

Google Developer Policy - April 16, 2020

Tillsammans bygger vi världens mest tillförlitliga källa för appar och spel

Det är utvecklarnas innovationer som ligger till grund för vår gemensamma framgång, men med det följer ansvar. Dessa programpolicyer för utvecklare i kombination med [distributionsavtalet för utvecklare](#) säkerställer att vi tillsammans kan leverera världens mest innovativa och tillförlitliga appar till över en miljard människor via Google Play. Ta del av våra policyer nedan eller i en [utskriftsvy](#).

Begränsat innehåll

Google Play används varje dag av personer över hela världen för att ladda ner appar och spel. Säkerställ därför att den app du skickar in är lämplig för Google Play och i enlighet med lokal lagstiftning.

Fara för barn

Appar med innehåll som sexualiserar minderåriga tas omedelbart bort från Butiken. Vi tillåter inte appar som riktar sig till barn men innehåller barnförbjudna ämnen.

Om vi upptäcker innehåll som visar sexuellt utnyttjande av barn anmäler vi det till berörda myndigheter och tar bort Google-kontona för de som är inblandade i distributionen.

I syfte att säkerställa att Google Play förblir en säker och respektfull plattform har vi skapat standarder som definierar och förbjuder innehåll som är skadligt eller opassande för våra användare.

I syfte att säkerställa att Google Play förblir en säker och respektfull plattform har vi skapat standarder som definierar och förbjuder innehåll som är skadligt eller opassande för våra användare.

Sexuellt innehåll

Vi tillåter inte appar som innehåller eller marknadsför sexuellt innehåll, till exempel pornografi, eller innehåll och tjänster vars syfte är att vara sexuellt tilltalande. Innehåll som visar nakenhet kan vara tillåtet om det syftar till att vara utbildande, dokumentärt, vetenskapligt eller konstnärligt och inte är opåkallat.

I syfte att säkerställa att Google Play förblir en säker och respektfull plattform har vi skapat standarder som definierar och förbjuder innehåll som är skadligt eller opassande för våra användare.

Avbildningar av nakenhet där modellen är naken eller lättklädd, och utstyrseln inte är acceptabel i en offentlig kontext.

Avbildningar, animeringar eller illustrationer av sexuella handlingar eller sexuellt suggestiva poser.

Innehåll som avbildar sexuella hjälpmedel och fetischer.

Innehåll som anses oanständigt eller anstötligt.

Innehåll som avbildar, beskriver eller uppmuntrar till tidelag.

Främjande av sexuellt relaterad underhållning, eskorttjänster eller andra tjänster som kan tolkas som att sexuella tjänster erbjuds mot betalning i appar.

Hatreterik

Vi tillåter inte appar som uppmuntrar till våld eller som väcker hat mot individer utifrån etniskt ursprung, religion, funktionshinder, ålder, nationalitet, veteranstatus, sexuell läggning, kön, könsidentitet eller annan egenskap som är kopplad till systematisk diskriminering eller marginalisering.

I syfte att säkerställa att Google Play förblir en säker och respektfull plattform har vi skapat standarder som definierar och förbjuder innehåll som är skadligt eller opassande för våra användare.

Sammanställningar av påståenden vars syfte är att bevisa att en skyddad grupp är undermänsklig, underlägsen eller förtjänar hat.

Appar som innehåller teorier om att en skyddad grupp uppvisar negativa särdrag (t.ex. är illvillig, korrupt eller ondskefull) eller uttryckligen eller underförstått hävdar att gruppen utgör ett hot.

Innehåll eller retorik som försöker uppmuntra andra till att tro att individer som tillhör en skyddad grupp bör hatas eller diskrimineras.

Våld

Vi tillåter inte appar som avbildar eller underlättar överdrivet våld eller andra farliga aktiviteter.

I syfte att säkerställa att Google Play förblir en säker och respektfull plattform har vi skapat standarder som definierar och förbjuder innehåll som är skadligt eller opassande för våra användare.

Detaljerade avbildningar eller beskrivningar av realistiskt våld eller hot om våld mot människa eller djur.

Appar som främjar självskadebeteende, självmord, ätstörningar, strypningslekar eller andra handlingar som kan leda till allvarliga skador eller dödsfall.

Terroristinneåll

Det är inte tillåtet för terroristorganisationer att publicera appar på Google Play i något syfte, inklusive rekrytering.

Vi tillåter inte appar med innehåll kopplat till terrorism, till exempel innehåll som främjar terroristhandlingar, uppmanar till våld eller hyllar terroristattacker. Om innehåll som är relaterat till terrorism läggs upp i ett pedagogiskt, dokumentärt, vetenskapligt eller konstnärligt syfte är det viktigt att du ger tillräckligt med information så att användarna förstår sammanhanget.

Känsliga händelser

Vi tillåter inte appar vars innehåll är okänsligt mot naturkatastrofer, illdåd, konflikter, dödsfall eller andra tragiska händelser eller försöker utnyttja dessa ekonomiskt.

I syfte att säkerställa att Google Play förblir en säker och respektfull plattform har vi skapat standarder som definierar och förbjuder innehåll som är skadligt eller opassande för våra användare.

- uppvisa okänslighet med avseende på riktiga personers eller gruppers bortgång till följd av självmord, överdos, naturliga orsaker osv.

- förneka större tragiska händelser

- förefalla dra nytta av en tragisk händelse utan att detta gagnar offren på ett märkbart sätt

Mobbning och trakasserier

Vi tillåter inte appar som innehåller eller möjliggör hot, trakasserier eller mobbning.

I syfte att säkerställa att Google Play förblir en säker och respektfull plattform har vi skapat standarder som definierar och förbjuder innehåll som är skadligt eller opassande för våra användare.

- mobba offer för internationella eller religiösa konflikter

- lägga upp innehåll vars syfte är att utnyttja andra genom bland annat utpressning

- lägga upp innehåll vars syfte är att förnedra någon offentligt

- trakassera offer för tragiska händelser eller deras familj och vänner.

Farliga produkter

Vi tillåter inte appar som underlättar försäljningen av sprängämnen, skjutvapen, ammunition eller vissa tillbehör för skjutvapen.

- Bland tillbehören som begränsas finns sådana som möjliggör att skjutvapen simulerar automateld, tillbehör som omvandlar ett skjutvapen till automatvapen (t.ex. fjädrande kolvar, gatling-avtryckare, automatiska avtryckare, omvandlingssatser) och magasin eller ammunitionsbälten som rymmer fler än 30 patroner.

Vi tillåter inte appar som tillhandahåller anvisningar för tillverkning av sprängämnen, skjutvapen, ammunition, begränsade skjutvapentillbehör eller andra vapen. Detta inbegriper anvisningar om hur man omvandlar ett skjutvapen till automatvapen eller simulerar automateld.

Marijuana

Vi tillåter inte appar som underlättar försäljning av marijuana eller marijuanaprodukter, oavsett laglig status.

I syfte att säkerställa att Google Play förblir en säker och respektfull plattform har vi skapat standarder som definierar och förbjuder innehåll som är skadligt eller opassande för våra användare.

- Låter användare beställa marijuana via en kundvagnsfunktion i appen.

- Hjälper användare att ordna leverans eller upphämtning av marijuana.

- Underlättar försäljning av produkter som innehåller THC.

Tobak och alkohol

Vi tillåter inte appar som underlättar försäljning av tobak (inbegripet e-cigarett) eller uppmuntrar till oansvarig användning av alkohol eller tobak.

I syfte att säkerställa att Google Play förblir en säker och respektfull plattform har vi skapat standarder som definierar och förbjuder innehåll som är skadligt eller opassande för våra användare.

- Avbildar eller uppmuntrar försäljning av alkohol eller tobak till minderåriga.

- Antyder att konsumtion av tobak kan förbättra social, sexuell, yrkesmässig, intellektuell eller idrottslig status.

- Positiva framställningar av överdrivet drickande, inbegripet positiva framställningar av måttlöst drickande, hetsdrickande eller drickande i tävlingssyfte.

Finansiella tjänster

Vi tillåter inte appar som utsätter användare för vilseledande eller skadliga finansiella produkter och tjänster.

I denna policy definierar vi finansiella produkter och tjänster som produkter eller tjänster kopplade till hantering eller investering av pengar och kryptovalutor, inklusive personlig rådgivning.

Om appen innehåller eller marknadsför finansiella produkter och tjänster måste du följa delstatliga och lokala föreskrifter för alla regioner eller länder som appen riktar sig till, såsom att inkludera specifika redogörelser som krävs enligt lokal lagstiftning.

Binära optioner

Vi tillåter inte appar som ger användarna möjlighet att handla i binära optioner.

Kryptovalutor

Vi tillåter inte appar som tillhandahåller verktyg för kryptovaluta-mining på enheter. Vi tillåter däremot appar via vilka man kan hantera kryptovaluta-mining från andra ställen.

Privatlån

Vi definierar privatlån som ett engångslån från en privatperson, en organisation eller ett rättssubjekt till en enskild konsument där syftet inte är finansiering av ett köp av en anläggningstillgång eller utbildning. Konsumenter av privatlån behöver information om kvalitet, egenskaper, avgifter, risker och förmåner med låneprodukter för att kunna fatta välinformerade beslut om de ska ta ett lån eller inte.

Exempel: Privatlån, snabblån, person-till-person-lån, lån med bil som säkerhet.

Ingår inte: hypotekslån, billån, studielån, revolverande krediter (som kreditkort, personliga krediter).

Appar för privatlån måste tillhandahålla följande information i appens metadata:

den kortaste och längsta återbetalningsperioden
högsta årliga räntesats (APR), vilken oftast inkluderar ränta plus avgifter och andra kostnader under ett år eller en annan, liknande kostnad som har räknats ut i enlighet med lokal lagstiftning
ett typexempel på den totala kostnaden för lånet, inklusive alla aktuella avgifter.

Vi tillåter inte appar som marknadsför privatlån och kräver fullständig återbetalning inom 60 dagar eller mindre från den dag lånet utfärdades (vi kallar dessa "kortsiktiga privatlån"). Denna policy gäller appar som erbjuder lån direkt, genererar potentiella kunder och sådana som sätter konsumenter i kontakt med tredje part.

Privata högräntelån

I USA tillåter vi inte appar för privatlån med en APR på 36 % eller högre. Appar för privatlån i USA måste visa information om högsta APR, beräknad i enlighet med [Truth in Lending Act \(TILA\)](#).

Denna policy gäller appar som erbjuder lån direkt, genererar potentiella kunder och sådana som sätter konsumenter i kontakt med tredje part.

Hasardspel

Vi tillåter innehåll, tjänster och annonser för hasardspel om de uppfyller vissa krav. Vi tillåter även appar för daglig fantasysport som uppfyller vissa krav.

Appar med hasardspel

(tillåts för närvarande endast i Storbritannien, Irland och Frankrike)

Vi tillåter innehåll och tjänster som förmedlar hasardspel om de uppfyller följande krav:

Utvecklaren måste [genomgå ansökningsprocessen](#) för att distribuera appen på Play.

Appen måste följa alla tillämpliga lagar och branschstandarder som gäller i länder där den distribueras.

Utvecklaren måste ha en giltig licens för hasardspel för varje land där appen distribueras.

Appen måste förhindra att minderåriga användare spelar i appen.

Appen måste förhindra användning i länder som inte omfattas av licensen för hasardspel som tillhandahålls av utvecklaren.

Appen får INTE vara en betalapp på Google Play eller använda sig av fakturering via Google Play för köp i appar.

Appen måste gå att ladda ned utan kostnad och installeras från Play Butik.

Appen måste klassificeras som Endast för vuxna eller motsvarande IARC-klassificering. Information om ansvarsfullt spelande måste visas tydligt i appen och appinformationen.

Vi tillåter inte innehåll eller tjänster som förmedlar hasardspel på internet, inbegripet men inte begränsat till onlinekasinon, odds och lotterier samt spel med chans att vinna pengar eller andra vinster, på några andra platser.

Annonser för hasardspel i appar som distribueras på Play

Vi tillåter annonser som förmedlar hasardspel om de uppfyller följande krav:

Appen och annonsen (inklusive annonsörer för hasardspel) måste följa alla tillämpliga lagar och branschstandarder som gäller på alla platser där annonser för hasardspel visas.

Annonsen måste uppfylla licenskraven för alla hasardspelsrelaterade produkter och tjänster som marknadsförs.

Appen får inte visa annonser för hasardspel för individer som man vet är under 18 år.

Appen får inte vara en del av programmet Designed for Families.

Appen får inte rikta sig till individer som är under 18 år som sin primära målgrupp.

Annonsen måste tydligt visa information om ansvarsfullt spelande på målsidan, i appuppgifterna eller i appen.

Appar som visar annonser för hasardspel får inte vara en app för simulerat hasardspel (ett underhållningsspel med hasardspel utan riktiga pengar).

I syfte att säkerställa att Google Play förblir en säker och respektfull plattform har vi skapat standarder som definierar och förbjuder innehåll som är skadligt eller opassande för våra användare.

En KIDS 123-app som visar en annons som marknadsför tjänster för hasardspel

Appar med daglig fantasysport (Daily Fantasy Sports, DFS)

Vi tillåter appar med daglig fantasysport så länge de uppfyller följande krav:

Appar får endast tillåta åtkomst och distribueras inom USA. Appar med daglig fantasysport som är inriktade på rättsskipningsområden utanför USA måste inhämta berättigande via processen för Real Money Gambling Apps.

Utvecklaren måste genomgå processen för [ansökan om daglig fantasysport](#) och godkännas för att distribuera appen på Play.

Appen måste följa alla tillämpliga lagar och branschstandarder som gäller i de amerikanska delstater eller territorier där den distribueras.

Utvecklaren måste ha en giltig licens för var och en av de amerikanska delstaterna och territorierna där en licens krävs för appar för daglig fantasysport.

Appen måste förhindra att minderåriga satsar pengar eller genomför monetära transaktioner i appen.

Appen måste förhindra användning i de amerikanska delstater eller territorier där utvecklaren inte innehar den licens som krävs för appar för daglig fantasysport.

Appar måste förhindra användning i de amerikanska delstater eller territorier där appar för daglig fantasysport inte är lagliga.

Appen får INTE vara en betalapp på Google Play eller använda sig av fakturering via Google Play för köp i appar.

Appen måste gå att ladda ned utan kostnad och installeras från Play Butik.

Appen måste klassificeras som Endast för vuxna eller motsvarande IARC-klassificering. Information om ansvarsfullt spelande måste visas tydligt i appen och appinformationen.

Olagliga aktiviteter

Vi tillåter inte appar som förmedlar eller marknadsför olagliga aktiviteter.

I syfte att säkerställa att Google Play förblir en säker och respektfull plattform har vi skapat standarder som definierar och förbjuder innehåll som är skadligt eller opassande för våra användare.

Förmedling av försäljning eller köp av olagliga droger eller receptbelagda läkemedel utan recept.

Skildring av eller uppmuntran till användning eller försäljning av droger, alkohol eller tobak till minderåriga.

Instruktioner för odling eller tillverkning av olagliga droger.

Användargenererat innehåll

Användargenererat innehåll är innehåll som användare bidrar med till en app och vilket är synligt eller tillgängligt för åtminstone en del av appens användare. Stötande innehåll är innehåll som strider mot våra policyer.

Appar som innehåller användargenererat innehåll måste uppfylla följande krav:

De måste kräva att användarna godkänner appens användarvillkor och/eller användarpolicy innan användarna kan skapa eller ladda upp användargenererat innehåll.

De måste på ett sätt som är förenligt med andan i Google Plays policy för utvecklare definiera vilken typ av användargenererat innehåll som är stötande, och förbjuda sådant användargenererat innehåll i appens användarvillkor eller användarpolicy.

De måste implementera kraftfull, effektiv och ständig moderering av användargenererat innehåll på ett sätt som är rimligt och överensstämmer med de typer av användargenererat innehåll som finns i appen.

Appen måste tillhandahålla ett användarvänligt system för rapportering och borttagning av användargenererat innehåll.

Om livestreaming förekommer i appen måste problematiskt användargenererat innehåll tas bort så nära realtid som möjligt.

Ta bort eller blockera trakasserande användare som bryter mot appens användarvillkor och/eller användarpolicy.

Tillhandahåll skyddsåtgärder som förhindrar att intäktsgenerering i appen uppmuntrar användare till olämpligt beteende.

Appar vars primära syfte är att presentera stötande användargenererat innehåll tas bort från Google Play. Även appar som visar sig användas först och främst till att tillhandahålla stötande användargenererat innehåll, eller som utvecklar ett rykte bland användarna om att vara ett ställe där sådant innehåll är vanligt förekommande, tas bort från Google Play.

I syfte att säkerställa att Google Play förblir en säker och respektfull plattform har vi skapat standarder som definierar och förbjuder innehåll som är skadligt eller opassande för våra användare.

Främja sexuellt explicit användargenererat innehåll, däribland genom att implementera betalfunktioner som främst uppmuntrar till delning av olämpligt innehåll.

Appar med användargenererat innehåll som saknar tillräckligt skydd mot hot, trakasserier eller mobbning, framför allt mot minderåriga.

Inlägg, kommentarer eller bilder i en app som i första hand är avsedda att trakassera eller urskilja en annan person för trakasserier, attacker eller förlöjligande.

Appar som vid upprepade tillfällen misslyckas med åtgärda användares klagomål om stötande innehåll.

Otillåtna ämnen

Google Play tillåter inte appar som marknadsför eller säljer otillåtna ämnen, oavsett om dessa påstås vara lagliga. Exempel:

allt på denna icke uttömmande lista över [förbjudna läkemedel och kosttillskott](#) produkter som innehåller efedra

produkter som innehåller humant koriongonadotropin (hCG) i samband med viktninskning eller viktkontroll, eller som marknadsförs i samband med anabola steroider

naturläkemedel och kosttillskott med aktiva farmaceutiska eller farliga ingredienser

falska eller vilseledande hälsopåståenden, däribland påståenden som låter påskina att en produkt är lika effektiv som receptbelagda läkemedel eller kontrollerade ämnen
produkter som inte har godkänts av myndigheterna och som marknadsförs på ett sätt som låter påskina att de är säkra eller effektiva att använda för att förhindra, bota eller behandla en viss sjukdom eller krampa
produkter som har varit föremål för åtgärder eller varningar från stat eller myndighet
produkter med namn som är förvillande lika ett icke godkänt läkemedel, kosttillskott eller begränsat ämne.

