关的操作，例如下载第三方应用、发短信等；
1.1.4.12 广告和推送干扰第三方应用以及其中的广告；
1.1.4.13 广告中包含不良或违法信息。

# OPPO

1.1 不应存在严重 Bug（如无法添加和打开、无法返回和退出、卡顿严重等），不能造成客户端崩溃或程序本身崩溃。
1.2 快应用运行中不能出现频繁唤醒、内存 CPU 占用过高等功耗异常的行为，不能出现内存泄露。
1.3 若快应用中存在帐号关系或付费内容，需提供测试号，包含帐号和密码，保证审核者可以体验所有功能。
1.4 快应用内每个功能都能正常实现，包括：账号登录注册、支付充值、播放暂停等。
2 不能模仿系统通知或警告诱导用户点击。
3 快应用界面内应提供功能正常且易于发现的“退出”按钮选项；进入程序后点击 back 键可实现返回或退出功能。
4 在数据网络下，使用大量流量需要在用户主动确认的情况下才能继续进行。
5 不能出现主要功能为营销或广告用途，传播骚扰信息、恶意营销和垃圾信息等。
二、安全广告

---

未经用户同意，不能非法收集或窃取用户密码或其他个人数据；在采集或使用用户数据之前，必须确保经过用户同意，并向用户如实披露数据用途、使用范围等相关信息。
快应用内任一模块所需权限都必须取得用户同意才能进行，如：不能在用户不知情的情况下，使用录音功能。
不能要求用户降低手机操作系统安全性（如 ROOT 等）后才能使用相关功能。
不能对其他软件或硬件系统模块进行恶意干扰、修改、屏蔽的行为（如不能使用音量键加减等）。
执行支付动作前，必须要有二次确认，即在页面中对用户有明确的提示。
提交的快应用不能出现木马病毒或潜在危险（包括代码等可疑行为）的行为。
广告弹出场景、频率、内容不能影响应用正常使用，且在广告界面中需提供去除选项。

