

# डेवलपर कार्यक्रम की नीतियां (5 मई, 2021 से लागू)

आइए, ऐप्लिकेशन और गेम के लिए दुनिया का सबसे भरोसेमंद प्लैटफॉर्म बनाएं

आपके नए ऐप्लिकेशन, आपकी और हमारी सफलता को आगे बढ़ाते हैं। हालांकि, इसके साथ नई ज़िम्मेदारियां भी आती हैं। डेवलपर कार्यक्रम की इन नीतियों और डेवलपर डिस्ट्रिब्यूशन एग्रीमेंट से यह पक्का होता है कि हम साथ मिलकर दुनिया के सबसे अनोखे और भरोसेमंद ऐप्लिकेशन को Google Play की मदद से करोड़ों लोगों तक पहुंचाएंगे। नीचे दी गई हमारी नीतियों के बारे में जानें।

## पाबंदी वाला कॉन्टेंट

दुनिया भर के लोग हर दिन ऐप्लिकेशन और गेम डाउनलोड करने के लिए, Google Play का इस्तेमाल करते हैं। ऐप्लिकेशन सबमिट करने से पहले, पक्का करें कि आपका ऐप्लिकेशन Google Play के लिए सही हो और स्थानीय कानूनों का पालन करता हो।

## बच्चों के लिए खतरनाक कॉन्टेंट

जिन ऐप्लिकेशन में नाबालिगों को सेक्शुअल कॉन्टेंट में शामिल किया गया हो उन्हें 'Play स्टोर' से तुरंत हटा दिया जाता है। इनमें नाबालिग बच्चों को टारगेट करके, उनके यौन शोषण या गलत तरीके से बातचीत (उदाहरण के लिए, गलत ढंग से छूना या सहलाना) जैसी अन्य गतिविधियों को बढ़ावा देने वाले ऐप्लिकेशन शामिल हैं।

इसके अलावा, उन ऐप्लिकेशन को अनुमति नहीं दी जाती जो बच्चों को टारगेट करते हों, लेकिन उनकी थीम वयस्कों वाली होती है। साथ ही, इसमें वे ऐप्लिकेशन भी शामिल हैं जो बहुत ज़्यादा हिंसा, मारपीट, और खून-खराबा जैसी अन्य नुकसानदायक और खतरनाक गतिविधियों को दिखाते हैं या उन्हें बढ़ावा देते हैं। हम ऐसे ऐप्लिकेशन को भी अनुमति नहीं देते जिनमें शरीर या छवि को लेकर गलत चीज़ों को बढ़ावा दिया जाता है। इनमें मनोरंजन के मकसद से, प्लास्टिक सर्जरी, वज़न घटाने, और किसी व्यक्ति के शरीर को आकर्षक दिखाने के लिए उसमें किए गए कॉस्मेटिक बदलाव को दिखाने वाले ऐप्लिकेशन शामिल हैं।

अगर हमें बच्चों का यौन शोषण दिखाने वाले कॉन्टेंट के बारे में पता चलता है, तो हम उचित अधिकारियों से इसकी शिकायत करेंगे। साथ ही, इस तरह के ऐप्लिकेशन को उपयोगकर्ताओं तक पहुंचाने वाले लोगों के Google खाते भी मिटा देंगे।

## गलत कॉन्टेंट

यह पक्का करने के लिए कि Google Play एक सुरक्षित और सम्मानजनक प्लैटफॉर्म बना रहे, हमने ऐसे कॉन्टेंट को तय करने और उस पर पाबंदी लगाने के मानक बनाए हैं जो हमारे ऐप्लिकेशन इस्तेमाल करने वाले लोगों के लिए नुकसानदायक या गलत हो।

## सेक्शुअल कॉन्टेंट और धर्म का अपमान करने वाला कॉन्टेंट

हम ऐसे ऐप्लिकेशन को अनुमति नहीं देते जो सेक्शुअल कॉन्टेंट या धर्म का अपमान करने वाले कॉन्टेंट को बढ़ावा देते हैं। इनमें पोर्नोग्राफी या यौन संतुष्टि देने वाले कॉन्टेंट या सेवाएं शामिल हैं। नग्नता वाले कॉन्टेंट को अनुमति दी जा सकती है, लेकिन उसका मुख्य मकसद शिक्षा देने, डॉक्यूमेंट्री, वैज्ञानिक या कलात्मक होना चाहिए। इसके अलावा, जब ऐसे कॉन्टेंट की ज़रूरत हो, तब ही इन्हें ऐप्लिकेशन में शामिल किया जाना चाहिए।

यहां आम तौर पर होने वाले उल्लंघनों के कुछ उदाहरण दिए गए हैं:

- यौन नग्नता या ऐसी अश्लील मुद्राएं दिखाना जिसमें व्यक्ति नग्न हो, धुंधला हो या उसने बहुत कम कपड़े पहने हों और/या किसी सार्वजनिक जगह के लिहाज़ से ऐसे कपड़े सही न हों।
- ऐनिमेशन, तस्वीरों या किसी और तरह से यौन गतिविधियों को दिखाना या अश्लील मुद्राएं या शरीर के अंगों को यौन रूप से दिखाना।
- ऐसा कॉन्टेंट जिसमें सेक्स को ज़्यादा मज़ेदार बनाने या कामुकता जगाने के बारे में बताया जाता है। साथ ही, जिसमें सेक्स गाइड, गैरकानूनी यौन थीम, और यौन गतिविधियां दिखाई गई हों।
- इसमें ऐसा कॉन्टेंट शामिल है जो ऐप्लिकेशन या स्टोर पेज में शामिल होता है। साथ ही, जो कामुक हो या धर्म का अपमान करता हो। इस कॉन्टेंट में धर्म का अपमान करने वाली बातें, किसी व्यक्ति का अपमान करने वाली बातें, अश्लील मैसेज, और वयस्क/यौन कीवर्ड शामिल हो सकते हैं। इसमें इनके अलावा, और भी चीज़ें शामिल हो सकती हैं।

- जानवरों के साथ यौन गतिविधि दिखाने, इसके बारे में जानकारी देने या इसे बढ़ावा देने वाला कॉन्टेंट.
- ऐसे ऐप्लिकेशन जो सेक्स से जुड़े मनोरंजन, एस्कॉर्ट सेवाओं या ऐसी दूसरी सेवाओं का प्रचार करते हों उन्हें पैसे या किसी और चीज़ के एवज़ में सेक्स क्रियाएं देने वाली सेवा समझा जा सकता है.
- ऐसे ऐप्लिकेशन जो लोगों को नीचा दिखाते हों या उनका अपमान करते हों.

## नफ़रत फैलाने वाली भाषा

हम ऐसे ऐप्लिकेशन को अनुमति नहीं देते जो किसी व्यक्ति या समूह के खिलाफ़ उनकी नस्ल या जातीय मूल, धर्म, दिव्यांगता, उम्र, राष्ट्रियता, सैन्य सेवा के अनुभव, यौन रुझान, लिंग, लैंगिक पहचान, सामाजिक भेदभाव या अधिकार छीनने से जुड़ी दूसरी बातों की वजह से नफ़रत फैलाते हैं या हिंसा को बढ़ावा देते हैं.

जिन ऐप्लिकेशन में नाज़ियों से जुड़ा ईडीएसए कॉन्टेंट (शिक्षा, डॉक्यूमेंटरी, विज्ञान या कला) शामिल है उन्हें स्थानीय कानूनों और नियमों के हिसाब से कुछ देशों में ब्लॉक किया जा सकता है.

यहां आम तौर पर होने वाले उल्लंघनों के उदाहरण दिए गए हैं:

- ऐसा कॉन्टेंट या भाषण जो दावा करे कि कोई सुरक्षित ग्रुप अमानवीय, सामाजिक तौर पर कमतर या नफ़रत के लायक है.
- ऐसे ऐप्लिकेशन जिनमें नफ़रत फैलाने वाली टिप्पणियां, रूढ़िवादी या किसी सुरक्षित ग्रुप के बारे में नकारात्मक बातें (जैसे कि नुकसान पहुंचाने वाला, भ्रष्ट, बुरा वगैरह) कही गई हैं. इसके अलावा, साफ़ तौर पर या किसी दूसरे तरीके से यह दावा किया गया है कि किसी समूह से खतरा है.
- ऐसा कॉन्टेंट या भाषण जो दूसरों को यह मानने के लिए बढ़ावा देता है कि लोगों से नफ़रत या भेदभाव किया जाना चाहिए, क्योंकि वे किसी सुरक्षित ग्रुप के सदस्य हैं.
- ऐसा कॉन्टेंट जो नफ़रत फैलाने वाले प्रतीकों को बढ़ावा देता है, जैसे कि झंडे, प्रतीक, प्रतीक चिह्न या नफ़रत फैलाने वाले समूहों से जुड़ा व्यवहार.

## हिंसा

हम ऐसे ऐप्लिकेशन को अनुमति नहीं देते जिनमें गैर-ज़रूरी हिंसा या दूसरी खतरनाक गतिविधियों को दिखाया जाता है या जो ऐसा करने को बढ़ावा देते हैं. आम तौर पर, ऐसे ऐप्लिकेशन को अनुमति दी जाती है जो किसी गेम के हिसाब से काल्पनिक हिंसा को दिखाते हैं, जैसे कि शिकार या फ़िशिंग करते हुए कार्टून.

यहां आम तौर पर होने वाले उल्लंघनों के कुछ उदाहरण दिए गए हैं:

- किसी भी व्यक्ति या पशु के खिलाफ़ वास्तविक हिंसा या हिंसक धमकियों को ग्राफ़िक की मदद से दिखाना या उनके बारे में जानकारी देना.
- ऐसे ऐप्लिकेशन जो खुद को नुकसान पहुंचाने, खुदकुशी करने, धमकाने, उत्पीड़न करने, खाने से जुड़ी बीमारियां, चोकिंग गेम या ऐसी दूसरी गतिविधियों का प्रचार करते हैं जिनसे गंभीर चोट लग सकती है या किसी की जान भी जा सकती है.

## आतंकवाद से जुड़ा कॉन्टेंट

हम आतंकवादी संगठनों को किसी भी काम के लिए Google Play पर ऐप्लिकेशन प्रकाशित नहीं करने देते. इसमें भर्ती करना भी शामिल है.

हम ऐसे ऐप्लिकेशन को मंजूरी नहीं देते हैं जिनमें आतंकवाद से जुड़ा कॉन्टेंट होता है, जैसे कि आतंकी गतिविधियों को बढ़ावा देने, हिंसा करने के लिए उकसाने या आतंकी हमलों का जश्न मनाने का कॉन्टेंट. अगर आप शिक्षा, डॉक्यूमेंटरी, विज्ञान या कला को ध्यान में रखकर आतंकवाद से जुड़ा कॉन्टेंट पोस्ट कर रहे हैं, तो ध्यान रखें कि आप इतनी जानकारी ज़रूर दें कि लोग यह समझ सकें कि किस बारे में बात हो रही है.

## संवेदनशील घटनाएं

हम ऐसे ऐप्लिकेशन को अनुमति नहीं देते जो प्राकृतिक आपदा, कूरता, झगड़ा, मौत या किसी दूसरी दुखद घटना को लेकर उचित संवेदनशीलता नहीं दिखाते या उसका फ़ायदा लेने की कोशिश करते हैं. आम तौर पर, ऐसे ऐप्लिकेशन को अनुमति दी जाती है जिनमें संवेदनशील घटना से जुड़ा ऐसा कॉन्टेंट होता है जिसमें ईडीएसए (शिक्षा, डॉक्यूमेंटरी, विज्ञान या कला) वैल्यू हो या जिसका इरादा ऐप्लिकेशन इस्तेमाल करने वाले लोगों को सतर्क करने या जागरूकता फैलाने का हो.

यहां आम तौर पर होने वाले उल्लंघनों के उदाहरण दिए गए हैं:

- आत्महत्या, दवा की ज़्यादा मात्रा, प्राकृतिक वजहों वगैरह से किसी व्यक्ति या समूह में लोगों की मौत होने से जुड़ी संवेदनशीलता में कमी.
- किसी बड़ी दुखद घटना को नकारना.

- ऐसी दुखद घटना से फ़ायदा लेते दिखना जिसके पीड़ितों को कोई सीधा फ़ायदा न मिला हो.

## धमकाना और उत्पीड़न करना

हम ऐसे ऐप्लिकेशन को अनुमति नहीं देते जिनमें धमकियां देने, उत्पीड़न करने या प्रताड़ित करने जैसी बातें शामिल हों या जो ऐसी चीज़ों को बढ़ावा देते हों.

यहां आम तौर पर होने वाले उल्लंघनों के उदाहरण दिए गए हैं:

- अंतरराष्ट्रीय या धार्मिक टकरावों से पीड़ित लोगों को धमकाना.
- ऐसा कॉन्टेंट जो दूसरों का फ़ायदा उठाने की कोशिश करता है जिसमें जबरन वसूली, ब्लैकमेल करना वगैरह शामिल है.
- किसी व्यक्ति को सार्वजनिक रूप से अपमानित करने के लिए कॉन्टेंट पोस्ट करना.
- किसी दुखद घटना के पीड़ितों या उनके दोस्तों और परिवार के सदस्यों को परेशान करना.

## ऐसे प्रॉडक्ट जिनसे किसी भी तरह का खतरा हो

हम ऐसे ऐप्लिकेशन को मंजूरी नहीं देते हैं जिनमें विस्फोटकों, बंदूकों, गोला बारूद या बंदूकों से जुड़ी चीज़ों की बिक्री की जाती है.

- जिन चीज़ों पर रोक लगाई गई है उनमें मैगज़ीन या गोलियों के 30 राउंड से ज़्यादा गोलियों वाले बेल्ट और वें चीज़ें शामिल हैं जो किसी बंदूक को अपने-आप चलने में मदद करती हैं या किसी बंदूक को अपने-आप चलने वाला बना देती हैं (उदाहरण के लिए, बंप स्टॉक, गैटलिंग ट्रिगर, ड्रॉप-इन ऑटो सियर, बदलने वाले सामान).

हम ऐसे ऐप्लिकेशन को मंजूरी नहीं देते हैं जिनमें विस्फोटक, बंदूक, गोला-बारूद, दूसरे हथियार या बंदूक से जुड़ी ऐसी चीज़ों को बनाने के निर्देश होते हैं जिन पर दरअसल रोक लगाई गई है. इसमें किसी बंदूक को अपने-आप चलने वाली बंदूक में बदलने या उसको अपने-आप चलने में मदद करने, उसकी गोलियां दागने की क्षमताओं को बढ़ाने या घटाने में मदद करने के बारे में निर्देश शामिल हैं.

## गांजा

हम ऐसे ऐप्लिकेशन को अनुमति नहीं देते जो गांजा या इससे बने प्रॉडक्ट बेचने की सुविधा देते हैं, भले ही इसे कानूनी रूप से मंजूरी क्यों न मिली हो.

यहां आम तौर पर होने वाले उल्लंघनों के कुछ उदाहरण दिए गए हैं:

- इस्तेमाल करने वालों को ऐप्लिकेशन में मौजूद खरीदारी कार्ट की सुविधा की मदद से गांजा मंगवाने देना.
- गांजे की डिलीवरी या पिक अप में इसका इस्तेमाल करने वालों की मदद करना.
- टीएचसी (टेट्राहाइड्रोकैनाबिनॉल) वाले प्रॉडक्ट को बेचने की सुविधा देना. इनमें सीबीडी तेल जैसे प्रॉडक्ट शामिल हैं, जिनमें टीएचसी होता है.

## तंबाकू और शराब

हम ऐसे ऐप्लिकेशन को अनुमति नहीं देते जो तंबाकू (इसमें ई-सिगरेट और वेप पेन भी शामिल हैं) बेचने की सुविधा देते हैं या जो तंबाकू या शराब के गैरकानूनी और गलत इस्तेमाल को बढ़ावा देते हैं.

यहां आम तौर पर होने वाले उल्लंघनों के उदाहरण दिए गए हैं:

- शराब या तंबाकू के इस्तेमाल को दिखाना या बढ़ावा देना. इसके अलावा, ये चीज़ें नाबालिगों को बेचते हुए दिखाना या इसे बढ़ावा देना.
- यह मानना कि तंबाकू खाने से सामाजिक, यौन, पेशेवर, बौद्धिक या एथलेटिक स्थिति में सुधार आ सकता है.
- किसी की मंजूरी के साथ बहुत ज़्यादा शराब पीते हुए दिखाना, जिसमें बहुत ज़्यादा शराब पीना, शराब पीने का उत्सव या शराब पीने की प्रतियोगिता को दिखाना शामिल है.

## वित्तीय सेवाएं

हम ऐसे ऐप्लिकेशन को अनुमति नहीं देते जो लोगों को धोखा देने वाले या नुकसान पहुंचाने वाले वित्तीय प्रॉडक्ट और सेवाएं मुहैया कराते हैं.

इस नीति के तहत, हम पैसों और आभासी मुद्राओं के मैनेजमेंट या निवेश के काम को वित्तीय प्रॉडक्ट और सेवा मानते हैं। इसमें इस्तेमाल करने वाले व्यक्ति की ज़रूरतों के हिसाब से सुझाव देना भी शामिल है।

अगर आपके ऐप्लिकेशन में वित्तीय प्रॉडक्ट या सेवाएं शामिल हैं या वह इनका प्रचार करता है, तो आप जिस इलाके या देश के लोगों को टारगेट कर रहे हैं आपको उस राज्य और इलाके के नियमों का पालन करना होगा। उदाहरण के लिए, आपको स्थानीय कानून के मुताबिक ज़रूरी जानकारी सार्वजनिक करनी होगी।

## बाइनरी ऑप्शन

हम ऐसे ऐप्लिकेशन को अनुमति नहीं देते जो लोगों को बाइनरी ऑप्शन का कारोबार करने की सुविधा देते हैं।

## आभासी मुद्राएं

हम ऐसे ऐप्लिकेशन को मंजूरी नहीं देते हैं जो डिवाइस पर आभासी मुद्राएं बनाते हैं। हम ऐसे ऐप्लिकेशन को अनुमति देते हैं जो कहीं और से आभासी मुद्रा बनाए जाने को मैनेज करते हैं।

## निजी कर्ज़

निजी कर्ज़ लेने वाले लोगों को इसकी क्वालिटी, सुविधाओं, शुल्क, पैसे लौटाने के शेड्यूल, जोखिमों, और इससे होने वाले फ़ायदों की जानकारी होनी चाहिए, ताकि वे कर्ज़ के बारे में सोच-समझकर फ़ैसला ले सकें। निजी कर्ज़ लेने वालों को कर्ज़ की क्वालिटी, सुविधाओं, शुल्क, जोखिमों, और उस कर्ज़ से होने वाले फ़ायदों की जानकारी होनी चाहिए, ताकि वे कर्ज़ लेने या न लेने के बारे में फ़ैसला ले सकें।

- उदाहरण के लिए: निजी कर्ज़, दिन के हिसाब से मिलने वाले कर्ज़ (पेडे कर्ज़), खास लोगों और संगठन वाली वेबसाइटों से मिलने वाले कर्ज़ (पीयर-टू-पीयर कर्ज़), गाड़ी को गिरवी रखकर मिलने वाले कर्ज़ (टाइटल कर्ज़)
- इसमें ये शामिल नहीं हैं: संपत्ति या घर गिरवी रखकर लिया जाने वाला कर्ज़, कार के लिए लिया जाने वाला कर्ज़, पढ़ाई के लिए लिया जाने वाला कर्ज़, और तय की गई किसी उपलब्ध रकम के लिए पेशकश करना (जैसे कि क्रेडिट कार्ड या ज़रूरत पड़ने पर अनिश्चित ब्याज दर पर लिया जाने वाला कर्ज़)

ऐसे ऐप्लिकेशन जो निजी कर्ज़ देते हैं उन्हें ऐप्लिकेशन के मेटाडेटा में नीचे दी गई जानकारी देनी होगी। इनमें वे ऐप्लिकेशन शामिल हैं जो सीधे तौर पर कर्ज़ देते हैं, लीड बनाते हैं, और ग्राहकों को तीसरे पक्ष के कर्ज़ देने वालों से मिलाते हैं। इसमें इनके अलावा, और भी चीज़ें शामिल हो सकती हैं:

- पैसे लौटाने के लिए तय किए गए, कम से कम और ज़्यादा से ज़्यादा दिनों की संख्या
- सालाना ब्याज की ज़्यादा से ज़्यादा दर (एपीआर), जिसमें आम तौर पर साल भर की ब्याज की दर, शुल्क, और अन्य लागतें शामिल होती हैं या फिर जिसमें स्थानीय कानून के हिसाब से लगने वाली इसी तरह की दूसरी दरें शामिल होती हैं
- सभी तरह के लागू शुल्क को जोड़कर कर्ज़ की कुल कीमत का एक उदाहरण
- ऐसी निजता नीति जिसमें ऐप्लिकेशन इस्तेमाल करने वाले व्यक्ति के निजी और संवेदनशील डेटा को एक्सेस करने, इकट्ठा करने, इस्तेमाल करने, और शेयर करने के बारे में पूरी तरह से बताया गया हो।

हम निजी कर्ज़ का प्रचार करने वाले ऐसे ऐप्लिकेशन को अनुमति नहीं देते जो कर्ज़ की पूरी रकम लौटाने के लिए, 60 दिन या उससे कम समय की शर्त रखते हैं (इन्हें हम "कम अवधि वाले निजी कर्ज़" कहते हैं)।

### ज़्यादा एपीआर वाले निजी कर्ज़

हम अमेरिका में ऐसे ऐप्लिकेशन को निजी कर्ज़ देने की अनुमति नहीं देते जिनके सालाना ब्याज की दर (एपीआर) 36% या उससे ज़्यादा होती है। अमेरिका में निजी कर्ज़ की सुविधा देने वाले ऐप्लिकेशन के लिए, [दुथ इन लेंडिंग ऐक्ट \(टिला\)](#) के तहत उनका ज़्यादा से ज़्यादा लिया जाने वाला एपीआर दिखाना ज़रूरी है।

यह नीति उन ऐप्लिकेशन पर लागू होती है जो सीधे तौर पर कर्ज़ की सुविधा देते हैं, लीड बनाते हैं, और जो ग्राहकों को कर्ज़ देने वाले तीसरे पक्ष के लोगों से मिलाते हैं।

यहां आम तौर पर होने वाले उल्लंघनों का एक उदाहरण दिया गया है:

< Back ↑ ☰



### Easy Loans

offers in app purchases

★ ★ ★ ★ ★ 1255

Install

Are you looking for a speedy loan?

Easy Loans Finance can help you get cash in your bank account in an hour!

- Get cash sent to your bank account!
- Safe and easy
- Great short-term rate
- Fast lender approval
- Easy to use
- Loan delivered in an hour
- Download our app and get cash easy!