Mer information om otillåtna eller vilseledande läkemedel och kosttillskott som vi granskar finns på www.legitscript.com.

Identitetsstöld och immateriell egendom

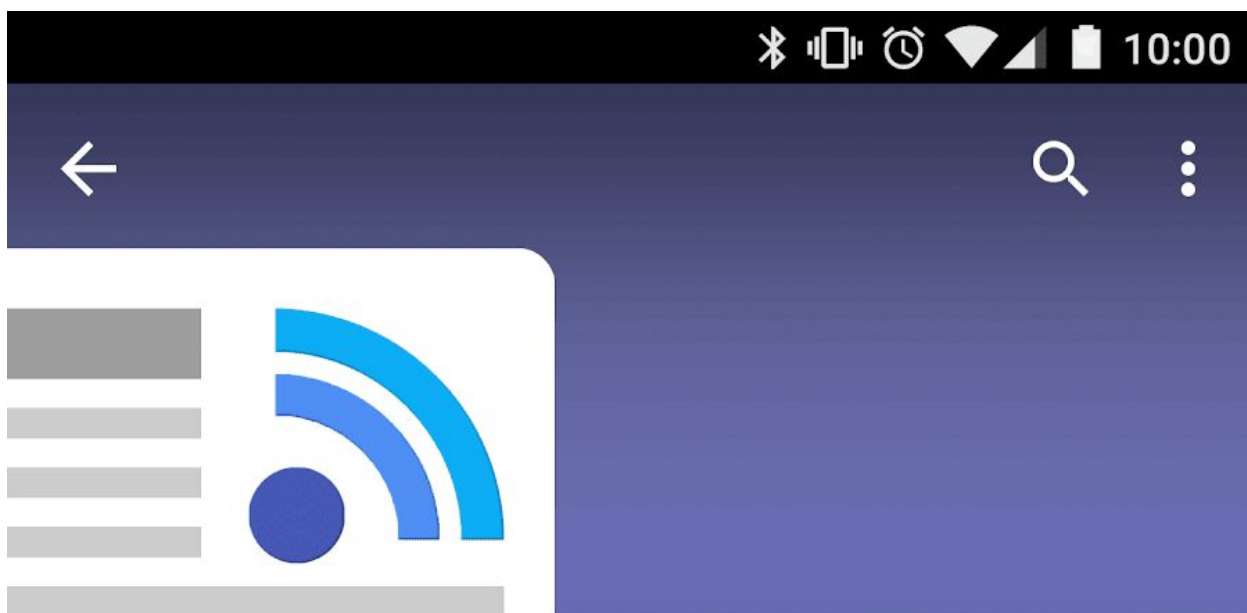
Om utvecklare kopierar någon annans arbete eller vilseleder användarna skadar det både användarna och andra utvecklare. Använd dig inte av andras arbete på ett vilseledande eller otillåtet sätt.

Identitetsstöld

Vi tillåter inte appar som använder en annan apps eller rättsfigurs varumärke, titel, logotyp eller namn på ett sätt som kan vilseleda användare. Utge dig inte för att samarbeta eller ha anknytning till någon annan rättsfigur om det inte är sant. Det kan vara identitetsstöld även om det inte finns någon avsikt att vilseleda, så var försiktig när du refererar till varumärken som inte tillhör dig. Det gäller även om varumärket i fråga inte finns på Google Play ännu.

I syfte att säkerställa att Google Play förblir en säker och respektfull plattform har vi skapat standarder som definierar och förbjuder innehåll som är skadligt eller opassande för våra användare.

Utvecklare som felaktigt påstår att de har en anknytning till en annan rättsfigur:



1

RSS News Aggregator

Google Developer

E Everyone

INSTALL



Downloads



161,251 



News &
Magazines



Similar

All the best news, aggregated in one spot!



WHAT'S NEW

- Push notifications now enabled.

- Customize your feed based on your current location!

① Det utvecklarnamn som anges för appen antyder en officiell koppling till Google trots att det inte finns någon.

Apptitlar och appikoner som är så lika titlarna och ikonerna för befintliga produkter eller tjänster att användarna kanske vilseleds:

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

Appar som felaktigt utges för att vara officiella appar för etablerade rättsfigurer. Titlar som Justin Bieber Official får inte användas utan tillåtelse eller rättigheter.

Appar som bryter mot [Androids riktlinjer för varumärkning](#).

Immateriell egendom

Vi tillåter inte appar eller utvecklarkonton som inkräktar på andras immateriella rättigheter (inklusive varumärken, upphovsrätt, patent, affärshemligheter och andra äganderättigheter). Vi tillåter heller inte appar som uppmanar eller uppmuntrar till intrång i immateriella rättigheter.

Vi vidtar åtgärder om intrång i upphovsrätten anmäls till oss. Om du vill ha mer information eller skicka en DMCA-begäran besöker du vår sida för [upphovsrättsprocesser](#).

Om du vill skicka ett klagomål gällande försäljning eller marknadsföring av förfalskade varor i en app skickar du ett [meddelande om förfalskningar](#).

Om du äger ett varumärke och anser att det finns en app på Google Play som gör intrång i varumärket rekommenderar vi att du kontaktar utvecklaren direkt för att lösa problemet. Om du inte kan nå en lösning med utgivaren skickar du ett varumärkesanspråk med det här [formuläret](#).

Om du har skriven dokumentation som bevisar att du har behörighet att använda immateriella rättigheter som tillhör en tredje part i appen eller butiksuppgifterna (t.ex. varumärkesnamn, logotyper och grafiska tillgångar) [kontaktar du Google Play-teamet](#) innan du skickar in appen, så att den inte avslås på grund av överträdelse i form av identitetsstöld eller intrång i immateriella rättigheter.

Obehörig användning av upphovsrättsskyddat material

Vi tillåter inte appar som bryter mot upphovsrätten. Att ändra upphovsrättsskyddat innehåll kan också innebära ett intrång. Utvecklare kan behöva bevisa att de har rätt att använda det upphovsrättsskyddade innehållet.

Var försiktig när du använder upphovsrättsskyddat innehåll för att visa hur din app fungerar. Oftast är det säkrast att skapa eget originalinnehåll.

I syfte att säkerställa att Google Play förblir en säker och respektfull plattform har vi skapat standarder som definierar och förbjuder innehåll som är skadligt eller opassande för våra användare.

- Omslagsbilder till musikalbum, tv-spel och böcker.

- Marknadsföringsbilder från filmer, TV eller TV-spel.

- Konstverk eller bilder från serietidningar, tecknade serier, filmer, musikvideor eller TV.

- Logotyper för collegelag och proffslag.

- Bilder tagna från en offentlig persons konto på sociala medier.

- Professionella bilder av offentliga personer.

- Reproduktioner eller fan art som inte går att urskilja från upphovsrättsskyddade original.

- Appar där det spelas upp ljudklipp från upphovsrättsskyddat innehåll.

- Fullständiga reproductioner eller översättningar av böcker som inte är allmän egendom.

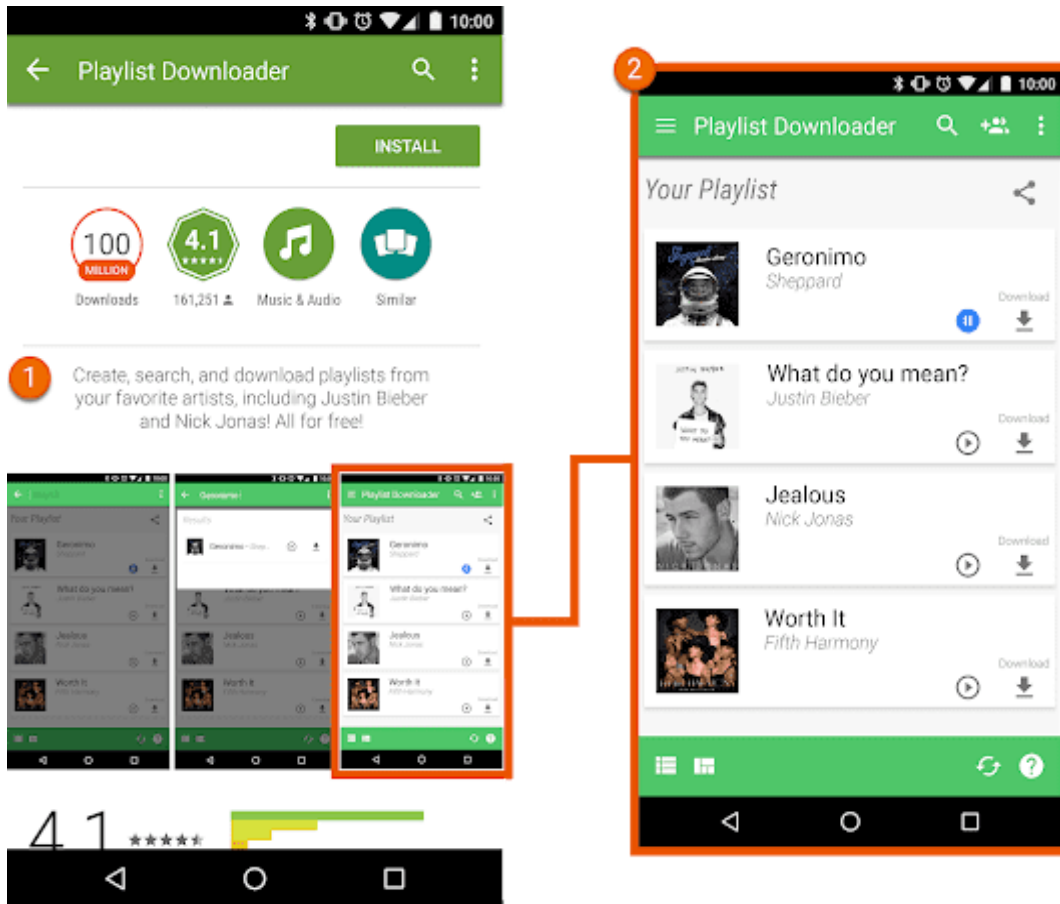
Uppmuntran till intrång i upphovsrätten

Vi tillåter inte appar som uppmuntrar eller uppmanar till intrång i upphovsrätten. Fundera över om din app uppmuntrar till intrång i upphovsrätten innan du publicerar den och sök juridisk hjälp om det behövs.

I syfte att säkerställa att Google Play förblir en säker och respektfull plattform har vi skapat standarder som definierar och förbjuder innehåll som är skadligt eller opassande för våra användare.

- Streamingappar som gör att användarna kan ladda ned en lokal kopia av upphovsrättsskyddat material utan tillåtelse.

- Appar som uppmuntrar användarna att streama och ladda ned upphovsrättsskyddat material, inklusive musik och video, i strid mot gällande upphovsrättslagstiftning.



- ① Beskrivningen i appuppgifterna uppmuntrar användarna att ladda ned upphovsrättsskyddat material utan tillåtelse.
- ② Skärmdumpen i appuppgifterna uppmuntrar användarna att ladda ned upphovsrättsskyddat material utan tillåtelse.

Varumärkesintrång

Vi tillåter inte appar som gör intrång i andras varumärken. Ett varumärke är ett ord, en symbol eller kombination som identifierar källan till en vara eller tjänst. En ägare som har förvärvat ett varumärke äger den exklusiva rätten att använda varumärket med avseende på vissa varor eller tjänster.

Varumärkesintrång är felaktig eller obehörig användning av ett identiskt eller liknande varumärke på ett sätt som kan orsaka förvirring angående källan till produkten. Om en annan parts varumärken används på ett sätt som kan orsaka förvirring i din app kan din app stängas av.

Förfalskning

Vi tillåter inte försäljning eller marknadsföring av förfälskade varor i appar. Förfälskningar har varumärken eller logotyper som är identiska med eller snarlika någon annans varumärke. De efterliknar egenskaper hos en produkt av ett visst varumärke i syfte att framstå som äkta vara från varumärkets ägare.

Integritet, säkerhet och bedrägeri

Det är viktigt för oss att skydda användarnas integritet och att erbjuda dem en säker miljö. Appar som är vilseledande, skadliga eller som skapats i syfte att använda nätverk, enheter eller personuppgifter på otillåtna sätt är strikt förbjudna.

Användardata

Du måste vara tydlig med hur du hanterar användaruppgifter (t.ex. uppgifter som har samlats in från eller om en användare, däribland enhetsinformation). Detta innebär att du ska uppgge åtkomst, insamling, användning och delning av uppgifter i appen och begränsa användningen av uppgifterna till de syften du har angett. Om appen hanterar personliga eller känsliga användaruppgifter ska du dessutom läsa kraven i avsnittet Personliga och känsliga uppgifter nedan. Dessa krav för Google Play gäller utöver de eventuella krav som föreskrivs i tillämpliga sekretess- och dataskyddslagar.

Personlig och känslig information

Personliga och känsliga användaruppgifter inbegriper, men är inte begränsade till, uppgifter som kan kopplas till en specifik individ, ekonomiska uppgifter och betalningsuppgifter, autentiseringsinformation, telefonbok, kontakter, [enhetens plats](#), uppgifter om sms och samtal, data från mikrofoner och kameror samt övrig känslig enhets- eller användningsinformation. Om appen hanterar känsliga användaruppgifter måste du göra följande:

Begränsa åtkomsten till, insamlingen, delningen och användningen av personliga och känsliga uppgifter som har förvärvats via appen till syften som är direkt relaterade till att tillhandahålla och förbättra appens funktioner (t.ex. efterlängttade funktioner som dokumenteras och lyfts fram i appens beskrivning i Play Butik). Appar som utökar användningen av sådan data i syfte att visa annonser måste efterleva vår [annonspolicy](#). Lägga upp en sekretesspolicy i det avsedda fältet i Play Console och i själva appen. Sekretesspolicyn ska, tillsammans med eventuella redogörelser i appen, tydligt beskriva hur appen får åtkomst till, samlar in, använder och delar användaruppgifter. I sekretesspolicyn måste du redogöra för vilka typer av personliga och känsliga uppgifter som appen kommer åt, samlar in, använder och delar samt vilken sorts parter som personliga eller känsliga användaruppgifter delas med. Hantera alla användaruppgifter på ett säkert sätt, till exempel genom att överföra dem med moderna krypteringsmetoder (till exempel via HTTPS).

Be om körningsbehörigheter om möjligt innan du kommer åt data som skyddas av [Android-behörigheter](#).

Inte sälja personliga eller känsliga användaruppgifter.

Tydlig redogörelse och krav på samtycke

I de fall då användare inte rimligen kan förvänta sig (enligt Plays bedömning efter eget gottfinnande) att deras personliga eller känsliga användaruppgifter krävs för att tillhandahålla eller förbättra funktioner som efterlever policyn i appen måste du uppfylla följande krav:

Du måste tillhandahålla en redogörelse i appen för hur du samlar in, använder och delar uppgifter. Redogörelsen i appen

- måste finnas i själva appen och inte bara i appbeskrivningen eller på en webbplats
- måste visas vid normal användning av appen och får inte kräva att användaren öppnar en meny eller inställningarna
- måste beskriva vilka uppgifter som appen har tillgång till eller samlar in
- måste redogöra för hur uppgifterna används och/eller delas
- får inte finnas enbart i en sekretesspolicy eller i användarvillkoren
- får inte slås ihop med andra redogörelser som inte har koppling till insamling av personliga och känsliga uppgifter

Redogörelsen i appen måste medfölja och direkt föregå en begäran om användarens samtycke och, om möjligt, en tillhörande begäran om körningsbehörigheter. Du får inte komma åt eller samla in några personliga eller känsliga användaruppgifter innan användaren har gett sitt samtycke. En begäran om samtycke i appen:

- Dialogrutan för samtycke måste visas på ett tydligt och otvetydigt sätt.

- Användaren måste ge sitt samtycke via en aktiv åtgärd (till exempel ett tryck för att godkänna eller en kryssruta som markeras).

- Om användaren navigerar bort från redogörelsen (till exempel genom att trycka på tillbakaknappen eller hemknappen) får det inte tolkas som samtycke.

- Meddelanden om samtycke får inte stängas automatiskt eller vara tidsbegränsade.

I syfte att säkerställa att Google Play förblir en säker och respektfull plattform har vi skapat standarder som definierar och förbjuder innehåll som är skadligt eller opassande för våra användare.

- En app som har åtkomst till användarens lista över installerade appar och inte behandlar dessa uppgifter som personuppgifter eller känsliga uppgifter i enlighet med sekretesspolicyn eller kraven på säker överföring och tydlig redogörelse.

- En app som har åtkomst till uppgifter i användarens telefon- eller kontaktbok och inte behandlar dessa uppgifter som personuppgifter eller känsliga uppgifter i enlighet med sekretesspolicyn eller kraven på säker överföring och tydlig redogörelse.

- Om användarens skärm spelas in i appen och sådan data inte behandlas som personliga eller känsliga uppgifter i enlighet med den här policyn.

En app som samlar in [enhetens plats](#) utan tydlig beskrivning av hur uppgifterna används i enlighet med kraven ovan .

Begränsningar av åtkomst till känsliga uppgifter

Utöver de krav som beskrivs ovan gäller de krav som anges i tabellen nedan för specifika aktiviteter.

Aktivitet	Krav
Appen hanterar ekonomiska uppgifter, betalningsuppgifter, eller id-nummer som har utfärdats av en myndighet	Personliga eller känsliga användaruppgifter som är relaterade till ekonomiska uppgifter, betalningsuppgifter eller id-nummer som har utfärdats av en myndighet får inte spridas till allmänheten.
Appen hanterar telefonboks- eller kontaktuppgifter som inte är tillgängliga för allmänheten	Vi tillåter inte obehörig publicering eller spridning av andra personers kontaktuppgifter som inte är tillgängliga för allmänheten.
Appen innehåller antivirus- eller säkerhetsfunktioner, till exempel skydd mot virus, skadliga program eller säkerhetsfunktioner	Appen måste visa en sekretesspolicy som tillsammans med eventuella meddelanden i appen förklarar vilka användaruppgifter som samlas in och överförs, hur de används och med vilka parter de delas.