# VIVO

**1、应用功能**

**1.1、应用无法正常运行或功能存在问题**

1.1.1、应用无法正常安装或安装时提示解析失败；

1.1.2、应用无法正常卸载；

1.1.3、应用在启动时容易崩溃；

1.1.4、应用在运行时容易崩溃；

1.1.5、应用分辨率无法适配 vivo 手机；

1.1.6、如应用必须注册账号才能使用，应用审核时尝试 3 次都无法成功注册；

1.1.7、如应用必须登录账号才能使用，应用审核时尝试 3 次都无法成功登录；

1.1.8、如应用必须登录账号才能使用，但应用内不提供注册通道；

1.1.9、应用中内容无法正常显示或无法获取；

1.1.10、应用内按钮点击无反应或点击报错；

1.1.11、应用内 Tab 无法切换或切换报错；

1.1.12、应用修改系统默认设置后用户无法更改这些设置；

1.1.13、应用功能需要依赖于第三方应用才能实现；

1.1.14、APP 内容非完整内容或需要用户跳转其他 APP 或网址获取内容；

1.1.15、APP 是简单的网站页面打包或套用模板，或者内容没有持续更新的 APP；

1.1.16、APP 打开立即会提示用户进行更新；

**2.1、申请危险权限或者权限给用户造成干扰**

2.1.1、应用申请的权限和其实际功能不符，如计算器申请通讯录权限；

2.1.2、不能通过通知栏信息判定所弹出信息的归属应用；

2.1.3、应用实际功能不需常驻通知栏却常驻通知栏；

2.1.4、应用未经用户许可或无法关闭常驻通知栏；

2.1.5、应用实际功能不需开机启动却开机启动；

2.1.6、应用在安装或者运行前，提示用户重启手机或强制重启手机；

2.1.7、应用未提示用户或未经用户授权情况下，搜集、传输或者使用用户的隐私数据，如位置信息、通讯录、照片、短信记录、密码、生日等；

**2.2、应用存在恶意行为**

2.2.1、应用存在病毒；

2.2.2、应用存在吸费行为(如：未经用户二次确认主动扣费)；

2.2.3、应用消耗过多的网络流量；

2.2.4、应用未启动、未在后台运行或已结束进程，但是仍会启动 GPS、蓝牙等系统功能；

2.2.5、应用允许匿名或未经用户许可拨打电话或发送信息（短信、彩信、语音、文件或视频等)；

2.2.6、应用允许修改去电号码且主要功能用于欺骗接电用户；

**3、应用展示信息**

**3.1、平台专有性**

3.1.1、应用运行闪屏界面或者应用描述中包含其他应用市场的图标、水印、文字等；

3.1.2、应用截图中存在其他应用市场图标、水印、文字等；

3.1.3、应用截图中使用非 Android 系统设备；

3.1.4、应用截图中存在其他手机品牌标志、名称、商标等；

3.1.5、vivo 应用商店暂时不收录应用市场属性（主体功能为下载、更新和搜索应用等功能）的应用；

3.1.6、应用运行时会弹窗或主动推送下载第三方应用市场；

3.1.7、应用介绍或更新内容中包含其他第三方市场名称、介绍、引述等内容；

**3.2、应用展示内容存在问题**

3.2.1、应用名称过长：手机端应用显示名称+描述语不能超过 8 个汉字字符或 16 个英文字符；

3.2.2、应用名称或者应用描述存在特殊符号；行文不规范（如标点不正确，大量空格和换行）或者低于 50 字内容描述；

3.2.3、应用描述中没有简体中文介绍；

3.2.4、vivo 应用商店已存在和您提交的应用名称相同的应用，为了避免用户使用中的迷惑以及可能对其他应用商标或版权的侵犯，建议修改您应用的名称；

3.2.5、vivo 应用商店里提交应用名称和设备中显示的名称差异较大；

3.2.6、应用名称包含非法内容（如色情、反动、人身攻击等)；

3.2.7、应用名称、内容、图标等应用信息存在侵权行为（侵犯商标、版权或著作权等）；

3.2.8、应用的分类、描述、名称与应用的实际内容或功能不符；

3.2.9、开发者需要对应用匹配适当的 Tag 关键字，添加应用功能及内容无关的关键字；

3.2.10、应用 Tag 关键字中包含非法（色情、反动、人身攻击等）关键字；

3.2.11、应用 Tag 关键字中包含侵权内容（侵犯其他应用商标、版权或著作权等）；

3.2.12、应用描述包含非法（色情、反动、人身攻击等）内容；

**3.3、应用展示的图片资源存在问题**

3.3.1、应用截图和应用实际的界面不符；

3.3.2、应用截图中有一张或多张重复；

3.3.3、应用截图模糊不清，无法分辨截图内容；

3.3.4、应用截图的分辨率不符合 320px*480px；

3.3.5、应用截图存在拉伸、黑边、压缩等情况；

3.3.6、应用截图存在非法（色情、反动、人身攻击等）内容；

3.3.7、应用截图存在侵权（图标、商标、版权等）行为；

3.3.8、应用截图的通知栏提示中包含与应用功能无关内容；

3.3.9、应用的 ICON 和已上架应用的 ICON 存在类似或相同情况；

3.3.10、应用展示的 ICON 和安装到手机上的 ICON 不一致；

3.3.11、应用 ICON 存在非法（色情、反动、人身攻击等）内容；

3.3.12、应用 ICON 存在侵权（图标、商标、版权等）行为；

**4、应用广告相关**

4.1.1、应用存在诱导用户点击广告的行为；

4.1.2、应用首页或一级菜单界面为应用墙入口；

4.1.3、应用的主要目的是展示广告或者市场营销；

4.1.4、应用存在强制积分墙，在使用界面提示强制下载应用换取积分；

4.1.5、应用存在强制积分墙，在使用过程中提示强制下载应用换取积分；

4.1.6、通知栏推送与自身产品无关的内容，且点击内容时无明显提示用户是否打开广告或下载软件、通知栏广告不可清除；

4.1.7、应用未经用户许可创建桌面快捷方式、书签、图标或修改默认设置等方式来进行广告展示；

4.1.8、应用广告存在模仿系统通知或警告的行为；

4.1.9、应用广告中包含不良或违法广告或信息（如色情、赌博、反动等）；

4.1.10、应用功能只有下载应用赚取积分以兑换奖品等分发类 app 暂不收录；

4.1.11、应用未经用户许可默认安装第三方应用或内嵌应用市场；

4.1.12、应用程序已关闭，广告依然存在；

**5、应用内容**

**5.1、应用存在暴力内容**

5.1.1、任何带有诽谤、人身攻击或者侮辱个人或者团体的应用将被驳回；

5.1.2、应用主要内容是人类或动物被杀或者被虐待、拷打或伤害的图片或内容的将被驳回；

5.1.3、应用过分描述暴力或虐待儿童将被驳回；

5.1.4、应用对武器进行过于逼真的表述（如不能涉及武器的制造工艺和参数等），并鼓励违法或滥用武器将被驳回；

**5.2、应用存在色情内容**

5.2.1、应用包含色情内容，或者过分展现性器官又不是旨在艺术审美或情感的将被驳回；

5.2.2、应用中存在允许用户提交色情内容的将被驳回，如允许用户发布色情照片等；

**5.3、应用存在非法金钱交易或内容**

5.3.1、应用具有现金或者流通货币赌博功能；

**5.4、政治问题**

5.4.1、政治讽刺作家或漫画家的作品也不能带有诽谤、人身攻击或者侮辱性的内容；

5.4.2、应用包含反政府、反社会内容；

5.4.3、存在政治错误的应用将被驳回，如 VPN、翻墙、反动等；

**5.5 应用的抽奖、彩票功能或内容不符合要求**

5.5.1、应用中的竞赛和抽奖活动必须由该应用开发者来发起；

5.5.2、竞赛和抽奖活动必须在应用的用户协议中有清晰详细的描述，且这些竞赛或抽奖活动和 vivo 应用商店无关，不承担任何相关法律责任；

5.5.3、理财类、银行帐户托管类、彩票类软件涉及交易的需提供政府主管部门授权文件；

**6、游戏特殊条款**

6.1.1、游戏包含“赌场”字样、或者涉及扎金花、梭哈、六合彩类等赌博内容的游戏；

6.1.2、游戏中存在诱导付费行为；

6.1.3、游戏存在强制关卡付费；

6.1.4、网络游戏未接入 vivo 支付 SDK。

**7、开发者不当行为条款**

**7.1、取消开发者资格或者封停**

7.1.1、开发者对已经明确有版权归属的 APP 私自进行破解、汉化、反编译、重新打包、换皮等二次开发后提交 2 次以上，APP 将被驳回且将被取消 vivo 应用商店开发者资格；