**Violations**

- No minimum and maximum period for repayment
- Doesn't disclose Maximum Annual Percentage Rate (APR), which generally includes interest rate plus fees and other costs for a year, or similar other rate calculated consistently with local law
- No representative example of the total cost of the loan, including all applicable fees

## असली पैसे दांव पर लगाकर खेला जाने वाला जुआ, गेम, और प्रतियोगिताएं

हम उन ऐप्लिकेशन जिनमें असली पैसे दांव पर लगाकर जुआ खेला जाता है, उससे जुड़े विज्ञापनों, गेमिफ़ाइट नतीजों वाले लॉयल्टी कार्यक्रम, और डेली फ्रैंटेसी स्पोर्ट वाले ऐप्लिकेशन को सिर्फ़ तब अनुमति देते हैं, जब वे ज़रूरी शर्तों को पूरा करते हैं।

### जुए वाले ऐप्लिकेशन

Google Play की सभी नीतियों से जुड़ी पाबंदियों के साथ उनका पालन करते हुए, हम नीचे दी गई टेबल में शामिल देशों में ऑनलाइन जुए की सुविधा देने वाले ऐप्लिकेशन को सिर्फ़ तब तक अनुमति देते हैं, जब तक डेवलपर [आवेदन की प्रक्रिया](#) पूरी करता है। Google Play पर वितरित होने वाले जुए से जुड़े ऐप्लिकेशन को ऑपरेटर के तौर पर सरकार की ओर से मंजूरी मिली है और/या, किसी खास देश में जुआ खेलने के नियम-कानून तय करने वाले विभाग ने उसे रजिस्टर किया हो। साथ ही, वे ऑनलाइन जुए से जुड़ा जिस तरह का प्रॉडक्ट ऑफ़र करना चाहते हैं उसके लिए उस देश में मान्य ऑपरेटिंग लाइसेंस दिया गया हो।

हम मान्य लाइसेंस वाले या जुए से जुड़े सिर्फ़ उन ऐप्लिकेशन को मंजूरी देते हैं जिनमें जुए से जुड़े नीचे दिए गए ऑनलाइन प्रॉडक्ट होते हैं। कृपया हर देश में जुए से जुड़े खास प्रॉडक्ट की जानकारी के लिए, नीचे दी गई टेबल देखें:

- ऑनलाइन कसीनो गेम
- लॉटरी
- स्पोर्ट्स बेटिंग
- डेली फ्रैंटेसी स्पोर्ट्स

ऑस्ट्रेलिया

बेल्जियम

---

ब्राज़ील

---

कनाडा

---

कोलंबिया

---

डेनमार्क

---

फ़िनलैंड

---

फ़्रांस

---

जर्मनी

---

आयरलैंड

---

जापान

---

मेक्सिको

---

न्यूज़ीलैंड

---

नॉर्वे

---

रोमानिया

---

स्पेन

---

स्वीडन

---

यूनाइटेड किंगडम

---

अमेरिका

---

मंजूरी पाने वाले ऐप्लिकेशन को नीचे बताई गई ज़रूरी शर्तें पूरी करनी होंगी:

- Play पर अपने ऐप्लिकेशन को उपलब्ध कराने के लिए, डेवलपर को [ऐप्लिकेशन प्रोसेस](#) सही तरीके से पूरी करनी होगी;
- ऐप्लिकेशन को हर उस देश में लागू सभी कानूनों और उद्योग के मानकों का पालन करना चाहिए जहां उसे उपलब्ध कराया जाता है;

- डेवलपर के पास हर उस देश या राज्य/इलाके के लिए जुए का एक मान्य लाइसेंस होना चाहिए जहां ऐप्लिकेशन को उपलब्ध कराया जाता है;
- डेवलपर को जुए से जुड़ा ऐसा कोई भी प्रॉडक्ट उपलब्ध नहीं कराना चाहिए जो जुए से जुड़े उसके लाइसेंस के दायरे से बाहर हो;
- कम उम्र के लोगों को ऐप्लिकेशन का इस्तेमाल करने से रोकना चाहिए;
- ऐप्लिकेशन को उन देशों, राज्यों/इलाकों या भौगोलिक जगह पर इसे एक्सेस करने और इस्तेमाल करने से रोकना चाहिए जो डेवलपर के, जुए के लाइसेंस में शामिल नहीं हैं;
- ऐप्लिकेशन को Google Play पर, पैसे चुकाकर या Google Play इन-ऐप्लिकेशन बिलिंग का इस्तेमाल करके खरीदे जाने वाले ऐप्लिकेशन के तौर पर मौजूद नहीं होना चाहिए;
- ऐप्लिकेशन ऐसा हो जिसे 'Play स्टोर' से मुफ्त में डाउनलोड और इंस्टॉल किया जा सके;
- ऐप्लिकेशन को AO (सिर्फ वयस्क) या IARC के तौर पर रेट किया जाना चाहिए; और
- ऐप्लिकेशन और उसकी ऐप्लिकेशन लिस्टिंग में, सही तरीके से जुआ खेलने से जुड़ी जानकारी को साफ़ तौर पर दिखाया जाना चाहिए.

## असली पैसे दांव पर लगाकर खेले जाने वाले अन्य गेम, प्रतियोगिताएं, और टूर्नामेंट ऐप्लिकेशन

जुए से जुड़े ऐप्लिकेशन की ऊपर बताई गई ज़रूरी शर्तों को पूरा न करने वाले अन्य सभी ऐप्लिकेशन के लिए, हम ऐसे कॉन्टेंट या सेवाओं को अनुमति नहीं देते जो ऐप्लिकेशन का इस्तेमाल करने वाले लोगों को दांव लगाने, हिस्सेदारी या असली पैसों (इसमें पैसों से खरीदे गए इन-ऐप्लिकेशन आइटम भी शामिल हैं) के बदले में हिस्सा लेने की सुविधा देते हैं। ऐसा इसलिए किया जाता है, ताकि उन्हें ऐसा इनाम मिले जिसकी असल दुनिया में कोई कीमत है। इसमें ऑनलाइन कसीनो, स्पोर्ट बेटिंग, लॉटरी, और ऐसे गेम भी आते हैं जो नकद या असल दुनिया के अन्य इनाम ऑफ़र करते हैं। हालांकि, यह इन ही तक सीमित नहीं है। इसमें, गेम से जुड़े लॉयल्टी कार्यक्रम के बारे में नीचे बताई गई ज़रूरी शर्तों के तहत मंजूरी पाने वाले कार्यक्रम शामिल नहीं हैं।

### उल्लंघनों के उदाहरण

- ऐसे गेम जो इनाम के तौर पर असली चीज़ या असली पैसे जीतने के मौके के बदले में पैसे लेते हैं
- वे ऐप्लिकेशन जिनमें नेविगेट किए जा सकने वाले ऐसे एलिमेंट या सुविधाएं (जैसे, मेन्यू आइटम, टैब, बटन, वेबव्यू वगैरह) शामिल हैं जो असली पैसों का इस्तेमाल करके खेले जाने वाले गेम, प्रतियोगिताएं या टूर्नामेंट में दांव लगाने, हिस्सेदारी लेने या हिस्सा लेने के लिए "कॉल टू ऐक्शन" की सुविधा देती हैं। उदाहरण के लिए, ऐसे नेविगेशनल एलिमेंट (मेन्यू आइटम, टैब, बटन वगैरह) जो लोगों को टूर्नामेंट में नकद इनाम जीतने का मौका देने के लिए "बेटिंग करने" या "रजिस्टर करने" या "खेलने" के लिए न्योता भेजते हैं।
- ऐसे ऐप्लिकेशन जो जुआ खेलने वाले लोगों, इन-ऐप्लिकेशन मुद्राओं, जीते गए इनाम को मंजूरी देते हैं या उन्हें मैनेज करते हैं। इसके अलावा, ऐसे ऐप्लिकेशन जो जुआ खेलने के लिए पैसे जमा करते हैं या इनाम के तौर पर असली चीज़ या असली पैसे ऑफ़र करते हैं।

## गेम से जुड़े लॉयल्टी कार्यक्रम

जहां कानूनी तौर पर अनुमति हो और जुए या गेमिंग के लाइसेंस से जुड़ी अन्य ज़रूरी शर्तें लागू न हों वहां हम उन लॉयल्टी कार्यक्रमों को अनुमति देते हैं जो उपयोगकर्ताओं को असली इनाम या पैसे देते हैं। ये गेम 'Play स्टोर' की नीचे बताई गई ज़रूरी शर्तों के मुताबिक हैं:

### सभी ऐप्लिकेशन के लिए (गेम और गेम के अलावा अन्य ऐप्लिकेशन):

- लॉयल्टी कार्यक्रम के फ़ायदे, सुविधाएं या इनाम, ऐप्लिकेशन में पैसे के किसी भी मान्य लेन-देन के लिए पूरी तरह से पूरक और अलग होने चाहिए। पैसे का कोई भी मान्य लेन-देन, सामान या सेवाओं के लिए ऐसा असली लेन-देन होना चाहिए जो लॉयल्टी कार्यक्रम पर निर्भर न करता हो। यह न तो खरीदारी पर निर्भर होना चाहिए और न ही किसी भी तरह की अदला-बदली से जुड़ा होना चाहिए। ऐसा न होने पर, पैसे दांव पर लगाकर खेले जाने वाले जुए, गेम, और प्रतियोगिताओं से जुड़ी नीति का उल्लंघन होगा।
- उदाहरण के लिए, पैसे के किसी भी मान्य लेन-देन का कोई भी हिस्सा लॉयल्टी कार्यक्रम में हिस्सा लेने के लिए शुल्क या दांव पर लगाई गई रकम नहीं दिखा सकता। साथ ही, पैसे के किसी भी मान्य लेन-देन से उसकी सामान्य कीमत से ज़्यादा कीमत वाले सामान या सेवाएं नहीं खरीदनी चाहिए।

### गेम ऐप्लिकेशन के लिए:

- पैसे के किसी भी मान्य लेन-देन से जुड़े फ़ायदों, सुविधाओं या इनाम वाले लॉयल्टी पॉइंट या इनाम सिर्फ़ तय अनुपात के आधार पर ही दिए और रिडीम किए जाने चाहिए। इस अनुपात के बारे में, ऐप्लिकेशन के साथ-साथ कार्यक्रम के लिए सार्वजनिक तौर पर उपलब्ध आधिकारिक नियमों में भी साफ़ तौर पर बताया जाता है। साथ ही, मिलने वाले फ़ायदों या छूट वाली कीमत का इस्तेमाल, गेम की परफ़ॉर्मंस या मौके पर आधारित नतीजों, इनाम या फ़ायदे के तौर पर नहीं होना चाहिए।

## गेम के अलावा अन्य ऐप्लिकेशन के लिए:

- लॉयल्टी पॉइंट या इनाम, किसी प्रतियोगिता या मौके पर आधारित नतीजों के साथ जोड़े जा सकते हैं। इसके लिए, उन्हें नीचे दी गई शर्तों को पूरा करना होगा। पैसे के किसी भी मान्य लेन-देन से जुड़े फ़ायदों, सुविधाओं या इनाम वाले लॉयल्टी कार्यक्रम के लिए इन शर्तों को पूरा करना ज़रूरी है:
- कार्यक्रम के आधिकारिक नियमों को ऐप्लिकेशन में प्रकाशित करें।
- ऐसे कार्यक्रमों के लिए जिनमें वैरिएबल, किसी भी क्रम में मिलने वाले इनाम सिस्टम या जोखिम शामिल हों: कार्यक्रम के लिए बताई गई आधिकारिक शर्तों के तहत ज़ाहिर करें, 1) इनाम पता करने की संभावना वाले इनाम कार्यक्रमों में, इनाम पाने की कितनी संभावना है और 2) इस तरह के बाकी सभी कार्यक्रमों के लिए, चुनने के तरीके (जैसे कि इनाम का पता लगाने में इस्तेमाल किए जाने वाले वैरिएबल)।
- ड्रॉइंग, स्वीपस्टैक्स या इसी तरह के अन्य प्रचार वाले कार्यक्रम की आधिकारिक शर्तों में, हर प्रचार के लिए विजेताओं की तय संख्या, हिस्सा लेने की आखिरी तारीख, और इनाम पाने की तारीख के बारे में खास तौर पर बताएं।
- ऐप्लिकेशन या कार्यक्रम की आधिकारिक शर्तों के तहत, लॉयल्टी पॉइंट या लॉयल्टी इनाम को बढ़ाने और रिडीम करने के लिए, किसी तय अनुपात के बारे में खास तौर पर बताएं।

लॉयल्टी कार्यक्रम वाले ऐप्लिकेशन	लॉयल्टी गेमिफ़िकेशन और कई इनाम	तय अनुपात/ शेड्यूल के हिसाब से लॉयल्टी इनाम	लॉयल्टी कार्यक्रम के लिए ज़रूरी नियम और शर्तें	नियम और शर्तों में, मौके के हिसाब से काम करने वाले किसी भी लॉयल्टी कार्यक्रम से जुड़ी संभावनाओं या चुनने के तरीके की जानकारी देनी चाहिए
गेम	अनुमति नहीं है	अनुमति है	ज़रूरी	लागू नहीं (गेम ऐप्लिकेशन, लॉयल्टी कार्यक्रम में मौके के हिसाब से काम करने वाले एलिमेंट का इस्तेमाल नहीं कर सकते)
गेम के अलावा अन्य ऐप्लिकेशन	अनुमति है	अनुमति है	ज़रूरी	ज़रूरी

## Play पर मौजूद ऐप्लिकेशन में जुए या असली पैसे दांव पर लगाकर खेले जाने वाले गेम, प्रतियोगिताएं, और टूर्नामेंट से जुड़े विज्ञापन

जुए, असली पैसे दांव पर लगाकर खेले जाने वाले गेम, प्रतियोगिताओं, और टूर्नामेंट के प्रमोशन से जुड़े विज्ञापन दिखाने वाले ऐप्लिकेशन को तब ही अनुमति दी जाती है, जब वे नीचे दी गई ज़रूरी शर्तों को पूरा करते हैं:

- किसी भी इलाके में विज्ञापन दिखाने के लिए, ऐप्लिकेशन और विज्ञापन (इसमें विज्ञापन देने वाले लोग भी शामिल हैं) को उस इलाके में लागू होने वाले सभी कानूनों और उद्योग के मानकों का पालन करना होगा;
- विज्ञापन को जुए से जुड़े ऐसे सभी प्रॉडक्ट और सेवाओं के प्रचार के लाइसेंस के लिए लागू होने वाली सभी ज़रूरी स्थानीय शर्तों को पूरा करना चाहिए;
- ऐप्लिकेशन में जुए से जुड़ा कोई विज्ञापन, 18 साल से कम उम्र के लोगों को नहीं दिखाना चाहिए;
- ऐप्लिकेशन को 'परिवार के लिए बनाए गए' कार्यक्रम का हिस्सा नहीं होना चाहिए;
- ऐप्लिकेशन को 18 साल से कम उम्र के लोगों को टारगेट नहीं करना चाहिए;
- अगर जुए से जुड़े ऐप्लिकेशन का प्रचार किया जा रहा है (जैसा कि ऊपर बताया गया है), तो विज्ञापन के लैंडिंग पेज पर, विज्ञापन में दिखने वाली ऐप्लिकेशन लिस्ट या ऐप्लिकेशन के अंदर, ज़िम्मेदारी से खेले जाने वाले जुए के बारे में साफ़ तौर पर जानकारी दिखानी चाहिए;
- ऐप्लिकेशन में नकली जुए से जुड़ा कॉन्टेंट नहीं होना चाहिए। उदाहरण के लिए, सोशल कसीनो ऐप्लिकेशन और वर्चुअल स्लॉट मशीन वाले ऐप्लिकेशन;
- ऐप्लिकेशन में जुए या असली पैसे दांव पर लगाकर खेले जाने वाले गेम, लॉटरी या टूर्नामेंट में मदद करने वाली या इनके साथ काम करने वाली सुविधाएं नहीं दी जानी चाहिए। उदाहरण के लिए, ऐसी सुविधा जो जुआ खेलने, पेआउट, खेल के स्कोर/ऑड्स/परफॉर्मंस को ट्रैक करने या इनमें हिस्सा लेने के लिए दिए जाने वाले पैसे को मैनेज करने में मदद करती है;

- ऐप्लिकेशन के कॉन्टेंट में जुए या असली पैसे दांव पर लगाकर खेले जाने वाले गेम, लॉटरी या टूर्नामेंट का प्रमोशन नहीं होना चाहिए। इसके अलावा, इसे ऐसी सेवाएं देने वाले पेज पर भी लोगों को नहीं ले जाना चाहिए

ऊपर दिए गए सेक्शन में बताई गई सभी ज़रूरी शर्तों को पूरा करने वाले ऐप्लिकेशन ही जुए या असली पैसे देकर खेले जाने वाले गेम, लॉटरी या टूर्नामेंट के विज्ञापन दिखा सकते हैं। जुआ या असली पैसे को दांव पर लगाकर खेले जाने वाले गेम, लॉटरी या टूर्नामेंट के विज्ञापन उन ऐप्लिकेशन में दिखाए जा सकते हैं जिन्हें जुए से जुड़े (जैसा कि ऊपर बताया गया है) या डेली फ्रैंटेसी स्पोर्ट (जैसा कि नीचे बताया गया है) वाले ऐप्लिकेशन के तौर पर अनुमति मिल चुकी है। साथ ही, वे ऊपर बताए गए एक से छह बिन्दु तक की सभी ज़रूरी शर्तों को पूरा करते हैं।

### उल्लंघनों के उदाहरण

- ऐसा ऐप्लिकेशन जो कम उम्र के लोगों के लिए डिज़ाइन किया गया है और उसमें जुए की सेवाओं का प्रचार करने वाला विज्ञापन दिखाया जाता है
- ऐसा नकली कसीनो गेम जो असली पैसे देकर खेले जाने वाले कसीनो का प्रचार करता है या लोगों को इस तरह के पेज पर ले जाता है
- खेल के ऑड्स को ट्रैक करने वाला ऐसा ऐप्लिकेशन जिसमें जुए से जुड़े विज्ञापन दिखाए जाते हैं। ये विज्ञापन, लोगों को स्पोर्ट बेटिंग साइट पर ले जाते हैं
- जिन ऐप्लिकेशन में जुए से जुड़े ऐसे विज्ञापन दिखाए जाते हैं जो **धोखाधड़ी वाले विज्ञापन** की हमारी नीति का उल्लंघन करते हैं। उदाहरण के लिए, ऐप्लिकेशन इस्तेमाल करने वाले लोगों को बटन, आइकॉन या ऐप्लिकेशन के दूसरे इंटरैक्टिव एलिमेंट के तौर पर दिखाए जाने वाले विज्ञापन

## डेली फ्रैंटेसी स्पोर्ट (DFS) वाले ऐप्लिकेशन

हम डेली फ्रैंटेसी स्पोर्ट (DFS) वाले ऐप्लिकेशन को सिर्फ तब अनुमति देते हैं, जब वे स्थानीय कानून के मुताबिक नीचे दी गई ज़रूरी शर्तों को पूरा करते हैं:

- ऐप्लिकेशन या तो 1) सिर्फ अमेरिका में उपलब्ध हो या उसे 2) अमेरिका के अलावा दूसरे देशों में, जुए से जुड़े ऐप्लिकेशन की ऊपर बताई गई ज़रूरी शर्तों और ऐप्लिकेशन प्रोसेस के तहत मंजूरी दी गई हो;
- 'Play स्टोर' पर ऐप्लिकेशन को उपलब्ध कराने के लिए, डेवलपर को **DFS ऐप्लिकेशन** प्रोसेस सही तरीके से पूरा करना होगा;
- ऐप्लिकेशन को हर उस देश में लागू सभी कानूनों और उद्योग के मानकों का पालन करना चाहिए जहां उसे उपलब्ध कराया जाता है;
- ऐप्लिकेशन को कम उम्र के लोगों को ऐप्लिकेशन में जुआ खेलने या पैसे का लेन-देन करने से रोकना चाहिए;
- ऐप्लिकेशन को Google Play पर, पैसे चुकाकर या Google Play इन-ऐप्लिकेशन बिलिंग का इस्तेमाल करके खरीदे जाने वाले ऐप्लिकेशन के तौर पर मौजूद नहीं होना चाहिए;
- ऐप्लिकेशन 'Play स्टोर' से मुफ्त में डाउनलोड और इंस्टॉल किए जा सकने वाला होना चाहिए;
- ऐप्लिकेशन को AO (सिर्फ वयस्क) या **IARC** के तौर पर रेट किया जाना चाहिए;
- ऐप्लिकेशन और उसकी ऐप्लिकेशन लिस्टिंग में, सही तरीके से जुआ खेलने से जुड़ी जानकारी को साफ़ तौर पर दिखाया जाना चाहिए;
- ऐप्लिकेशन को अमेरिका के हर उस राज्य या इलाके में लागू सभी कानूनों और उद्योग मानकों का पालन करना होगा जहां उसे उपलब्ध कराया जाता है;
- डेवलपर के पास अमेरिका के हर उस राज्य या इलाके के लिए मान्य लाइसेंस होना चाहिए जहां रोज़ाना के फ्रैंटेसी स्पोर्ट वाले ऐप्लिकेशन के लिए लाइसेंस की ज़रूरत होती है;
- ऐप्लिकेशन के इस्तेमाल को अमेरिका के उन राज्यों या इलाकों में रोकना चाहिए जहां डेवलपर के पास रोज़ाना के फ्रैंटेसी स्पोर्ट वाले ऐप्लिकेशन के लिए ज़रूरी लाइसेंस नहीं है; और
- अमेरिका के जिन राज्यों और इलाकों में डेली फ्रैंटेसी स्पोर्ट वाले ऐप्लिकेशन गैरकानूनी हैं वहां ऐप्लिकेशन इस्तेमाल करने की अनुमति नहीं होनी चाहिए।

## गैरकानूनी गतिविधियां

हम ऐसे ऐप्लिकेशन को अनुमति नहीं देते जो गैरकानूनी गतिविधियों की सुविधा देते हैं या उनका प्रचार करते हैं।

यहां आम तौर पर होने वाले उल्लंघनों के कुछ उदाहरण दिए गए हैं:

- गैरकानूनी दवाएं या डॉक्टर की सलाह के बिना दवाएं खरीदने या बेचने की सुविधा देना.
- नाबालिगों को किसी नशीली दवा, शराब या तंबाकू का इस्तेमाल करते हुए या बेचते हुए दिखाना या बढ़ावा देना.
- गैरकानूनी दवाएं उगाने या बनाने के निर्देश.