Privacy Shield-ramverket mellan EU och USA

Om du har åtkomst till, använder eller behandlar personliga uppgifter med ursprung i EU eller Schweiz ("Personliga uppgifter inom EU") som direkt eller indirekt identifierar en individ och som har gjorts tillgängliga av Google måste du

följa alla tillämpliga lagar, direktiv, föreskrifter och regler gällande sekretess, datasäkerhet och dataskydd
endast ta del av, använda eller behandla Personliga uppgifter inom EU för ändamål som är förenliga med det samtycke som har inhämtats från den individ vilka dessa Personliga uppgifter inom EU avser
vidta lämpliga organisatoriska och tekniska åtgärder i syfte att skydda Personliga uppgifter inom EU mot förlust, obehörig användning och obehörig eller olaglig åtkomst, yppande, ändringar eller förstörelse
skyddsnivån som krävs enligt [uppfyllasekretessprinciperna för Privacy Shield](#).

Du är skyldig att regelbundet kontrollera efterlevnaden av dessa villkor. Om du vid något tillfälle inte kan uppfylla dessa villkor (eller om det finns en betydande risk att du inte kommer att kunna uppfylla dem) måste du omedelbart meddela oss via e-post på data-protection-office@google.com och antingen sluta att behandla Personliga uppgifter inom

EU med omedelbart verkan eller vidta rimliga och lämpliga åtgärder för att återställa skyddet till en tillfredsställande nivå.

Behörigheter

Behörighetsbegäranden ska vara begripliga för användarna. Du får endast begära behörigheter som krävs för att befintliga funktioner och tjänster i appen som står med i butiksuppgifterna ska kunna implementeras. Du får inte använda behörigheter som ger åtkomst till användaruppgifter eller enhetsinformation för syften som inte har uppgetts, inte har implementerats eller inte är tillåtna. Personliga och känsliga uppgifter som du får åtkomst till via behörigheter får aldrig säljas.

Begär behörighet att få åtkomst till uppgifter när de ska användas (via stegvis autentisering) så att användarna förstår varför behörigheten begärs i appen. Uppgifterna ska endast användas för de syften som användaren har gett sitt samtycke till. Om du vid ett senare tillfälle vill använda uppgifterna för andra syften måste du fråga användarna och försäkra dig om att du har deras godkännande till att använda uppgifterna för dessa ytterligare syften.

Begränsade behörigheter

I tillägg till ovanstående har begränsade behörigheter markerats med **Signatur** eller **Farlig** i vår utvecklardokumentation och omfattas av de ytterligare krav och begränsningar som följer:

Känsliga användar- eller enhetsuppgifter som du får åtkomst till via begränsade behörigheter får endast överföras till tredje part om det är nödvändigt för att tillhandahålla eller förbättra befintliga funktioner eller tjänster i appen där uppgifterna samlades in. Du får även överföra uppgifter som nödvändigt för att efterleva tillämpliga lagar eller vid förvärv, sammanslagningar eller försäljning av tillgångar om användarna meddelas på ett juridiskt adekvat sätt. All annan överföring eller försäljning av användaruppgifter är förbjuden.

Respektera användarnas beslut om de avvisar en begäran om begränsade behörigheter. Användarna får inte manipuleras eller tvingas att samtycka till behörigheter som inte är absolut nödvändiga. Du måste vidta rimliga åtgärder för att tillmötesgå användare som inte ger åtkomst till känsliga behörigheter (till exempel genom att låta användaren själv ange ett telefonnummer om han eller hon har nekat åtkomst till samtalsloggar).

Vissa begränsade behörigheter omfattas av ytterligare krav enligt nedan. Syftet med dessa begränsningar är att skydda användarnas integritet. Vi kan bevilja undantag från kraven nedan i begränsad utsträckning i de sällsynta fall där en app tillhandahåller en mycket användbar eller viktig funktion och det inte finns alternativa metoder för att tillhandahålla funktionen. Vi väger föreslagna undantag mot eventuell sekretess- eller säkerhetspåverkan för användarna.

Behörigheter för sms och samtalshistorik

Behörigheter för sms och samtalshistorik anses utgöra [personliga eller känsliga användaruppgifter](#) och omfattas av policyn om personliga och känsliga uppgifter och följande begränsningar:

Begränsad behörighet

Krav

Behörighetsgruppen Samtalshistorik (t.ex. READ_CALL_LOG, WRITE_CALL_LOG, PROCESS_OUTGOING_CALLS)

Appen måste medvetet ha registrerats som standardhanteraren för telefon och assistans på enheten.

Behörighetsgruppen Sms (t.ex. READ_SMS, SEND_SMS, WRITE_SMS, RECEIVE_SMS, RECEIVE_WAP_PUSH, RECEIVE_MMS)

Den måste medvetet ha registrerats som standardhanteraren för sms och assistans på enheten.

Appar som saknar funktioner för standardhantering av sms, telefon eller assistentfunktioner får inte ange i manifestfilen att behörigheterna ovan ska användas. Detta omfattar exempeltext i manifestfilen. Appen måste dessutom medvetet ha registrerats som standardhanterare av sms, telefon eller assistentfunktioner innan användarna uppmanas att godkänna någon av ovanstående behörigheter och måste omedelbart sluta använda behörigheten när den inte längre är standardhanterare. Mer information om tillåten användning och undantag finns på [den här sidan i hjälpcentret](#).

Appar får endast använda behörigheten (och eventuella uppgifter som härrör från behörigheten) i syfte att tillhandahålla godkända grundfunktioner i appen. Med appens grundfunktion avses huvudsyftet för appen. Detta kan utgöras av en uppsättning grundfunktioner som alla måste framhävas i dokumenteringen och lyftas fram i appbeskrivningen. Utan huvudfunktionen går appen sönder eller blir obrukbar. Överföring, delning eller licensierad användning av dessa uppgifter får endast ske i syfte att tillhandahålla grundfunktioner eller tjänster i appen och användningen får inte utökas för något annat syfte (t.ex. för att förbättra andra appar eller tjänster eller för annonsering och marknadsföring). Du får inte använda alternativa metoder (inklusive andra behörigheter, API:er eller tredjepartskällor) för att härleda uppgifter som tillskrivs behörigheter med koppling till samtalshistoriken och sms.

Platsbehörigheter

Uppdatering den 16 april 2020: Vi är medvetna om att vissa utvecklare kan behöva utföra omfattande arbete för att uppfylla kraven i platspolicyn. Därför får du mer tid på dig att göra de nödvändiga ändringarna. Du hittar tidsplaner och andra uppdateringar i vårt [hjälpcenter](#).

[Enhetens plats](#) anses utgöra personliga eller känsliga användaruppgifter och omfattas av policyn om [personliga och känsliga uppgifter](#) och följande krav:

Appar får inte komma åt data som skyddas med platsbehörigheter (till exempel ACCESS_FINE_LOCATION, ACCESS_COARSE_LOCATION,

ACCESS_BACKGROUND_LOCATION) när de inte längre krävs för att befintliga funktioner och tjänster i appen ska kunna användas.

Du får aldrig begära platsbehörighet av användarna om annonsering eller analyser är det enda syftet. Appar som utökar den tillåtna användningen av sådan data i syfte att visa annonser måste efterleva vår [annonspolicy](#).

Den minsta möjliga omfattningen (t.ex. ungefärlig plats i stället för exakt plats och i förgrunden i stället för i bakgrunden) som behövs för att tillhandahålla den befintliga funktionen eller tjänsten som kräver platsåtkomst ska begäras i appen och användare ska rimligen kunna anta att funktionen eller tjänsten behöver avgöra platsen med precisionen för den nivå som har begärts. Vi kan till exempel ge avslag för appar som begär eller kommer åt plats i bakgrunden utan rimligt skäl.

Platsåtkomst i bakgrunden får endast användas för att tillhandahålla funktioner som användaren har nytta av och som hänger ihop med appens huvudfunktion.

Platsåtkomst via behörigheten för förgrundstjänster (när appen bara har platsåtkomst i förgrunden, t.ex. medan appen används) är tillåten om användningen

har inletts som en direkt följd av en användarinitierad åtgärd i appen avslutas omedelbart när det avsedda användningsfallet för den användarinitierade åtgärden har slutförts i appen.

Appar som särskilt riktar sig till barn måste följa policyn för [Avsett för familjer](#).

Otillåten användning av enheter och nätverk

Vi tillåter inte appar som stör, skadar eller på ett otillåtet sätt får åtkomst till användarens enhet, andra enheter eller datorer, servrar, nätverk, programmeringsgränssnitt (API:er) eller tjänster, inklusive men utan begränsning till andra appar på enheten, Googles tjänster eller en auktoriserad operatörs nätverk.

Alla appar på Google Play måste följa systemoptimeringskraven för Android som beskrivs i [riktlinjerna för grundläggande appkvalitet för Google Play](#).

I syfte att säkerställa att Google Play förblir en säker och respektfull plattform har vi skapat standarder som definierar och förbjuder innehåll som är skadligt eller opassande för våra användare.

Appar som blockerar eller stör en annan app som visar annonser.

Fuskappar som påverkar spelet i andra appar.

Appar som förmedlar eller ger instruktioner om hur man hackar tjänster, programvara eller maskinvara, eller hur man kringgår säkerhetsskydd.

Appar som får åtkomst till eller använder en tjänst eller ett API på ett sätt som bryter mot dess användarvillkor.

Appar som försöker kringgå [systemets strömhantering](#) som inte uppfyller [kraven för godkännande](#).

Appar som underlättar proxytjänster till tredje part får endast göra så om detta är appens primära och grundläggande syfte som visas för användarna.

Skadligt beteende

Vi tillåter inte appar som stjälar uppgifter, i hemlighet övervakar eller skadar användare eller som är skadliga på andra sätt.

En app som distribueras via Google Play får inte ändra, ersätta eller uppdatera sig själv med någon annan metod än Google Plays uppdateringsfunktion. Dessutom får enbart körbar kod (t.ex. filformaten dex, JAR och .so) från Google Play laddas ned av en app. Denna begränsning gäller inte för kod som körs i en virtuell dator och som har begränsad tillgång till Android API (till exempel JavaScript i WebView eller webbläsare).

Ytterligare appresurser (till exempel speltillgångar) får endast laddas ned om användaren annars inte kan fortsätta att använda appen. Resursnedladdningar måste efterleva alla Google Plays policyer. Före nedladdningen ska användarna meddelas i appen och nedladdningsstorleken tydligt meddelas.

Övervakningsappar eller kommersiella spionprogram är uttryckligen förbjudna på Google Play. Endast appar som uppfyller kraven i våra policyer och som har utformats och marknadsförts för föräldrakontroll (inklusive familjeadministration) eller företagshantering får distribueras med spårnings- och rapportfunktioner i Butiken, förutsatt att de uppfyller alla ovanstående krav.

Följande förbjuds uttryckligen:

- Virus, trojaner, skadliga program, spionprogram och annan skadlig programvara.

- Appar som länkar till eller förmedlar distribution eller installation av skadlig programvara.

- Appar eller SDK:er där körbar kod, till exempel dex-filer och plattformsspecifik kod, laddas ned från en annan källa än Google Play.

- Appar som skapar eller utnyttjar säkerhetsbrister.

- Appar som stjälar en användares autentiseringsinformation (till exempel användarnamn eller lösenord) eller som härmar andra appar eller webbplatser för att lura användare att avslöja personuppgifter eller autentiseringsinformation.

- Appar får inte utan samtycke visa överifierade eller riktiga telefonnummer, kontakter eller adresser till personer eller rättssubjekt eller uppgifter som kan kopplas till en specifik individ eller ett specifikt rättssubjekt.

- Appar som installerar andra appar på en enhet utan användarens föregående samtycke.

- Appar där ett nätverk för innehållsleverans (NFI) används för nedladdningar men användaren inte meddelas eller informeras om nedladdningsstorleken före nedladdningen.

- Appar som är avsedda att i hemlighet registrera enhetsanvändningen, till exempel kommersiella spionappar.

Appar som övervakar eller följer en användares beteende på en enhet måste följa dessa krav:

Appar får inte presenteras som lösningar för spioneri eller hemlig övervakning.

Appar får inte dölja spårningsbeteende eller försöka vilseleda användare om sådana funktioner.

Användarna måste se ett beständigt meddelande och en unik ikon som tydligt identifierar appen.

Appar och appuppgifter på Google Play får inte innehålla funktioner som aktiverar eller ger åtkomst till funktioner som bryter mot dessa villkor, till exempel länkar till APK utanför Google Play som inte följer villkoren.

Du är själv ansvarig för att avgöra om appen är laglig i det land eller på den plats där den finns tillgänglig. Appar som befinns vara olagliga på platser där de publiceras tas bort.

Kolla in vårt [program för förbättrad appsäkerhet](#) om du vill veta mer om de senaste säkerhetsproblemen som har flaggats för utvecklare på Google Play. Information om säkerhetsrisker och åtgärder hittar du via länkarna till kampanjernas supportsidor.

Vilseledande funktioner

Vi tillåter inte appar som försöker vilseleda användare eller möjliggör ohederligt beteende. Detta omfattar men är inte begränsat till appar som bedöms innehålla funktioner som är tekniskt omöjliga. Appar ska ha en korrekt redogörelse, beskrivning och bilder eller video av hur funktionerna fungerar i alla delar av metadatan och de ska fungera på ett sätt som användaren har rimlig anledning att förvänta sig. Appar får inte imitera funktioner eller varningar från operativsystem eller andra appar. Eventuella ändringar i enhetsinställningar måste göras med användarens vetskap och samtycke och vara lätta att återställas av användaren.

Vilseledande påståenden

Vi tillåter inte appar som innehåller falska eller vilseledande uppgifter eller påståenden i appens beskrivning, titel, ikon, skärmdumpar och så vidare.

I syfte att säkerställa att Google Play förblir en säker och respektfull plattform har vi skapat standarder som definierar och förbjuder innehåll som är skadligt eller opassande för våra användare.

Appar som beskriver sina funktioner på ett missvisande eller otydligt sätt:

En app som påstås vara ett racingspel i beskrivningen och skärmdumparna, men i själva verket är ett pusselspel med en bild av en bil.

En app som påstås vara en antivirusapp, men som bara innehåller en textbeskrivning av hur virus kan tas bort.

Namn på utvecklare eller appar som på ett felaktigt sätt anger sin aktuella status eller resultat på Play. (T.ex. "Redaktionens val", "Bästa appen", "Storsäljare").

Appar med medicinska eller hälsorelaterade funktioner och innehåll som är vilseledande eller potentiellt skadliga.

Appar som utges för att ha funktioner som är omöjliga att implementera.

Appar som är felaktigt kategoriserade.

Bevisligen vilseledande innehåll som kan påverka röstningsprocesser.

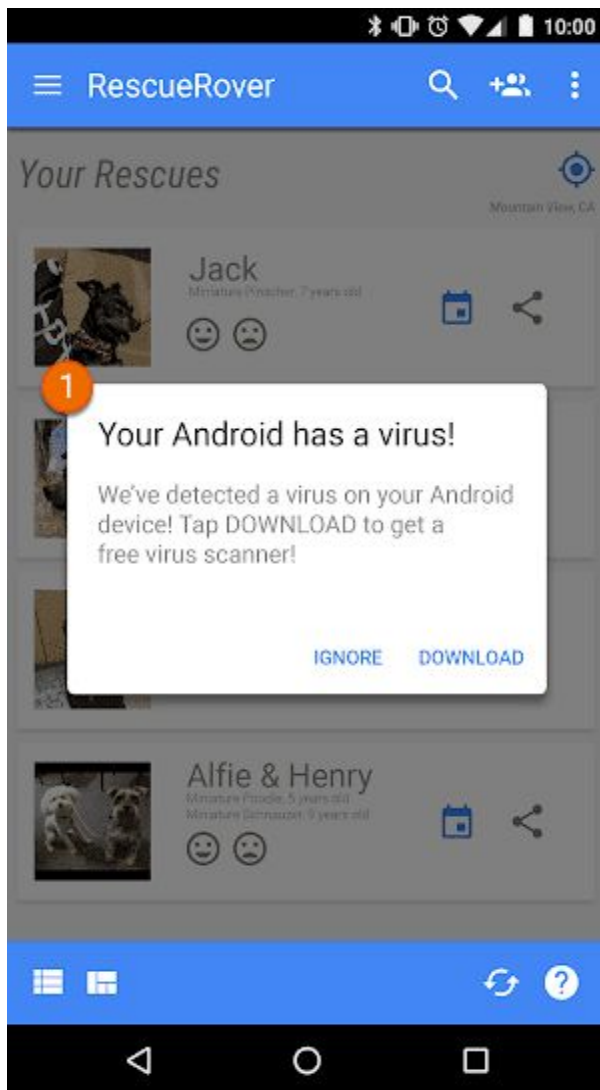
Appar som felaktigt påstås ha anknytning till en myndighet eller tillhandahålla eller förmedla myndighetstjänster som appen inte har auktoriserats för.

Obehörig användning eller imitation av systemfunktioner

Vi tillåter inte appar eller annonser som härmar eller stör systemets funktioner, till exempel aviseringar eller varningar. Aviseringar på systemnivå får bara användas för viktiga funktioner appen, till exempel en flygbolagsapp som meddelar användarna om specialerbjudanden eller ett spel som meddelar användarna om kampanjer i spelet.

I syfte att säkerställa att Google Play förblir en säker och respektfull plattform har vi skapat standarder som definierar och förbjuder innehåll som är skadligt eller opassande för våra användare.

Appar eller annonser som levereras via ett systemmeddelande eller en varning:



① Systemmeddelandet som visas i appen används för att visa en annons.

Fler exempel som rör annonser finns i [annonspolicyn](#).

Vilseledande ändringar av enhetsinställningar

Vi tillåter inte appar som ändrar användarens enhetsinställningar eller funktioner utanför appen utan användarens vetskap och samtycke. Enhetsinställningar och enhetsfunktioner omfattar systemets och webbläsarens inställningar, bokmärken, genvägar, ikoner, widgetar och visningen av appar på startskärmen.

Vi tillåter inte heller:

Appar som ändrar enhetsinställningar eller enhetsfunktioner med användarens samtycke, men på ett sätt som inte är lätt att återställa.