7.1.2、开发者一周内重复提交相似内容 APP5 次或同一开发者帐号一月内提交超过 10 款相似内容 APP 将被取消 vivo 应用商店开发者资格；

7.1.3、被驳回应用无任何修改，再次提交 3 次将被封停开发者帐号 30 天；

7.1.4、批量注册、伪造资质将被取消 vivo 应用商店开发者资格；

**7.2、开发者应用下架**

7.2.1、开发者使用非正常手段伪造或欺骗下载，操纵或者欺骗用户评论影响 vivo 应用商店的排名，APP 将会下架或排名清空；

7.2.2、开发者应用频繁更换证书签名，超过 3 次；

7.2.3、上线应用涉及审核规范不允许的行为；

# 魅族

一、 应用基本信息

应用基本信息仅限使用中文或英文，且不得含有危害国家安全、低俗、情色等非法内容。

1. 应用名称规范

1) 应用命名格式：主标题（应用名称）-副标题，仅限使用中文或英文；

2) 为取得最佳展示效果，建议应用名称+副标题不超过 10 个中文字符（即 20 个英文字符）；

3) 应用名称请勿使用类别词，包括但不限于：贷款、壁纸、电话、铃声、儿童、免费小说等；

4) 填写的应用名称需与安装到手机桌面上显示的应用名称一致；

5) 不存在与线上应用重名行为；

6) 不存在恶意 ASO 行为；

7) 不存在侵权行为，如应用名称使用未授权的商标名称。

2. 应用描述与关键字

1) 应用描述请尽量用简洁的语言对应用本身功能、特点进行描述，需不少于 50 个中文字符（即 100 个英文字符），仅限使用中文或英文；

2) 应用描述/版本描述不使用特殊字符（如：@、#、*、& 等）、大量空格或换行符；

3) 应用描述/版本描述不使用极限描述词或虚假承诺等违反新广告法的内容，包括但不限于：最、第一、唯一、NO.1、必备、免费送、100% 、全球、顶尖、首；

4) 推荐语即应用一句话介绍，不超过 14 个中文字符；

5) 关键字之间仅限使用空格分隔，不超过 100 个中文字符；

6) 关键字不包含与应用无关的内容。

3. 应用 Icon 规范

1) Icon 展示在应用商店，需与安装到手机桌面显示的 Icon 一致，不可与其他已上架应用相同；

2) Icon 请勿擅自添加标签，包括但不限于：有奖、首发、精品、官方、正版、推荐、hot 等；

3) Icon 不存在拉伸、压缩、模糊、黑（白）边、黑（白）角；

4) Icon 不存在使用美女图片（含情色、引诱、误导等）；

5) Icon 不存在侵权行为。

4. 应用截图与启动页

1) 每个应用可上传 3-5 张应用截图，单张图片请勿重复上传，不可上传与应用无关的图片；

2) 应用截图推荐使用魅族手机外观（点击下载），或不带品牌标识的 Android 手机外观，不可使用其他品牌手机外观素材（如 iPhone、小米等）；

3) 应用截图与启动页不存在拉伸、压缩、模糊、黑（白）边；

4) 应用截图与启动页不存在第三方市场 Logo。

二、 版权与资质

1. 应用版权

1) 应用不存在重新打包第三方应用的行为；
2) 应用不存在破解、盗版或未获得版权所有者授权的行为；
3) 多次提交上述应用将会取消开发者资质。

2. 应用上架资质

1) 特殊类别应用需要提供对应的资质才可申请上架，点击查看应用资质文档；
2) 企业开发者提交非本企业应用，需提供相关企业授权；
3) 个人开发者提交企业应用，需提供相关企业授权；
4) 个人开发者暂不支持接入以下类型应用，包括但不限于：新闻、电台、赚钱、金融、医疗、影视、GPS、旅游、票务、彩票、音乐专辑、明星写真、婚恋交友。

三、 安装与权限

1. 安装与卸载

1) 需保证提交的应用版本为最新版，且可以正常安装与卸载；
2) 不存在安装时静默/捆绑安装其他 APP；
3) 不存在安装时未经用户许可创建桌面图标；
4) 不存在应用启动或运行过程中闪退（崩溃）。

2. 应用权限

1) 应用不得申请与应用无关的权限；
2) 应用不得出现无法关闭的常驻通知栏；
3) 应用不得强制开机启动；
4) 应用不得未经用户许可发送短信或拨打电话。

四、 内容、功能与广告

1. 应用内容

1) 应用语言仅限使用简体中文、繁体中文与英文；
2) 应用不存在大量测试数据；
3) 应用不存在网络正常时无法获取内容；
4) 应用不存在涉黄、涉恐、涉暴、反政府、反社会等内容；
5) 应用不存在套用模板（界面设计和架构、内容极其相似）行为。

2. 应用功能

1) 应用需具备完整的功能才能进行提交；
2) 应用需适配以下分辨率，包括但不限于：1920*1080、1800*1080；
3) 应用不存在功能单一、设计粗糙；
4) 应用不存在依赖跳转网页或第三方 APP 获取内容；
5) 应用不存在 Tab 无法切换或按钮无法点击；
6) 应用仅限部分城市或特定人群使用，需在应用描述中注明具体开通城市或指定人群。