## यूज़र जनरेटेड कॉन्टेंट (यूजीसी)

यूज़र जनरेटेड कॉन्टेंट (यूजीसी) ऐसा कॉन्टेंट है जिसे लोग किसी ऐप्लिकेशन में जोड़ते हैं। साथ ही, जो ऐप्लिकेशन इस्तेमाल करने वाले लोगों के कम से कम एक ग्रुप को दिखता है या वे उसे एक्सेस कर सकते हैं।

ऐसे ऐप्लिकेशन जिनमें यूजीसी (लोगों का बनाया कॉन्टेंट) होता है या जो इसकी सुविधा देते हैं उनके लिए ज़रूरी है कि:

- ऐप्लिकेशन इस्तेमाल करने वाले लोग यूजीसी बनाने या अपलोड करने से पहले ऐप्लिकेशन को इस्तेमाल करने की शर्तों और/या उपयोगकर्ता नीति को स्वीकार करें;
- आपत्तिजनक कॉन्टेंट और व्यवहार को तय करें (Google Play के डेवलपर कार्यक्रम की नीतियों के मुताबिक) और ऐप्लिकेशन के इस्तेमाल की शर्तों और उपयोगकर्ता नीतियों के तहत उन पर पाबंदी लगाई जाए;
- बेहतर, असरदार, और लगातार होने वाला यूजीसी मॉडरेशन लागू किया जाए। ऐप्लिकेशन पर होस्ट किया गया इस तरह का यूजीसी उचित और अनुकूल होता है
  - लाइव स्ट्रीमिंग ऐप्लिकेशन के मामले में, लोगों के लिए बनाए गए आपत्तिजनक कॉन्टेंट को रीयल-टाइम में जितना जल्दी हो सके उतना जल्दी हटा देना चाहिए;
  - ऑगमेंटेड रिएलिटी ऐप्लिकेशन के मामले में, यूजीसी मॉडरेशन (जिसमें इन-ऐप्लिकेशन रिपोर्टिंग सिस्टम शामिल है) को, आपत्तिजनक एआर यूजीसी (उदाहरण के लिए, अश्लील यौन एआर इमेज) और संवेदनशील एआर एंकरिंग की जगह (उदाहरण के लिए, एआर एंकरिंग से उन जगहों के मालिकों को समस्या हो सकती है जिन पर पाबंदी लगी होती है, जैसे कि सेना का बेस या निजी संपत्ति) के लिए ज़िम्मेदार होना चाहिए;
- ऐप्लिकेशन के अंदर ऐसा सिस्टम देना चाहिए जो ऐप्लिकेशन इस्तेमाल करने वाले लोगों के लिए आसान हो। साथ ही, यूजीसी सही न होने पर इस सिस्टम की मदद से, लोग इसकी शिकायत कर सकें और कार्रवाई कर सकें;
- बुरा बर्ताव करने वाले ऐसे लोग जो ऐप्लिकेशन के इस्तेमाल की शर्तों और/या उपयोगकर्ता नीति का उल्लंघन करते हैं उन्हें हटा देना चाहिए या ब्लॉक कर देना चाहिए;
- ऐप्लिकेशन के अंदर कमाई करने की सुविधा को इस्तेमाल करने वाले उपयोगकर्ताओं के आपत्तिजनक बर्ताव को बढ़ावा नहीं देना चाहिए।

ऐसे ऐप्लिकेशन जिनका मुख्य मकसद आपत्तिजनक यूजीसी को शामिल करना है उन्हें Google Play से हटा दिया जाएगा। इसी तरह, उन ऐप्लिकेशन को भी Google Play से हटा दिया जाएगा जो मुख्य रूप से आपत्तिजनक यूजीसी होस्ट करने के लिए इस्तेमाल किए जाते हैं या ऐप्लिकेशन इस्तेमाल करने वाले लोगों के बीच आपत्तिजनक यूजीसी दिखाने वाले ऐप्लिकेशन की छवि बनाते हैं।

यहां आम तौर पर होने वाले उल्लंघनों के कुछ उदाहरण दिए गए हैं:

- यौन रूप से अश्लीलता फैलाने वाले ऐसे यूज़र जनरेटेड कॉन्टेंट को बढ़ावा देना जिसमें मुख्य रूप से पैसे लेकर आपत्तिजनक कॉन्टेंट को बढ़ावा या अनुमति देने वाली सुविधाएं शामिल हैं।
- यूज़र जनरेटेड कॉन्टेंट वाले ऐसे ऐप्लिकेशन जिनमें डराने, उत्पीड़न करने या धमकियां देने के खिलाफ़ ज़रूरी सुरक्षा उपायों की कमी हो, खासकर नाबालिगों को लेकर।
- किसी ऐप्लिकेशन में शामिल ऐसी पोस्ट, टिप्पणियां या फ़ोटो जिनका मुख्य मकसद किसी दूसरे व्यक्ति के साथ बुरा बर्ताव करना, नुकसान पहुंचाने वाला हमला करना या मज़ाक़ उड़ाने के लिए उसे प्रताड़ित करना या अकेला छोड़ देना हो।
- ऐसे ऐप्लिकेशन जो आपत्तिजनक कॉन्टेंट के बारे में लोगों की शिकायतों को हल करने में लगातार नाकामयाब होते हैं।

## ऐसी चीज़ें जिनकी बिक्री या प्रचार की अनुमति नहीं है

Google Play कानूनी दावे के बावजूद भी, ऐसे ऐप्लिकेशन को अनुमति नहीं देता जो ऐसी चीज़ों की बिक्री या प्रचार करते हैं जिनकी अनुमति नहीं है। उदाहरण:

- [पाबंदी वाली दवाओं और सप्लीमेंट](#) की सूची के सभी आइटम। इस लिस्ट में और भी चीज़ें शामिल हो सकती हैं।
- ऐसे प्रॉडक्ट जिनमें इफ़ेड्रा है

- वज़न घटाने या वज़न नियंत्रण से जुड़े या एनाबॉलिक स्टेरॉइड के साथ प्रचार किए गए ह्यूमन कोरियोनिक गॉनाडोट्रोपिन (एचसीजी) वाले प्रॉडक्ट
- एक्टिव फ़ार्मास्यूटिकल या खतरनाक सामग्री वाले हर्बल और डाइट सप्लीमेंट
- स्वास्थ्य से जुड़े झूठे या गुमराह करने वाले दावे, जिनमें यह कहा गया है कि प्रॉडक्ट डॉक्टर से सुझाई गई दवाओं या नियंत्रित पदार्थों की तरह काम करता है
- किसी खास बीमारी या रोग को रोकने, उसकी चिकित्सा या इलाज करने के लिए सुरक्षित या प्रभावी होने के दावे के साथ बेचे जाने वाले ऐसे प्रॉडक्ट जिनकी सरकार ने मंजूरी न दी हो
- किसी भी सरकारी या कानूनी कार्रवाई या चेतावनी के तहत आने वाले प्रॉडक्ट
- ऐसे प्रॉडक्ट जिनका नाम बिना मंजूरी वाली दवाओं या सप्लीमेंट या कंट्रोल किए जाने वाले नियंत्रित पदार्थों से मिलता है

हम बिना मंजूरी वाली या गुमराह करने वाली जिन दवाओं और सप्लीमेंट पर नज़र रखते हैं उनके बारे में ज़्यादा जानकारी के लिए, कृपया [www.legitscript.com](http://www.legitscript.com) पर जाएं.

## बौद्धिक संपत्ति

जब डेवलपर किसी और के काम की नकल करते हैं या बिना किसी ज़रूरी अनुमति के उसका इस्तेमाल करते हैं, तो इससे उस काम के मालिक को नुकसान पहुंच सकता है. दूसरे लोगों के काम का इस तरह से इस्तेमाल न करें कि वह गलत हो.

### बौद्धिक संपत्ति

हम ऐसे ऐप्लिकेशन या डेवलपर खातों को अनुमति नहीं देते जो दूसरे लोगों के बौद्धिक संपत्ति के अधिकारों का उल्लंघन करते हैं. इनमें ट्रेडमार्क, कॉपीराइट, पेटेंट, कारोबार से जुड़ी गोपनीय जानकारी, और अन्य मालिकाना अधिकार शामिल हैं. हम ऐसे ऐप्लिकेशन को भी अनुमति नहीं देते हैं जो बौद्धिक संपत्ति के अधिकारों का उल्लंघन करते हैं या ऐसा करने का बढ़ावा देते हैं.

हम कॉपीराइट के कथित उल्लंघन के आरोपों वाली, साफ़ तौर पर दी गई सूचनाओं का जवाब देंगे. ज़्यादा जानकारी पाने के लिए या डीएमसीए (DMCA) अनुरोध दर्ज करने के लिए, हमारी [कॉपीराइट से जुड़ी प्रक्रियाओं](#) वाले पेज पर जाएं.

किसी ऐप्लिकेशन में हो रही नकली सामान की बिक्री या प्रचार के बारे में शिकायत करने के लिए, कृपया [नकली सामान की सूचना](#) सबमिट करें.

अगर आप ट्रेडमार्क के मालिक हैं और आपको लगता है कि Google Play पर मौजूद कोई ऐप्लिकेशन आपके ट्रेडमार्क अधिकारों का उल्लंघन करता है, तो हमारा सुझाव है कि अपनी समस्या हल करने के लिए सीधे डेवलपर से संपर्क करें. अगर आपकी समस्या फिर भी हल नहीं होती है, तो कृपया इस [फ़ॉर्म](#) को भरकर ट्रेडमार्क के बारे में शिकायत दर्ज करें.

अगर आपके पास यह बताने वाला दस्तावेज़ है कि आपके पास अपने ऐप्लिकेशन या स्टोर पेज में किसी तीसरे पक्ष की बौद्धिक संपत्ति (जैसे कि ब्रैंड का नाम, लोगो, और ग्राफ़िक रचना) का इस्तेमाल करने की अनुमति है, तो आप सबमिट करने से पहले ही [Google Play की टीम से संपर्क करें](#). इससे, आप यह पक्का कर सकते हैं कि आपका ऐप्लिकेशन बौद्धिक संपत्ति के उल्लंघन के लिए अस्वीकार न हो जाए.

### कॉपीराइट वाले कॉन्टेंट का बिना अनुमति के इस्तेमाल करना

हम ऐसे ऐप्लिकेशन को अनुमति नहीं देते जो कॉपीराइट का उल्लंघन करते हैं. कॉपीराइट कॉन्टेंट में बदलाव करने से भी उल्लंघन हो सकता है. ऐसा हो सकता है कि डेवलपर को, कॉपीराइट वाले कॉन्टेंट को इस्तेमाल करने के अधिकारों का सबूत देने को कहा जाए.

जब आप अपने ऐप्लिकेशन की सुविधा के बारे में बता रहे हों, तो उसमें कॉपीराइट वाले कॉन्टेंट का इस्तेमाल करते समय कृपया ध्यान रखें. आम तौर पर, सुरक्षित तरीका यह है कि कुछ ऐसा बनाएं जो पूरी तरह से आपका ही हो.

यहां कॉपीराइट किए गए ऐसे कॉन्टेंट के कुछ उदाहरण दिए गए हैं जो बगैर अनुमति के या कानूनी रूप से मान्य वजह के बिना आम तौर पर इस्तेमाल किए जाते हैं:

- म्यूज़िक एल्बम, वीडियो गेम, और किताबों के लिए कवर आर्ट.
- फ़िल्मों, टेलिविज़न या वीडियो गेम की मार्केटिंग इमेज.
- कॉमिक बुक, कार्टून, फ़िल्मों, संगीत वीडियो या टेलिविज़न के आर्टवर्क या इमेज.
- कॉलेज और पेशेवर खेल टीम के लोगो.
- किसी लोकप्रिय हस्ती के सोशल मीडिया खाते से ली गई फ़ोटो.

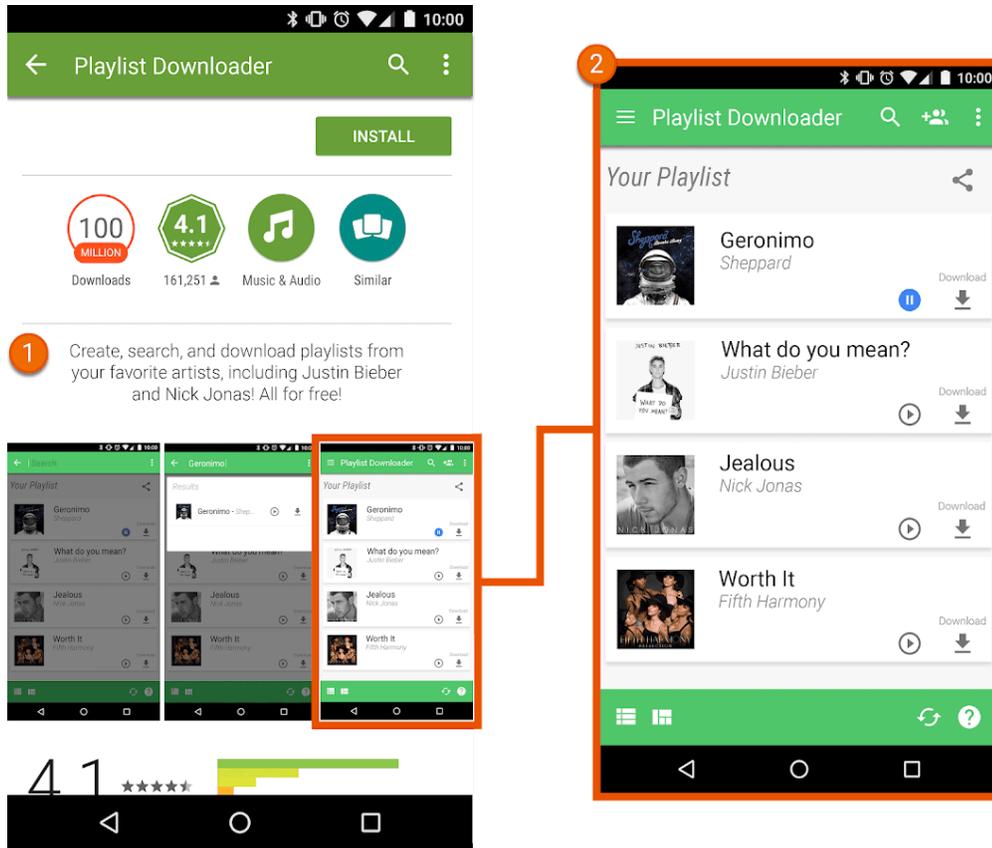
- लोकप्रिय हस्तियों की पेशेवर फ़ोटो.
- कॉपीराइट के तहत आने वाला ऐसा रीप्रोडक्शन या "फ़ैन-आर्ट" जिसे मूल काम से अलग न किया जा सकता हो.
- वे ऐप्लिकेशन जिनमें ऐसे साउंडबोर्ड होते हैं जो कॉपीराइट वाले कॉन्टेंट की ऑडियो क्लिप चलाते हैं.
- ऐसी किताबों का पूरा रीप्रोडक्शन या अनुवाद जो सार्वजनिक डोमेन में मौजूद नहीं है.

## कॉपीराइट के उल्लंघन को बढ़ावा देना

हम ऐसे ऐप्लिकेशन को अनुमति नहीं देते जो कॉपीराइट के उल्लंघन को बढ़ावा देते हैं या उसके लिए उकसाते हैं. अपना ऐप्लिकेशन प्रकाशित करने से पहले, पता लगाएं कि आपका ऐप्लिकेशन कॉपीराइट उल्लंघन को बढ़ावा तो नहीं दे रहा. साथ ही, अगर ज़रूरी हो, तो कानूनी सलाह लें.

यहां आम तौर पर होने वाले उल्लंघनों के कुछ उदाहरण दिए गए हैं:

- ऐसे स्ट्रीमिंग ऐप्लिकेशन जो बिना किसी अनुमति के ऐप्लिकेशन इस्तेमाल करने वाले लोगों को कॉपीराइट वाले कॉन्टेंट की लोकल कॉपी डाउनलोड करने देते हैं.
- ऐसे ऐप्लिकेशन जो लागू कॉपीराइट कानून का उल्लंघन करते हुए और कॉपीराइट किए गए काम, संगीत, और वीडियो को स्ट्रीम करने और डाउनलोड करने के लिए लोगों को बढ़ावा देते हैं:



- ① इस ऐप्लिकेशन लिस्टिंग में दी गई जानकारी, लोगों को कॉपीराइट वाले कॉन्टेंट को बिना अनुमति के डाउनलोड करने के लिए बढ़ावा देती है.
- ② इस ऐप्लिकेशन लिस्टिंग में दिया गया स्क्रीनशॉट, लोगों को कॉपीराइट वाले कॉन्टेंट को बिना अनुमति के डाउनलोड करने के लिए बढ़ावा देता है.

## ट्रेडमार्क का उल्लंघन करना

हम ऐसे ऐप्लिकेशन को अनुमति नहीं देते जो दूसरों के ट्रेडमार्क का उल्लंघन करते हैं. ट्रेडमार्क एक ऐसा शब्द, चिह्न या दोनों का मिला-जुला रूप है जिससे पता चलता है कि किसी सामान या सेवा का स्रोत क्या है. पहचान के बाद ट्रेडमार्क, मालिक को कुछ वस्तुओं या सेवाओं के संबंध में ट्रेडमार्क के इस्तेमाल के लिए खास अधिकार देता है.

ट्रेडमार्क के उल्लंघन का मतलब है किसी एक जैसे या मिलते-जुलते ट्रेडमार्क का गलत तरीके से या बिना अनुमति के इस तरह इस्तेमाल करना कि प्रॉडक्ट के स्रोत को लेकर गलतफ़हमी होने की संभावना हो. अगर आप अपने ऐप्लिकेशन के लिए किसी दूसरे पक्ष के ट्रेडमार्क का इस्तेमाल इस

तरीके से करते हैं जिससे भ्रम की स्थिति पैदा हो सकती है, तो आपका ऐप्लिकेशन निलंबित किया जा सकता है।

## नकली सामान बेचना या उसे बढ़ावा देना

हम ऐसे ऐप्लिकेशन को मंजूरी नहीं देते जो नकली सामान की बिक्री या उनकी बिक्री के लिए प्रचार करते हैं। नकली सामान पर किसी अन्य सामान के ट्रेडमार्क से मेल खाने वाला या साफ़ तौर पर पहचाना न जा सकने वाला एक ट्रेडमार्क या लोगो होता है। इस तरह के प्रॉडक्ट, किसी ब्रैंड के प्रॉडक्ट में मिलने वाली सुविधाओं (ब्रैंड सुविधाओं) की नकल करके खुद को ब्रैंड मालिक के असली प्रॉडक्ट की तरह पेश करते हैं।

## निजता, धोखाधड़ी, और डिवाइस का गलत इस्तेमाल

हम ऐप्लिकेशन इस्तेमाल करने वाले लोगों की निजता की सुरक्षा करने और उन्हें पूरी तरह सुरक्षित माहौल देने का वादा करते हैं। ऐसे ऐप्लिकेशन पर सख्त पाबंदी है जो धोखाधड़ी करते हैं, नुकसान पहुंचाते हैं या जिनका इरादा किसी नेटवर्क, डिवाइस या निजी डेटा से छेड़छाड़ करना या उसका गलत इस्तेमाल करना है।

### ऐप्लिकेशन इस्तेमाल करने वाले व्यक्ति का डेटा

आप ऐप्लिकेशन इस्तेमाल करने वाले व्यक्ति के डेटा को कैसे मैनेज करते हैं, इस बारे में आपको साफ़ तौर पर जानकारी देनी चाहिए। इसमें ऐप्लिकेशन इस्तेमाल करने वाले किसी व्यक्ति से इकट्ठा की गई या उसके बारे में जानकारी के अलावा, डिवाइस की जानकारी भी शामिल है। इसका मतलब है कि आपके ऐप्लिकेशन का ऐक्सेस, डेटा को इकट्ठा करने, इस्तेमाल करने, और उसे शेयर करने की जानकारी देना। साथ ही, डेटा का इस्तेमाल सिर्फ़ बताए गए उद्देश्यों के लिए करना। इसके अलावा, अगर आपका ऐप्लिकेशन उपयोगकर्ता का निजी या संवेदनशील डेटा मैनेज करता है, तो कृपया नीचे "निजी और संवेदनशील जानकारी" सेक्शन में बताई गई दूसरी ज़रूरतों को भी देखें। Google Play की ये ज़रूरी शर्तें, निजता और डेटा सुरक्षा के लागू कानूनों में बताई गई ज़रूरी शर्तों से अलग हैं।

### निजी और संवेदनशील जानकारी

निजी और संवेदनशील डेटा में, ऐप्लिकेशन इस्तेमाल करने वाले व्यक्ति की व्यक्तिगत पहचान से जुड़ी जानकारी, वित्तीय और क्रेडिट/डेबिट कार्ड की जानकारी, पुष्टि करने की जानकारी, फ़ोनबुक, संपर्क, [डिवाइस की जगह की जानकारी](#), मैसेज (एसएमएस) और कॉल से जुड़ा डेटा, माइक्रोफ़ोन, कैमरा, और अन्य संवेदनशील डिवाइस या इस्तेमाल किए गए डेटा जैसी अन्य जानकारी भी शामिल है। अगर आपका ऐप्लिकेशन लोगों का संवेदनशील डेटा मैनेज करता है, तो आपको इन बातों का ध्यान रखना चाहिए:

- ऐप्लिकेशन से मिले निजी और संवेदनशील डेटा के ऐक्सेस, संग्रह, इस्तेमाल, और इसे शेयर करने को उन मकसदों तक सीमित करना जो ऐप्लिकेशन की सुविधाएं देने और उन्हें बेहतर बनाने के लिए सीधे तौर पर जुड़े हैं। उदाहरण के लिए, ऐप्लिकेशन इस्तेमाल करने वाले व्यक्ति की उम्मीद के मुताबिक काम करने का तरीका, जिसे दस्तावेज़ में बताया गया है और 'Play स्टोर' में ऐप्लिकेशन की जानकारी में जिसका प्रचार किया गया है। विज्ञापन दिखाने के लिए, इस डेटा के इस्तेमाल की अनुमति लेने वाले ऐप्लिकेशन को हमारी [विज्ञापन नीति](#) का पालन करना होगा।
- Play Console में तय की गई फ़्रील्ड और ऐप्लिकेशन, दोनों में निजता नीति पोस्ट करें। निजता नीति को ऐप्लिकेशन में ज़ाहिर की गई जानकारी के साथ, इस बात की पूरी जानकारी देनी चाहिए कि आपका ऐप्लिकेशन कैसे उपयोगकर्ता के डेटा को ऐक्सेस, इकट्ठा, शेयर, और इस्तेमाल करता है। आपकी निजता नीति को बताना चाहिए कि आपका ऐप्लिकेशन किस तरह के निजी और संवेदनशील डेटा को ऐक्सेस, इकट्ठा, इस्तेमाल, और शेयर करता है। साथ ही, यह भी बताना चाहिए कि ये डेटा किस तरह के ग्रुप के साथ शेयर किया जाता है।
- आधुनिक क्रिप्टोग्राफी (उदाहरण के लिए, एचटीटीपीएस पर) का इस्तेमाल करके, ऐप्लिकेशन इस्तेमाल करने वाले व्यक्ति का निजी और संवेदनशील डेटा दूसरी जगह तक पहुंचाने के साथ ही सुरक्षित रूप से मैनेज करना चाहिए।
- [Android की अनुमतियों](#) से सुरक्षित किया गया डेटा ऐक्सेस करने से पहले, उपलब्ध होने पर रनटाइम की अनुमतियों के अनुरोध का इस्तेमाल करें।
- ऐप्लिकेशन इस्तेमाल करने वाले व्यक्ति के निजी या संवेदनशील डेटा की बिक्री न करें।

### खास जानकारी ज़ाहिर करना और सहमति की ज़रूरत

उन मामलों में जहां हो सकता है कि ऐप्लिकेशन इस्तेमाल करने वाले लोगों को इस बात की उम्मीद न हो कि उनका निजी या संवेदनशील डेटा, आपके ऐप्लिकेशन में नीति का पालन करने वाली सुविधाओं या काम करने के तरीके में सुधार करने के लिए ज़रूरी होगा, जैसे कि डेटा संग्रह आपके ऐप्लिकेशन के बैकग्राउंड में होता है। इसके अलावा, आपको नीचे बताई गई ज़रूरी शर्तों को भी पूरा करना होगा:

आपको डेटा को ऐक्सेस करने, इकट्ठा करने, इस्तेमाल करने, और शेयर करने के बारे में ऐप्लिकेशन में जानकारी देनी होगी। ऐप्लिकेशन में दी जाने वाली जानकारी:

- ऐप्लिकेशन के अंदर होनी चाहिए, न कि सिर्फ ऐप्लिकेशन के ब्यौरे में या किसी वेबसाइट पर;
- ऐप्लिकेशन के सामान्य इस्तेमाल के दौरान दिखनी चाहिए और उपयोगकर्ता को इसके लिए मेन्यू या सेटिंग में जाने की ज़रूरत नहीं पड़नी चाहिए;
- इसमें ऐक्सेस या इकट्टा किए जा रहे डेटा की पूरी जानकारी दी जानी चाहिए;
- इसमें यह बताया जाना चाहिए कि डेटा को इस्तेमाल और/या शेयर कैसे किया जाएगा;
- इसे सिर्फ किसी निजता नीति या सेवा की शर्तों में नहीं रखा जा सकता; और
- इसको ऐसी दूसरी जानकारी में शामिल नहीं किया जा सकता जो निजी या संवेदनशील डेटा इकट्टा करने से जुड़ी नहीं है।

ऐप्लिकेशन में दी जाने वाली जानकारी के साथ, ऐप्लिकेशन इस्तेमाल करने वाले व्यक्ति की सहमति लेने का अनुरोध शामिल होना चाहिए। साथ ही, जहां यह मौजूद हो वहां एक रनटाइम अनुमति भी होनी चाहिए। आप उपयोगकर्ता की सहमति के बिना किसी भी निजी डेटा को ऐक्सेस या इकट्टा नहीं कर पाएंगे। सहमति लेने के लिए ऐप्लिकेशन का अनुरोध:

- सहमति संवाद साफ़ और सीधे तौर पर दिया जाना चाहिए;
- ऐप्लिकेशन इस्तेमाल करने वाले व्यक्ति के लिए, यह ज़रूरी है कि वह स्वीकार करने लायक कार्रवाई करें। जैसे कि स्वीकार करने के लिए टैप करना, सही का निशान लगाकर चुनना;
- सहमति से बाहर निकलने या कहीं और जाने को सहमति नहीं समझा जाना चाहिए। इसमें टैप करके बाहर जाने या वापस जाने के लिए बैक या होम बटन दबाना शामिल है; और
- ऐप्लिकेशन इस्तेमाल करने वाले व्यक्ति की सहमति लेने के लिए, अपने-आप खारिज या खत्म होने वाले मैसेज का इस्तेमाल नहीं किया जाना चाहिए।

यहां आम तौर पर होने वाले उल्लंघनों के कुछ उदाहरण दिए गए हैं:

- ऐसा ऐप्लिकेशन जो इस्तेमाल करने वाले व्यक्ति के इंस्टॉल किए गए ऐप्लिकेशन की इन्वेंट्री ऐक्सेस करता है और इस डेटा को ऊपर बताई गई निजता नीति, डेटा मैनेज करने, और खास तौर पर सहमति से जानकारी देने की ज़रूरी शर्तों के तहत आने वाले निजी या संवेदनशील डेटा के रूप में नहीं देखता है।
- ऐसा ऐप्लिकेशन जो किसी व्यक्ति के फ़ोन या संपर्क सूची के डेटा को ऐक्सेस करता है और इस डेटा को ऊपर बताई गई निजता नीति, डेटा मैनेज करने, खास तौर पर जानकारी देने, और सहमति पाने की ज़रूरी शर्तों के मुताबिक, निजी या संवेदनशील डेटा के रूप में नहीं देखता है।
- ऐसा ऐप्लिकेशन जो किसी व्यक्ति की स्क्रीन रिकॉर्ड करता है और इस डेटा को इस नीति के मुताबिक, निजी या संवेदनशील डेटा के रूप में नहीं देखता है।
- ऐसा ऐप्लिकेशन जो **डिवाइस की जगह की जानकारी** इकट्टा करता है और इसके इस्तेमाल के बारे में पूरी जानकारी नहीं देता है। साथ ही, ऊपर बताई गई ज़रूरी शर्तों के मुताबिक सहमति भी नहीं लेता है।
- ऐसा ऐप्लिकेशन जो ट्रैकिंग, रिसर्च या मार्केटिंग के मकसद से ऐप्लिकेशन के बैकग्राउंड में पाबंदी वाली अनुमतियों को इकट्टा करता है और पूरी तरह से इसके इस्तेमाल की जानकारी नहीं देता है। साथ ही, ऊपर दी गई ज़रूरी शर्तों के मुताबिक सहमति लेता है।

संवेदनशील डेटा के ऐक्सेस पर खास पाबंदियां

ऊपर दी गई शर्तों के अलावा, नीचे दिए गए टेबल में खास गतिविधियों के लिए ज़रूरी शर्तों के बारे में बताया गया है।

गतिविधि	ज़रूरी शर्त
आपका ऐप्लिकेशन वित्तीय या पैसे चुकाने के बारे में जानकारी या सरकारी पहचान की संख्याओं को मैनेज करता है	आपके ऐप्लिकेशन को वित्तीय या भुगतान से जुड़ी गतिविधियों या किसी भी सरकारी पहचान संख्या से जुड़ी कोई भी व्यक्तिगत या संवेदनशील उपयोगकर्ता डेटा सार्वजनिक तौर पर ज़ाहिर नहीं करना चाहिए।
आपका ऐप्लिकेशन गैर-सार्वजनिक फ़ोनबुक या संपर्क जानकारी को मैनेज करता है	हम लोगों के गैर-सार्वजनिक संपर्कों को बिना मंजूरी प्रकाशित करने या उनकी जानकारी देने की अनुमति नहीं देते।
आपके ऐप्लिकेशन में एंटी-	आपके ऐप्लिकेशन को ऐसी निजता नीति पोस्ट करनी चाहिए जिसमें ऐप्लिकेशन में दी गई किसी जानकारी के

वायरस या सुरक्षा के लिए काम करने वाले फ़ंक्शन, जैसे कि एंटी-वायरस, एंटी-मैलवेयर या सुरक्षा से जुड़ी सुविधाएं हैं साथ यह भी बताया जाए कि आपका ऐप्लिकेशन, इस्तेमाल करने वाले व्यक्ति का कौनसा डेटा इकट्ठा करता है और दूसरों तक पहुंचाता है। साथ ही, नीति में यह भी बताया जाए कि उस डेटा का इस्तेमाल किस तरह से किया जाता है। इसके अलावा, निजता नीति में उन ग्रुप की जानकारी भी शामिल होनी चाहिए जिनके साथ डेटा शेयर किया जाता है।

## EU-U.S. Privacy Shield (यूरोपीय संघ-अमेरिका Privacy Shield)

अगर आप Google की ओर से उपलब्ध कराई गई ऐसी व्यक्तिगत जानकारी को एक्सेस करते हैं, इस्तेमाल या प्रोसेस करते हैं जो सीधे तौर पर या किसी दूसरे तरीके से, किसी ऐसे व्यक्ति की पहचान करती है जो मूल रूप से यूरोपीय संघ या स्विट्ज़रलैंड ("यूरोपीय संघ निजी जानकारी") का है, तो आपको ये काम करने होंगे:

- सभी लागू निजता, डेटा सुरक्षा, और डेटा संरक्षण कानूनों, निर्देशों, नियामकों और नियमों का पालन करना;
- ईयू (यूरोपीय संघ) निजी जानकारी सिर्फ़ ऐसे मकसद से एक्सेस करना, इस्तेमाल करना या प्रोसेस करना जो उस व्यक्ति से मिलने वाली सहमति के मुताबिक हो जिससे ईयू (यूरोपीय संघ) की निजी जानकारी जुड़ी है;
- ईयू (यूरोपीय संघ) की निजी जानकारी को नुकसान, गलत इस्तेमाल, और गलत या गैर-कानूनी एक्सेस, जानकारी देने, बदले जाने और नुकसान से बचाने के लिए, संगठन के स्तर पर और तकनीकी स्तर पर ज़रूरी कदम उठाना; और
- उसी स्तर की सुरक्षा मुहैया कराना जैसी **Privacy Shield के सिद्धांतों** में ज़रूरी बताई गई है।

आपको समय-समय पर देखना होगा कि इन शर्तों का पालन ठीक तरीके से हो रहा है या नहीं। अगर, किसी भी समय, आप इन शर्तों का पालन नहीं कर पाते हैं (या अगर इस बात का जोखिम ज़्यादा है कि आप उनका पालन नहीं कर पाएंगे), तो आपको हमें [data-protection-office@google.com](mailto:data-protection-office@google.com) पर ईमेल करके तुरंत बताना चाहिए और यूरोपीय संघ निजी जानकारी से जुड़े काम तुरंत रोक देने चाहिए या सुरक्षा के स्तर को पहले जैसा बनाए रखने के लिए ज़रूरी कदम उठाने चाहिए।

## अनुमतियां

उन ही अनुमतियों का अनुरोध करना चाहिए जो इस्तेमाल करने वाले लोगों के लिए काम की हों। आप सिर्फ़ वे अनुमतियां मांग सकते हैं जो आपके ऐप्लिकेशन में, उन मौजूदा सुविधाओं या सेवाओं को लागू करने के लिए ज़रूरी हैं जिनके बारे में आपने 'Play स्टोर' के अपने पेज पर बताया है। आप ऐसी अनुमतियों का इस्तेमाल नहीं कर सकते जिनमें उपयोगकर्ताओं या डिवाइस डेटा को बताई नहीं गई, लागू नहीं की गई या अनुमति नहीं दी गई जैसी सुविधाओं का एक्सेस मिल जाता है। अनुमतियां लेकर एक्सेस किया गया निजी या संवेदनशील डेटा कभी भी बेचा नहीं जा सकता।

ज़रूरत के मुताबिक (बढ़ती हुई मंजूरी की मदद से) डेटा एक्सेस करने का अनुरोध करें, ताकि इस्तेमाल करने वाले यह समझ सकें कि आपके ऐप्लिकेशन को अनुमति क्यों चाहिए। डेटा का इस्तेमाल सिर्फ़ उन ही मकसदों से करें जिनके लिए इस्तेमाल करने वाले ने सहमति दी है। अगर आप बाद में दूसरे मकसद के लिए डेटा का इस्तेमाल करना चाहते हैं, तो आपको उपयोगकर्ताओं से पूछना होगा और यह पक्का करना होगा कि वे डेटा के दूसरे इस्तेमाल के लिए पूरी तरह से सहमत हों।

## पाबंदी वाली अनुमतियां

ऊपर बताई गई अनुमतियों के अलावा, पाबंदी वाली अनुमतियां वे होती हैं जिन्हें हमारे डेवलपर दस्तावेज़ में, [खतरनाक](#), [विशेष](#) या [हस्ताक्षर](#) के तौर पर शामिल किया गया है। साथ ही, इन पर आगे दी गई दूसरी ज़रूरी शर्तें और पाबंदियां लागू होती हैं:

- पाबंदी वाली अनुमति की मदद से, एक्सेस किए जाने वाले उपयोगकर्ता या डिवाइस के संवेदनशील डेटा को तीसरे पक्ष को ट्रांसफ़र तब ही किया जा सकता है, जब यह उस ऐप्लिकेशन की मौजूदा सुविधाएं या सेवाएं देने या उन्हें बेहतर बनाने के लिए ज़रूरी हो जिससे डेटा इकट्ठा किया गया था। आप लागू कानून का पालन करने या मर्जर, मालिकाना हक या एसेट की बिक्री के लिए भी, उपयोगकर्ताओं को कानूनी रूप से ज़रूरी सूचना देकर डेटा ट्रांसफ़र कर सकते हैं। इसके अलावा, किसी भी तरह से उपयोगकर्ता के डेटा ट्रांसफ़र करने पर पाबंदी है।
- अगर उपयोगकर्ता पाबंदी वाली अनुमति देने से मना कर देते हैं, तो उनके फ़ैसलों का सम्मान करें। साथ ही, किसी गैर ज़रूरी अनुमति पर सहमति देने के लिए उपयोगकर्ताओं पर दबाव नहीं बनाया जा सकता, न ही उनके फ़ैसले को बदलने की कोशिश की जा सकती है। ऐप्लिकेशन इस्तेमाल करने वाले वे लोग जो अपनी संवेदनशील जानकारी का एक्सेस नहीं देते, उनसे अनुमति लेने के लिए ज़रूरी कोशिशें करनी होंगी। (उदाहरण के तौर पर, अगर वे कॉल लॉग का एक्सेस नहीं देते, तो उन्हें मैन्युअल तरीके से फ़ोन नंबर डालने की अनुमति देना)।

कुछ पाबंदी वाली अनुमतियों पर नीचे बताए गए शर्तों के मुताबिक, दूसरी ज़रूरी शर्तें भी लागू हो सकती हैं। इन पाबंदियों का मकसद ऐप्लिकेशन को इस्तेमाल करने वालों की निजता को सुरक्षित रखना है। हम नीचे दी गई ज़रूरी शर्तों में गिनती के अपवादों की अनुमति दे सकते हैं। ऐसा हम उन बेहद

खास मामलों में ही कर सकते हैं जहां ऐप्लिकेशन काफ़ी दमदार या बहुत ज़रूरी सुविधा देते हों और उसे मुहैया कराने का कोई दूसरा तरीका मौजूद नहीं हो। हम दिए गए अपवादों का आकलन, ऐप्लिकेशन इस्तेमाल करने वाले लोगों की निजता या सुरक्षा पर पड़ने वाले असर के मुताबिक करते हैं।

## मैसेज (एसएमएस) और कॉल लॉग की अनुमतियां

मैसेज (एसएमएस) और कॉल लॉग की अनुमतियों को [निजी और संवेदनशील जानकारी](#) नीति, और आगे दी गई पाबंदियों के तहत, इस्तेमाल करने वाले व्यक्ति का संवेदनशील और निजी डेटा माना जाता है:

### पाबंदी वाली अनुमति

### ज़रूरी शर्त

अगर आपका ऐप्लिकेशन मेनिफ़ेस्ट, कॉल लॉग की अनुमति समूह का अनुरोध करता है (जैसे कि `READ_CALL_LOG`, `WRITE_CALL_LOG`, `PROCESS_OUTGOING_CALLS`), तो

इसे डिवाइस पर डिफ़ॉल्ट मैसेज (एसएमएस) या Assistant हैंडलर के रूप में चालू तौर पर रजिस्टर किया जाना चाहिए.

अगर आपका ऐप्लिकेशन मेनिफ़ेस्ट, मैसेज (एसएमएस) अनुमति समूह का अनुरोध करता है (जैसे कि `READ_SMS`, `SEND_SMS`, `WRITE_SMS`, `RECEIVE_SMS`, `RECEIVE_WAP_PUSH`, `RECEIVE_MMS`), तो

इसे डिवाइस पर डिफ़ॉल्ट मैसेज (एसएमएस) या सहायक हैंडलर के रूप में चालू तौर पर रजिस्टर किया जाना चाहिए.

जिन ऐप्लिकेशन में डिफ़ॉल्ट मैसेज (एसएमएस), फ़ोन या सहायक हैंडलर की सुविधा नहीं है, हो सकता है कि वे मेनिफ़ेस्ट में ऊपर दी गई अनुमतियों के बारे में न बताएं। इसमें मेनिफ़ेस्ट का प्लेसहोल्डर टेक्स्ट भी शामिल है। इसके अलावा, उपयोगकर्ताओं को ऊपर दी गई कोई भी अनुमति स्वीकार करने का संकेत देने से पहले, मैसेज (एसएमएस), फ़ोन या सहायक हैंडलर के रूप में ऐप्लिकेशन रजिस्टर होने चाहिए और जब वे डिफ़ॉल्ट हैंडलर न रह जाएं, तो उन्हें उसी समय अनुमति का इस्तेमाल करना बंद कर देना चाहिए। अनुमति दिए गए इस्तेमाल और अपवाद [इस सहायता केंद्र पेज](#) पर दिए गए हैं।

ऐप्लिकेशन सिर्फ़ स्वीकार की हुई मुख्य सुविधाएं देने के लिए अनुमति (और अनुमति से मिलने वाले किसी भी डेटा) का इस्तेमाल कर सकते हैं। मुख्य सुविधा, किसी ऐप्लिकेशन का मुख्य मकसद होती हैं। इसमें ऐसी मुख्य सुविधाओं का एक सेट शामिल हो सकता है जिन्हें ऐप्लिकेशन की जानकारी में खास तौर से बताया जाना चाहिए और उनका प्रचार किया जाना चाहिए। मुख्य सुविधा के बिना, ऐप्लिकेशन “अधूरा” रहता है या किसी काम का नहीं रहता। इस डेटा का ट्रांसफ़र, शेयर या लाइसेंस के ज़रिए इस्तेमाल, सिर्फ़ ऐप्लिकेशन के अंदर मुख्य सुविधाओं या सेवाओं को देने के लिए होना चाहिए। इसका इस्तेमाल किसी और मकसद (जैसे कि दूसरे ऐप्लिकेशन या सेवाओं को बेहतर बनाने, विज्ञापन या मार्केटिंग) के लिए नहीं किया जा सकता है। कॉल लॉग या मैसेज (एसएमएस) से जुड़ी अनुमति से मिलने वाले डेटा के लिए, आप दूसरे तरीकों का इस्तेमाल नहीं कर सकते हैं। इन तरीकों में दूसरी अनुमतियां, एपीआई या तीसरे-पक्ष के स्रोत शामिल हैं।

## जगह की जानकारी की अनुमतियां

[डिवाइस की जगह की जानकारी](#) को [निजी और संवेदनशील जानकारी](#) नीति और नीचे दी गई ज़रूरी शर्तों के तहत, इस्तेमाल करने वाले का निजी और संवेदनशील डेटा माना जाता है:

- ऐप्लिकेशन, जगह की जानकारी की अनुमति की मदद से सुरक्षित डेटा को एक्सेस तब नहीं कर सकते (उदाहरण के लिए, `ACCESS_FINE_LOCATION`, `ACCESS_COARSE_LOCATION`, `ACCESS_BACKGROUND_LOCATION`), जब मौजूदा सुविधाओं या सेवाओं को डिलीवर करने के लिए इसकी ज़रूरत न हो।
- सिर्फ़ विज्ञापन दिखाने या आंकड़े पाने के लिए, आपको कभी भी ऐप्लिकेशन इस्तेमाल करने वाले लोगों से, जगह की जानकारी इस्तेमाल करने की अनुमति का अनुरोध नहीं करना चाहिए। विज्ञापन दिखाने के लिए, इस डेटा के इस्तेमाल की अनुमति देने वाले ऐप्लिकेशन को हमारी [विज्ञापन नीति](#) का पालन करना होगा।
- ऐप्लिकेशन को मौजूदा सुविधा या सेवा देने के लिए उतने ही दायरे का अनुरोध करना चाहिए जो ज़रूरी है। उदाहरण के लिए, अच्छे की बजाय ठीक और बैकग्राउंड की बजाय फ़ोरग्राउंड. साथ ही, ऐप्लिकेशन इस्तेमाल करने वाले लोगों को यह उम्मीद करनी चाहिए कि सुविधा या सेवा को जगह की उतनी जानकारी की ज़रूरत है जितनी के लिए एक्सेस का अनुरोध किया गया है। उदाहरण के लिए, हम ऐसे ऐप्लिकेशन अस्वीकार कर सकते हैं जो कोई खास वजह बताए बिना बैकग्राउंड की जगह की जानकारी का अनुरोध करते हैं या इसे एक्सेस करते हैं।
- बैकग्राउंड में जगह की जानकारी का इस्तेमाल सिर्फ़ ऐसी सुविधाएं देने के लिए हो सकता है जो ऐप्लिकेशन इस्तेमाल करने वालों के लिए फ़ायदेमंद हों और ऐप्लिकेशन के मुख्य फ़ंक्शन से जुड़ी हों।

फ़ोरग्राउंड सेवा (ऐप्लिकेशन के पास ऐक्सेस सिर्फ़ तब हो, जब वह स्क्रीन पर दिख रहा हो, जैसे कि "इस्तेमाल के दौरान") की अनुमति का इस्तेमाल करके, ऐप्लिकेशन की जगह की जानकारी को ऐक्सेस कर सकते हैं। ऐसा सिर्फ़ तब होना चाहिए, जब जगह की जानकारी का इस्तेमाल:

- ऐप्लिकेशन इस्तेमाल करने वालों की शुरू की गई इन-ऐप्लिकेशन कार्रवाई को जारी रखने के लिए करना पड़े और
- ऐप्लिकेशन इस्तेमाल करने वाले व्यक्ति की शुरू की गई कार्रवाई पूरी होने के तुरंत बाद, इसे बंद कर दिया जाए।

खास तौर पर, बच्चों के लिए बनाए गए ऐप्लिकेशन को [परिवार के लिए बनाए गए ऐप्लिकेशन](#) की नीति का पालन करना होगा।

## सभी फ़ाइलों को ऐक्सेस करने की अनुमति

ऐप्लिकेशन इस्तेमाल करने वाले किसी व्यक्ति के डिवाइस पर मौजूद फ़ाइलें और डायरेक्ट्री की विशेषताएं, [निजी और संवेदनशील डेटा](#) नीति और नीचे दी गई ज़रूरी शर्तों के तहत ऐप्लिकेशन इस्तेमाल करने वाले व्यक्ति की निजी और संवेदनशील जानकारी मानी जाती है:

- ऐप्लिकेशन को डिवाइस की सिर्फ़ उस मेमोरी के ऐक्सेस का अनुरोध करना चाहिए जो ऐप्लिकेशन के काम करने के लिए ज़रूरी है। साथ ही, ऐप्लिकेशन को किसी तीसरे पक्ष के लिए डिवाइस की उस मेमोरी के ऐक्सेस का अनुरोध नहीं करना चाहिए जो लोगों के इस्तेमाल की जाने वाली सुविधाओं से जुड़ी नहीं है।
- जो Android डिवाइस, R (Android 11, एपीआई लेवल 30) या उसके आगे के वर्शन पर काम कर रहे हैं उन्हें डिवाइस की शेयर की गई मेमोरी का ऐक्सेस मैनेज करने के लिए, [MANAGE\\_EXTERNAL\\_STORAGE](#) की अनुमति की ज़रूरत होगी। वे सभी ऐप्लिकेशन जो R वर्शन को टारगेट करते हैं और डिवाइस की शेयर की गई मेमोरी ("सभी फ़ाइलों का ऐक्सेस") के लिए ऐक्सेस का दायरा बढ़ाने का अनुरोध करते हैं उन्हें प्रकाशित किए जाने से पहले एक समीक्षा होगी। उनके लिए ज़रूरी है कि वे इस समीक्षा में फ़ैसला लें कि उन्हें इस ऐक्सेस की सच में ज़रूरत है या नहीं। जो ऐप्लिकेशन इस अनुमति का इस्तेमाल करते हैं उन्हें ऐप्लिकेशन इस्तेमाल करने वाले लोगों को साफ़ तौर पर यह सूचना देनी चाहिए कि वे "खास ऐप्लिकेशन के लिए ऐक्सेस" सेटिंग में जाकर इस तरह के ऐप्लिकेशन के लिए, "सभी फ़ाइलों का ऐक्सेस" चालू करें। R वर्शन से जुड़ी ज़रूरी शर्तों के बारे में ज़्यादा जानकारी के लिए, यह [सहायता लेख](#) पढ़ें।

## डिवाइस और नेटवर्क का गलत इस्तेमाल

हम ऐसे ऐप्लिकेशन को अनुमति नहीं देते जो उपयोगकर्ता के डिवाइस, किसी दूसरे डिवाइस या कंप्यूटर, सर्वर, नेटवर्क, ऐप्लिकेशन प्रोग्रामिंग इंटरफ़ेस (एपीआई) या सेवाओं में दखल देते हैं। इसके अलावा, उनमें गड़बड़ी या नुकसान करते हैं या गलत तरीके से उन्हें ऐक्सेस करते हैं। साथ ही, इनमें डिवाइस पर मौजूद दूसरे ऐप्लिकेशन, Google की कोई सेवा या अनुमति पा चुके इंटरनेट सेवा देने वाली कंपनी के नेटवर्क भी शामिल हैं। हालांकि, इसमें इनके अलावा, और भी चीज़ें शामिल हो सकती हैं

Google Play पर मौजूद सभी ऐप्लिकेशन को, [Google Play पर ऐप्लिकेशन से जुड़ी क्वालिटी के मुख्य दिशा-निर्देशों](#) में बताए गए, डिफ़ॉल्ट Android सिस्टम ऑप्टिमाइज़ेशन की ज़रूरी शर्तों को पूरा करना होगा।

Google Play से इंस्टॉल होने वाले ऐप्लिकेशन में फेरबदल करने, अपडेट करने या ऐप्लिकेशन बदलने के लिए, सिर्फ़ Google Play के अपडेट का तरीका इस्तेमाल किया जा सकता है। किसी और तरीके से शायद आप ऐसा न कर पाएं। इसी तरह, कोई ऐप्लिकेशन Google Play के अलावा किसी दूसरे स्रोत से एक्जीक्यूटेबल कोड (उदाहरण dex, JAR, .so फ़ाइलें) डाउनलोड नहीं कर सकता। यह पाबंदी ऐसे कोड पर लागू नहीं होती जो किसी वर्चुअल मशीन पर काम करता है और जिसके पास Android एपीआई का सीमित ऐक्सेस होता है। जैसे: वेबव्यू या ब्राउज़र में JavaScript।

हम सुरक्षा में जोखिम की संभावना पैदा करने वाले या उनका फ़ायदा उठाने वाले कोड को अनुमति नहीं देते। डेवलपर के लिए हाल ही में प्रलैग की गई सुरक्षा की समस्याओं के बारे में जानने के लिए, [ऐप्लिकेशन की सुरक्षा को बेहतर बनाने वाला प्रोग्राम](#) देखें।

यहां आम तौर पर होने वाले उल्लंघनों के कुछ उदाहरण दिए गए हैं:

- ऐसे ऐप्लिकेशन जो विज्ञापन दिखाने पर दूसरे ऐप्लिकेशन को ब्लॉक कर देते हैं या फिर उनमें रुकावट डालते हैं।
- गेम में धोखाधड़ी करने वाले ऐप्लिकेशन जो दूसरे ऐप्लिकेशन के गेमप्ले पर असर डालते हैं।
- ऐसे ऐप्लिकेशन जो सेवाओं, सॉफ़्टवेयर या हार्डवेयर को हैक करने का तरीका बताते हैं या उसकी सुविधा देते हैं। साथ ही, सुरक्षा उपायों को खराब करने में भी मदद करते हैं।
- ऐसे ऐप्लिकेशन जो किसी सेवा या एपीआई का इस्तेमाल या ऐक्सेस इस तरह करते हैं, जिससे इसकी सेवा की शर्तों का उल्लंघन होता है।
- ऐसे ऐप्लिकेशन जिन्हें [व्हाइटलिस्ट करने की मंजूरी](#) नहीं है और जो [सिस्टम पावर मैनेजमेंट](#) को अनदेखा करने की कोशिश करते हैं।
- ऐसे ऐप्लिकेशन जो तीसरे पक्ष को प्रॉक्सी सेवा देते हैं, वे ऐसा सिर्फ़ उन ऐप्लिकेशन में कर सकते हैं जिनका मुख्य मकसद ही प्रॉक्सी सेवा देना है।

- ऐप्लिकेशन या तीसरे पक्ष के कोड (उदाहरण के लिए, SDK टूल) जो Google Play के अलावा, किसी दूसरे स्रोत से इस्तेमाल किया जा सकने वाला कोड डाउनलोड करते हैं। इस तरह के कोड में dex फ़ाइलें और नेटिव कोड शामिल हैं।
- ऐसे ऐप्लिकेशन जो इस्तेमाल करने वाले व्यक्ति की अनुमति के बिना, दूसरे ऐप्लिकेशन को डिवाइस में इंस्टॉल करते हैं।
- ऐसे ऐप्लिकेशन जो नुकसान पहुंचाने वाले सॉफ़्टवेयर से जुड़े होते हैं या लोगों तक उन्हें पहुंचाने या इंस्टॉल करने की सुविधा देते हैं।

## धोखाधड़ी वाला व्यवहार

हम ऐसे ऐप्लिकेशन को अनुमति नहीं देते जो लोगों के साथ धोखाधड़ी करने की कोशिश करते हैं या बेईमानी करते हैं। इनमें वे ऐप्लिकेशन भी शामिल हैं जो ऐसी सुविधाएं देने का दावा करते हैं जिन्हें पूरा नहीं किया जा सकता। ऐप्लिकेशन को पूरे मेटाडेटा में अपनी सुविधाओं के बारे में सही जानकारी, ब्यौरा, और फ़ोटो/वीडियो देना ज़रूरी है। ऐप्लिकेशन को ऑपरेटिंग सिस्टम या दूसरे ऐप्लिकेशन की सुविधाओं या चेतावनियों की नकल करने की कोशिश नहीं करनी चाहिए। डिवाइस की सेटिंग में किए जाने वाले किसी भी तरह के बदलाव, डिवाइस इस्तेमाल करने वाले व्यक्ति की जानकारी और सहमति से किए जाने चाहिए। ये बदलाव ऐसे हों जिन्हें उपयोगकर्ता पहले जैसा कर सके।

## गुमराह करने वाले दावे

हम ऐसे ऐप्लिकेशन को अनुमति नहीं देते जिनमें झूठी या गुमराह करने वाली जानकारी या दावे शामिल होते हैं। इस जानकारी में, विवरण, शीर्षक, आइकॉन, और स्क्रीनशॉट शामिल हैं।

यहां आम तौर पर होने वाले उल्लंघनों के कुछ उदाहरण दिए गए हैं:

- ऐसे ऐप्लिकेशन जो अपनी सुविधाओं को गलत तरीके से पेश करते हैं या सही जानकारी नहीं देते हैं:
  - ऐसा ऐप्लिकेशन जो अपनी जानकारी और स्क्रीनशॉट में रेंसिंग गेम होने का दावा करता है, जबकि वह टाइल स्लाइड करने की पहली वाला गेम है जिसमें टाइल पर कार की तस्वीर बनी होती है।
  - ऐसा ऐप्लिकेशन जो एंटीवायरस ऐप्लिकेशन होने का दावा करता है, लेकिन उसमें सिर्फ वायरस हटाने का तरीका बताने वाली गाइड दी गई हो।
- ऐसे डेवलपर और ऐप्लिकेशन के नाम जो Google Play पर अपनी मौजूदा स्थिति या प्रदर्शन को गलत तरीके से दिखाते हैं। (उदाहरण के लिए, “संपादक की पसंद,” “नंबर 1 ऐप्लिकेशन,” “टॉप पेड”)
- ऐप्लिकेशन जिनमें इलाज या सेहत के बारे में गुमराह करने वाला या संभावित रूप से नुकसान पहुंचाने वाला कॉन्टेंट है।
- ऐप्लिकेशन जो ऐसी सुविधाएं देने का दावा करते हैं जो नहीं दी जा सकती, जैसे कि कीड़े भगाने वाले ऐप्लिकेशन। भले ही, इसे शरारत, नकली, मज़ाक़ वगैरह के रूप में पेश किया जाए।
- ऐसे ऐप्लिकेशन जिन्हें गलत कैटगरी में रखा गया है। हालांकि, इनमें ऐप्लिकेशन की रेटिंग या ऐप्लिकेशन की कैटगरी के अलावा और भी बातें शामिल हैं।
- गुमराह करने वाला ऐसा कॉन्टेंट जिसका इस्तेमाल मतदान की प्रक्रिया में दखल देने के लिए हो सकता है।
- ऐसे ऐप्लिकेशन जो सरकार की किसी इकाई से जुड़े होने का झूठा दावा करते हैं या ऐसी सरकारी सेवाएं देने का दावा करते हैं जिनकी उन्हें अनुमति नहीं है।
- ऐसे ऐप्लिकेशन जो किसी जानी-मानी इकाई का आधिकारिक ऐप्लिकेशन होने का झूठा दावा करते हैं। ज़रूरी अनुमतियों या अधिकारों के बिना “जस्टिन बीबर आधिकारिक” जैसे शीर्षकों का इस्तेमाल नहीं कर सकते।

1



## 100% Cancer Prevention

Finally, this is your  
**CANCER CURE!**

LOADING...

2

## Breath analyser



**Are you drunk?**

Blow on your phone to get the results.

Yes

No

- (1) यह ऐप्लिकेशन, इलाज या स्वास्थ्य से जुड़ी ऐसी सुविधाएं (जैसे कि कैंसर का इलाज) देने का दावा करता है जो गुमराह करती हैं  
(2) यह ऐप्लिकेशन, ऐसी सुविधाएं देने का दावा करता है जो नहीं दी जा सकती (जैसे कि अपने फ़ोन को सांस जांचने वाले डिवाइस के तौर पर इस्तेमाल करना)

## डिवाइस की सेटिंग में गुमराह करने वाले बदलाव

हम ऐसे ऐप्लिकेशन को अनुमति नहीं देते जो इस्तेमाल करने वाले व्यक्ति की जानकारी और सहमति के बिना, उनके डिवाइस की सेटिंग या सुविधाओं में बदलाव करते हैं। डिवाइस की सेटिंग और सुविधाओं में, सिस्टम और ब्राउज़र की सेटिंग, बुकमार्क, शॉर्टकट, आइकॉन, विजेट, और होमस्क्रीन पर ऐप्लिकेशन के दिखने से जुड़ी चीज़ें शामिल हैं।

इसके अलावा, हम इस तरह के ऐप्लिकेशन को भी अनुमति नहीं देते हैं:

- ऐसे ऐप्लिकेशन जो डिवाइस की सेटिंग या सुविधाओं में बदलाव तो उपयोगकर्ता की सहमति से करते हैं, लेकिन ये बदलाव इस तरह किए जाते हैं कि इन्हें पहले जैसा करना आसान नहीं होता।
- ऐसे ऐप्लिकेशन या विज्ञापन जो तीसरे पक्ष की सेवाओं को पूरा करने या विज्ञापन दिखाने के मकसद से, डिवाइस की सेटिंग या सुविधाओं में बदलाव कर देते हैं।
- ऐसे ऐप्लिकेशन जो तीसरे पक्ष के ऐप्लिकेशन को हटाने या बंद करने के लिए या डिवाइस की सेटिंग या सुविधा में बदलाव के लिए, उपयोगकर्ताओं को गुमराह करते हैं।
- ऐसे ऐप्लिकेशन जो लोगों को तीसरे पक्ष के ऐप्लिकेशन हटाने या बंद करने या डिवाइस की सेटिंग और सुविधाओं में बदलाव करने को बढ़ावा देते हैं। ऐसे ऐप्लिकेशन को तब तक अनुमति नहीं दी जाती है, जब तक वह किसी ऐसी सुरक्षा सेवा का हिस्सा न हो जिसकी पुष्टि हो चुकी हो।

## धोखाधड़ी को बढ़ावा देना

हम ऐसे ऐप्लिकेशन को अनुमति नहीं देते जो दूसरे लोगों को गुमराह करने में उपयोगकर्ताओं की मदद करते हैं या जिनका मकसद किसी भी तरीके की धोखाधड़ी करना हो। ऐसे ही कुछ ऐप्लिकेशन के उदाहरण हैं: आईडी कार्ड, सोशल सिक्वॉरिटी नंबर, पासपोर्ट, डिप्लोमा, क्रेडिट कार्ड, और ड्राइविंग लाइसेंस। इसमें इनके अलावा, और भी चीज़ें शामिल हो सकती हैं ऐप्लिकेशन को नाम, ब्यौरे, और सुविधाओं से जुड़ी इमेज/वीडियो और/या कॉन्टेंट के बारे में सही जानकारी देनी होगी। इसके अलावा, ऐप्लिकेशन को उपयोगकर्ता की उम्मीद के मुताबिक काम करना चाहिए।

ऐप्लिकेशन के दूसरे संसाधन (जैसे कि गेम एसेट) सिर्फ तब डाउनलोड किए जा सकेंगे, जब वे उपयोगकर्ता के ऐप्लिकेशन में इस्तेमाल के लिए बहुत जरूरी हों। डाउनलोड किए गए संसाधन, Google Play नीतियों के मुताबिक होने चाहिए। साथ ही, डाउनलोड करने से पहले, ऐप्लिकेशन के उपयोगकर्ताओं को डाउनलोड साइज़ के बारे में साफ़ तौर पर बताया जाना चाहिए।

अगर किसी ऐप्लिकेशन के लिए दावा किया जाता है कि उसका मकसद "मनोरंजन के लिए" (या ऐसी ही मिलती-जुलती बात) "शरारत" करने से जुड़ा है, तो इससे ऐप्लिकेशन को हमारी नीतियों से छूट नहीं मिलती।

यहां आम तौर पर होने वाले उल्लंघनों के कुछ उदाहरण दिए गए हैं:

- ऐसे ऐप्लिकेशन जो दूसरे ऐप्लिकेशन या वेबसाइट की नकल करते हैं और इस्तेमाल करने वाले लोगों को धोखे से अपनी निजी जानकारी या पुष्टि करने से जुड़ी जानकारी देने के लिए कहते हैं।
- ऐसे ऐप्लिकेशन जो बिना पुष्टि वाले या असली फ़ोन नंबर, संपर्क, और पते दिखाते हैं। इसके अलावा, व्यक्ति या किसी इकाई की सहमति के बिना निजी रूप से पहचान करने वाली जानकारी भी दिखाते हैं।
- ऐसे ऐप्लिकेशन जिनकी मुख्य सुविधाएं, इस्तेमाल करने वाले व्यक्ति के इलाके, डिवाइस पैरामीटर या इस्तेमाल करने वाले लोगों से मिलने वाले अन्य डेटा पर निर्भर हो और इनकी वजह से आने वाले बदलाव के बारे में स्टोर पेज में साफ़ तौर पर नहीं बताया गया हो।
- ऐसे ऐप्लिकेशन जो इस्तेमाल करने वाले व्यक्ति को बिना सूचना दिए, वर्शन में ज़रूरी बदलाव करते हैं (उदाहरण के लिए, ['नया क्या है' सेक्शन](#)) और स्टोर पेज अपडेट करते हैं।
- ऐसे ऐप्लिकेशन जो समीक्षा के दौरान व्यवहार में बदलाव करते हैं या उलझाने की कोशिश करते हैं।
- कॉन्टेंट डिलीवरी नेटवर्क (सीडीएन) वाले ऐसे ऐप्लिकेशन जो डाउनलोड करने की सुविधा देते हैं और डाउनलोड करने से पहले ऐप्लिकेशन इस्तेमाल करने वाले व्यक्ति को डाउनलोड साइज़ के बारे में सही जानकारी नहीं देते हैं।

## ऐसा कॉन्टेंट जिसमें छेड़छाड़ की गई हो

हम ऐसे ऐप्लिकेशन को अनुमति नहीं देते जो तस्वीरों, वीडियो, और/या टेक्स्ट की मदद से गलत या गुमराह करने वाली जानकारी या दावे करने का प्रचार करते हैं या उन्हें बनाने में मदद करते हैं। हम ऐसे ऐप्लिकेशन को अनुमति नहीं देते हैं जो हमेशा गुमराह करने वाली जानकारी का प्रचार करते हैं या ऐसी तस्वीरों, वीडियो और/या टेक्स्ट का प्रचार करते हैं जो धोखाधड़ी को बढ़ावा देते हैं। इनकी वजह से संवेदनशील घटना, राजनैतिक, सामाजिक या दूसरे सार्वजनिक मामलों को नुकसान पहुंच सकता है।

कुछ ऐप्लिकेशन चीज़ों को साफ़ तौर पर दिखाने या क्वालिटी सुधारने के लिए, पारंपरिक और संपादकीय रूप से स्वीकार किए गए कॉन्टेंट में बदलाव करते हैं या उन्हें दूसरे तरीके से दिखाते हैं। ऐसे ऐप्लिकेशन को साफ़ तौर पर कॉन्टेंट में बदलाव की जानकारी देनी चाहिए या वॉटरमार्क के साथ पेश करना चाहिए। इससे एक आम व्यक्ति को यह पता चल सकेगा कि कॉन्टेंट में बदलाव किया गया है। हालांकि, लोगों की पसंद, व्यंग्य या पैरोडी वाले कॉन्टेंट के लिए छूट मिल सकती है।

यहां आम तौर पर होने वाले उल्लंघनों के कुछ उदाहरण दिए गए हैं:

- ऐसे ऐप्लिकेशन जो किसी जानी-मानी हस्ती को राजनैतिक रूप से संवेदनशील घटना के विरोध प्रदर्शनों से जोड़कर दिखाते हैं।
- ऐसे ऐप्लिकेशन जो स्टोर पेज पर वीडियो/फ़ोटो में बदलाव करने की अपनी सुविधा का प्रचार करने के लिए, किसी संवेदनशील घटना से ली गई मीडिया या जानी-मानी हस्ती के फ़ुटेज का इस्तेमाल करते हैं।
- ऐसे ऐप्लिकेशन जो मीडिया क्लिप में बदलाव करके, किसी न्यूज़ ब्रॉडकास्ट की नकल करते हैं।



(1) यह ऐप्लिकेशन न्यूज़ ब्रॉडकास्ट की नकल करने के लिए, मीडिया क्लिप में बदलाव करते हैं और वॉटरमार्क के बिना क्लिप में मशहूर और जानी-मानी हस्तियों को जोड़ने की सुविधा देता है।

## गलत तरीके से पेश करना

हम ऐसे ऐप्लिकेशन या डेवलपर खातों को अनुमति नहीं देते हैं जो:

- किसी दूसरे व्यक्ति या संगठन के नाम पर काम करते हों। हम उन ऐप्लिकेशन या डेवलपर खातों को भी अनुमति नहीं देते जो किसी दूसरे व्यक्ति या संगठन के मालिकाना हक या असल मकसद को छिपाते हों या गलत तरीके से पेश करते हों।
- गिरोह बनाकर लोगों को गुमराह करने की गतिविधि से जुड़े हों। इसमें ऐसे ऐप्लिकेशन या डेवलपर खाते शामिल हैं जो अपने मूल देश के बारे में गलत जानकारी देते हैं या अपने मूल देश की जानकारी छिपाते हैं या किसी दूसरे देश के लोगों को कॉन्टेंट भेजते हैं। इसमें इनके अलावा, और भी चीज़ें शामिल हो सकती हैं।
- डेवलपर या ऐप्लिकेशन की पहचान छिपाने या उसे गलत तरीके से पेश करने के लिए, दूसरे ऐप्लिकेशन, साइटों, डेवलपर या दूसरे खातों के साथ मिलकर काम करते हैं। इसके अलावा, दूसरी गलत जानकारी को भी छिपाते हैं या उसे गलत तरीके से पेश करते हैं। यह उन मामलों के लिए होगा जिनमें आपका कॉन्टेंट, राजनीति, सामाजिक मुद्दों या लोगों से जुड़ा है।

## मैलवेयर

मैलवेयर एक ऐसा कोड है जो किसी भी उपयोगकर्ता, उसके डेटा या डिवाइस को खतरे में डाल सकता है। मैलवेयर में नुकसान पहुंचा सकने वाले ऐप्लिकेशन (पीएचए), बाइनरी या फ्रेमवर्क में बदलाव के साथ दूसरी खतरनाक चीज़ें भी शामिल हो सकती हैं। इसमें ट्रोजन, फ़िशिंग, और स्पायवेयर ऐप्लिकेशन जैसी कैटगरी शामिल हैं जिसमें हम लगातार नई कैटगरी को अपडेट कर रहे हैं और जोड़ रहे हैं।

## मैलवेयर

हमारी मैलवेयर नीति बहुत आसान है। हम मानते हैं कि Android नेटवर्क और उपयोगकर्ता के डिवाइस, नुकसान पहुंचाने वाली गतिविधियों (जैसे कि मैलवेयर) से दूर रहने चाहिए। Android नेटवर्क में 'Google Play स्टोर' भी शामिल है। इस बुनियादी सिद्धांत के साथ, हम अपने ऐप्लिकेशन इस्तेमाल करने वाले लोगों और उनके Android डिवाइस के लिए सुरक्षित Android नेटवर्क उपलब्ध कराने की कोशिश करते हैं।

मैलवेयर एक कोड होता है जो किसी भी उपयोगकर्ता, उसके डेटा या डिवाइस को खतरे में डाल सकता है। मैलवेयर में नुकसान पहुंचा सकने वाले ऐप्लिकेशन (पीएचए), बाइनरी या फ्रेमवर्क में बदलाव के साथ दूसरी खतरनाक चीजें भी शामिल हो सकती हैं। इनमें ट्रोजन, फिशिंग, और स्पायवेयर ऐप्लिकेशन जैसी कैटगरी शामिल हैं। इसके अलावा, हम लगातार नई कैटगरी जोड़ रहे हैं और उन्हें अपडेट कर रहे हैं।

हालांकि, मैलवेयर कई तरह के होते हैं और उसके नुकसान पहुंचाने की क्षमता अलग-अलग होती है, फिर भी उनका मकसद इनमें से एक होता है:

- उपयोगकर्ता के डिवाइस की सुरक्षा खतरे में डालना।
- उपयोगकर्ता के डिवाइस को कंट्रोल करना।
- किसी सायबर हमलावर को कहीं से भी उपयोगकर्ता का डिवाइस एक्सेस करने देना, ताकि वह डिवाइस का गलत इस्तेमाल कर सके या डिवाइस को नुकसान पहुंचा सके।
- उपयोगकर्ता की सहमति या जानकारी के बिना, डिवाइस से निजी डेटा शेयर करना या क्रेडेंशियल चुराना।
- किसी मैलवेयर वाले डिवाइस से दूसरे डिवाइस को प्रभावित करने के लिए नेटवर्क पर स्पैम या खतरा पैदा करने वाले निर्देश फैलाना।
- उपयोगकर्ता से धोखाधड़ी करना।

किसी ऐप्लिकेशन, बाइनरी या फ्रेमवर्क में बदलाव करना खतरनाक हो सकता है। इस वजह से, नुकसान पहुंचाने वाली गतिविधियां हो सकती हैं, भले ही उनका इरादा खतरा पैदा करना न हो। ऐसा इसलिए होता है, क्योंकि ऐप्लिकेशन, बाइनरी या फ्रेमवर्क में होने वाले बदलाव अलग तरह से काम कर सकते हैं। ऐसा कई तरह के वैरिएबल मौजूद होने की वजह से होता है। इसलिए, अगर कोई चीज एक Android डिवाइस के लिए खतरनाक है, तो यह जरूरी नहीं कि वह दूसरे डिवाइस के लिए भी खतरनाक हो। उदाहरण के लिए, कुछ ऐप्लिकेशन, डिवाइस को नुकसान पहुंचाने के लिए पुराने एपीआई का इस्तेमाल करते हैं। Android के नए वर्शन का इस्तेमाल करने वाले डिवाइस पर ऐसे ऐप्लिकेशन का असर नहीं पड़ता। हालांकि, पुराने वर्शन वाले Android डिवाइस को इससे खतरा हो सकता है। ऐप्लिकेशन, बाइनरी या फ्रेमवर्क में हुए बदलाव को मैलवेयर या पीएचए के रूप में प्रत्येक किया जाता है। ऐसा तब किया जाता है, जब वे कुछ या सभी Android डिवाइस और उपयोगकर्ताओं के लिए खतरा पैदा करते हैं।

नीचे दी गई मैलवेयर कैटगरी, हमारी उस सोच के बारे में बताती हैं कि उपयोगकर्ता इस बात को समझें कि कैसे उनके डिवाइस को सुरक्षित तरीके से इस्तेमाल करने के लिए बनाया जा रहा है। यह सुरक्षित नेटवर्क को बेहतर बनाने में बढ़ावा देता है, ताकि उपयोगकर्ता भरोसा कर सकें।

ज़्यादा जानकारी के लिए, [Google Play Protect](#) पर जाएं।

## बैकडोर

ऐसा कोड जो डिवाइस पर अनचाही, नुकसान पहुंचाने वाली, और कहीं से भी कंट्रोल की जाने वाली कार्रवाइयों की अनुमति देता है।

इन कार्रवाइयों में ऐसी गतिविधि शामिल हो सकती है जो उपयोगकर्ता की अनुमति के बिना ही, ऐप्लिकेशन, बाइनरी या फ्रेमवर्क में हुए बदलाव को किसी भी तरह के मैलवेयर में शामिल कर सकती है। सामान्य तौर पर, बैकडोर की मदद से यह देखा जाता है कि किसी डिवाइस पर संभावित रूप से हानिकारक ऑपरेशन कैसे हो सकता है। इसलिए, यह बिलिंग से जुड़ी धोखाधड़ी करने वाली या कारोबारी स्पायवेयर से थोड़ा अलग होता है। इस वजह से, कुछ मामलों में बैकडोर के खास सेट को Google Play Protect के तहत जोखिम से भरा माना जाता है।

## बिलिंग की धोखाधड़ी

ऐसा कोड जो ऐप्लिकेशन इस्तेमाल करने वाले लोगों से जान-बूझकर और धोखाधड़ी करके, अपने-आप शुल्क लेता है।

मोबाइल बिलिंग की धोखाधड़ी में एसएमएस, कॉल, और टोल नंबर की धोखाधड़ी शामिल हैं।

### एसएमएस की धोखाधड़ी

ऐसा कोड जो लोगों से बिना उनकी अनुमति के प्रीमियम मैसेज भेजने पर शुल्क लेता है। इसके अलावा, पहचान ज़ाहिर करने वाली जानकारी को छिपाते हुए, ऐसे मैसेज भेजता है जिससे उपयोगकर्ता को अनजाने में पैसे चुकाने पड़ते हैं। इतना ही नहीं, धोखाधड़ी करने वाला, लोगों को मोबाइल सेवा देने वाली कंपनी की तरफ से ऐसे मैसेज भेजता है जिनमें शुल्क काटने या सदस्यताएं लेने की पुष्टि करने की जानकारी होती है।