Appar eller annonser som ändrar enhetens inställningar eller funktioner som en tjänst till tredje part eller i annonseringssyfte.

Appar som vilseleder användarna för att få dem att ta bort eller inaktivera tredje parts appar eller ändra enhetsinställningar eller enhetsfunktioner.

Appar som uppmuntrar eller sporrar användarna till att ta bort eller inaktivera appar från tredje part eller ändra enhetsinställningar eller enhetsfunktioner. Detta gäller inte för verifierbara säkerhetstjänster.

Möjliggöra ohederligt beteende

Vi tillåter inte appar som hjälper användare att vilseleda andra eller innehåller funktioner som är bedrägliga på något sätt. Detta omfattar men är inte begränsat till appar som skapar eller underlättar skapande av id-kort, personnummer, pass, examensbevis, kreditkort eller körkort.

Appar ska ha en korrekt redogörelse, titel, beskrivning och bilder eller video av appens funktioner och/eller innehåll och ska fungera på ett sätt som användaren har rimlig anledning att förvänta sig.

Påståenden om att en app är en skämtapp eller ska användas i underhållningssyfte (eller annat synonymt uttryck) undantar inte appen från våra policyer.

Manipulerad media

Vi tillåter inte appar som främjar eller skapar falsk eller vilseledande information eller påståenden med hjälp av bilder, videor och/eller text. Vi tar bort appar som anses främja eller sprida bevisligt vilseledande eller bedrägliga bilder, videor och/eller texter som kan vara skadliga med avseende på känsliga händelser, politik, sociala frågor eller annat som är av intresse för allmänheten.

Appar som manipulerar eller förändrar media utöver vedertagna och redaktionella klarhets- och kvalitetsjusteringar måste tydligt meddela eller vattenstämpla manipulerad media om det kanske inte framgår för vanliga människor att den har förändrats. Undantag kan ges för media som är av intresse för allmänheten eller uppenbart satir eller parodi.

I syfte att säkerställa att Google Play förblir en säker och respektfull plattform har vi skapat standarder som definierar och förbjuder innehåll som är skadligt eller opassande för våra användare.

Appar som lägger till en offentlig person i en demonstration vid en politiskt känslig händelse.

Appar som använder offentliga personer eller media från en känslig händelse i syfte att marknadsföra funktioner för att manipulera media i appens butiksuppgifter.

Appar som manipulerar medieklipp för att efterlikna en nyhetssändning.

Felaktig framställning

Vi tillåter inte appar eller utvecklarkonton i annan persons eller organisations namn eller som döljer eller felaktigt framställer ägarens identitet eller vad det primära syftet är. Vi tillåter inte appar eller utvecklarkonton som ägnar sig åt samordnade aktiviteter i syfte att vilseleda användare. Detta inbegriper men är inte begränsat till appar och utvecklarkonton som döljer eller felaktigt framställer sitt ursprungsland och som riktar innehåll till användare i ett annat land.

Skadlig programvara

Vår policy om skadlig programvara är enkel: ingen skadlig programvara ska finnas på Google Play Butik, i användarnas enheter eller resten av Androids ekosystem. Utifrån denna grundläggande princip strävar vi efter att Androids ekosystem ska vara säkert för användarna och deras Android-enheter.

All kod som kan utgöra en risk för användare, användarnas data eller enheter räknas som skadlig programvara. Skadlig programvara omfattar men är inte begränsat till potentiellt skadliga appar, binärfiler eller modifiering av ramverk inom kategorier som trojaner, nätfiske och spionprogram. Vi uppdaterar ständigt listan och lägger till nya kategorier.

Skadlig programvara kan vara av olika typer eller ha skilda funktioner, men målet är oftast ett av följande:

- Få tillgång till användarens enhet.

- Få kontroll över användarens enhet.

- Aktivera fjärrstyrda åtgärder så att angriparen kan komma åt, använda eller på annat sätt utnyttja den infekterade enheten.

- Överföra personuppgifter eller användaruppgifter från enheten utan tydlig redogörelse och utan samtycke.

- Sprida skräppost eller ge kommandon från den infekterade enheten i syfte att påverka andra enheter eller nätverk.

- Utsätta användaren för bedrägeri.

Det finns potentiellt skadliga appar, binärfiler och modifieringar för ramverk. Dessa kan vara oavsiktligt skadliga. Detta beror på att appar, binärfiler och modifieringar för ramverk kan fungera på olika sätt utifrån olika variabler. Därför kan något vara skadligt på en Android-enhet men inte utgöra någon risk alls på en annan. Om till exempel en enhet har den senaste versionen av Android påverkas den inte av skadliga appar som utnyttjar utfasade API:er, medan en enhet som fortfarande använder en tidigare version av Android kan utsättas för fara. Appar, binärfiler och modifieringar för ramverk flaggas som skadliga eller potentiellt skadliga om de utgör en tydlig risk för vissa eller alla Android-enheter och -användare.

Det är viktigt för oss att användarna ska förstå hur deras enhet används samt att ekosystemet är både säkert och har utrymme för både innovation och en trygg användarupplevelse. Det är grundstenen för kategorierna för skadlig programvara nedan.

Besök [Google Play Protect](#) om du vill veta mer.

Bakdörrar

Kod som möjliggör att oönskade eller potentiellt skadliga fjärrstyrda åtgärder utförs på en enhet.

Dessa åtgärder kan omfatta beteenden som skulle placera appen, binärfilen eller modifieringen av ramverket i en av de andra kategorierna för skadlig programvara om de utfördes automatiskt. Ordet bakdörr används i allmänhet som en beskrivning av hur en potentiellt skadlig åtgärd kan ske på en enhet och stämmer därför inte helt överens med kategorier som faktureringsbedrägeri eller kommersiella spionprogram. Därför kan bakdörrar under vissa omständigheter behandlas som säkerhetsbrister i Google Play Protect.

Faktureringsbedrägeri

Kod som automatiskt debiterar användaren på ett avsiktligt bedrägligt sätt.

Bedrägeri via mobilräkningen delas in i sms-bedrägeri, samtalsbedrägeri och avgiftsbedrägeri.

Sms-bedrägeri

Kod som debiterar användare för betal-sms som skickats utan samtycke eller som försöker dölja sms-aktiviteter genom att gömma avtal eller sms från mobiloperatören där användaren aviseras om avgifter eller får bekräftelse på prenumerationer.

Viss kod introducerar ytterligare funktioner som möjliggör sms-bedrägeri, även om den tekniskt informerar om att sms skickas. Det kan till exempel innebära att delar av ett avtal döljs från användaren och blir oläsliga eller att sms från mobiloperatören till användaren med avisering om avgifter eller bekräftelse på prenumerationer under vissa förutsättningar inte visas.

Samtalsbedrägeri

Kod som debiterar användare genom att ringa till betalnummer utan användarens samtycke.

Avgiftsbedrägeri

Kod som lurar användare till att prenumerera på eller köpa innehåll via mobilräkningen.

I avgiftsbedrägeri ingår all typ av fakturering med undantag för betal-sms och betalsamtal. Några exempel är direktdebitering via operatören, trådlös åtkomstpunkt (WAP) och överföring av telefonens saldo. Bedrägeri relaterat till WAP tillhör den vanligaste formen av avgiftsbedrägeri. Användare kan luras till att klicka på en knapp på en transparent WebView som lästs in i bakgrunden. När åtgärden utförs startar en återkommande prenumeration, och bekräftelsemeddelandet kapas ofta så att användare inte ska upptäcka den ekonomiska transaktionen.

Kommersiella spionprogram

Kod som överför personliga uppgifter från enheten utan tydlig avisering och utan samtycke och som inte visar en beständig avisering om att detta händer.

Kommersiella spionprogram överför data till andra än leverantören av de potentiellt skadliga apparna. Legitima former av sådana appar kan användas av föräldrar som vill se var deras barn befinner sig. Dessa appar får inte användas för att spåra någon (till exempel en partner) utan personens vetskap eller tillåtelse om inte en beständig avisering visas medan data överförs.

Överbelastningsattack (DoS)

Kod som, utan användarens vetskap, utför en överbelastningsattack (DoS) eller är en del av en distribuerad överbelastningsattack mot andra system och resurser.

Detta kan till exempel ske genom att ett stort antal HTTP-förfrågningar skickas i syfte att åstadkomma mycket hög belastning på fjärrservrar.

Fientliga nedladdare

Kod som i sig inte är potentiellt skadlig men som laddar ned andra appar som är det.

Koden kan vara en fientlig nedladdare om

- det finns skäl att misstänka att den skapats för att sprida potentiellt skadliga appar och har laddat ned sådana appar eller om den innehåller kod som kan ladda ned och installera appar eller
- minst 5 % av de appar som den har laddat ned är potentiellt skadliga appar med en lägsta gräns på 500 faktiska nedladdningar (25 faktiska nedladdningar av potentiellt skadliga appar).

Större webbläsare och fildelningsappar betraktas inte som fientliga nedladdare så länge som

- de inte inleder nedladdningar utan interaktion med användaren, och
- alla nedladdningar av potentiellt skadliga appar initieras av användare som samtycker.

Hot som inte drabbar Android

Kod som innehåller hot som inte drabbar Android.

Dessa appar är inte skadliga för Android-enheter eller Android-användare, men de har komponenter som kan vara skadliga på andra plattformar.

Nätfiske

Kod som utges för att komma från en betrodd källa, begär åtkomst till användarens autentiserings- eller faktureringsuppgifter och skickar datan till tredje part. Den här kategorin omfattar även kod som kapar användaruppgifter när de skickas.

Målet med nätfiske är att komma över bland annat användaruppgifter till banktjänster, kreditkortsnummer och kontouppgifter för sociala nätverk och spel online.

Otillåten användning av eskalerade behörigheter

Kod som får tillgång till systemet genom att skada appens sandlåda, ändra eller inaktivera åtkomsten till viktiga säkerhetsfunktioner eller skaffa sig högre behörigheter.

Exempel:

- Appar som inte följer Androids behörighetsmodell eller stjälar användaruppgifter (till exempel OAuth-token) från andra appar.

- Appar som utnyttjar funktioner på otillåtna sätt så att det inte går att stoppa eller avinstallera dem.

- Appar som inaktiverar SELinux.

Appar som eskalerar behörigheter för att kunna roota enheter utan användarens tillstånd klassificeras som rootningsappar.

Utpressningsvirus

Kod som delvis eller fullständigt tar kontroll över en enhet eller data på en enhet och kräver att användaren betalar eller utför åtgärder för att få tillbaka kontrollen.

En del utpressningsvirus krypterar data på enheten och kräver betalning i utbyte mot att datan dekrypteras och/eller utnyttjar administratörsfunktioner så att viruset inte kan tas bort av den genomsnittliga användaren. Exempel:

- Låser användaren ute från enheten och kräver pengar i utbyte mot att ge tillbaka kontrollen.

- Krypterar data på enheten och kräver betalning, till synes i utbyte mot att dekryptera datan.

- Utnyttjar funktioner för att hantera policyer för enheten och omöjliggöra borttagning av användaren.

Kod som distribueras tillsammans med enheten vars huvudsyfte är att minska enhetshanteringen kan undantas från utpressningsviruskategorin om den uppfyller kraven om säker låsning och hantering, samtycke samt tydligt informerar användaren.

Rootning

Kod som rootar enheten.

Det är skillnad på icke-skadlig och skadlig rootningskod. Icke-skadliga rootningsappar informerar exempelvis användaren innan de rootar enheten, och de utför inga andra av de potentiellt skadliga åtgärderna i de övriga kategorierna.

Skadliga rootningsappar meddelar inte användaren att enheten är på väg att rootas, eller så meddelar de användaren om rootningen i förväg men utför även andra åtgärder som hör hemma i samma kategori som andra potentiellt skadliga appar.

Spam

Kod som skickar oönskade meddelanden till användarens kontakter eller förvandlar enheten till ett skräppostrelä.

Spionprogram

Kod som överför personuppgifter från enheten utan tydligt meddelande och utan samtycke.

Om till exempel något av följande överförs utan redogörelse eller på ett för användaren oväntat sätt klassas koden som spionprogram:

- Kontaktlistor

- Foton eller andra filer som inte ägs av appen eller som överförs från SD-kortet

- Innehåll från användarens e-postkonto

- Samtalshistorik

- Sms-loggar

- Webbhistorik eller bokmärken från standardwebbläsaren

- Information från katalogerna /data/ i andra appar

Allt spionage på användaren kan flaggas som spionprogram. Till exempel om ljud eller samtal på telefonen spelas in eller appdata stjäls.

Trojan

Kod som verkar vara genuin, till exempel ett spel som utges för att bara vara ett spel, men som utför oönskade åtgärder mot användaren.

Den här klassificeringen används oftast tillsammans med andra kategorier för potentiella skadliga appar. En trojan har en harmlös komponent och en skadlig, dold komponent. Till exempel ett spel som skickar avgiftsbelagda sms från enheten i bakgrunden utan användarens vetskap.

Information om ovanliga appar

Nya och unika appar kan klassificeras som ovanliga om det inte finns tillräcklig information för att säkerställa att de är säkra i Google Play Protect. Detta innebär inte nödvändigtvis att appen är skadlig, bara att den behöver granskas närmare för att säkerställa att den är säker.

Information om bakdörrskategorin

Klassificeringen för kategorin om programvara som är skadlig på grund av en bakdörr beror på hur koden fungerar. Ett villkor för att koden ska klassas som en bakdörr är att den möjliggör

beteenden som skulle placera koden i en av de andra kategorierna för skadlig programvara om den kördes automatiskt. Om till exempel dynamisk kod kan läsas in i appen och sms samlas in med hjälp av den dynamiskt inlästa koden klassificeras den som programvara som är skadlig på grund av en bakdörr.

Om godtycklig kod kan köras i appen och vi inte har någon anledning att tro att koden har lagts till i skadesyfte kan däremot appen anses ha en säkerhetsbrist i stället för en bakdörr. Då blir utvecklaren ombedd att korrigera programmet.

Vi tillåter inte appar som innehåller vilseledande eller störande annonser. Annonser får bara visas i appen som de förekommer i. Vi anser att annonser som visas i din app är en del av appens innehåll. Alla annonser som visas i appen måste därför efterleva våra policyer. Klicka [här](#) om du vill läsa våra policyer gällande annonser för hasardspel.

Google Play har stöd för ett flertal vinstgivande strategier för utvecklare och användare, bland annat sponsrad distribution, produkter i appar, prenumerationer och annonsbaserade modeller. Vi kräver att du följer våra policyer för att ge användaren bästa möjliga upplevelse.

Payments

Appar som erbjuder köp i butiken eller i appen måste följa följande riktlinjer:

Köp i butiken: Utvecklare som säljer appar och nedladdningar på Google Play måste använda Google Plays betalningssystem.

Köp i appar:

Utvecklare som säljer åtkomst till spelinnehåll eller produkter i ett spel som laddats ned på Google Play måste använda [fakturerings via Google Play för köp i appar](#) som betalningsmetod.

Utvecklare som säljer produkter i något annat slags app som laddats ned på Google Play måste använda [fakturerings via Google Play för köp i appar](#) som betalningsmetod utom i följande fall:

- Betalningen gäller enbart för fysiska produkter

- Betalningen gäller digitalt innehåll som kan konsumeras utanför själva appen (t.ex. låtar som kan spelas upp i andra musikspelare).

Virtuella valutor i appar får bara användas i den app eller det spel valutan köptes för.

Utvecklare får inte ge användarna vilseledande information om apparna eller apparnas tjänster, varor, innehåll och funktioner som de säljer. Om produktbeskrivningen på Google Play hänvisar till funktioner i appen som är avgiftsbelagda eller medför ytterligare avgifter måste det klart framgå i beskrivningen att användarna måste betala för att använda dessa funktioner.

I appar som innehåller funktioner för att få slumpmässigt utvalda virtuella objekt vid köp (dvs. "lootboxes") måste oddsen för att få sådana objekt tydligt meddelas före köpet.

Prenumerationer

Du som utvecklare får inte vilseleda användare om de prenumerationstjänster eller det innehåll du erbjuder i appen. Det är avgörande att du är tydlig i kampanjer i appar eller på välkomstkärmar.

I appen: Du måste vara transparent om erbjudandet. Detta omfattar dina erbjudandevillkor, kostnaden för prenumerationen, hur lång faktureringsperioden är och om en prenumeration krävs för att använda appen. Användarna ska kunna granska informationen utan att behöva utföra ytterligare åtgärder.

I syfte att säkerställa att Google Play förblir en säker och respektfull plattform har vi skapat standarder som definierar och förbjuder innehåll som är skadligt eller opassande för våra användare.

- Månadsprenumerationer där användarna inte informeras om att debitering och förnyelse av prenumerationen sker varje månad.

- Årsprenumerationer där priset per månad framhävs.

- Priser och villkor för prenumerationer som inte har lokaliserats fullständigt.

- Kampanjer i appar där det inte framgår att användaren får tillgång till innehållet utan en prenumeration (om tillgängligt).

- Missvisande namn på SKU:er för prenumerationer, till exempel Gratis provperiod för en prenumeration som förnyas automatiskt.

Get AnalyzeAPP Premium

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

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

Try for \$12.50!

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

- ① Knappen Stäng syns inte tydligt och det kanske inte framgår för användarna att de får tillgång till funktionerna utan att tacka ja till prenumerationserbudet.
- ② Priset för erbjudandet visas bara per månad och det kanske inte framgår för användarna att de debiteras för sex månader i taget när de börjar prenumerera.
- ③ Endast introduktionspriset för erbjudandet visas och det kanske inte framgår för användarna att de debiteras automatiskt när introduktionsperioden löper ut.
- ④ Erbjudandet ska lokaliseras på samma språk som användarvillkoren så att användarna kan göra sig en bild av hela erbjudandet.

Gratis provperioder och introduktionserbjudanden

Innan användare kan registrera sig för prenumerationen: Du måste beskriva villkoren för erbjudandet så tydligt som möjligt, bland annat tidslängden, priset och ange vilket innehåll och

vilka tjänster som är tillgängliga. Se till att informera användarna om hur och när en gratis provperiod övergår i en betalprenumeration, hur mycket betalprenumerationen kostar och att användaren kan avsluta prenumerationen om betalversionen inte önskas.