3. 应用广告

1) 支持应用接入内置广告，广告面积不得超过手机屏幕的 50%，且不得包含空白广告位；
2) 禁止应用存在通知栏广告；
3) 禁止应用在手机主桌面上添加以广告为目的图标；
4) 禁止应用在使用过程中频繁弹出悬浮窗广告，中断用户操作；
5) 禁止应用包含插屏广告代码、积分墙广告代码或风险代码。

五、 不收录的应用类型

以下应用暂不收录

| | |
|---|---|
| 应用类别 | 平板应用 |
| | 竞拍/夺宝应用 |
| | 高频彩相关应用 |
| | 游戏/游戏攻略/游戏外挂应用 |
| | 单一游戏的非官方攻略、社区应用 |
| | 单一壁纸、主题或锁屏应用 |
| | 社交 APP 衍生的对话生成器类应用 |
| | 包含政治敏感内容及相关辅助工具，如 VPN、翻墙、反动、境外媒体、加速器等 |
| 功能内容相关 | 支持手游充值的应用 |
| | 支持自动抢红包的应用 |
| | 支持赌博或非法金钱交易的应用 |
| | 支持伪装机身电话号码或伪装通话声音的应用 |
| | 主功能需要 Root 的应用 |
| | 主功能需付费才能使用的应用 |
| | 含积分墙的 WiFi 破解应用 |
| | 积分墙应用（通过下载 APP 赚取积分以兑换奖品） |
| | 赚取积分以兑换话费、现金等奖品的应用 |
| | 诱导用户分享至社交媒体赚取收益的应用 |
| | 含应用分发属性的应用（如支持下载、搜索和更新应用功能） |
| | 同质化严重的应用（P2P 理财类、赚钱类(包括夺宝/彩票/红包等)、游戏助手类(游戏礼包/游戏盒子等)、视频及播放器类、各种相机相册、浏览器类、系统工具类、WIFI 流量类、医疗类、微商类、微商工具类、空间刷赞类、答题赢奖类、众筹类、淘宝优惠券类等） |

# 小米

1、应用功能

1.1 应用无法正常运行或功能存在问题

1.1.1 应用存在功能问题

1.1.2 应用无法正常安装或安装时提示解析失败

1.1.3 应用无法正常卸载或卸载报错

1.1.4 应用在启动时崩溃

1.1.5 应用在运行时崩溃

1.1.6 应用中内容无法正常显示或无法获取
1.1.7 应用内按钮点击无反应或点击报错
1.1.8 应用内 Tap 无法切换或切换报错
1.1.9 应用强制或诱导修改系统默认设置
1.1.10 应用功能需要依赖于第三方应用才能实现
1.1.11 应用描述中介绍的功能在应用内不具备或不一致
1.1.12 应用需要登录，但应用内不提供注册通道，请在完善资处填写测试账号。
1.1.13 注册账号功能不可用，审核时尝试 3 次都无法成功注册
1.1.14 应用登录账号功能不可用，应用审核时尝试 3 次都无法成功登录
1.1.15 应用界面模糊或拉伸
1.1.16 应用分辨率无法适配 Mi 2、Mi 2A、Mi 2S、红米或红米 Note，要求分辨率为 1280px*720px
1.1.17 应用分辨率无法适配 Mi 3、Mi 4，要求分辨率为 1920px*1080px
1.1.18 应用分辨率无法适配 Mi Note，要求分辨率为 2560px*1440px
1.1.19 应用分辨率无法适配 Mi Pad，启动界面模糊或存在拉伸，要求分辨率为 2048px*1536px
1.1.20 应用分辨率无法适配 Mi Pad，引导界面模糊或存在拉伸，要求分辨率为 2048px*1536px
1.1.21 应用分辨率无法适配 Mi Pad，界面未填满屏幕，要求分辨率为 2048px*1536px
1.1.22 应用分辨率无法适配 Mi Pad，文字模糊，要求分辨率为 2048px*1536px
1.1.23 应用分辨率无法适配 Mi Pad，为手机版放大，要求分辨率为 2048px*1536px
1.1.24 应用分辨率无法适配 Mi Pad，应用中的按钮、文字、图片或 ICON 过小，要求分辨率为 2048px*1536px
1.1.25 应用分辨率无法适配 Mi Pad，应用中的按钮、文字、图片或 ICON 等存在错位，要求分辨率为 2048px*1536px
1.1.26 应用分辨率无法适配 Mi Pad，应用中的按钮、文字、图片或 ICON 等存在拉伸，要求分辨率为 2048px*1536px
1.1.27 应用分辨率无法适配 Mi Pad，要求分辨率为 2048px*1536px
1.1.28 应用需要其他硬件设备支持，审核人员无法进行测试

2.1 应用描述和实际功能不符
2.1.1 应用介绍或更新日志中介绍的功能在应用内不具备或不一致
2.1.2 应用存在欺骗用户下载使用的行为

2.2 申请危险权限或权限和功能不符
2.2.1 应用申请的权限和其实际功能不符
2.2.2 应用实际功能不需常驻通知栏却常驻通知栏
2.2.3 应用无法关闭常驻通知提示
2.2.4 通知栏显示图标与应用 ICON 不相同
2.2.5 应用实际功能不需开机启动却开机启动
2.2.6 应用在安装或者运行前提示用户重启设备
2.2.7 应用在安装或者运行前强制重启设备