कुछ कोड भले ही, तकनीकी रूप से मैसेज भेजने से जुड़ी शर्तों को ज़ाहिर करते हैं, लेकिन उनमें दूसरे तरीकों से मैसेज से की जाने वाली धोखाधड़ी शामिल होती है। इसमें उपयोगकर्ता से, किसी शर्त को ज़ाहिर करने की जानकारी के हिस्से को छिपाया जाता है और इन शर्तों को न पढ़ने लायक भी बनाया जाता है। साथ ही, इसमें वे मैसेज शामिल होते हैं जो लोगों को मोबाइल सेवा देने वाली कंपनी की तरफ़ से पैसे चुकाने या सदस्यता लेने की पुष्टि करने की जानकारी देते हैं।

### कॉल की धोखाधड़ी

ऐसा कोड जो ऐप्लिकेशन इस्तेमाल करने वाले लोगों से बिना उनकी अनुमति के प्रीमियम नंबर पर कॉल करके शुल्क लेता है।

### टोल नंबर की धोखाधड़ी

ऐसा कोड जिससे ऐप्लिकेशन इस्तेमाल करने वाले लोग अनजाने में अपने मोबाइल फ़ोन के बिल से कॉन्टेंट खरीदते या सदस्यता लेते हैं।

टोल नंबर से होने वाली धोखाधड़ी में प्रीमियम मैसेज और प्रीमियम कॉल के अलावा, बिलिंग से जुड़ी किसी भी तरह की धोखाधड़ी शामिल होती है। इसमें डायरेक्ट कैरियर बिलिंग, वायरलेस एक्सेस पॉइंट (WAP), और मोबाइल सेवा के इस्तेमाल पर लगने वाले शुल्क को ट्रांसफ़र करना शामिल है। टोल नंबर से होने वाली धोखाधड़ी में सबसे ज़्यादा धोखाधड़ी WAP से होती है। WAP से होने वाली धोखाधड़ी में, उपयोगकर्ताओं को धोखे से किसी बटन पर क्लिक करवाकर फंसाया जाता है। यह बटन ऐसे वेबव्यू पर होता है जिसे इस्तेमाल करने वाला देख नहीं पाता है और न ही इसके लोड होने का पता चल पाता है। इस कार्रवाई को करने से, बार-बार पैसे देकर ली जाने वाली सदस्यता शुरू हो जाती है। वहीं, इसकी पुष्टि करने वाला मैसेज या ईमेल आम तौर पर हार्डजैक कर लिया जाता है, ताकि उपयोगकर्ता को पैसे के लेन-देन की जानकारी न मिल सके।

## Stalkerware

ऐसा कोड जो डिवाइस में मौजूद, उपयोगकर्ता का निजी या संवेदनशील डेटा इकट्ठा और/या शेयर करता हो। साथ ही, ऐसा बिना सहमति लिए या ज़रूरी सूचना दिए किया जाता हो और लगातार सूचना देकर इस बारे में बताया भी न जाता हो।

Stalkerware ऐप्लिकेशन, डिवाइस के उपयोगकर्ताओं को टारगेट करते हैं। इसके लिए, उपयोगकर्ताओं के निजी या संवेदनशील डेटा की निगरानी की जाती है। इसके अलावा, यह डेटा शेयर किया जाता है या तीसरे पक्षों को इसका एक्सेस दिया जाता है।

सिर्फ़ उन ऐप्लिकेशन को निगरानी करने वाले ऐप्लिकेशन के रूप में मंजूरी दी जाती है जो खास तौर पर, बच्चों पर नज़र रखने में अभिभावकों की मदद करने या एंटरप्राइज़ मैनेजमेंट के लिए बनाए और बेचे जाते हों। साथ ही, ज़रूरी है कि ये ऐप्लिकेशन नीचे दी गई ज़रूरी शर्तों का पूरी तरह से पालन करते हों। लगातार सूचना दिखाने के बावजूद, इन ऐप्लिकेशन का इस्तेमाल करके किसी अन्य व्यक्ति (उदाहरण के लिए, पति या पत्नी) की निगरानी नहीं की जा सकती। ऐसा तब भी नहीं किया जा सकता, जब उसे इस बात की जानकारी दी गई हो और उसकी अनुमति ली गई हो।

'Play स्टोर' पर कुछ ऐसे ऐप्लिकेशन होते हैं जो stalkerware ऐप्लिकेशन नहीं होते, लेकिन डिवाइस पर उपयोगकर्ता की गतिविधि की निगरानी करते हैं या उस पर नज़र रखते हैं। ऐसे ऐप्लिकेशन को कम से कम, इन ज़रूरी शर्तों का पालन करना होगा:

- ऐप्लिकेशन को पेश करने के तरीके से ऐसा नहीं लगना चाहिए कि वे जासूसी के लिए बने हैं या गुप्त तौर पर निगरानी करने की सेवा देते हैं।
- ऐप्लिकेशन को निगरानी से जुड़ी गतिविधियां नहीं छिपानी चाहिए या उससे जुड़ी किसी जानकारी को गलत तरीके से पेश नहीं करना चाहिए। इसके अलावा, ऐसी सुविधा के बारे में लोगों को गुमराह नहीं करना चाहिए।
- जब ऐप्लिकेशन काम कर रहा हो, उस दौरान उपयोगकर्ताओं को लगातार सूचना दिखनी चाहिए। साथ ही, एक खास आइकॉन भी दिखना चाहिए, ताकि ऐप्लिकेशन को साफ़ तौर पर पहचाना जा सके।
- Google Play पर मौजूद ऐप्लिकेशन और ऐप लिस्टिंग में, किसी भी सुविधा को चालू करने या उसे एक्सेस करने का ऐसा कोई तरीका उपलब्ध नहीं कराना चाहिए जिससे इन शर्तों का उल्लंघन होता हो। उदाहरण के लिए, Google Play से बाहर होस्ट किए गए और शर्तों का पालन न करने वाले APK से लिंक करना।
- अपने ऐप्लिकेशन के लिए टारगेट की गई स्थान-भाषा की सभी कानूनी ज़िम्मेदारी आपकी है। अगर ऐप्लिकेशन उन जगहों पर गैर-कानूनी बताए जाते हैं जहां के लिए उन्हें प्रकाशित किया गया है, तो उन्हें हटा दिया जाएगा।

## सेवा में रुकावट (DoS)

ऐसा कोड जो उपयोगकर्ता को बिना बताए, सेवा में रुकावट (DoS) पैदा करता है। इसके अलावा, यह किसी दूसरे सिस्टम और संसाधनों पर सेवा में रुकावट पैदा करने वाले मैलवेयर का हिस्सा भी हो सकता है।

उदाहरण के लिए, रिमोट सर्वर पर लोड बढ़ाने के लिए, भारी संख्या में एचटीटीपी अनुरोध भेजकर ऐसा किया जा सकता है।

## गलत तरीके से डाउनलोड करने वाले मैलवेयर

ऐसा कोड जो डिवाइस को नुकसान नहीं पहुंचाता, लेकिन दूसरे तरह के पीएचए डाउनलोड करता है।

वह कोड जो गलत तरीके से डाउनलोड करने वाला हो सकता है, अगर:

- यह वजह हो सकती है कि इसे पीएचए फ़ैलाने के लिए बनाया गया हो या यह पीएचए डाउनलोड कर सकता है। इसके अलावा, इसमें ऐसा कोड शामिल है जो ऐप्लिकेशन इंस्टॉल और डाउनलोड कर सकता है;
- इसके ज़रिए डाउनलोड किए गए कम से कम 5% ऐप्लिकेशन ऐसे हो सकते हैं जो पीएचए हों। हमने ऐसा, डाउनलोड किए गए 500 ऐप्लिकेशन में पाया है। इनमें 25 पीएचए डाउनलोड देखे गए।

मुख्य ब्राउज़र और फ़ाइल शेयर करने वाले ऐप्लिकेशन को तब तक गलत तरीके से डाउनलोड करने वाला नहीं माना जाता, जब तक:

- वे उपयोगकर्ता की अनुमति के बिना डाउनलोड नहीं होते; और
- ऐप्लिकेशन इस्तेमाल करने वाले लोगों की अनुमति मिलने पर ही सभी पीएचए डाउनलोड होते हैं।

## ऐसे डिवाइस को नुकसान पहुंचाने वाले मैलवेयर जो Android प्लैटफ़ॉर्म पर काम नहीं करते

ऐसा कोड जो Android प्लैटफ़ॉर्म पर काम न करने वाले डिवाइस को नुकसान पहुंचाता है।

ये ऐप्लिकेशन Android इस्तेमाल करने वाले व्यक्ति या डिवाइस को नुकसान नहीं पहुंचाते हैं। हालांकि, इनमें ऐसे कॉम्पोनेंट होते हैं जो Android के अलावा, अन्य प्लैटफ़ॉर्म पर चलने वाले डिवाइस को नुकसान पहुंचा सकते हैं।

## फ़िशिंग

ऐसा कोड जो किसी भरोसेमंद स्रोत से आने का दावा करता है, ऐप्लिकेशन का इस्तेमाल करने वाले व्यक्ति की पुष्टि करने वाले क्रेडेंशियल या बिलिंग की जानकारी पाने के लिए अनुरोध करता है, और डेटा को किसी तीसरे पक्ष को भेजता है। यह कैटगरी उस कोड पर भी लागू होती है जो उपयोगकर्ता के क्रेडेंशियल शेयर करते समय उसमें रोक लगाता है।

आम तौर पर, सोशल नेटवर्क और गेम के लिए फ़िशिंग के टारगेट, बैंकिंग क्रेडेंशियल, क्रेडिट कार्ड नंबर, और खाते के ऑनलाइन क्रेडेंशियल होते हैं।

## खास अधिकारों का गलत इस्तेमाल

ऐसा कोड जो ऐप्लिकेशन के सैंडबॉक्स और खास अधिकारों को एक्सेस करता है। इसके अलावा, सुरक्षा से जुड़ी मुख्य गतिविधियों के एक्सेस को बदलता है या उसे एक्सेस करने से रोकता है। ऐसा करके, यह कोड ऐप्लिकेशन इस्तेमाल करने वाले व्यक्ति के डिवाइस को खतरे में डालता है।

उदाहरणों में ये शामिल हैं:

- ऐसा ऐप्लिकेशन जो Android की अनुमतियों के मॉडल का उल्लंघन करता है या दूसरे ऐप्लिकेशन से क्रेडेंशियल (जैसे कि OAuth टोकन) चुराता है।
- ऐसे ऐप्लिकेशन जो सुविधाओं का गलत इस्तेमाल करते हैं और खुद को अनइंस्टॉल होने या बंद होने से रोकते हैं।
- ऐसा ऐप्लिकेशन जो SELinux को काम करने से रोकता है।

ऐसे प्रिविलेज एस्केलेशन ऐप्लिकेशन जो इस्तेमाल करने वाले व्यक्ति की अनुमति के बिना डिवाइस को रूट करते हैं। वे डिवाइस को रूट करने वाले ऐप्लिकेशन की कैटगरी में आते हैं।

## रैंसमवेयर

ऐसा कोड जो डिवाइस या उसमें मौजूद डेटा का कुछ या पूरा कंट्रोल अपने पास रखता है। साथ ही, इस्तेमाल करने वाले व्यक्ति से पैसे चुकाने या डिवाइस पर ऐसी कार्रवाई करने की मांग करता है जिससे इस्तेमाल करने वाला व्यक्ति अपना कंट्रोल ऐप्लिकेशन को सौंप दे।

कुछ रैंसमवेयर, डिवाइस पर डेटा को एन्क्रिप्ट करते हैं और डेटा को पढ़ने लायक बनाने के लिए उपयोगकर्ता से पैसे चुकाने की मांग करते हैं। साथ ही, डिवाइस के एडमिन की सुविधाओं का फ़ायदा उठाते हैं, ताकि उन्हें कोई भी डिवाइस से न हटा सके। उदाहरणों में ये शामिल हैं:

- उपयोगकर्ता को उनके डिवाइस को ऐक्सेस करने से रोकना और उन्हें फिर से कंट्रोल देने के लिए पैसे की मांग करना।
- डिवाइस के डेटा को एन्क्रिप्ट करके, फिर उसी डेटा को पढ़ने लायक बनाने के लिए उपयोगकर्ता से पैसे चुकाने की मांग करना।
- डिवाइस के पॉलिसी मैनेजर की सुविधाओं का फ़ायदा उठाना और उपयोगकर्ता उन्हें हटा न पाएं, इसलिए उनके ऐक्सेस पर रोक लगाना।

ऐसा कोड जो डिवाइस में पहले से मौजूद होता है उसे रैंसमवेयर की कैटगरी से बाहर रखा जा सकता है। इसका मुख्य काम डिवाइस के मैनेजमेंट को सब्सिडाइज़ करना है। यह कोड, सुरक्षित लॉक और मैनेजमेंट के लिए ज़रूरी शर्तें पूरी करता है। साथ ही, लोगों को पूरी जानकारी देता है और उनसे सहमति लेने की ज़रूरी शर्तें पूरी करता है।

## रूट करना

ऐसा कोड जो डिवाइस को रूट करता है।

नुकसान पहुंचाने के लिए डिवाइस को रूट करने वाला कोड और नुकसान नहीं पहुंचाने वाला कोड, दोनों में अंतर है। उदाहरण के लिए, नुकसान नहीं पहुंचाने के लिए डिवाइस को रूट करने वाले ऐप्लिकेशन, लोगों को डिवाइस रूट करने की जानकारी पहले ही दे देते हैं। साथ ही, ये ऐप्लिकेशन ऐसी कार्रवाइयां नहीं करते हैं जो डिवाइस की अन्य पीएचए कैटगरी पर लागू होती हैं।

नुकसान पहुंचाने के लिए डिवाइस रूट करने वाले ऐसे ऐप्लिकेशन जो इस्तेमाल करने वाले व्यक्ति को बिना जानकारी दिए डिवाइस रूट कर देते हैं। यह इस्तेमाल करने वाले व्यक्ति को रूट करने की जानकारी पहले देते हैं, लेकिन ये दूसरी ऐसी कार्रवाइयां करते हैं जो डिवाइस की दूसरी पीएचए कैटगरी पर लागू होती हैं।

## स्पैम

ऐसा कोड जो इस्तेमाल करने वाले व्यक्ति के डिवाइस की संपर्क सूची में मौजूद लोगों को अनचाहे मैसेज भेजता है या उनके डिवाइस का इस्तेमाल ईमेल स्पैम भेजने के लिए करता है।

## स्पायवेयर

ऐसा कोड जो बिना अनुमति या सूचना के डिवाइस में मौजूद निजी डेटा को शेयर करता है।

उदाहरण के लिए, ऐसा कोड जो यहां दी गई किसी भी जानकारी को बिना अनुमति के शेयर करता है या इस तरह से शेयर करता है जिसकी उम्मीद इस्तेमाल करने वाला व्यक्ति नहीं कर सकता, उसे स्पायवेयर माना जाता है:

- संपर्क सूची
- एसडी कार्ड में सेव फ़ोटो या दूसरी फ़ाइलें जो ऐप्लिकेशन से जुड़ी नहीं हैं
- उपयोगकर्ता के ईमेल का कॉन्टेंट
- कॉल लॉग
- एसएमएस लॉग
- डिफ़ॉल्ट ब्राउज़र का वेब इतिहास या ब्राउज़र के बुकमार्क
- दूसरे ऐप्लिकेशन के /डेटा/ डायरेक्ट्री से मिली जानकारी।

ऐसी गतिविधियां जो उपयोगकर्ता की जासूसी कर सकती हैं उन्हें भी स्पायवेयर माना जा सकता है। उदाहरण के लिए, फ़ोन से ऑडियो रिकॉर्ड करना या फ़ोन कॉल रिकॉर्ड करना या ऐप्लिकेशन की जानकारी चुराना।

## ट्रोजन

ऐसा कोड जिसकी पहचान बेनाइन के तौर पर होती है, जैसे कि एक ऐसा गेम जो सिर्फ़ गेम होने का दावा करता है, लेकिन वह ऐप्लिकेशन इस्तेमाल करने वाले व्यक्ति की अनुमति के बिना कार्रवाइयां करता है।

आम तौर पर, इस तरह के मैलवेयर किसी दूसरे पीएचए कैटगरी के साथ मिलकर काम करते हैं। ट्रोजन में एक नुकसान न पहुंचाने वाला कॉम्पोनेंट और एक नुकसान पहुंचाने वाला, छिपा हुआ कॉम्पोनेंट होता है। उदाहरण के लिए, एक गेम जो उपयोगकर्ता की जानकारी के बिना बैकग्राउंड में ही

उसके डिवाइस से प्रीमियम मैसेज भेजता है.

## असामान्य ऐप्लिकेशन पर नोट

अगर Google Play Protect के पास किसी नए और असामान्य ऐप्लिकेशन को सुरक्षित बताने के लिए पूरी जानकारी नहीं है, तो इन ऐप्लिकेशन को असामान्य की कैटगरी में रखा जाएगा. इसका मतलब यह नहीं है कि वह ऐप्लिकेशन नुकसान पहुंचाने वाला है, लेकिन बिना समीक्षा किए इसे सुरक्षित भी नहीं कहा जा सकता.

## बैकडोर कैटगरी वाले मैलवेयर पर नोट

कोड की कार्रवाईयों के आधार पर बैकडोर मैलवेयर की कैटगरी तय होती है. किसी कोड को तब बैकडोर माना जाता है, जब वह डिवाइस पर नुकसान पहुंचाने वाली गतिविधि को बिना अनुमित के कार्रवाई करने देता है. इसकी वजह से वह कोड किसी अन्य मैलवेयर कैटगरी में शामिल हो सकता है. उदाहरण के लिए, अगर कोई ऐप्लिकेशन डाइनैमिक कोड को लोड होने की अनुमति देता है और यह कोड, मैसेज की जानकारी हासिल करता है, तो इसे बैकडोर मैलवेयर की तरह माना जाएगा.

हालांकि, अगर कोई ऐप्लिकेशन आर्बिट्ररी कोड को कार्रवाई करने की अनुमति देता है और हमें लगता है कि इस कोड की वजह से डिवाइस को नुकसान पहुंचाने वाली गतिविधि को बढ़ावा नहीं मिला है, तो उस ऐप्लिकेशन को बैकडोर मैलवेयर के तौर पर देखने के बजाय, जोखिम की संभावना वाले ऐप्लिकेशन के तौर पर देखा जाएगा. साथ ही, डेवलपर से इसे पैच करने के लिए कहा जाएगा.

## मोबाइल का अनचाहा सॉफ्टवेयर

यह नीति, [Android नेटवर्क](#) और 'Google Play स्टोर' के सिद्धांतों से Google की अनचाही सॉफ्टवेयर नीति पर बनाई जाती है. इन सिद्धांतों का उल्लंघन करने वाला सॉफ्टवेयर संभावित रूप से ऐप्लिकेशन इस्तेमाल करने वाले व्यक्ति के अनुभव को नुकसान पहुंचा सकता है और हम इस्तेमाल करने वाले व्यक्ति को इससे बचाने के लिए कदम उठाएंगे.

### मोबाइल का अनचाहा सॉफ्टवेयर

Google का मानना है कि अगर हम ऐप्लिकेशन इस्तेमाल करने वाले व्यक्ति पर ध्यान देंगे, तो बाकी सब भी अपने-आप बेहतर हो जाएगा. हम अपने [सॉफ्टवेयर सिद्धांत](#) और [अनचाही सॉफ्टवेयर नीति](#) में सॉफ्टवेयर के लिए ऐसे सामान्य सुझाव देते हैं जो ऐप्लिकेशन इस्तेमाल करने वाले व्यक्ति को बेहतरीन अनुभव देता है. यह नीति, [Android नेटवर्क](#) और 'Google Play स्टोर' के सिद्धांतों से Google की अनचाही सॉफ्टवेयर नीति पर बनाई जाती है. इन सिद्धांतों का उल्लंघन करने वाला सॉफ्टवेयर संभावित रूप से ऐप्लिकेशन इस्तेमाल करने वाले व्यक्ति के अनुभव को नुकसान पहुंचा सकता है और हम इस्तेमाल करने वाले व्यक्ति को इससे बचाने के लिए कदम उठाएंगे.

[अनचाही सॉफ्टवेयर नीति](#) के आधार पर, हमें पता चला है कि ज़्यादातर अनचाहे सॉफ्टवेयर एक या उससे ज़्यादा विशेषताएं दिखाते हैं:

- अनचाहा सॉफ्टवेयर ऐसी फ़ाइल या ऐसा मोबाइल ऐप्लिकेशन होता है जिससे लोगों के साथ धोखाधड़ी की जाती है. यह ऐसी खास बात का वादा करता है जिसे पूरा नहीं किया जा सकता.
- यह सॉफ्टवेयर को इंस्टॉल किए जाने के लिए लोगों को चकमा देने की कोशिश करता है या फिर वह किसी दूसरे प्रोग्राम के साथ जुड़कर इंस्टॉल हो जाता है.
- यह सॉफ्टवेयर इस्तेमाल करने वाले व्यक्ति को अपने सिद्धांतों और ज़रूरी सुविधाओं के बारे में नहीं बताता है.
- यह इस्तेमाल करने वाले व्यक्ति के सिस्टम पर गलत असर डालते हैं.
- यह सॉफ्टवेयर लोगों को बिना बताए, उनकी निजी जानकारी को इकट्ठा करता है या उसे दूसरों तक पहुंचाता है.
- यह सॉफ्टवेयर सुरक्षा इंटरजाम के बिना ही निजी जानकारी को इकट्ठा करता है या उसे दूसरों तक पहुंचाता है (उदाहरण के लिए, एचटीटीपीएस पर शेयर करना)
- यह सॉफ्टवेयर दूसरे सॉफ्टवेयर के साथ शामिल होता है और इसकी मौजूदगी का पता नहीं चलता.

मोबाइल डिवाइस पर सॉफ्टवेयर, ऐप्लिकेशन, बाइनरी, फ़्रेमवर्क में बदलाव वगैरह एक कोड के रूप में होता है. ऐसे सॉफ्टवेयर जो सॉफ्टवेयर नेटवर्क को नुकसान पहुंचाते हैं या उपयोगकर्ता के अनुभव में रुकावट डालते हैं उन्हें रोकने के लिए, इन सिद्धांतों का उल्लंघन करने वाले कोड पर कार्रवाई की जाएगी.

नीचे दी गई नीति को हमने अनचाहे सॉफ्टवेयर के आधार पर बनाया है, ताकि इसे मोबाइल सॉफ्टवेयर पर लागू किया जा सके. नीचे दी गई नीति के मुताबिक, हम मोबाइल के अनचाहे सॉफ्टवेयर के नए तरह के गलत इस्तेमाल को रोकने के लिए नीति को बेहतर बनाना जारी रखेंगे.