I syfte att säkerställa att Google Play förblir en säker och respektfull plattform har vi skapat standarder som definierar och förbjuder innehåll som är skadligt eller opassande för våra användare.

Erbjudanden där det inte tydligt meddelas hur länge introduktionspriset eller den gratis provperioden varar.

Erbjudanden där det inte tydligt meddelas att användaren automatiskt registreras för en betalprenumeration i slutet av erbjudandeperioden.

Erbjudanden där det inte tydligt framgår att användaren får tillgång till innehållet även utan en provperiod (om tillgängligt).

Priser och villkor för erbjudanden som inte har lokaliserats fullständigt.

The image is a screenshot of a mobile application interface for 'Get AnalyzeAPP Premium'. It features a light blue background with a dark blue border. At the top, the title 'Get AnalyzeAPP Premium' is displayed in a bold, dark blue font, with a small green circle containing the number '1' next to it. Below the title is a circular illustration of a person with dark hair, wearing a blue shirt, sitting at a desk and looking at a computer monitor. The monitor displays various data visualizations, including a bar chart and a pie chart. Below the illustration, the text '16 issues found in your data!' is written in a bold, dark blue font, followed by 'Subscribe to see how we can help' in a smaller, lighter blue font. To the left of this text is a green circle containing the number '2'. Below the text is a dark blue button with a white star icon and the text 'Try for free now!'. Below the button is a green circle containing the number '3', followed by the text 'During your free trial, experience all of the great features our app can offer!'. At the bottom, there is a green circle containing the number '4', followed by the text 'Cancele su suscripción en cualquier momento. Por favor, consulte nuestra política de privacidad para más información.' in a smaller, lighter blue font.

- ① Knappen Stäng syns inte tydligt och det kanske inte framgår för användarna att de får tillgång till funktionerna utan att registrera sig för en gratis provperiod.
- ② I erbjudandet lyfts den gratis provperioden fram och det kanske inte framgår för användarna att de debiteras automatiskt när provperioden löpt ut.
- ③ Det anges inte i erbjudandet hur lång provperioden är och det kanske inte framgår för användarna hur länge de får gratis tillgång till prenumerationens innehåll.
- ④ Erbjudandet ska lokaliseras på samma språk som användarvillkoren så att användarna kan göra sig en bild av hela erbjudandet.

Hantera och säga upp prenumerationer

Utvecklare måste tydligt meddela hur användare kan hantera eller avsluta sin prenumeration på appen.

Om en användare säger upp en prenumeration som köpts från en app på Google Play är vår policy att användaren inte får en återbetalning för den innevarande faktureringsperioden. Användaren fortsätter i stället att få innehållet i prenumerationen under återstoden av den innevarande faktureringsperioden, oavsett vilket datum prenumerationen sades upp. Användarens uppsägning börjar gälla när den innevarande faktureringsperioden är slut.

Du (som innehålls- eller åtkomstleverantör) kan införa en mer flexibel återbetalningspolicy direkt för dina användare. Det är ditt ansvar att meddela användarna om eventuella ändringar i din prenumurations-, uppsägnings- eller återbetalningspolicy och att se till att de följer gällande lag.

Vi tillåter inte appar som innehåller vilseledande eller störande annonser. Annonser får bara visas i appen som de förekommer i. Vi anser att annonser som visas i din app är en del av appens innehåll. Alla annonser som visas i appen måste därför efterleva våra policyer. Klicka [här](#) om du vill läsa våra policyer gällande annonser för hasardspel.

Vi tillåter inte appar som innehåller vilseledande eller störande annonser. Annonser får bara visas i appen som de förekommer i. Vi anser att annonser som visas i din app är en del av appens innehåll. Alla annonser som visas i appen måste därför efterleva våra policyer. Klicka [här](#) om du vill läsa våra policyer gällande annonser för hasardspel.

Använda platsdata för annonser

Appar där användningen av behörighetsbaserad data om enhetens plats har utökats i syfte att visa annonser omfattas av policyn om [personliga och känsliga uppgifter](#). De måste dessutom uppfylla följande krav:

Det måste vara tydligt för användaren att behörighetsbaserad data om enhetens plats används eller samlas in i annonssyfte. Det måste även dokumenteras i appens obligatoriska sekretesspolicy, bland annat med länkar till relevanta sekretesspolicyer för annonsnätverk som rör användningen av platsdata.

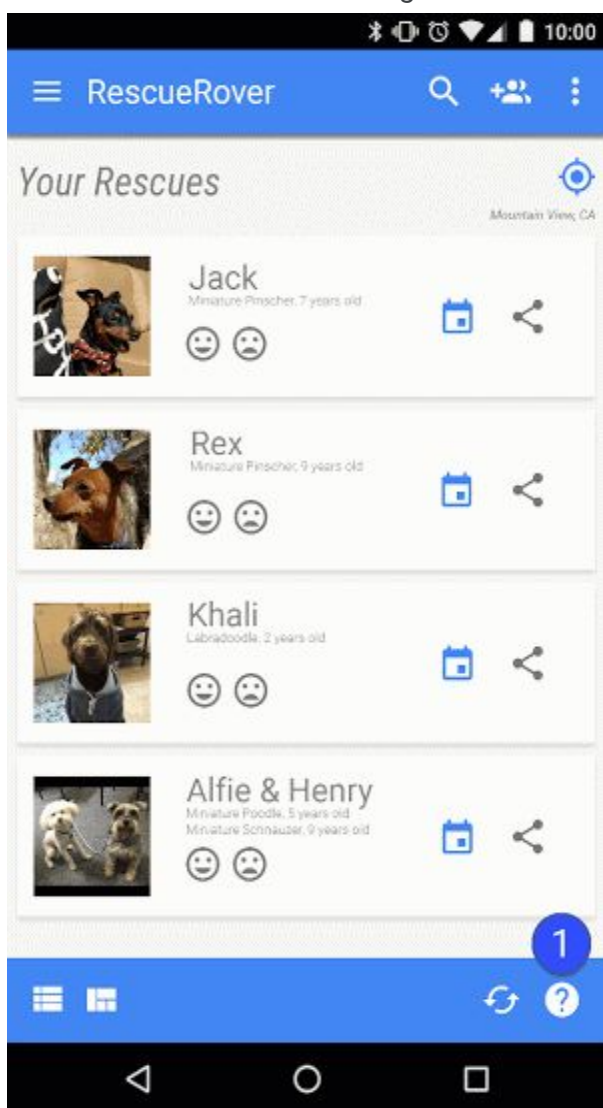
I enlighet med kraven för **platsbehörighet** får platsbehörighet endast begäras för implementering av befintliga funktioner eller tjänster i appen. Du får inte begära platsbehörighet för enheten om annonsvisning är det enda syftet.

Vilseledande annonser

Annonser får inte efterlikna eller imitera användargränssnittet i en app eller systemmeddelanden eller varningar i ett operativsystem. Det måste vara tydligt för användaren vilken app som visar varje annons.

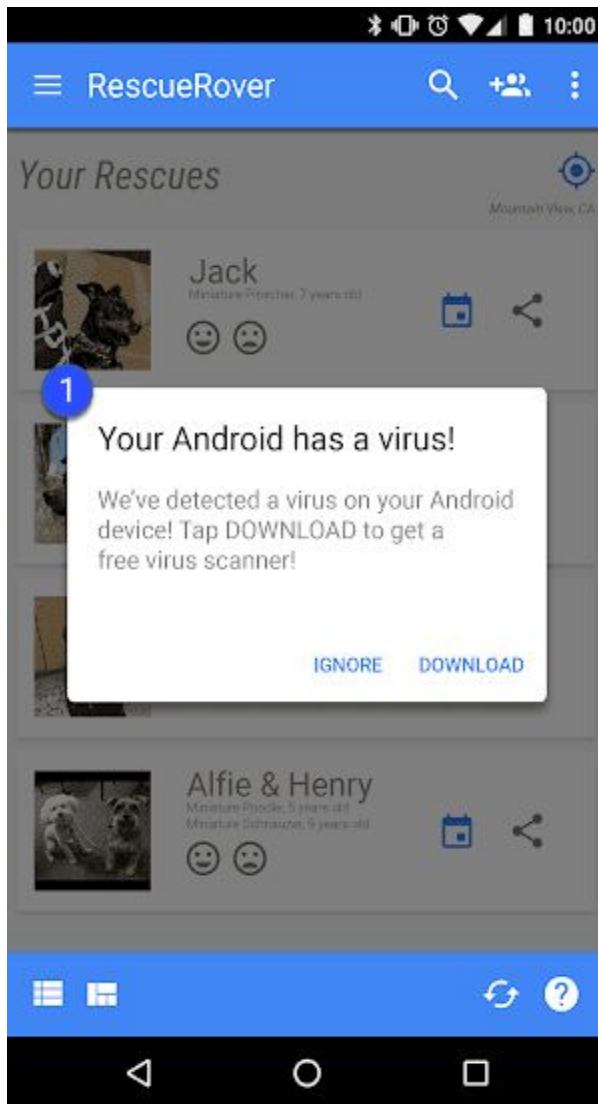
I syfte att säkerställa att Google Play förblir en säker och respektfull plattform har vi skapat standarder som definierar och förbjuder innehåll som är skadligt eller opassande för våra användare.

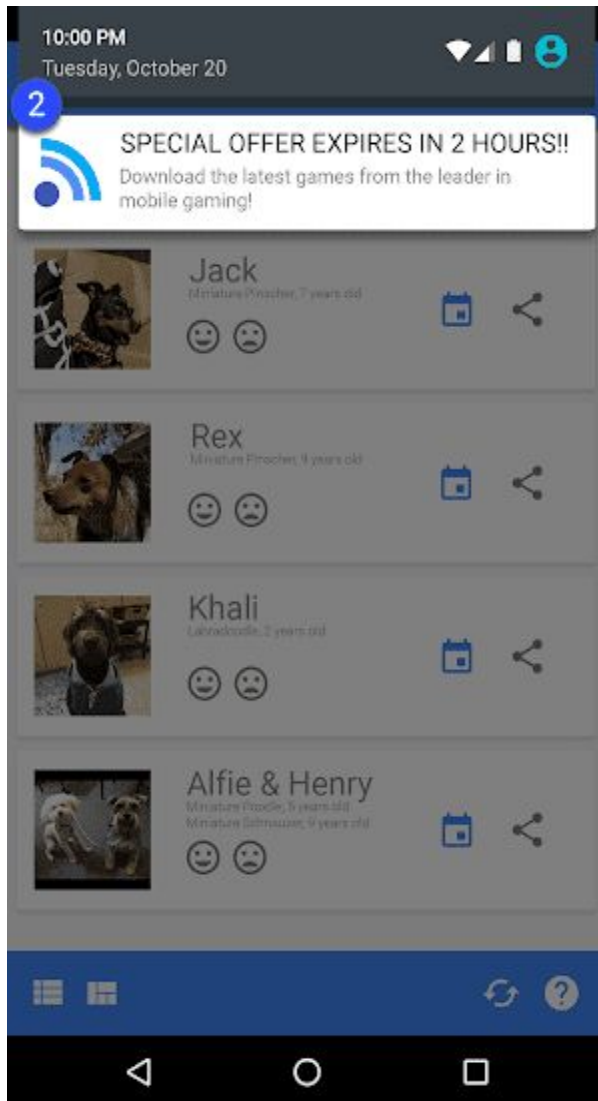
Annonser som liknar användargränssnittet i en app:



① Frågetecknet i den här appen är en annons som leder till en extern målsida.

Annonser som liknar ett systemmeddelande:





① ② Exempler ovan visar annonser som liknar olika systemmeddelanden.

Intäktsgenerering via låsskärm

Appar får inte införa annonser eller funktioner som genererar intäkter på enheters låsskärmar, såvida inte appens enda syfte är att fungera som låsskärm.

Störande annonser

Annonser ska inte visas på ett sätt som leder till oavsiktliga klick. Det är förbjudet att tvinga användare att klicka på annonser eller uppgive personuppgifter för att kunna använda appen till fullo.

Mellansidesannonser får bara visas i appen som de ingår i. Om mellansidesannonser eller andra annonser som stör normal användning av appen visas måste de gå att stänga utan negativa konsekvenser.

I syfte att säkerställa att Google Play förblir en säker och respektfull plattform har vi skapat standarder som definierar och förbjuder innehåll som är skadligt eller opassande för våra användare.

Annonser som tar upp hela skärmen eller stör normal användning, och som inte har något tydligt sätt att stänga annonsen:



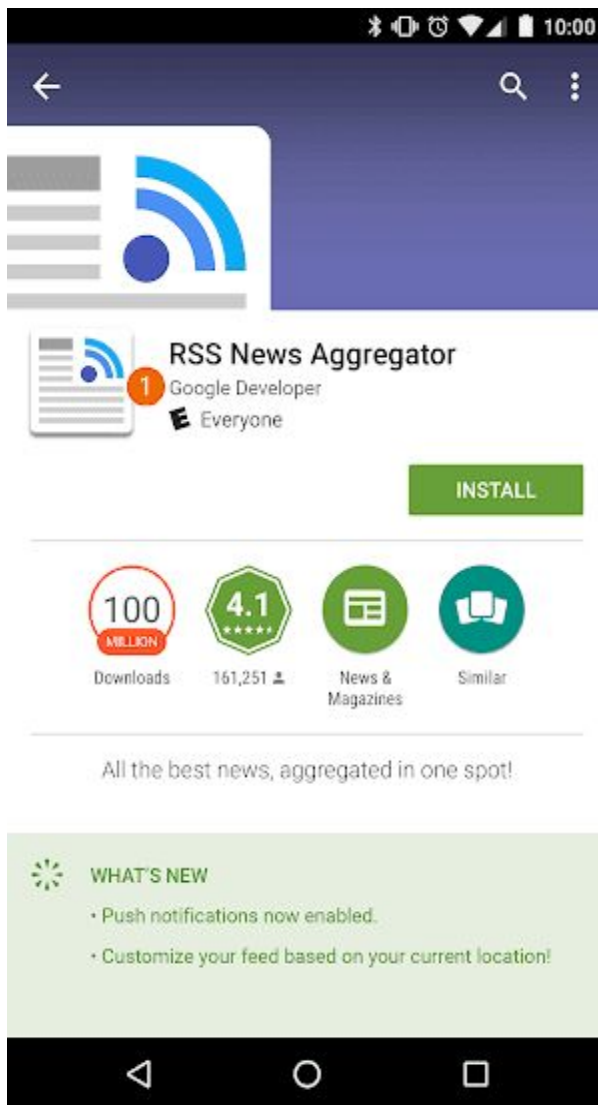
① Det finns ingen stängningsknapp för den här annonsen.

Störa appar, tredjepartsannonser eller enhetsfunktioner

Annonser som är kopplade till din app får inte störa andra appar, annonser eller enhetens funktion, inklusive system- eller enhetsknappar och -portar. Detta omfattar överlagringar, tillhörande funktioner och annonsenheter i form av widgetar. Annonser får bara visas i appen som de förekommer i.

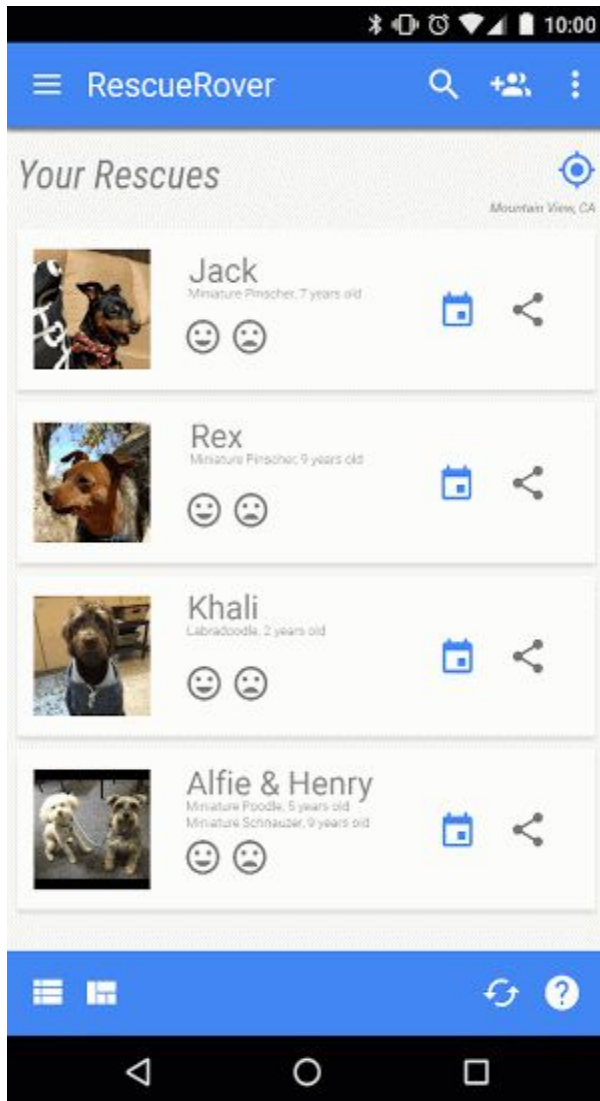
I syfte att säkerställa att Google Play förblir en säker och respektfull plattform har vi skapat standarder som definierar och förbjuder innehåll som är skadligt eller opassande för våra användare.

Annonser som visas utanför appen som de tillhör:



Beskrivning: Användaren navigerar till startskärmen från appen. Plötsligt visas en annons på startskärmen.