2.3 应用功能存在使用限制

2.3.1 应用功能仅供部分用户使用，比如限制用户的地域或仅供组织内部使用等，请在应用介绍内说明具体限制范围

2.4 应用存在恶意行为
2.4.1 应用存在恶意行为
2.4.2 应用未经用户许可发送短信，建议使用返回验证码等方式
2.4.3 应用存在病毒
2.4.4 应用存在吸费行为
2.4.5 应用消耗过多的网络流量
2.4.6 应用未经用户许可拨打电话
2.4.7 应用修改主叫号码，主要功能用于欺骗被叫用户
2.4.8 应用未运行，但是仍会启动 GPS、蓝牙等系统功能

3 应用展示和广告（App Properties & AD）
3.1 平台专有性
3.1.1 应用闪屏界面（或启动引导界面）包含其他应用市场的图标、水印、文字等
3.1.2 应用闪屏界面（或启动引导界面）使用非 Android 设备照片或外观图（例如：苹果手机外观素材）
3.1.3 应用闪屏界面（或启动引导界面）包含其他品牌手机商标
3.1.4 应用截图中存在其他应用市场图标、水印、文字等
3.1.5 应用截图中的应用界面非 Android 系统（例如：苹果 iOS 系统界面）
3.1.6 应用截图中存在其他设备品牌标志、名称、商标等
3.1.7 应用截图中手机外观素材非 Android 设备（例如：苹果手机外观）
3.1.8 应用描述中包含其他应用市场的名称，
3.1.9 应用介绍中包含第三方市场名称、介绍、引述等内容
3.1.10 应用更新日志中包含第三方市场名称、介绍、引述等内容
3.1.11 游戏攻略类应用暂不收录（包含公会、社区、礼包、论坛、视频、游戏分发或其他游戏推荐功能）
3.1.12 应用含有应用市场属性（允许下载、更新和搜索应用等功能）
3.1.13 应用运行时会弹窗或主动推送下载第三方应用市场

3.2 应用展示内容存在问题
3.2.1 应用内容存在侵权行为
3.2.2 应用名称+描述语不能超过 8 个汉字字符或 16 个英文字符
3.2.3 应用名称本身就已经超过 8 个汉字或 16 个英文字符，只能使用应用的原名称，不能添加描述语
3.2.4 应用名称存在占位符文本、大量空格等非法字符（如：#、*、& 等）
3.2.5 应用名称与线上已存在的应用的名称相同，请您修改名称，应用名称为 Wechat 和 WECHA 也属于同名称；若拥有相应名称的商标权，请按照下面的链接进行申诉
/doc/?p=194
3.2.6 应用在商店中显示的名称和安装到设备中显示的名称差异较大
3.2.7 应用名称包含非法内容
3.2.8 应用名称存在侵权行为

3.2.9 应用名称仅以类别词命名，如以壁纸、标签、电话、桌面、安全助手、wifi 等名称做为应用的名称

3.2.10 应用介绍或更新说明包含非法内容

3.2.11 应用介绍或更新说明中包含侵权内容

3.2.12 应用介绍或更新日志中存在占位符文本、大量空格空行、非法字符（如：@、#、*、& 等）

3.2.13 更新说明和旧版本的更新日志相同，请填写本次更新说明

3.2.14 应用更新说明中包含其他应用市场名称或内容

3.2.15 更新说明无效，请填写正确的更新说明

3.2.16 应用的分类与应用的实际内容或功能不符，建议分类为：

3.2.17 应用的二级分类与应用的实际内容或功能不符，建议分类为：

3.2.18 应用的二级分类与应用的实际内容或功能不符，若无对应二级分类，请选择“其它”

3.2.19Tag 关键字中包含与应用无关的关键字

3.2.20Tag 关键字中包含非法关键字

3.2.21Tag 关键字中包含侵权内容

3.2.21 一句话简介中使用了极限词或虚假承诺等违反新广告法的内容（如“最”“第一”“唯一”“NO.1”“必备”“免费送”“100%”　“全球”“顶尖”“首”等)；