पारदर्शिता वाला व्यवहार और साफ़ जानकारी

सभी कोड को इस्तेमाल करने वाले व्यक्ति से किए गए वादों को पूरा करना चाहिए। ऐप्लिकेशन को सुविधाओं की सभी जानकारी देनी चाहिए। ऐप्लिकेशन को लोगों को भ्रमित नहीं करना चाहिए।

- ऐप्लिकेशन को सुविधाओं और इरादों के बारे में साफ़ तौर पर बताना चाहिए।
- कृपया, ऐप्लिकेशन इस्तेमाल करने वाले व्यक्ति को साफ़ और सही जानकारी दें कि ऐप्लिकेशन, सिस्टम में किस तरह के बदलाव करेगा। साथ ही, ऐप्लिकेशन इस्तेमाल करने वाले लोगों को सभी ज़रूरी इंस्टॉल करने के विकल्पों और बदलावों की समीक्षा करने और उन्हें मंजूरी देने की अनुमति दें।
- सॉफ़्टवेयर को, डिवाइस की स्थिति को इस्तेमाल करने वाले व्यक्ति के लिए गलत तरीके से पेश नहीं करना चाहिए। उदाहरण के लिए, दावा करना कि सिस्टम की सुरक्षा को गंभीर खतरा है या सिस्टम में वायरस है।
- विज्ञापन ट्रैफ़िक और/या ऐप्लिकेशन इंस्टॉल करने वाले लोगों की संख्या बढ़ाने के लिए डिज़ाइन की गई गलत गतिविधि की मदद न लें।
- हम ऐसे ऐप्लिकेशन को अनुमति नहीं देते जो किसी दूसरे व्यक्ति या ऐप्लिकेशन की पहचान चुराकर लोगों को गुमराह करते हैं। जैसे: दूसरे डेवलपर, कंपनी, इकाई। अगर आपके ऐप्लिकेशन को किसी व्यक्ति से अनुमति नहीं मिली है और न ही यह किसी व्यक्ति से जुड़ा है, तो इसका झूठा दावा न करें।

उल्लंघनों के उदाहरण:

- विज्ञापन से होने वाली धोखाधड़ी
- किसी दूसरे के नाम पर काम करना

ऐप्लिकेशन इस्तेमाल करने वाले व्यक्ति के डेटा की सुरक्षा करना

ऐप्लिकेशन इस्तेमाल करने वाले व्यक्ति के निजी और संवेदनशील डेटा को एक्सेस करने, इस्तेमाल करने, इकट्ठा करने, और शेयर किए जाने के बारे में साफ़ और सही जानकारी दें। जहां भी लागू हो, वहां ऐप्लिकेशन इस्तेमाल करने वाले व्यक्ति के डेटा को इस्तेमाल करने के लिए सभी ज़रूरी नीतियों का पालन करना चाहिए। साथ ही, डेटा की सुरक्षा के लिए सभी सावधानियां रखें।

- लोगों के डिवाइस से डेटा भेजने और इकट्ठा करने से पहले, उनसे डेटा को इकट्ठा करने की सहमति लें। इसमें तीसरे पक्ष के खाते, ईमेल, फ़ोन नंबर, इंस्टॉल किए गए ऐप्लिकेशन, फ़ाइलें, जगह की जानकारी, और किसी भी तरह का ऐसा दूसरा निजी और संवेदनशील डेटा शामिल हैं जिसे इस्तेमाल करने वाले व्यक्ति को इकट्ठा किए जाने की उम्मीद नहीं होगी।
- ऐप्लिकेशन इस्तेमाल करने वाले व्यक्ति के इकट्ठा किए गए निजी और संवेदनशील डेटा को सुरक्षित तरीके से हैंडल किया जाना चाहिए, जिसमें आधुनिक क्रिप्टोग्राफी (उदाहरण के लिए, एचटीटीपीएस पर) का इस्तेमाल करना भी शामिल है।
- मोबाइल ऐप्लिकेशन समेत सॉफ़्टवेयर को उपयोगकर्ता के निजी और संवेदनशील डेटा को सिर्फ़ सर्वर पर भेजना चाहिए, क्योंकि यह ऐप्लिकेशन की सुविधाओं से जुड़ा हुआ है।

उल्लंघनों के उदाहरण:

- डेटा इकट्ठा करना (cf [स्प्रायवेयर](#))
- पाबंदी वाली अनुमतियों का गलत इस्तेमाल

ऐप्लिकेशन इस्तेमाल करने वाले व्यक्ति के लिए डेटा की नीतियों का उदाहरण:

- [Google Play का इस्तेमाल करने वाले लोगों के लिए डेटा नीति](#)
- [Google मोबाइल सेवाओं \(GMS\) का इस्तेमाल करने वाले व्यक्ति के लिए डेटा की नीति से जुड़ी ज़रूरी शर्तें](#)
- [Google API की सेवा का इस्तेमाल करने वाले व्यक्ति के लिए डेटा नीति](#)

मोबाइल पर इस्तेमाल के अनुभव को नुकसान न पहुंचाएं

इस्तेमाल करने वाले व्यक्ति का अनुभव साफ़, समझने में आसान, और उसकी पसंद पर आधारित होना चाहिए। इसे इस्तेमाल करने वाले व्यक्ति को इसकी खास बातें साफ़ तौर पर बतानी चाहिए और विज्ञापन में बताए गए या उपयोगकर्ता के मनचाहे अनुभव में बदलाव नहीं होना चाहिए।

- उन विज्ञापनों को न दिखाएं जो अनचाहे तरीके से लोगों को दिखाते हैं। इन तरीकों में डिवाइस की सुविधाओं के इस्तेमाल में रुकावट डालना या हस्तक्षेप करना शामिल है। इसके अलावा, ट्रिगर करने वाले ऐप्लिकेशन के बाहर दिखाई देने या उन्हें आसानी से खारिज किए बिना और विशेषता के साथ दिखाना भी शामिल है।
- ऐप्लिकेशन को दूसरे ऐप्लिकेशन या डिवाइस के इस्तेमाल में रुकावट नहीं डालनी चाहिए

- अनइंस्टॉल करना, जहां भी लागू हो, साफ़ तौर पर बताया जाना चाहिए.
- मोबाइल सॉफ़्टवेयर को डिवाइस के ओएस या दूसरे ऐप्लिकेशन से मिलने वाली सूचनाओं की नकल नहीं करनी चाहिए. उपयोगकर्ता को दूसरे ऐप्लिकेशन या ऑपरेटिंग सिस्टम की चेतावनियां न दिखाएं. खास तौर पर ऐसी चेतावनियां जो ओएस में होने वाले बदलावों की सूचना इस्तेमाल करने वाले व्यक्ति को देते हैं.

उल्लंघनों के उदाहरण:

- परेशान करने वाले विज्ञापन
- सिस्टम की सुविधाओं का बिना अनुमति इस्तेमाल करना या उनकी नकल करना

## विज्ञापन से होने वाली धोखाधड़ी

विज्ञापन से जुड़ी धोखाधड़ी पर पूरी तरह से पाबंदी है. ऐसे उपयोगकर्ता की पसंद जिनकी पहचान की पुष्टि हो चुकी है उनसे किसी विज्ञापन नेटवर्क को भरोसे में लेकर ट्रैफ़िक पाने के गलत इरादे से बनाए गए विज्ञापन इंटरैक्शन, विज्ञापन से जुड़ी धोखाधड़ी हैं. यह **अमान्य ट्रैफ़िक** का एक रूप है. विज्ञापनों से होने वाली धोखाधड़ी तब हो सकती है, जब डेवलपर विज्ञापन दिखाने के लिए बिना अनुमति वाले तरीके इस्तेमाल करते हैं, जैसे कि छिपे हुए विज्ञापन दिखाना, उन पर अपने-आप क्लिक होना, जानकारी में बदलाव या उसमें छेड़छाड़ करना, और गैर-मानवीय कार्रवाइयों (स्पाइडर, बॉट वगैरह) का गलत तरीके से फ़ायदा लेना. साथ ही, अमान्य विज्ञापन ट्रैफ़िक लाने वाली मानव गतिविधि भी इनमें शामिल है. अमान्य ट्रैफ़िक और विज्ञापन से होने वाली धोखाधड़ी विज्ञापन देने वालों, डेवलपर, और लोगों को नुकसान पहुंचाती है. यह मोबाइल विज्ञापन नेटवर्क के भरोसे को भी लंबे समय तक नुकसान पहुंचा सकती है.

यहां आम तौर पर होने वाले उल्लंघनों के कुछ उदाहरण दिए गए हैं:

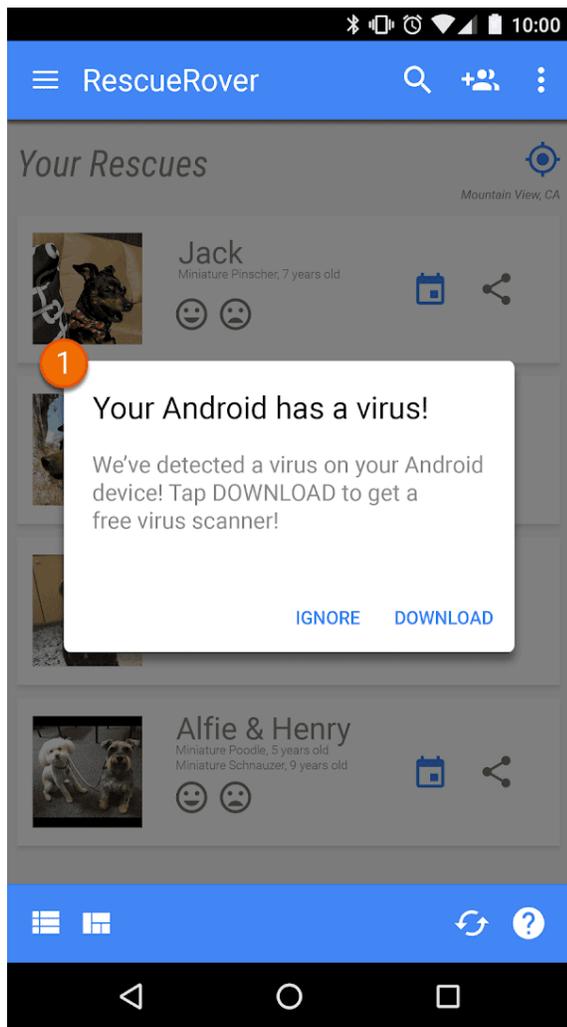
- ऐसा ऐप्लिकेशन जो इस्तेमाल करने वाले व्यक्ति को दिखाई न देने वाले विज्ञापन देता है.
- ऐसा ऐप्लिकेशन जो इस्तेमाल करने वाले व्यक्ति की इच्छा के बिना अपने-आप विज्ञापनों पर क्लिक करता है या धोखाधड़ी से विज्ञापनों पर क्लिक का क्रेडिट उपयोगकर्ता को देने के लिए, ऐसे किसी नेटवर्क का इस्तेमाल करता है.
- ऐसा ऐप्लिकेशन जो इंस्टॉल करने के पैसे पाने के लिए इंस्टॉल करने के नकली एट्रिब्यूशन क्लिक भेजता है और यह भेजने वाले के नेटवर्क से जनरेट नहीं किया गया होता है.
- ऐसा ऐप्लिकेशन जो इस्तेमाल करने वाले व्यक्ति के ऐप्लिकेशन इंटरफ़ेस में न होने पर भी पॉप-अप विज्ञापन दिखाता है.
- ऐसा ऐप्लिकेशन जो विज्ञापन इन्वेंट्री को गलत तरीके से दिखाता है. उदाहरण के लिए, वह ऐप्लिकेशन जो विज्ञापन नेटवर्क को बताता है कि यह iOS डिवाइस पर चल रहा है जबकि वह वास्तव में Android डिवाइस पर चल रहा होता है; वह ऐप्लिकेशन जो कमाई करने वाले पैकेज के नाम की गलत जानकारी देता है.

## सिस्टम की सुविधाओं का बिना अनुमति इस्तेमाल करना या उनकी नकल करना

हम ऐसे ऐप्लिकेशन या विज्ञापनों को अनुमति नहीं देते जो सूचना या चेतावनी जैसे सिस्टम की सुविधा की नकल करते हैं या उसमें दखल देते हैं. सिस्टम के लेवल से मिलने वाली सूचनाओं का इस्तेमाल सिर्फ़ किसी ऐप्लिकेशन की आंतरिक सुविधाओं के लिए किया जा सकता है, जैसे कि कोई ऐसा एयरलाइन ऐप्लिकेशन जो लोगों को खास ऑफ़र के बारे में सूचना देता है या ऐसा गेम जो लोगों को गेम में प्रचारों के बारे में सूचना देता है.

यहां आम तौर पर होने वाले उल्लंघनों के कुछ उदाहरण दिए गए हैं:

- ऐसे ऐप्लिकेशन या विज्ञापन जिन्हें सूचना या चेतावनी के रूप में भेजा जाता है:



① इस ऐप्लिकेशन में नज़र आ रही सूचना का इस्तेमाल विज्ञापन देने के लिए किया जा रहा है.

विज्ञापनों से जुड़े अन्य उदाहरणों के लिए, कृपया [विज्ञापन नीति](#) देखें.

## किसी दूसरे के नाम पर काम करना

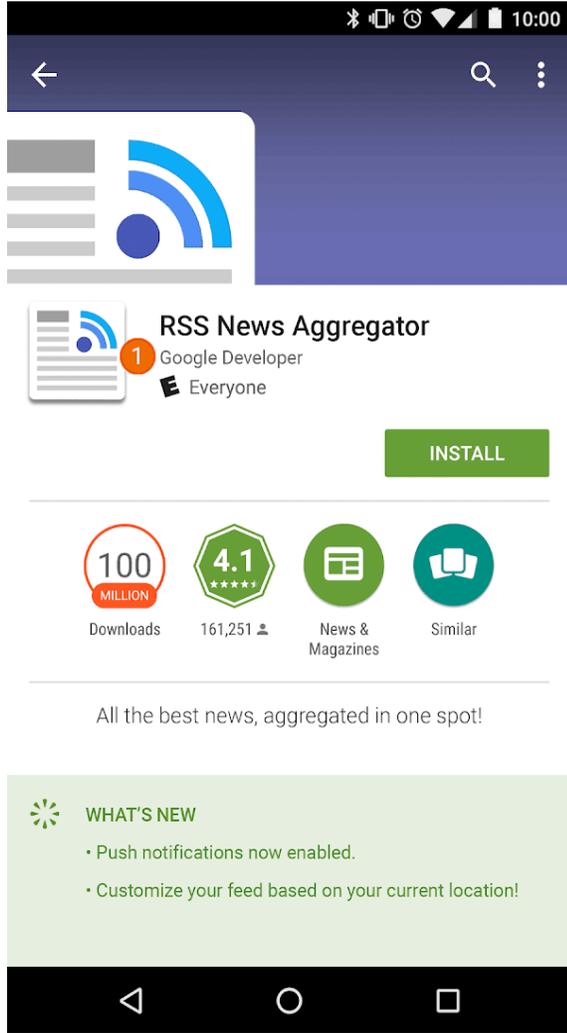
जब डेवलपर दूसरे लोगों या उनके ऐप्लिकेशन की पहचान चुराते हैं, तो इससे ऐप्लिकेशन इस्तेमाल करने वाले लोग गुमराह होते हैं. साथ ही, इससे डेवलपर समुदाय को नुकसान पहुंचता है. हम ऐसे ऐप्लिकेशन पर पाबंदी लगाते हैं जो किसी दूसरे की पहचान चुराकर लोगों को गुमराह करते हैं.

## किसी दूसरे के नाम पर काम करना

हम ऐसे ऐप्लिकेशन को अनुमति नहीं देते जो किसी दूसरे व्यक्ति (जैसे कि दूसरे डेवलपर, कंपनी, इकाई) या ऐप्लिकेशन की पहचान चुराकर लोगों को गुमराह करते हैं. अगर आपके ऐप्लिकेशन को किसी व्यक्ति से अनुमति नहीं मिली है और न ही ये किसी व्यक्ति से जुड़ा है, तो इसका झूठा दावा न करें. इस बात का ध्यान रखें कि आप अपने ऐप्लिकेशन में आइकॉन, जानकारी, शीर्षक या ऐप्लिकेशन के अंदर मौजूद ऐसी चीज़ों का इस्तेमाल न करें जो लोगों को किसी और या किसी दूसरे ऐप्लिकेशन से आपके ऐप्लिकेशन के संबंध के बारे में गुमराह कर सकता है.

यहां आम तौर पर होने वाले उल्लंघनों के कुछ उदाहरण दिए गए हैं:

- डेवलपर, जो किसी दूसरी कंपनी / डेवलपर से संबंध होने का झूठा दावा करते हैं:



① इस ऐप्लिकेशन के डेवलपर के नाम से, इसके Google से आधिकारिक तौर पर जुड़े होने का पता चलता है, जबकि दोनों के बीच ऐसा कोई संबंध नहीं है।

- ऐसे ऐप्लिकेशन जिनके शीर्षक और आइकॉन, पहले से मौजूद ऐसे प्रॉडक्ट या सेवाओं से मिलते-जुलते हैं जिससे इस्तेमाल करने वाले लोग गुमराह हो सकते हैं:

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

## कमाई करना और विज्ञापन

Google Play, डेवलपर और लोगों के फ़ायदे के लिए कमाई करने के कई तरीके देता है। इनमें पैसे चुकाकर लोगों तक ऐप्लिकेशन पहुंचाना, ऐप्लिकेशन में खरीदने के लिए प्रॉडक्ट, सदस्यताएं, और अलग-अलग तरह के विज्ञापन मॉडल के हिसाब से ऐप्लिकेशन तैयार करने जैसे तरीके शामिल हैं। लोगों को सुविधाओं का बेहतर अनुभव देने के लिए, हम चाहते हैं कि आप इन नीतियों का पालन करें।

# पैसे चुकाना

- Google Play से ऐप्लिकेशन इंस्टॉल और डाउनलोड कराने पर, जो रकम डेवलपर ले रहे हैं उसके लिए उन्हें Google Play के बिलिंग सिस्टम का इस्तेमाल पैसे चुकाने के तरीके के तौर पर करना होगा।
- 'Play स्टोर' पर मौजूद सभी ऐप्लिकेशन को किसी सुविधा या सेवा के एक्सेस के बदले पैसे चुकाने या स्वीकार करने के लिए, Google Play के बिलिंग सिस्टम का इस्तेमाल करना चाहिए. इनमें ऐप्लिकेशन की सुविधा, डिजिटल कॉन्टेंट या अन्य चीजें शामिल हैं.
  - Google Play के बिलिंग सिस्टम का इस्तेमाल करने वाले ऐप्लिकेशन की सुविधाओं या सेवाओं के उदाहरण में इन-ऐप्लिकेशन खरीदारी भी शामिल हैं. हालांकि, यह इन ही तक सीमित नहीं है:
    - आइटम (जैसे कि वर्चुअल मुद्राएं, खेलने के कुछ और मौके, खेलने के लिए कुछ और समय, कुछ और आइटम, किरदार और अवतार);
    - सदस्यता सेवाएं (जैसे कि फिटनेस, गेम, डेटिंग, शिक्षा, संगीत, वीडियो, और अन्य कॉन्टेंट से जुड़ी सदस्यता सेवाएं);
    - ऐप्लिकेशन की सुविधाएं या कॉन्टेंट (जैसे किसी ऐप्लिकेशन का बिना विज्ञापन वाला वर्शन या नई सुविधाएं जो बिना पैसे वाले वर्शन में मौजूद नहीं हैं); और
    - क्लाउड सॉफ्टवेयर और सेवाएं (जैसे कि डेटा इकट्ठा करने वाली सेवाएं, कारोबार उत्पादकता वाला सॉफ्टवेयर, और वित्तीय प्रबंधन वाला सॉफ्टवेयर).
  - इन मामलों में Google Play के बिलिंग सिस्टम का इस्तेमाल नहीं करना चाहिए जहां:
    - मुख्य तौर पर इनके लिए पैसा चुकाना होगा:  
ध्यान दें: कुछ बाजारों में, हम ऐसे ऐप्लिकेशन के लिए Google Pay ऑफ़र करते हैं जो सामान और/या सेवाएं बेचते हैं. ज़्यादा जानकारी के लिए, कृपया हमारे [Google Pay डेवलपर पेज](#) पर जाएं.
      - सामान खरीदने या किराये पर लेने के लिए (जैसे कि किराने का सामान, कपड़े, घरेलू सामान, इलेक्ट्रॉनिक्स);
      - सेवाओं की खरीदारी के लिए (जैसे कि परिवहन सेवाएं, सफ़ाई सेवाएं, हवाई किराया, जिम की सदस्यताएं, खाने की डिलीवरी, लाइव इवेंट के टिकट); या
      - क्रेडिट कार्ड या बिजली-पानी जैसी सुविधाओं के बिल (जैसे कि केबल और दूरसंचार सेवाएं) के लिए चुकाए गए पैसे;
      - पैसे चुकाने में, एक सहयोगी का दूसरे सहयोगी को पैसे चुकाना, ऑनलाइन नीलामी, और बिना टैक्स वाला दान शामिल हैं;
      - ऐसे कॉन्टेंट या सेवाओं के लिए पैसे चुकाना जो ऑनलाइन जुए से जुड़ी सुविधाएं देते हैं, जैसा कि [असली पैसे दांव पर लगाकर खेले जाने वाला जुआ, गेम, और प्रतियोगिताएं](#) वाले सेक्शन में [जुए से जुड़े ऐप्लिकेशन](#) की नीति में बताया गया है;
      - किसी भी ऐसी कैटगरी के उत्पाद के लिए पैसे चुकाए जाने हैं जो Google के [भुगतान केंद्र के कॉन्टेंट की नीति](#) के तहत गलत मानी जाती है.
- ऐसे ऐप्लिकेशन जो 2(b) बताए गए ऐप्लिकेशन से अलग हो सकते हैं, वे लोगों को Google Play के बिलिंग सिस्टम के अलावा, पैसे चुकाने के लिए किसी दूसरे तरीके पर नहीं ले जा सकते. लोगों को पैसे चुकाने के लिए किसी दूसरे तरीके पर ले जाने के लिए पाबंदी है. हालांकि, यह इन ही तक सीमित नहीं है:
  - Google Play में ऐप्लिकेशन की लिस्ट;
  - खरीदे जा सकने वाले कॉन्टेंट का ऐप्लिकेशन में प्रचार;
  - इन-ऐप्लिकेशन वेबव्यू, बटन, लिंक, मैसेज सेवा, विज्ञापन या दूसरे कॉल-टू-एक्शन; और
  - इन-ऐप्लिकेशन यूज़र इंटरफ़ेस फ़्लो के साथ खाता बनाने या साइन-अप वाले फ़्लो भी शामिल हैं. ये लोगों को उन फ़्लो के हिस्से के रूप में Google Play के बिलिंग सिस्टम के अलावा, ऐप्लिकेशन से लोगों को पैसे चुकाने के किसी दूसरे तरीके पर ले जाते हैं.
- इन-ऐप्लिकेशन वर्चुअल मुद्राओं का इस्तेमाल सिर्फ़ ऐसे ऐप्लिकेशन या गेम के शीर्षक में किया जाना चाहिए जिसके लिए उन्हें खरीदा गया था.
- डेवलपर के लिए ज़रूरी है कि वह इस्तेमाल करने वाले लोगों को अपने ऐप्लिकेशन की शर्तों और कीमत के बारे में साफ़ और सही जानकारी दे. इसके अलावा, कोई भी इन-ऐप्लिकेशन सुविधाओं या खरीदारी के लिए ऑफ़र की जा रही सदस्यताओं के बारे में भी साफ़ और सही जानकारी देनी चाहिए. इन-ऐप्लिकेशन कीमत को इस्तेमाल करने वाले व्यक्ति के 'Play बिलिंग' इंटरफ़ेस में दिख रही कीमत से मेल खाना चाहिए. अगर Google Play पर आपके उत्पाद की जानकारी में, ऐसी इन-ऐप्लिकेशन सुविधाओं के बारे में बताया गया हो जिनके लिए खास या किसी अन्य शुल्क की ज़रूरत हो सकती है, तो ऐप्लिकेशन की सूची में लोगों को साफ़ तौर पर बताना चाहिए कि उन सुविधाओं का इस्तेमाल करने के लिए पैसे चुकाना ज़रूरी है.
- कुछ ऐप्लिकेशन और गेम किसी खरीदारी के दौरान लोगों को वर्चुअल आइटम खरीदने के मौके देते हैं. इसमें "लूट बॉक्स" शामिल है, लेकिन यह इसी तक सीमित नहीं है. ऐसे ऐप्लिकेशन को खरीदारी से पहले ही साफ़ तौर पर बताना होगा कि उन आइटम को हासिल करने की संभावना

कितनी है. साथ ही, यह भी बताना होगा कि लोग उस आइटम को पाने के कितना करीब हैं.