Annonser som startas av knappen Startside eller andra funktioner som uttryckligen är avsedda att avsluta appen:

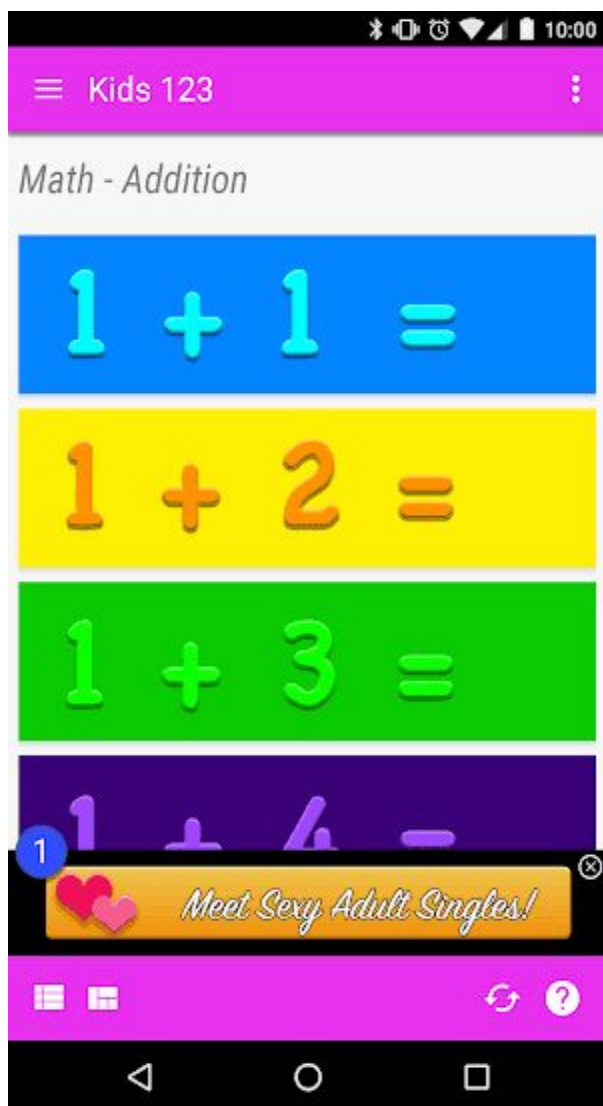


Beskrivning: Användaren försöker avsluta appen och navigera till startskärmen, men i stället avbryts det förväntade flödet av en annons.

Olämpliga annonser

Annonserna som visas i appen måste vara lämpliga för appens målgrupp, även om innehållet i sig följer våra policyer.

I syfte att säkerställa att Google Play förblir en säker och respektfull plattform har vi skapat standarder som definierar och förbjuder innehåll som är skadligt eller opassande för våra användare.



① Den här annonsen är inte lämplig för appens målgrupp.

Användning av Androids reklam-id

I version 4.0 av Google Play-tjänsterna introducerades nya API:er och ett id som kan användas av annonserings- och analysleverantörer. Villkoren för användning av detta id följer nedan.

Användning. Androids reklam-id får endast användas för annonsering och användningsanalys. Vid varje åtkomst till detta id måste inställningen Välj bort intressebaserad annonsering eller Välj bort Anpassning av annonser kontrolleras. Koppling till uppgifter som kan kopplas till en specifik individ och andra identifierare. Ingen koppling mellan detta reklam-id och uppgifter som kan kopplas till en specifik individ eller till ett beständigt enhets-id (t.ex. SSAID, MAC-adress, IMEI-kod osv.) får göras utan användarens uttryckliga samtycke.

Respektera användarnas val. Vid återställning till ett nytt reklam-id får detta inte kopplas till ett tidigare reklam-id eller till data som härrör från ett tidigare reklam-id utan

användarens uttryckliga samtycke. Du måste också rätta dig efter det val som användaren har gjort för inställningen Välj bort intressebaserad annonsering eller Välj bort Anpassning av annonser. Om användaren har aktiverat denna inställning får du inte använda detta reklam-id för att skapa användarprofiler för annonseringsändamål eller för att rikta in användare med anpassad annonsering. Till de aktiviteter som är tillåtna hör innehållsbaserad annonsering, frekvenstak, konverteringsspåring, rapportering och säkerhet och bedrägeriupptäckt.

Insyn för användarna. Användarna måste upplysas om att detta reklam-id används och samlas in och att de här villkoren efterlevs i ett juridiskt adekvat sekretessmeddelande. Läs mer om våra sekretesstandarder i vår policy om [användardata](#).

Följ användarvillkoren. Detta reklam-id får endast användas i enlighet med dessa villkor. Det gäller även för eventuella parter som du delar det med i ditt företag. Alla appar som laddas upp och publiceras på Google Play måste innehålla detta reklam-id (om det finns tillgängligt på enheten) i stället för andra enhets-id:n för alla annonseringsändamål.

Programmet för familjeannonser

Om du visar annonser i appen och endast barn ingår i målgruppen i enlighet med [familjepolicyn](#) måste du använda ett annons-SDK som har självcertifierat att det efterlever Google Plays policyer, inklusive certifieringskraven för annons-SDK:er nedan. Om både barn och äldre användare ingår i målgruppen för appen måste du implementera metoder för ålderskontroll och säkerställa att alla annonser som visas för barn kommer från ett av dessa självcertifierade annons-SDK:er. Endast självcertifierade annons-SDK:er får användas i appar som ingår i programmet Avsett för familjer.

Du måste bara använda Google Play-certifierade annons-SDK:er om du visar annonser för barn via annons-SDK:er. Följande är tillåtet om annons-SDK:et inte är egencertifierat för Google Play, men tänk på att du bär ansvaret för att säkerställa att annonsinnehåll och metoder för datainsamling efterlever Plays [policy om användaruppgifter](#) och [familjepolicy](#):

Intern annonsering där SDK:er används för hantering av korsmarknadsföring av dina appar eller annan media och andra produkter du säljer.

Ingå direktavtal med annonsörer där SDK:er används för hantering av annonsutrymme.

Krav för certifiering av annons-SDK

Definiera vad som utgör olämpligt innehåll och beteende i annonser och förbjud det i villkoren eller policyn för annons-SDK:et. Definitionen får inte resultera i att villkoren i Google Plays programpolicy för utvecklare inte kan efterlevas.

Utveckla en metod för att klassificera annonsmaterial efter lämplig åldersgrupp och inkludera minst grupperna Ingen åldersgräns och Olämpligt för barn.

Klassificeringsmetoden måste överensstämma med den metod som Google tillhandahåller för SDK:er som har fyllt i intresseanmälan nedan.

Tillåt att utvecklare begär, per app eller per begäran, att appen behandlas som avsedd för barn gällande visning av annonser. Sådan behandling måste efterleva alla tillämpliga lagar och föreskrifter, till exempel [den amerikanska lagen om barns personuppgifter på webben \(COPPA\)](#) och EU:s [allmänna dataskyddsförordning \(GDPR\)](#). Google Play kräver också att anpassade annonser, intressebaserad annonsering och remarketing inaktiveras när appen behandlas som avsedd för barn.

Se till att allt annonsmaterial som används i annonsering för barn som säljs via budgivning i realtid har granskats och att budgivarna är medvetna om de särskilda integritetskraven.

Tillhandahåll tillräckligt underlag för att Google ska kunna verifiera att annons-SDK:et efterlever alla certifieringskrav och svara inom rimlig tid på eventuella efterföljande begäranden om information.

Obs! Annonss-SDK:er måste ha stöd för visning av annonser som efterlever alla relevanta bestämmelser och förordningar gällande barn som kan tillämpas på deras utgivare.

Förmedlingskrav för annonsvisningsplattformar gällande annonser som visas för barn:

Använd endast Play-certifierade annons-SDK:er eller implementera de skyddsåtgärder som krävs för att säkerställa att alla annonser som visas från förmedlande nätverk efterlever dessa krav.

Inför nödvändig signalering av annonsinnehållets klassificering och eventuell tillämplig behandling som avsedd för barn.

Här hittar utvecklare en [lista över självcertifierade annons-SDK:er](#).

Utvecklare kan även dela detta [formulär för intresseanmälan](#) med annons-SDK:er som vill självcertifieras.

Butiksuppgifter och marknadsföring

Din apps marknadsföring och synlighet påverkar betydligt butikens kvalitet. Undvik butiksuppgifter med skräp, marknadsföring av låg kvalitet och att på ett oärligt sätt förbättra en apps synlighet på Google Play.

Marknadsföring av appar

Vi tillåter inte appar som direkt eller indirekt utnyttjar marknadsföringsmetoder som är vilseledande eller skadliga för användare eller utvecklare. Detta omfattar appar där följande förekommer:

Användning av vilseledande annonser på webbplatser, i appar eller andra egendomar, till exempel aviseringar som liknar systemmeddelanden och varningar.

Marknadsföring eller installationsstrategier som omdirigerar användare till Google Play eller laddar ned appar utan att användaren kan göra ett välinformerat val om det.

Oönskad marknadsföring via sms-tjänster.

Det är ditt ansvar att se till att eventuella annonsnätverk eller närstående bolag som är kopplade till din app också följer dessa policyer och inte använder några otillåtna marknadsföringsmetoder.

Metadata

Vi tillåter inte appar med vilseledande, felaktigt formaterad, otydlig, irrelevant, överflödig eller olämplig metadata. Det gäller bland annat appbeskrivningen, utvecklarens namn, appens namn, ikon, skärmdumpar och kampanjbilder. Utvecklare måste tillhandahålla en tydlig och välskriven beskrivning. Det är heller inte tillåtet att använda anonyma användarrekommendationer i appens beskrivning.

I syfte att säkerställa att Google Play förblir en säker och respektfull plattform har vi skapat standarder som definierar och förbjuder innehåll som är skadligt eller opassande för våra användare.



① Anonyma användarrekommandationer

② Jämförelser av uppgifter mellan appar och varumärken

③ Väggar av text eller horisontala eller vertikala listor av ord

Här är några exempel på olämpliga texter, bilder eller videor i uppgifterna:

Bilder eller videor med sexuellt innehåll. Undvik bilder och videor som innehåller bröst, rumpor, genitalier eller annan anatomi eller annat innehåll som ofta sexualiseras. Detta gäller både tecknat och otecknat material.

Språk som är olämpligt för en allmän målgrupp. Undvik svordomar och vulgärt språk i appuppgifterna. Om sådant innehåll är ett centralt inslag i din app måste du censurera dess presentation i butiksuppgifterna.

Framträdande våldsskildringar på appikoner, i kampanjbilder eller i videor.

Skildringar av illegal användning av droger. Innehåll i butiksuppgifterna måste vara lämpligt för alla målgrupper, även om det syftar till att vara utbildande, dokumentärt, vetenskapligt eller konstnärligt.

Här är några bra metoder:

Betona vad som är bra med din app. Dela intressanta och spännande fakta så att användarna förstår vad som gör appen speciell.

Försäkra dig om att appens titel och beskrivning beskriver appens funktioner på ett korrekt sätt.

Undvik upprepade eller irrelevanta sökord eller hänvisningar.

Skriv en kortfattad och saklig beskrivning för appen. Kortare beskrivningar fungerar bättre, särskilt på enheter med små skärmar. Beskrivningar som är överdrivet långa, detaljerade, felaktigt formaterade eller repetitiva kan utgöra en överträdelse av policyn.

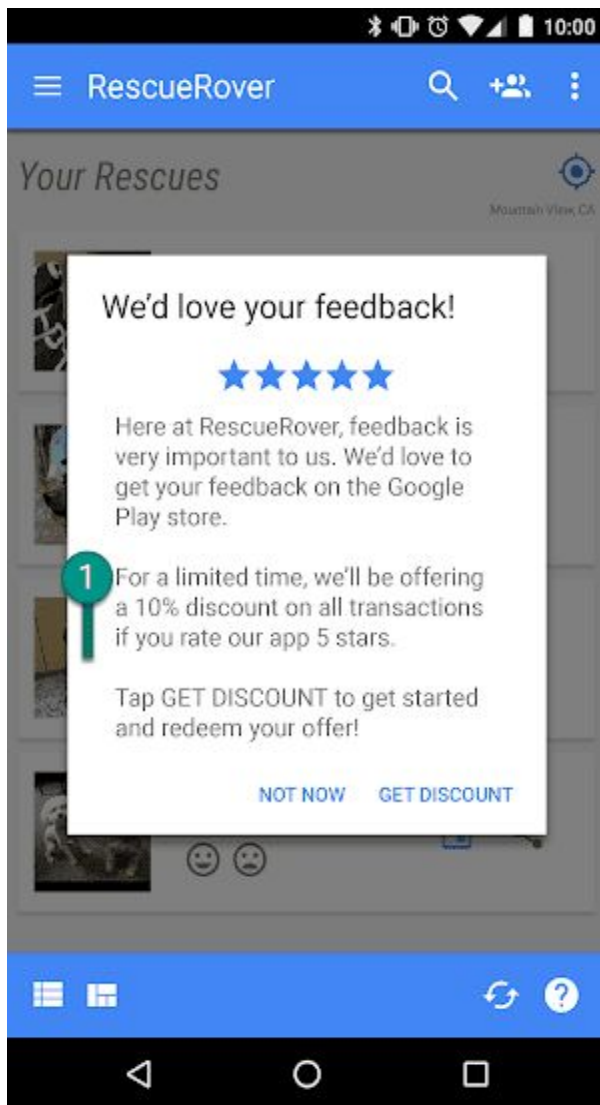
Tänk på att uppgifterna ska vara lämpliga för en allmän målgrupp. Använd inte text, bilder eller videor som är olämpliga i butiksuppgifterna och följ riktlinjerna ovan.

Användarbetyg, recensioner och installationer

Utvecklare får inte försöka ändra placeringen för appar i Google Play. Detta omfattar, men är inte begränsat till, att höja produktbetyg, recensioner eller antal installationer på otillåtna sätt, såsom bedrägliga installationer och att erbjuda ersättning för recensioner, betyg och installationer.

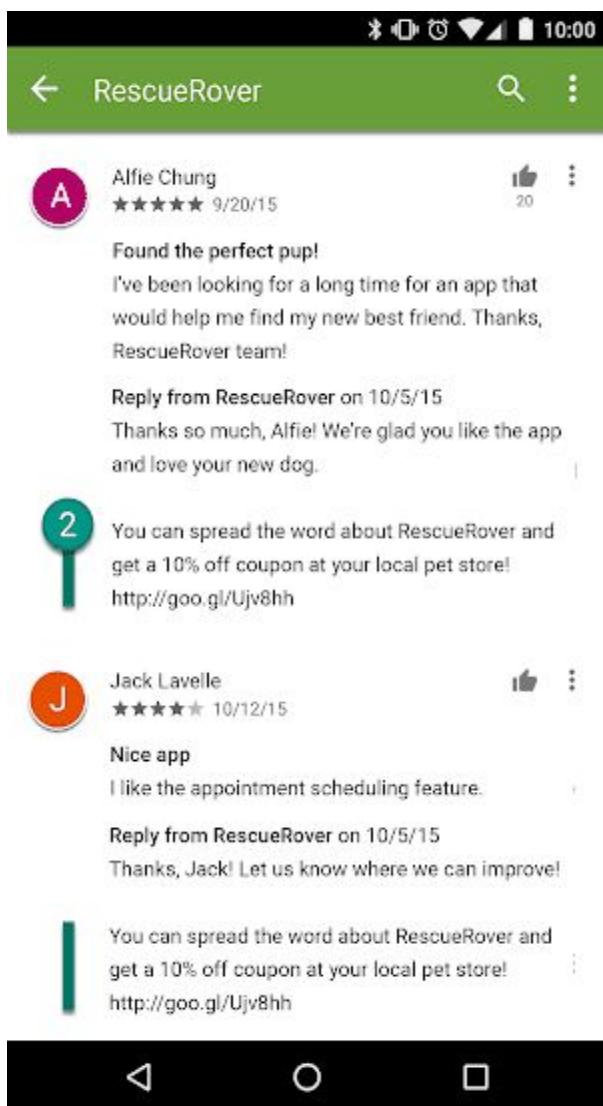
I syfte att säkerställa att Google Play förblir en säker och respektfull plattform har vi skapat standarder som definierar och förbjuder innehåll som är skadligt eller opassande för våra användare.

Be användarna att betygsätta din app och erbjuda ersättning:



① Det här meddelandet erbjuder användarna en rabatt i utbyte mot ett högt betyg.

Skicka betyg flera gånger för att påverka appens placering på Google Play.
Skicka eller uppmuntra användare att skicka recensioner som innehåller olämpligt innehåll, inklusive partners, kuponger, spelkoder, e-postadresser eller länkar till webbplatser eller andra appar:



② Den här recensionen uppmuntrar användare att marknadsföra appen RescueRover genom att erbjuda en kupong.

Betyg och recensioner är riktmärken för appens kvalitet. Användarna är beroende av att de är äkta och relevanta. Här är några bra tips när du svarar på användarrecensioner:

Fokusera på problemen i användarens kommentarer när du svarar och fråga inte efter ett högre betyg.

Ta med referenser till praktiska resurser som en supportadress eller en sida med vanliga frågor och svar.

Innehållsklassificeringar

Vårt system för innehållsklassificering omfattar officiella klassificeringar från [IARC \(International Age Rating Coalition\)](#) och är utformat för att hjälpa utvecklare att förse användarna med lokalt relevanta innehållsklassificeringar.

Så här används innehållsklassificeringar

Innehållsklassificeringar är avsedda att informera kunder, i synnerhet föräldrar, om innehåll i appar som kan vara stötande. De bidrar även till att blockera eller filtrera innehållet i vissa områden eller till vissa användare där så krävs enligt lag. Dessutom används de för att avgöra om appen uppfyller villkoren för vissa utvecklarprogram.

Så här tilldelas innehållsklassificeringar

För att få en innehållsklassificering måste du fylla i ett [klassificeringsformulär i Play Console](#) som handlar om apparnas innehåll. Din app tilldelas en innehållsklassificering från flera klassificeringsorganisationer baserat på svaren i frågeformuläret. Missledande information om appens innehåll kan resultera i att den tas bort eller stängs av tillfälligt. Det är därför viktigt att du ger korrekta svar i frågeformuläret.

För att undvika att appen listas som Ingen klassificering måste du fylla i klassificeringsformuläret för varje ny app som skickas till Play Console, samt för alla befintliga appar som är aktiva på Google Play. Appar utan innehållsklassificering tas bort från Play Butik.

Om du gör ändringar i appens innehåll eller funktioner som påverkar svaren i klassificeringsformuläret måste du skicka in ett nytt formulär i Play Console.

Besök [hjälpcentret](#) om du vill veta mer om de olika [klassificeringsorganisationerna](#) och om hur du fyller i klassificeringsformuläret.

Överklaga klassificeringar

Om du anser att IARC har gett din app en felaktig innehållsklassificering har du rätt att överklaga direkt till IARC med hjälp av länken som anges i certifikatmeddelandet.