3.2.22 一句话简介使用了疑问、反问等句式（请用陈述语句进行描述）

3.2.23 一句话简介中包含违规内容（如侵权、色情、恐怖暴力、反动等）

3.2.24 一句话简介存在占位符文本、大量空格等非法字符（如：#、*、& 等）

3.3 应用展示的图片资源存在问题

3.3.1 应用内容中的图片拉伸或模糊

3.3.2 应用截图和应用实际的界面不符

3.3.3 应用截图中存在重复

3.3.4 应用截图存在黑边

3.3.5 应用截图存在压缩

3.3.6 应用截图模糊不清，无法分辨截图内容

3.3.7 应用截图存在拉伸

3.3.8 应用截图内容显示不完整

3.3.9 应用截图的分辨率不符合 1280px*720px（对应 Mi 2、Mi 2S、Mi 2A、红米或红米 Note）

3.3.10 应用截图的分辨率不符合 1920px*1080px（对应 Mi 3，Mi 4）

3.3.11 应用截图的分辨率不符合 2560px*1440px（对应 Mi Note）

3.3.12 应用截图的分辨率不符合 2048px*1536px（对应 Mi Pad）

3.3.13 应用截图存在非法内容

3.3.14 应用截图存在侵权行为

3.3.15 应用截图的通知栏中包含与应用功能无关内容，请仅保留手机系统自带的信号、运营商信息等提示

3.3.16 应用截图和用户使用时的应用界面方向不符，横屏使用的界面请上传横屏截图，系统会自动作调整

3.3.17 应用的 ICON 和已上架应用的 ICON 完全相同

3.3.18 应用展示的 ICON 和安装到设备上的 ICON 不一致，请您自行对比应用在页面展示和

手机端展示的 ICON
3.3.19 应用 ICON 存在非法内容
3.3.20 应用 ICON 存在侵权行为
3.3.21 应用的 ICON 和已上架应用的 ICON 存在类似

3.4 广告相关
3.4.1 应用未经用户许可或默认勾选创建桌面快捷方式
3.4.2 应用未经用户许可默认安装或默认勾选安装第三方应用
3.4.3 应用未经用户许可修改系统默认设置
3.4.4 应用存在诱导用户点击广告的行为
3.4.5 应用内存在诱导用户评价功能，不得出现任何诱导用户进行评分、给应用好评的功能
3.4.6 应用介绍中不得包含任何诱导用户进行评分、给应用好评的功能或文字描述
3.4.7 应用存在通知栏广告
3.4.8 应用多次发现存在通知栏广告行为，将不再收录
3.4.9 应用存在强制积分墙，在启动时强制要求换取积分才能使用
3.4.10 应用存在强制积分墙，在使用时强制要求换取积分
3.4.11 应用具有诱导用户赚取积分兑换货币或奖品的功能
3.4.12 暂不收录：赚取积分以兑换话费、现金等奖品的应用
3.4.13 应用存在抢占锁屏的行为
3.4.14 应用广告存在模仿系统通知或警告的行为
3.4.15 应用的主要目的是展示广告或者市场营销
3.4.16 应用使用过程中频繁弹出悬浮窗广告，中断用户操作，影响用户体验
3.4.17 应用包含空广告栏位
3.4.18 应用中的广告不能干扰第三方的应用的广告展示
3.4.19 应用广告中包含不良或违法信息

3.5 用户使用体验
3.5.1 应用打开立即会提示更新，请确认您所上传的是否为最新版本
3.5.2 应用只有单一功能，设计较为粗糙，应用整体质量未达到小米应用商店收录标准，请丰富应用功能、提高应用质量后再上传
3.5.3 应用是简单的网站页面打包或套用模板
3.5.4 应用功能、界面和应用商店中已收录应用非常类似
3.5.5 应用功能、界面和应用商店中已收录应用完全雷同
3.5.6 开发者应将当地官方语言的应用描述放在应用描述最前
3.5.7 应用部分功能或内容需要访问调用其他应用获取
3.5.8 应用内容不完整，部分功能待开发
3.5.9 应用的用户界面过于复杂

4 应用内容（Contents of App）
4.1 应用存在暴力内容
4.1.1 任何带有诽谤、人身攻击或者侮辱个人或者团体的应用
4.1.2 应用存在人类或动物被杀、被虐待、被伤害等图片或内容
4.1.3 应用过分描述暴力或虐待儿童
4.1.4 应用对武器进行过于逼真的表述（如不能涉及武器的制造工艺和参数等），并鼓励违

法或滥用武器

4.2 应用存在色情内容
4.2.1 应用包含色情内容或者过分展现性器官，但又不是旨在艺术审美或情感
4.2.2 应用中存在允许用户提交色情内容，如允许用户发布色情照片、文字等
4.2.3 情趣用品商城类应用禁止存在社区、论坛等允许用户发布帖子、信息和评论帖子等功能和模块，请您将以下模块进行删除
4.2.4 应用介绍、应用截图、描述语等含有色情内容，详情如下：

4.3 应用存在非法金钱交易或内容
4.3.1 应用具有现金或者流通货币赌博功能

4.4 政治问题
4.4.1 应用不能包含对国家领导人诽谤、人身攻击或者侮辱性的内容
4.4.2 应用包含反政府、反社会内容
4.4.3 存在政治错误的应用，如 VPN、翻墙、涉恐涉暴等

4.5 用户使用感受
4.5.1 小米应用商店暂不收录：品类单一的主题、壁纸、锁屏类应用
4.5.2 小米应用商店暂不收录：短信收取服务费的应用
4.5.3 小米应用商店暂不收录：主要功能需要获取 Root 权限后才可使用的应用
4.5.4 应用设计的功能主要是令用户厌恶、恐惧
4.5.5 应用具有易引起用户不适或者比较粗俗的内容，如对血腥和色情场面的过分展现
4.5.6 应用中所有的“敌人”角色，都不能针对任何一个现实的种族、文化、政府或公司，以及任何一个真实的个体
4.5.7 应用中涉及的宗教内容都应该是翻译准确和使用恰当的，并且不存在误导行为。使用这些内容的目的应该是教育意义的而不是煽动性的
4.5.8 存在针对某一宗教、文化或种族的诽谤、侮辱或攻击的内容，或有可能让这部分群体人们造成情感伤害的内容