Spam och minimikrav på funktion

Appar måste uppfylla grundläggande krav på funktion med hänsyn till användarnas upplevelse. Appar som kraschar, på andra sätt inte uppfyller kraven för en fungerande användarupplevelse eller vars enda syfte är att spamma användare eller Google Play är inte appar som utökar katalogen på ett meningsfullt sätt.

Spam

Vi tillåter inte appar som visar spam för användarna eller på Google Play, exempelvis appar varifrån oönskade meddelanden skickas till användarna, eller appar som är repetitiva och av låg kvalitet.

Spammeddelanden

Vi tillåter inte appar som skickar sms, e-post eller andra meddelanden för användarens räkning utan att användaren kan bekräfta innehållet eller de avsedda mottagarna.

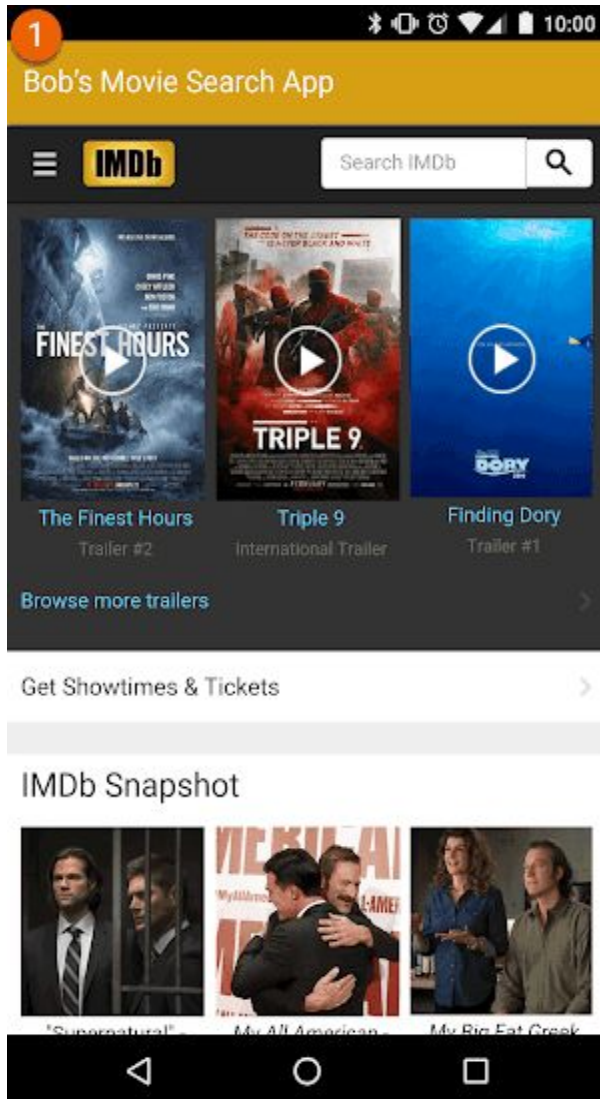
WebViews- och affiliate-spam

Vi tillåter inte appar vars primära syfte är att driva affiliate-trafik till en webbplats eller att visa en webbplats utan tillåtelse från webbplatsens ägare eller administratör.

I syfte att säkerställa att Google Play förblir en säker och respektfull plattform har vi skapat standarder som definierar och förbjuder innehåll som är skadligt eller opassande för våra användare.

En app vars primära syfte är att mot ersättning driva trafik till en webbplats så att användare registrerar sig eller köper något där.

Appar vars primära syfte är att visa en webbplats utan tillåtelse:



① Den här appen heter Bob's Movie Search App och är bara en visning av webbplatsen IMDb.

Repetitivt innehåll

Vi tillåter inte appar som endast tillhandahåller samma upplevelser som andra appar som redan finns på Google Play. Appar bör ge användarna mervärde genom att tillhandahålla innehåll eller tjänster som är unika.

I syfte att säkerställa att Google Play förblir en säker och respektfull plattform har vi skapat standarder som definierar och förbjuder innehåll som är skadligt eller opassande för våra användare.

Kopiera innehåll från andra appar utan att lägga till originellt innehåll eller värde.
Skapa flera appar med snarlika funktioner, innehåll och användarupplevelser. Om det finns väldigt lite innehåll i apparna bör utvecklaren överväga att sammanställa innehållet i en enda app.

Appar som har skapats med ett automatiskt verktyg, hjälpmedel eller utifrån en mall och har skickats till Google Play av den som driver tjänsten för andra personers räkning är inte tillåtna. Sådana appar är bara tillåtna om de publiceras av ett individuellt registrerat utvecklarkonto som tillhör den som använder det automatiska verktyget och inte den som driver tjänsten.

Made For-annonser

Vi tillåter inte appar vars primära syfte är att visa annonser.

I syfte att säkerställa att Google Play förblir en säker och respektfull plattform har vi skapat standarder som definierar och förbjuder innehåll som är skadligt eller opassande för våra användare.

Appar där mellansideannonser visas efter varje åtgärd användaren vidtar, vilket inbegriper men är inte begränsat till klick, svepningar osv.

Minimikrav på funktion

Säkerställ att användarupplevelsen i appen är stabil, engagerande och följsam.

I syfte att säkerställa att Google Play förblir en säker och respektfull plattform har vi skapat standarder som definierar och förbjuder innehåll som är skadligt eller opassande för våra användare.

Appar som inte har utformats för att göra något eller fylla någon funktion

Defekt funktion

Vi tillåter inte appar som kraschar, tvingas att stängas, låser sig eller på andra sätt inte fungerar som de ska.

I syfte att säkerställa att Google Play förblir en säker och respektfull plattform har vi skapat standarder som definierar och förbjuder innehåll som är skadligt eller opassande för våra användare.

Appar som inte går att installera

Appar som går att installera men inte att läsa in

Appar som går att läsa in men som inte svarar

Andra program

Appar som är utformade för andra Android-upplevelser och som distribueras via Google Play kan omfattas av programspecifika policykrav utöver de innehållspolicyer som anges på andra platser i detta policycenter. Granska nedanstående lista och ta reda på om någon av dessa policyer gäller din app.

Android Instant Apps

Vårt mål med Android Instant Apps är att skapa behagliga och smidiga användarupplevelser samtidigt som vi iakttar högsta standard för sekretess och säkerhet. Våra policyer är utformade i syfte att stödja det målet.

Utvecklare som väljer att distribuera Android Instant Apps via Google Play måste följa följande policyer, utöver övriga [programpolicyer för utvecklare på Google Play](#).

Identitet

Utvecklare måste integrera [Smart Lock för lösenord](#) för snabbappar med inloggningsfunktioner.

Stöd för länkar

Utvecklare av Android Instant Apps måste stödja länkar för andra appar. Om utvecklarens snabbappar eller installerade appar innehåller länkar som kan omvandlas till en snabbapp måste utvecklaren hänvisa användare till den snabbappen i stället för att exempelvis läsa in länkarna i [WebView](#).

Tekniska specifikationer

Utvecklare måste följa de tekniska specifikationer och krav för Android Instant Apps som anges av Google och som kan ändras emellanåt. Detta inkluderar de specifikationer och krav som anges i [vår offentliga dokumentation](#).

Erbjuda appinstallation

Snabbappen får erbjuda användaren den installerbara versionen, men det får inte vara snabbappens huvudsakliga syfte. Om installation erbjuds måste utvecklare:

- Använda [ikonen Ladda ned app från Material Design](#) och etiketten Installera som installationsknapp.

- Inte ha fler än 2–3 implicita installationsuppmaningar i snabbappen.

- Inte presentera installationsuppmeningen för användarna med hjälp av en banner eller annan annonsliknande teknik.

Du hittar mer information om snabbappar och riktlinjer för användarupplevelser i [Bästa metoder för användarupplevelse](#).

Ändra enhetens status

Snabbappar får inte genomföra ändringar av användarens enhet som varar längre än sessionen för snabbappen. Snabbappar får till exempel inte ändra användarens bakgrund eller skapa en widget på startskärmen.

Appens synlighet

Utvecklare måste se till att snabbappar är synliga för användare på ett sådant sätt att användaren alltid är medveten om att snabbappen körs på enheten.

Enhetsidentifierare

Snabbappar får inte ha åtkomst till enhetsidentifierare som både (1) finns kvar efter det att snabbappen har slutat att köras (2) inte kan återställas av användaren. Några exempel är

- Build Serial

- Mac-adresser till eventuella nätverkskretsar

- IMEI, IMSI

Snabbappar får ha åtkomst till telefonnummer om dessa har samlats in med körningsbehörighet. Utvecklaren får inte försöka skapa ett fingeravtryck för användare med hjälp av dessa identifierare eller andra metoder.

Nätverkstrafik

Nätverkstrafik inifrån snabbappen måste krypteras med ett TLS-protokoll, till exempel HTTPS.

Familjer

Google Play erbjuder en bred plattform för utvecklare där de kan visa upp innehåll av hög kvalitet som är lämpligt för alla åldrar och passar hela familjen. Du ansvarar för att säkerställa att din app lämpar sig för barn och efterlever all relevant lagstiftning innan du skickar en app till programmet Avsett för familjer eller skickar en app som riktar sig till barn till Google Play Butik.

[Läs mer om arbetsgången för familjeappar och gå igenom den interaktiva checklistan på Academy for App Success.](#)

Utforma appar för barn och familjer

Teknik används i allt större utsträckning för att berika familjens vardag och föräldrar efterfrågar säkert innehåll av hög kvalitet som de kan dela med sina barn. Din app kanske särskilt riktar sig till barn, eller så dras barn till din app ändå. Google Play vill underlätta för dig att säkerställa att din app är säker för alla användare, även familjer.

Ordet "barn" har olika betydelse på olika platser och i olika sammanhang. Det är viktigt att du rådgör med ditt juridiska ombud för att klargöra vilka förbindelser och/eller åldersgränser som gäller för din app. Eftersom du är expert på hur din app fungerar räknar vi med din hjälp för att se till att appar på Google Play är säkra att använda för familjer.

Appar som särskilt riktar sig till barn måste delta i programmet Avsett för familjer. Även om barn endast är en av målgrupperna som appen riktar sig till kan du se till att de rätta användarna hittar den genom att delta i programmet Avsett för familjer. Om du väljer att inte delta i programmet Avsett för familjer måste du ändå efterleva kraven i familjepolicyn för Google Play nedan och samtliga [programpolicyer för utvecklare på Google Play](#) och [distributionsavtalet för utvecklare](#).

Krav för Play Console

Målgrupp och innehåll

I avsnittet [Målgrupp och innehåll](#) i Google Play Console måste du ange målgruppen för appen innan publiceringen genom att välja åldersgrupper på listan som visas. Oavsett vad du anger i Google Play Console kan bedömningen av den uppgivna åldersgruppen påverkas av eventuella bilder och termer i appen som kan anses vara riktade till barn. Google Play förbehåller sig rätten att utföra en egen granskning av informationen du tillhandahåller om appen och avgöra huruvida den angivna målgruppen är korrekt.

Om du väljer en målgrupp där endast vuxna ingår men Google bedömer att den inte stämmer eftersom appen riktar sig till både barn och vuxna får du möjlighet att klargöra för användarna att appen inte riktar sig till barn genom att märka den med en varning.

Du bör endast välja flera åldersgrupper som målgrupp om appen är avsedd för användare i de valda åldersgrupperna och du har säkerställt appens lämplighet. Om appen till exempel är avsedd för småbarn och barn i förskoleåldern väljer du bara Upp till 5 år som åldersgrupp för appen. Om appen riktar sig till en specifik årskurs väljer du den åldersgrupp som bäst stämmer överens med årskursen. Välj bara åldersgrupper där både barn och vuxna ingår om appen verkligen riktar sig till alla åldrar.

Uppdateringar av avsnittet Målgrupp och innehåll

Du kan när som helst uppdatera informationen om appen i avsnittet Målgrupp och innehåll i Google Play Console. Informationen visas i Google Play Butik först efter en [appuppdatering](#). Ändringar i det här avsnittet i Google Play Console kan dock granskas för policyefterlevnad innan appuppdateringen skickas in.

Vi rekommenderar att du meddelar befintliga användare om du ändrar åldersgruppen för appen, börjar att visa annonser eller erbjuda köp i appen. Detta görs antingen i avsnittet Nyheter på sidan med butiksuppgifter för appen eller via aviseringar i appen.

Felaktig framställning i Play Console

Felaktig framställning av någon information om appen i Play Console, inbegripet i avsnittet Målgrupp och innehåll, kan resultera i att appen tas bort eller stängs av. Därför är det viktigt att uppgifterna är korrekta.

Krav för familjepolicyn

Följande krav måste efterlevas om barn ingår i en av målgrupperna för appen. Om kraven inte efterlevs kan det resultera i att appen tas bort eller stängs av.

1. Appens innehåll: Innehåll i appen som är tillgängligt för barn måste vara lämpligt för dem.
2. Svar i Google Play Console: Du måste uppge korrekta svar på frågor om appen i Google Play Console och uppdatera svaren så att de överensstämmer med eventuella ändringar av appen.
3. Annonser: Om annonser visas för barn eller användare i okänd ålder i appen måste du göra följande:

Endast visa annonser från [Google Play-certifierade annons-SDK:er](#) för sådana användare.

Säkerställa att annonser som visas för sådana användare inte innehåller intressebaserad annonsering och remarketing.

Säkerställa att annonser som visas för sådana användare är lämpliga för barn.

Säkerställa att annonser som visas för sådana användare uppfyller annonsformatkraven för Familjer.

Säkerställa att all tillämplig lagstiftning och branschstandarder för annonsering som riktar sig till barn efterlevs.

4. Insamling av data: Du måste meddela om några [personliga och känsliga uppgifter](#) samlas in från barn i appen, även via API:er och SDK:er som används eller anropas i appen. Känsliga uppgifter från barn omfattar men är inte begränsat till autentiseringsuppgifter, sensordata från mikrofoner och kameror, enhetsdata, Android-id, annonsanvändning och annons-id.
5. API:er och SDK:er: Du måste säkerställa att eventuella API:er och SDK:er implementeras korrekt i appen.

Appar som endast riktar sig till barn får inte innehålla några API:er eller SDK:er som inte är godkända för tjänster som riktar sig till barn. Detta omfattar Inloggning med Google (och alla andra Google API-tjänster som har åtkomst till data från ett Google-konto), Google Plays speltjänster och alla andra API-tjänster från Google som använder OAuth-teknik för autentisering och auktorisering. Implementera inte API:er och SDK:er som inte är godkända för tjänster som riktar sig till barn i appar som riktar sig både till barn och äldre målgrupper om de inte skyddas av en [skärm för ålderskontroll](#) eller implementeras på sådant vis att uppgifter om barn inte samlas in (t.ex. tillhandahålla Inloggning med Google som valfri funktion). Observera att alla användare måste ha åtkomst till appen och de funktioner som rimligen behövs.
6. Sekretesspolicy: Du måste ange en länk till sekretesspolicyn på sidan med butiksuppgifter för appen. Länken måste alltid vara tillgänglig så länge som appen finns i Play Butik och den måste leda till en sekretesspolicy som bland annat innehåller en korrekt beskrivning av insamlingen och användningen av data i appen.
7. Särskilda begränsningar:

Om förstärkt verklighet används i appen måste du inkludera en säkerhetsvarning som visas direkt när AR-avsnittet startas. Varningen ska innehålla följande:

 - Ett lämpligt meddelande om vikten av föräldrakontroll.
 - En påminnelse om vikten av att vara medveten om de fysiska risker som den verkliga världen medför (till exempel: Var uppmärksam på omgivningen).

Användning av enheter som inte är lämpliga för barn (t.ex. Daydream och Oculus) får inte krävas för appen.
8. Juridisk efterlevnad: Du måste säkerställa att appen, inbegripet alla API:er eller SDK:er som används i eller anropas av appen, efterlever den amerikanska lagen [COPPA \(Children's Online Privacy and Protection Act\)](#), [EU-lagen Allmänna dataskyddsförordningen \(GDPR\)](#) och alla andra tillämpliga lagar och bestämmelser.

I syfte att säkerställa att Google Play förblir en säker och respektfull plattform har vi skapat standarder som definierar och förbjuder innehåll som är skadligt eller opassande för våra användare.

Appar som marknadsförs som barnspel i butiksuppgifterna men innehållet är endast lämpligt för vuxna.

Appar där API:er vars användarvillkor förbjuder användning i appar som riktar sig till barn har implementerats.

Appar där alkohol, tobak eller begränsade ämnen beskrivs på ett förskönande sätt.
Appar som innehåller verkligt eller simulerat hasardspel.
Appar som innehåller våld, blodsutgjutelse eller stötande innehåll är inte lämpliga för barn.
Appar där dejtingtjänster eller sex- eller äktenskapsrådgivning erbjuds.
Appar som visar barnförbjudna annonser för barn.

Programmet Avsett för familjer

Appar som särskilt riktar sig till barn måste delta i programmet Avsett för familjer. Om appen riktar sig till alla, även barn och familjer, kan du ansöka om att delta i programmet.

Innan du kan få tillgång till programmet måste din app uppfylla alla krav i familjepolicyn och behörighetskraven för Avsett för familjer, utöver de krav som beskrivs i [Google Plays programpolicy för utvecklare](#) och [Distributionsavtalet för utvecklare](#).

Du hittar mer information om hur du ansöker om att din app ska ingå i programmet genom att klicka [här](#).

Behörighet till programmet

Både annons- och appinnehållet i alla appar som ingår i programmet Avsett för familjer måste vara relevant och lämpligt för barn samt efterleva samtliga krav nedan. Appar som ingår i programmet Avsett för familjer måste alltid efterleva samtliga krav för programmet. Google Play förbehåller sig rätten att efter eget gottfinnande avvisa och ta bort appar som anses vara olämpliga för programmet Avsett för familjer.