4.6 应用内抽奖、彩票相关功能及内容
4.6.1 应用中的竞赛和抽奖活动必须由该应用开发者来发起
4.6.2 竞赛和抽奖活动必须在应用的用户协议中有清晰详细的描述，且这些竞赛或抽奖活动和小米应用商店无关，不承担任何相关法律责任
4.6.3 彩票类软件都必须符合国家的相关法律条款
4.6.4 特殊行业类软件请根据以下链接 https://dev.mi.com/console/doc/detail?pId=1258 提交相关资质证明发送至 developer@xiaomi.com
4.6.5 理财应用提交的应用一句话简介，应用描述，更新日志，截图等所有在小米应用商店展示的信息，需符合理财 APP 内容审核要求 。
4.7 开发者行为不当
4.7.1 开发者重复提交结构、功能、内容相似的应用，重复提交的应用将被驳回或下架,情节严重者将被取消小米开发者资格
4.7.2 开发者对已经明确版权归属的应用私自进行破解、汉化、反编译或重新打包，应用将被驳回且开发者将被取消小米开发者资格

4.7.3 开发者提交的应用存在问题或开发者自身原因，开发者主动申请驳回、删除或下架

5 损坏设备（Damage to Device）
5.1 用户运行该应用有可能损坏设备
5.1.1 应用存在 bug 导致硬件无法正常使用

5.2 应用如会迅速消耗电量或者造成设备过热
5.2.1 应用未启动，但不断使用 GPS 等功能导致用户电量迅速消耗
5.2.2 应用未启动，但会长时间占用 CPU、内存等导致设备过热

6 法律要求（Legal requirements）
6.1 违反国家法律法规
6.1.1 应用都必须遵守当地的所有法律法规，开发者都有义务熟悉并遵守相关的法律法规
6.1.2 应用允许共享违法的文件或内容

6.2 应用允许共享违法的文件或内容
6.2.1 应用怂恿或鼓励犯罪或暴力行为
6.2.2 应用鼓励酒驾或公布没有经过交通管理部门允许的酒驾检测点数据
6.2.3 应用过度宣传酒精或者危险物品（如毒药、爆炸物等），或者鼓励未成年人消费香烟和酒精饮料

6.3 应用存在侵犯版权行为
6.3.1 应用为重新打包其他开发者的应用
6.3.2 应用为破解、盗版或未获得版权所有者授权的应用
6.3.3 单本图书类应用请提供版权证明 ，书城类应用请提供免责声明，免责声明模板可在以下文档中下载。/doc/?p=508

6.4 应用存在欺诈行为
6.4.1 开发者采用伪造或欺骗下载，以及其他任何不适当的方式，操纵或者欺骗用户评论影响小米应用商店的排名，应用将会下架或排名清空
6.4.2 应用存在欺骗、伪造或者误导用户的行为

6.5 隐私保护
6.5.1 应用未提示用户或未经用户授权情况下不得搜集、传输或者使用用户的位置信息
6.5.2 应用未经用户许可且在用户不知情的情况下传输和使用用户的隐私数据，如通讯录、照片和短信记录等
6.5.3 应用需要用户共享其个人信息，如邮件地址或生日等信息
6.5.4 应用搜集未成年人信息数据
6.5.5 开发者的应用会窃取用户密码或者其他用户个人数据的将被取消小米应用商店开发者资格

7 商务要求（Business Requirements）
7.1 应用存在扣费项
7.1.1 为了玩家利益请先接入小米 SDK，确保安全支付。请联系商务合作

migames@xiaomi.com
7.1.2 您的应用存在付费项，请联系商务合作 migames@xiaomi.com

8 活动审核（Activities）
8.1 活动相关
8.1.1 活动形式有诱导好评的嫌疑
8.1.2 暂不接受在应用商店内评论的活动形式
8.1.3 活动形式单一，缺乏创新（常见三种形式：应用内抽奖、全员礼包、借助第三方平台）
8.1.4 同一分类活动数量有限（将活动按分类划分，同一分类应用对比选出最优质的 1-2 个活动）
8.1.5 该应用活动申请存在以下问题（注：写在补充说明中）

8.2 活动奖品
8.2.1 活动金额不足（常规活动实物奖品总值不低于 5000 元人民币）
8.2.2 没有提供奖品单价，无法核实奖品总额
8.2.3 活动奖品不符合要求（若送手机、平板、盒子、电视等，只能赠送小米品牌，其他奖品无限制）
8.2.4 活动奖品吸引力不足

8.3 应用质量
8.3.1 产品评分过低（评分低于 3 分）
8.3.2 存有版权纠纷，不易于活动推荐
8.3.3 应用属于暂不接受活动申请的类别，不接受活动申请的应用类别详见《活动合作标准化流程》