Krav för Avsett för familjer

1. Appen måste klassificeras som Ingen åldersgräns, Från 10 år eller motsvarande.
2. I frågeformuläret för innehållsklassificering i Google Play Console måste du uppgge korrekta uppgifter om vilka interaktiva element som förekommer i appen, däribland huruvida
 - användare kan interagera eller utbyta information
 - personliga uppgifter som användare har angett delas med tredje part
 - användarens fysiska plats delas med andra användare i appen.
3. Om [Android Speech API](#) används i appen måste RecognizerIntent.EXTRA_CALLING_PACKAGE vara inställt på dess PackageName.
4. Endast [Google Play-certifierade annons-SDK:er](#) får användas i appar.
5. Platsbehörigheter får inte begäras i appar som särskilt riktar sig till barn.
6. Vid begäranden om Bluetooth-åtkomst i appen måste [Companion Device Manager \(CDM\)](#) användas om inte appen endast är inriktad på operativsystemsversioner som inte är kompatibla med CDM.

Här följer några exempel på vanliga sorters appar som inte är behöriga för programmet.

Appar som klassificeras som Ingen åldersgräns men som innehåller annonser för hasardspel

Appar för föräldrar eller vårdgivare (t.ex. amningsappar och guider om barns utveckling).
Guider för föräldrar eller appar för enhetshantering som är avsedda att användas av föräldrar eller vårdgivare.

Kategorier

Om du blir godkänd för programmet Avsett för familjer kan du välja en programspecifik tilläggskategori som beskriver din app. Här följer de tillgängliga kategorierna för appar som deltar i programmet Avsett för familjer.

Action och äventyr: Actionspel och -appar som omfattar allt från enkla racingspel och sagoäventyr till andra spännande appar och spel.

Hjärngympa: Spel som grundar sig på användarens tankeförmåga, bland annat pussel, matchningsspel, quiz och andra spel som utmanar minnet, intellektet och det logiska tänkandet.

Kreativitet: Appar och spel som sätter fart på kreativiteten, där användaren till exempel tecknar, målar eller programmerar samt andra appar och spel där man bygger saker.

Utbildning: Appar och spel som har utformats med hjälp av experter på inläring (t.ex. lärare, pedagoger och forskare) i syfte att uppmuntra till lärande. Detta omfattar till exempel akademisk, social och känslomässig, fysisk och kreativ inläring samt inläring kopplad till grundläggande livskunskap, kritiskt tänkande och problemlösning.

Musik och video: Appar och spel med musik- eller videokomponenter, vilket omfattar allt från appar som simulerar instrument till appar med musik- eller videoinnehåll.

Rollspel: Appar och spel där användaren kan spela en roll och till exempel låtsas vara kock, vårdgivare, prins eller prinsessa, brandman, polis eller en påhittad rollfigur.

Annonser och intäkter

Policyerna nedan gäller för all annonsering (både för dina appar och appar från tredje part), alla erbjudanden om köp i appen och allt övrigt kommersiellt innehåll (till exempel betald produktplacering) som visas för användare av appar som omfattas av kraven i familjepolicyn och/eller kraven för Avsett för familjer. All annonsering, alla erbjudanden om köp i appar och allt kommersiellt innehåll i dessa appar måste efterleva alla tillämpliga lagar och bestämmelser (inbegripet eventuella relevanta inbördes bestämmelser eller branschriktlinjer).

Google Play förbehåller sig rätten att vidta åtgärder mot appar som innehåller alltför påstridiga kommersiella strategier.

Annonssformatkrav

Det får inte förekomma missvisande innehåll i annonser och erbjudanden om köp i appen och de får inte vara utformade på ett sätt som leder till oönskade klick av barn. Följande är förbjudet:

Användning av [annonsväggar](#)

Annonser som stör normal appanvändning och inte går att stänga efter fem sekunder. Mellansidesannonser eller erbjudanden om köp i appen får inte visas direkt när appen startas.

Flera annonsplaceringar på samma sida.

Annonser eller erbjudanden om köp i appen som inte enkelt kan skiljas från innehållet i appen.

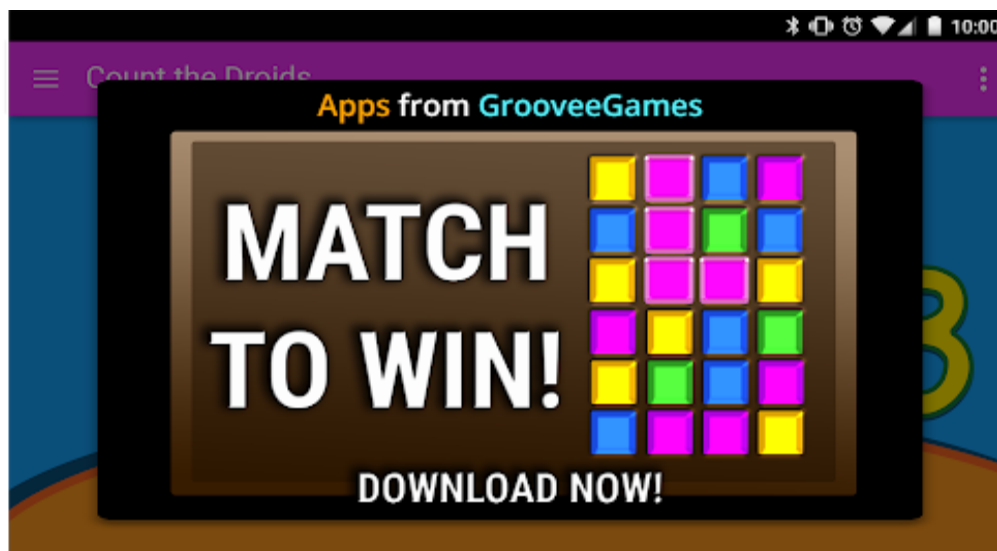
Användare manipuleras till att titta på annonser eller göra köp i appen med hjälp av känslomässig utpressning eller stötande innehåll.

Köp i appen som görs med virtuella pengar i spelet kan inte skiljas från köp med riktiga pengar.

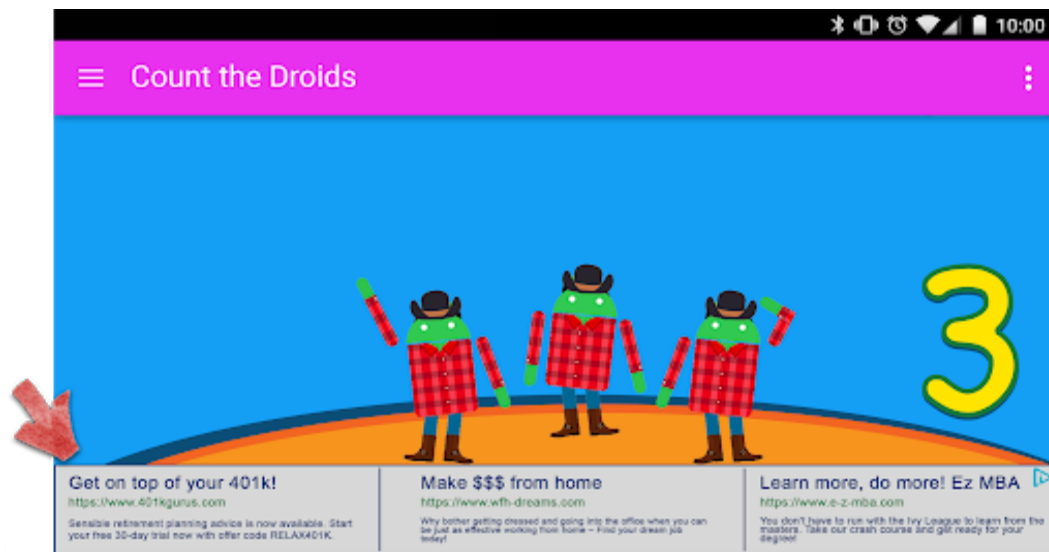
I syfte att säkerställa att Google Play förblir en säker och respektfull plattform har vi skapat standarder som definierar och förbjuder innehåll som är skadligt eller opassande för våra användare.

Annonser som flyttas undan användarens finger när användaren försöker att stänga dem.

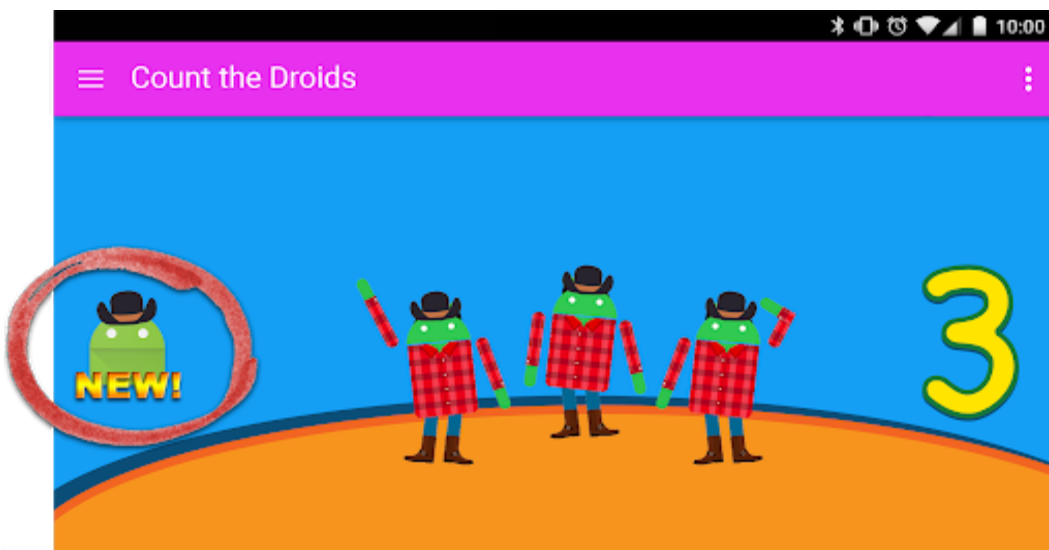
Annonser som tar upp stora delar av skärmen utan att användaren på ett enkelt sätt kan stänga dem, så som visas i exemplet nedan:



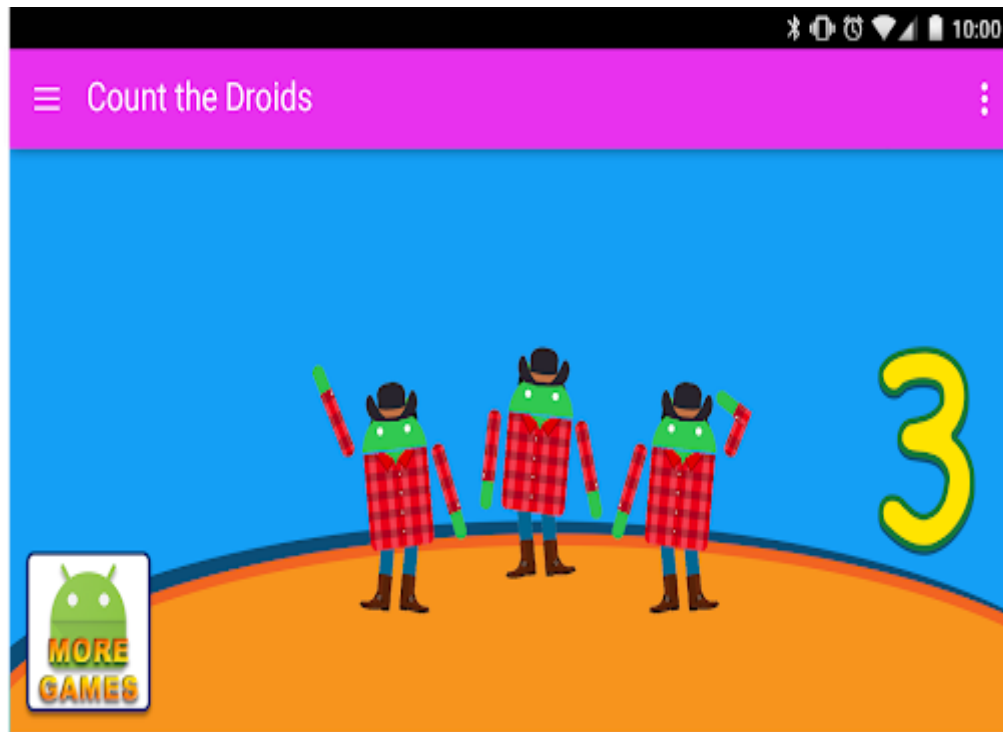
Bannerannonser som visar flera erbjudanden, så som visas i exemplet nedan:



Annonser som kan förväxlas med innehåll i appen av användaren, så som visas i exemplet nedan:



Marknadsföring för dina andra butiksuppgifter i Google Play med hjälp av knappar eller annonser som inte går att skilja från innehåll i appen, så som visas i exemplet nedan:



Här följer några exempel på olämpligt annonsinnehåll som inte ska visas för barn.

Olämpligt medieinnehåll: Annonser för tv-program, filmer, musikalbum eller annan media som är olämplig för barn.

Olämpliga tv-spel och nedladdningsbar programvara: Annonser för nedladdningsbar programvara och elektroniska tv-spel som är olämpliga för barn.

Begränsade eller skadliga ämnen: Annonser för alkohol, tobak, begränsade ämnen eller andra skadliga ämnen.

Hasardspel: Annonser för simulerade hasardspel, tävlingar eller sweepstake-kampanjer, även om det inte kostar något att delta.

Barnförbjudet eller sexuellt provokativt innehåll: Annonser med sexuellt, provokativt eller barnförbjudet innehåll.

Dejting och relationer: Annonser för webbplatser för dejting eller relationer mellan vuxna.

Våldsamhet innehåll: Annonser med våldsamhet och explicit innehåll som är olämpligt för barn.

SDK:er för annonser

Endast [Google Play-certifierade SDK:er](#) får användas för att visa annonser för barn. Endast Google Play-certifierade annons-SDK:er får användas i appar som ingår i programmet Avsett för familjer. Icke-certifierade annons-SDK:er får användas i appar som även riktar sig till vuxna

användare om en [skärm där användaren anger sin ålder](#) finns i appen och annonser som kommer från de icke-certifierade annons-SDK:erna endast visas för vuxna.

Mer information om dessa krav och den aktuella listan över godkända annons-SDK:er hittar du i [programpolicyn om annonser i Avsett för familjer](#).

Om du använder AdMob hittar du mer information om AdMobs produkter i [hjälpcentret för AdMob](#).

Du ansvarar för att säkerställa att appen efterlever alla krav gällande annonsering, köp i appen och kommersiellt innehåll. Kontakta SDK-leverantören om du behöver mer information om deras innehållspolicyer och tillvägagångssätt för annonsering.

Köp i appar

Google Play autentiserar alla användare igen innan några köp i appen sker för appar som deltar i programmet Avsett för familjer. Syftet med åtgärden är att säkerställa att det inte är barn utan parten med det ekonomiska ansvaret som godkänner köpet.

Tillämpning

Det är alltid bättre att undvika att bryta mot policyn än att hantera överträdelsen, men om det ändå händer är det viktigt för oss att utvecklarna förstår hur de kan se till att deras appar följer policyn. Kontakta oss om du [upptäcker några överträdelser](#) eller har frågor om hur du [hanterar en överträdelse](#).

Policyns täckning

Vår innehållspolicy gäller för allt innehåll som din app visar eller länkar till, inklusive annonser som visas för användare och användargenererat innehåll som visas i appen eller som appen länkar till. Den gäller dessutom för allt innehåll från ditt utvecklarkonto som visas offentligt på Google Play, bland annat ditt utvecklarnamn och målsidan för den angivna utvecklarewebbplatsen.

Vi tillåter inte appar som låter användare installera andra appar på sina enheter. Utvecklare av appar som ger åtkomst till andra appar, spel eller annan programvara utan installation, inklusive funktioner och upplevelser som tillhandahålls av tredje part, måste försäkra sig om att allt innehåll apparna ger åtkomst till följer alla [policyer för Google Play](#). Sådana appar kan även omfattas av ytterligare policygranskningar.

Termerna som används i den här policyn har samma innebörd som i [distributionsavtalet för utvecklare](#). Förutom att följa denna policy och distributionsavtalet för utvecklare måste appens innehåll klassificeras enligt våra [riktlinjer för innehållsklassificering](#).

Appar som kan vara olämpliga för en bred målgrupp eller försämra upplevelsen för våra slutanvändare kanske inte marknadsförs på Google Play. Däremot tas sådana appar inte bort från Google Play så länge de följer denna policy och distributionsavtalet för utvecklare.

Google förbehåller sig rätten att inkludera eller ta bort appar på Google Play efter eget gottfinnande. Vi kan vidta åtgärder utifrån ett antal olika faktorer, inklusive men inte begränsat till, ett mönster av skadligt beteende eller en risk för otillåten användning. Vi identifierar risk för otillåten användning utifrån flera olika omständigheter, t.ex. en tidigare historik med överträdelser, feedback från användare och användning av populära varumärken, figurer och andra tillgångar.

Tillämpningsprocess

Om din app bryter mot någon av våra policyer tas den bort från Google Play och du får ett e-postmeddelande med information om exakt varför appen togs bort. Upprepade eller allvarliga överträdelser (till exempel skadlig programvara, bedrägerier och appar som kan skada användaren eller enheten) av denna policy eller [distributionsavtalet för utvecklare](#) leder till att enskilda eller relaterade konton sägs upp.

Observera att meddelanden om borttagning eller administrativa meddelanden kanske inte tar upp alla enskilda fall av överträdelse av policy som finns i appen eller appkatalogen. Alla utvecklare ansvarar för att åtgärda flaggade policyproblem och för att se till att deras appar i övrigt följer policy i sin helhet. Utvecklare som inte åtgärdar överträdelser kan utsättas för ytterligare tvingande åtgärder, bland annat permanent borttagning av appen eller uppsägning av kontot.

Hantera och rapportera policyöverträdelser

Om du har frågor eller funderingar om något som har tagits bort, betyg eller kommentarer från en användare hittar du mer information i resurserna nedan. Du kan även kontakta oss via [hjälpcentret för Google Play](#). Vi kan dock inte erbjuda juridisk rådgivning. Om du behöver juridisk rådgivning rekommenderar vi att du kontaktar en jurist.

[Appverifiering och överklaganden](#)

[Rapportera en policyöverträdelse](#)

[Kontakta Google Play om du vill säga upp ett konto eller ta bort en app](#)

[Skäliga varningar](#)

[Rapportera olämpliga appar och kommentarer](#)

[Min app har tagits bort från Google Play](#)

[Information om uppsägningar av utvecklarkonto för Google Play](#)

[Developer Distribution Agreement](#)