9 完美图标审核（Icon）
9.1 完美图标内容审核
9.1.1 完美图标欠缺，要求上传四个尺寸，包括 90*90，136*136,192*192 的手机尺寸和 168*168 的平板尺寸
9.1.2 所有完美图标上的内容没有填满内容区，存在透明区域(如图标存在圆角)
9.1.3 90*90 完美图标上的内容没有填满内容区，存在透明区域(如图标存在圆角)
9.1.4 136*136 完美图标上的内容没有填满内容区，存在透明区域(如图标存在圆角)
9.1.5 192*192 完美图标上的内容没有填满内容区，存在透明区域(如图标存在圆角)
9.1.6 168*168 完美图标上的内容没有填满内容区，存在透明区域(如图标存在圆角)
9.1.7 224*224 完美图标上的内容没有填满内容区，存在透明区域(如图标存在圆角)
9.1.8 完美图标清晰度较低
9.1.9 完美图标与应用自带图标差异较大，难以认出
9..1.10 完美图标主要元素被蒙板裁切
9..1.11 图标主要中心元素不居中，展现不均匀
9.1.12 完美图标中心元素比例过大

10 应用视频预览审核（Video Demo Revie）

10.1 视频内容存在问题
10.1.1 应用视频暂不接受品宣广告，视频内容请以功能介绍为主
10.1.2 应用视频内容存在 iOS 系统界面（请使用 Android 系统）
10.1.3 应用视频内容出现非 Android 设备（如 iPhone 或 iPad，请使用 Android 设备）
10.1.4 应用视频内容过于简单，未突出应用特点，宣传价值较小
10.1.5 应用视频中，操作演示过快，请放慢演示
10.1.6 应用视频内容出现非小米品牌曝光（如：商标，设备，操作系统等）
10.1.7 视频音话不同步（如声音和字幕对不上或声音和操作对不上）
10.1.8 应用视频内容中，含无关元素过多，例如：
10.1.9 应用视频内容与应用功能或介绍信息不符
10.1.10 应用视频存在侵权内容
10.1.11 应用视频存在色情、血腥暴力、政治、赌博等内容
10.1.12 应用视频存在水印

10.2 视频播放存在问题
10.2.1 视频的尺寸比例错误（推荐录屏尺寸：1280*720；1920*1080；2560*1440
10.2.2 如果应用以竖屏操作为主，请竖屏情况下录制
10.2.3 如果应用以横屏操作为主，请横屏情况下录制
10.2.4 应用视频播放时间超过 30 秒
10.2.5 应用视频播放时间未到 15 秒
10.2.6 应用视频播放时有噪音
10.2.7 应用视频播放无声音
10.2.8 应用视频播放不清晰
10.2.9 应用视频无法播放
10.2.10 应用视频全屏播放时存在黑边

# 豌豆荚

1. 软件可以正常安装使用卸载
2. 不可包括强制性（严重影响使用）广告点击 软件推送下载 积分内容
3. 不能有除 google market 外第三方应用商店图标 连接 or 登录入口
4. 不能有攻击侮辱语言
5. 不能有敏感色情反社会内容
6. 收费内容应在描述中明确告知用户

# 百度

1.功能
App 需要正常使用安装卸载
明确告知用户通信费用及用途
不得存在严重 BUG 导致闪退崩溃或无法使用
2.广告
不得在用户未体验主要内容前强制下载其他 App 换取积分或换取后仍然无法使用

不得在通知栏推送无关内容
用户点击 App 广告后不得未经用户二次确认就开始下载
广告面积不得占屏幕一般
不得在手机屏幕上添加与自身无关 app
App 启动后不得立即提示用户更新
App 关闭后广告不得仍然存在
广告不可以影响体验或诱导点击
3.危险恶意
不得使用积分墙，强制用积分方可使用
不得未经用户授权发短信拨打电话联网下载或者获取用户信息
不得有病毒和风险代码
不得伪装机身电话号码
不得使用欺骗手段进行恶意扣费
不得捆绑无关应用
不得存在侵权行为

# 腾讯应用宝

**安装与权限**

1. 安装与卸载
1) 需保证提交的应用版本为最新版，且可以正常安装与卸载；
2) 不存在安装时静默/捆绑安装其他 APP；
3) 不存在安装时未经用户许可创建桌面图标；
4) 不存在应用启动或运行过程中闪退（崩溃）。

2. 应用权限
1) 应用不得申请与应用无关的权限；
2) 应用不得出现无法关闭的常驻通知栏；
3) 应用不得强制开机启动；
4) 应用不得未经用户许可发送短信或拨打电话。

四、 内容、功能与广告
1. 应用内容
1) 应用语言仅限使用简体中文、繁体中文与英文；
2) 应用不存在大量测试数据；
3) 应用不存在网络正常时无法获取内容；
4) 应用不存在涉黄、涉恐、涉暴、反政府、反社会等内容；
5) 应用不存在套用模板（界面设计和架构、内容极其相似）行为。

2. 应用功能
1) 应用需具备完整的功能才能进行提交；
2) 应用需适配以下分辨率，包括但不限于：1920*1080、1800*1080；
3) 应用不存在功能单一、设计粗糙；
4) 应用不存在依赖跳转网页或第三方 APP 获取内容；

5) 应用不存在 Tab 无法切换或按钮无法点击；

6) 应用仅限部分城市或特定人群使用，需在应用描述中注明具体开通城市或指定人群。

3. 应用广告

1) 支持应用接入内置广告，广告面积不得超过手机屏幕的 50%，且不得包含空白广告位；

2) 禁止应用存在通知栏广告；

3) 禁止应用在手机主桌面上添加以广告为目的图标；

4) 禁止应用在使用过程中频繁弹出悬浮窗广告，中断用户操作；

5) 禁止应用包含插屏广告代码、积分墙广告代码或风险代码。