## सदस्यताएं

डेवलपर के तौर पर, आपको अपने ऐप्लिकेशन में दी जाने वाली किसी सदस्यता सेवा या कॉन्टेंट के बारे में लोगों को गुमराह नहीं करना चाहिए. किसी भी स्प्लैश स्क्रीन या ऐप्लिकेशन के अंदर किए जाने वाले प्रचार में अपने सभी ऑफ़र से जुड़ी सही जानकारी देना ज़रूरी है.

अपने ऐप्लिकेशन में आपको अपने ऑफ़र के बारे में साफ़ तौर पर बताना चाहिए. आपको अपने ऑफ़र की शर्तों के बारे में भी साफ़ तौर पर बताना चाहिए, जैसे कि सदस्यता शुल्क कितना होगा, बिलिंग साइकल कितने दिन का होगा, और ऐप्लिकेशन इस्तेमाल करने के लिए सदस्यता ज़रूरी है या नहीं. लोगों को जानकारी की समीक्षा करने के लिए कोई और कार्रवाई करने की ज़रूरत नहीं होनी चाहिए.

यहां आम तौर पर होने वाले उल्लंघनों के कुछ उदाहरण दिए गए हैं:

- Monthly subscriptions that do not inform users they will be automatically renewed and charged every month.
- Annual subscriptions that most prominently display their pricing in terms of monthly cost.
- Subscription pricing and terms that are incompletely localized.
- In-app promotions that do not clearly demonstrate that a user can access content without a subscription (when available).
- SKU names that do not accurately convey the nature of the subscription, such as "Free Trial" for a subscription with an auto-recurring charge.

**1** Get AnalyzeAPP Premium

**2** 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%! MOST POPULAR PLAN	\$14.00/mo

**3** Try for \$12.50!

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

- ① Dismiss button is not clearly visible and users may not understand that they can access functionality without accepting the subscription offer.
- ② Offer only displays pricing in terms of monthly cost and users may not understand that they will be charged a six month price at the time they subscribe.
- ③ Offer only shows the introductory price and users may not understand what they will automatically be charged at the end of the introductory period.
- ④ Offer should be localized in the same language as the terms and conditions so that users can understand the entire offer.

## मुफ्त में आजमाने की सुविधा और शुरुआती ऑफ़र

किसी उपयोगकर्ता को आपके ऐप्लिकेशन की सदस्यता लेने से पहले: आपको ऑफ़र से जुड़ी शर्तों के बारे में लोगों को साफ़ और सही तरीके से बताना चाहिए. इन शर्तों में ऑफ़र की अवधि, किराया, और कॉन्टेंट या सेवाओं को एक्सेस करने की जानकारी शामिल है. लोगों को यह बताना न भूलें कि मुफ्त में आजमाने की सुविधा वाली सदस्यता कब और कैसे, पैसे देकर ली जाने वाली सदस्यता में बदलेगी. इसके अलावा, पैसे देकर ली जाने वाली सदस्यता की कीमत के बारे में बताएं और अगर वे इसे नहीं लेना चाहते, तो उन्हें सदस्यता रद्द करने का तरीका भी बताएं.

यहां आम तौर पर होने वाले उल्लंघनों के कुछ उदाहरण दिए गए हैं:

- Offers that do not clearly explain how long the free trial or introductory pricing will last.
- Offers that do not clearly explain that the user will be automatically enrolled in a paid subscription at the end of the offer period.
- Offers that do not clearly demonstrate that a user can access content without a trial (when available).
- Offer pricing and terms that are incompletely localized.

**Get AnalyzeAPP Premium**

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

**Try for free now!**

3 During your free trial, experience all of the great features our app can offer!

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

- ① Dismiss button is not clearly visible and users may not understand that they can access functionality without signing up for the free trial.
- ② Offer emphasizes the free trial and users may not understand that they will automatically be charged at the end of the trial.
- ③ Offer does not state a trial period and users may not understand how long their free access to subscription content will last.
- ④ Offer should be localized in the same language as the terms and conditions so that users can understand the entire offer.

## सदस्यताओं को मैनेज करना और उन्हें रद्द करना

डेवलपर के तौर पर, आपको अपने ऐप्लिकेशन में यह ज़रूर बताना चाहिए कि ऐप्लिकेशन इस्तेमाल करने वाला व्यक्ति अपनी सदस्यता को कैसे मैनेज या रद्द कर सकता है।

यह आपकी ज़िम्मेदारी है कि आप सदस्यता लेने, उसे रद्द कराने, और रिफंड पाने की नीतियों में होने वाले किसी भी बदलाव के बारे में लोगों को जानकारी दें। साथ ही, यह पक्का करें कि नीतियां लागू कानून का पालन करती हों।

## विज्ञापन

हम ऐसे ऐप्लिकेशन को अनुमति नहीं देते जिनमें गुमराह या परेशान करने वाले विज्ञापन शामिल होते हैं। विज्ञापन सिर्फ उस ऐप्लिकेशन में दिखाए जाने चाहिए जिसमें वे उपलब्ध कराए जा रहे हैं। हम आपके ऐप्लिकेशन में दिए गए विज्ञापनों को आपके ऐप्लिकेशन का हिस्सा मानते हैं। ऐप्लिकेशन में दिखने वाले विज्ञापन हमारी सभी नीतियों के हिसाब से होने चाहिए। जुए के विज्ञापनों से जुड़ी नीतियों के बारे में जानने के लिए, कृपया [यहां](#) क्लिक करें।

## विज्ञापनों के लिए जगह की जानकारी के डेटा का इस्तेमाल

ऐसे ऐप्लिकेशन जो अनुमति मांगकर लिए गए, डिवाइस की जगह की जानकारी के डेटा का इस्तेमाल विज्ञापन दिखाने के लिए भी करते हैं। वे [निजी और संवेदनशील जानकारी](#) की नीति के तहत आते हैं। साथ ही, उन्हें नीचे दी गई ज़रूरी शर्तों का भी पालन करना होगा:

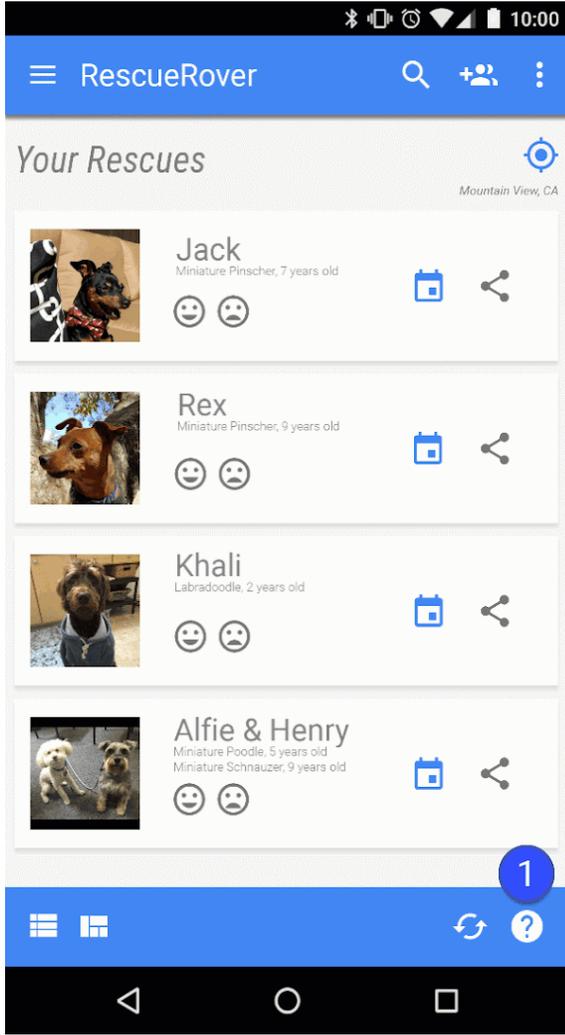
- ऐप्लिकेशन इस्तेमाल करने वाले व्यक्ति को ठीक से पता होना चाहिए कि विज्ञापन दिखाने के लिए, अनुमति मांगकर डिवाइस की जगह की जानकारी का डेटा क्यों लिया जाता है या उसका इस्तेमाल किस तरह किया जाता है। साथ ही, यह जानकारी ऐप्लिकेशन की ज़रूरी निजता नीति में दर्ज होनी चाहिए। इसके अलावा, किसी ऐसे काम के विज्ञापन नेटवर्क की निजता नीतियों का उदाहरण दिया जाना चाहिए जिसमें जगह की जानकारी के डेटा के इस्तेमाल के बारे में बताया गया हो।
- [जगह की जानकारी की अनुमति](#) की शर्तों के मुताबिक, जगह की जानकारी के ऐक्सेस का अनुरोध ऐप्लिकेशन में पहले से मौजूद सुविधाओं और सेवाओं को लागू करने के लिए ही किया जा सकता है, लेकिन सिर्फ विज्ञापन दिखाने के लिए नहीं।

## धोखाधड़ी करने वाले विज्ञापन

विज्ञापनों को किसी भी ऐप्लिकेशन के यूजर इंटरफ़ेस या किसी ऑपरेटिंग सिस्टम की सूचना या चेतावनी देने के तरीकों की नकल या उनकी पहचान नहीं चुरानी चाहिए। ऐप्लिकेशन इस्तेमाल करने वाले व्यक्ति को यह साफ़ तौर पर बताया जाना चाहिए कि हर एक विज्ञापन किस ऐप्लिकेशन की तरफ़ से उपलब्ध कराया जा रहा है।

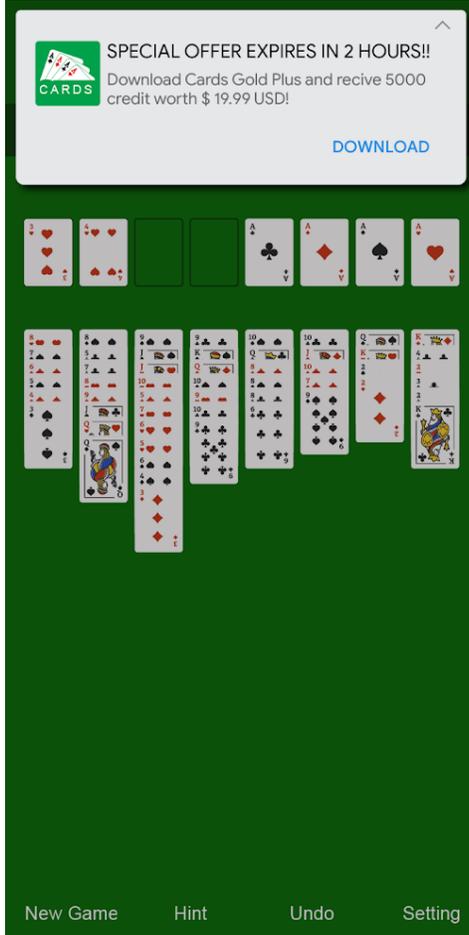
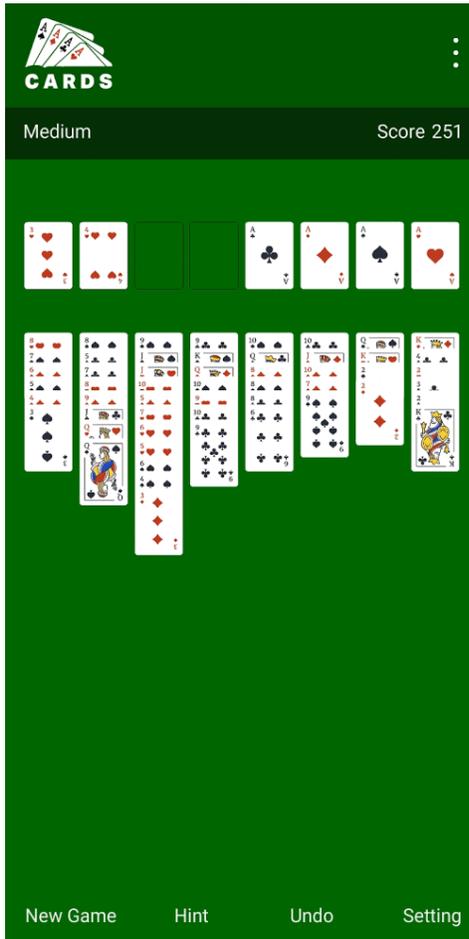
यहां आम तौर पर होने वाले उल्लंघनों के कुछ उदाहरण दिए गए हैं:

- ऐसे विज्ञापन जो किसी ऐप्लिकेशन के यूज़र इंटरफ़ेस (यूआई) की नकल करते हैं:



① इस ऐप्लिकेशन में दिया गया प्रश्नवाचक चिह्न का आइकॉन, एक ऐसा विज्ञापन है जो ऐप्लिकेशन इस्तेमाल करने वाले व्यक्ति को किसी बाहरी लैंडिंग पेज पर ले जाता है.

- ऐसे विज्ञापन जो सिस्टम सूचना की नकल करते हैं:



ऊपर दिए गए उदाहरण, अलग-अलग सिस्टम सूचनाओं की नकल करने वाले विज्ञापनों के बारे में बताते हैं।

## लॉकस्क्रीन पर कमाई करने की सुविधा

जब तक ऐप्लिकेशन किसी खास इरादे के लिए लॉकस्क्रीन का इस्तेमाल न करे, तब तक ऐप्लिकेशन पर ऐसे विज्ञापन या सुविधाएं नहीं दिखाए जाते जो डिवाइस की लॉकस्क्रीन पर कमाई करें।

## परेशान करने वाले विज्ञापन

परेशान करने वाले विज्ञापन ऐसे विज्ञापन होते हैं जो लोगों को अचानक दिखाए जाते हैं। ऐसे विज्ञापनों पर ऐप्लिकेशन इस्तेमाल करने वाला व्यक्ति गलती से किसी जगह क्लिक कर सकता है। साथ ही, इनसे डिवाइस की सुविधाओं के इस्तेमाल में रुकावट या खराबी भी आ सकती है।

आपका ऐप्लिकेशन, विज्ञापन के मकसद से उपयोगकर्ता को तब तक किसी विज्ञापन पर क्लिक करने या अपनी निजी जानकारी देने के लिए मजबूर नहीं कर सकता, जब तक वह ऐप्लिकेशन को पूरी तरह से इस्तेमाल नहीं करता है। साथ ही, पेज पर अचानक दिखने वाले विज्ञापन सिर्फ उसी ऐप्लिकेशन में दिखाए जा सकते हैं जिसमें वे मौजूद हैं। अगर आपका ऐप्लिकेशन पेज पर अचानक दिखने वाले विज्ञापन या ऐसे दूसरे विज्ञापन दिखाता है जो सामान्य इस्तेमाल में रुकावट डालते हैं, तो उन्हें ऐसा होना चाहिए कि पेनल्टी के बिना आसानी से खारिज किया जा सके।

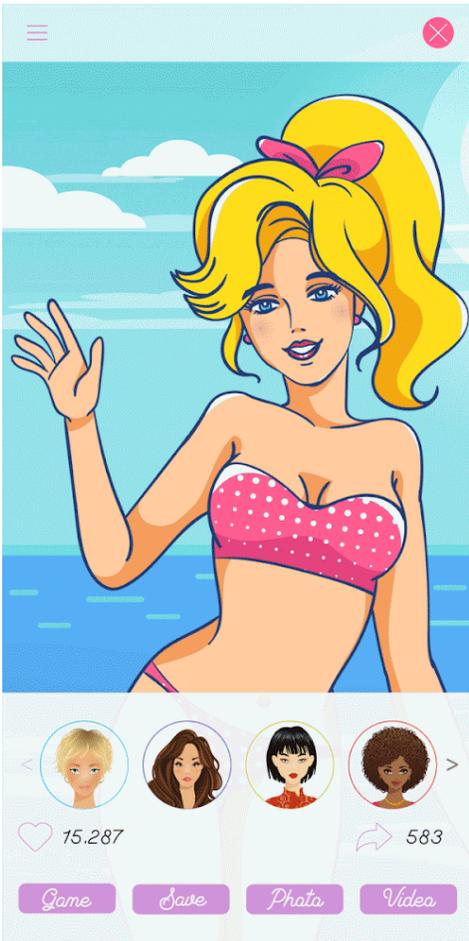
यहां आम तौर पर होने वाले उल्लंघनों के कुछ उदाहरण दिए गए हैं:

- ऐसे विज्ञापन जो पूरी स्क्रीन घेरते हैं या सामान्य तरीके से ऐप्लिकेशन इस्तेमाल करने में रुकावट डालते हैं और विज्ञापन हटाने का सही तरीका नहीं बताते:

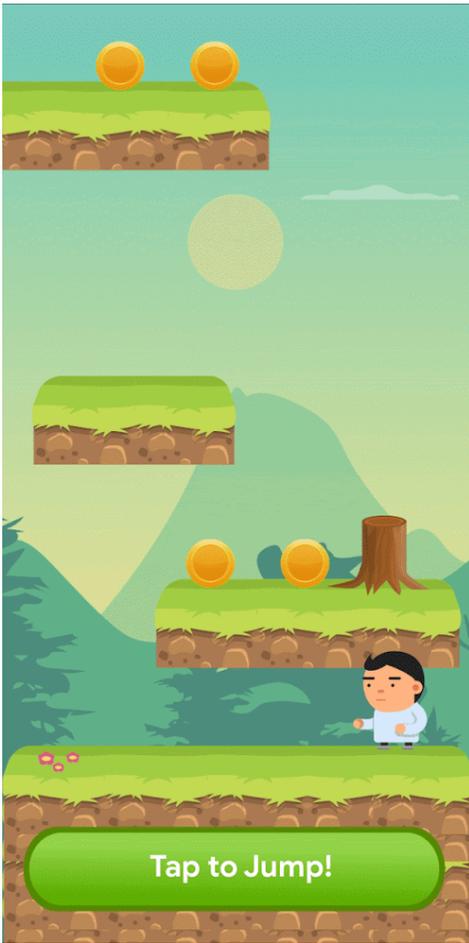


① इस विज्ञापन में 'खारिज करें' बटन नहीं है।

- ऐसे ऐप्लिकेशन जो इस्तेमाल करने वाले व्यक्ति को खारिज करने के गलत बटन पर क्लिक करने के लिए मजबूर करते हैं या ऐसी जगहों पर अचानक विज्ञापन दिखाते हैं जहां इस्तेमाल करने वाला व्यक्ति आम तौर पर दूसरी सुविधा के लिए टैप करता है।



ऐसा विज्ञापन जो खारिज करने के गलत बटन का इस्तेमाल करता है



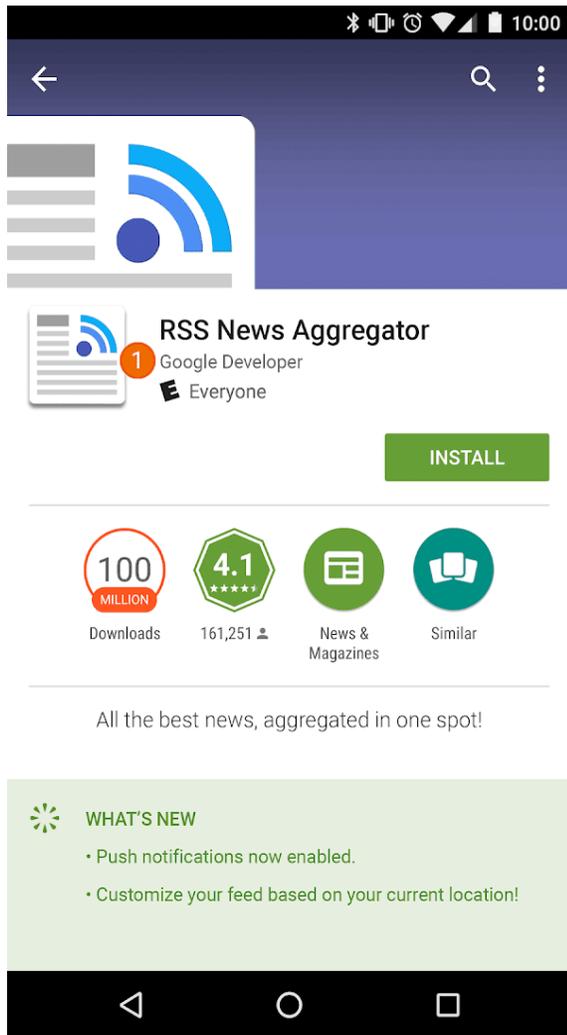
ऐसा विज्ञापन जो उस जगह पर अचानक दिखता है जहां ऐप्लिकेशन इस्तेमाल करने वाला व्यक्ति ऐप्लिकेशन की सुविधाओं के लिए आम तौर पर टैप करता है

## ऐप्लिकेशन, तीसरे पक्ष के विज्ञापन या डिवाइस के काम करने के तरीके में दखल देना

आपके ऐप्लिकेशन के विज्ञापनों को दूसरे ऐप्लिकेशन, विज्ञापनों या डिवाइस के काम में रुकावट नहीं डालनी चाहिए. इनमें सिस्टम या डिवाइस बटन और पोर्ट भी शामिल हैं. इसमें ओवरले, सहयोगी फ़ंक्शन, और विजेट के रूप में बनाई गई विज्ञापन इकाइयां शामिल हैं. विज्ञापन सिर्फ़ उस ऐप्लिकेशन में दिखाए जाने चाहिए जिसमें वे उपलब्ध कराए जा रहे हैं.

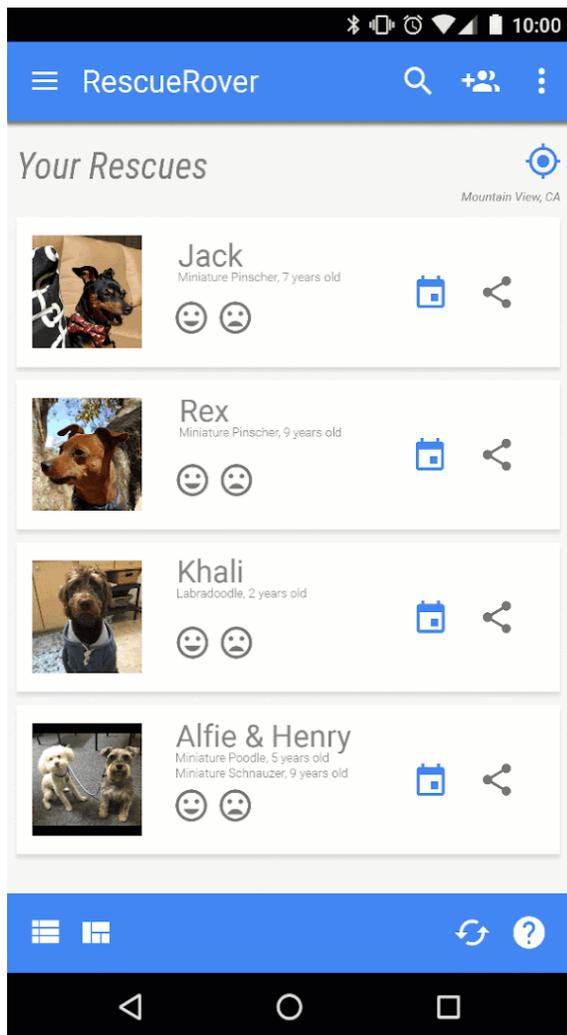
यहां आम तौर पर होने वाले उल्लंघनों के कुछ उदाहरण दिए गए हैं:

- ऐसे विज्ञापन जो उन्हें उपलब्ध कराने वाले ऐप्लिकेशन के बाहर दिखते हैं:



ब्यौरा: जब उपयोगकर्ता इस ऐप्लिकेशन से होम स्क्रीन पर जाता है, तो उसे होमस्क्रीन पर अचानक एक विज्ञापन दिखने लगता है.

- ऐसे विज्ञापन जो होम बटन या ऐसी दूसरी सुविधाओं से ट्रिगर होते हैं, वे साफ़ तौर पर ऐप्लिकेशन से बाहर निकलने के लिए बनाए गए हैं:

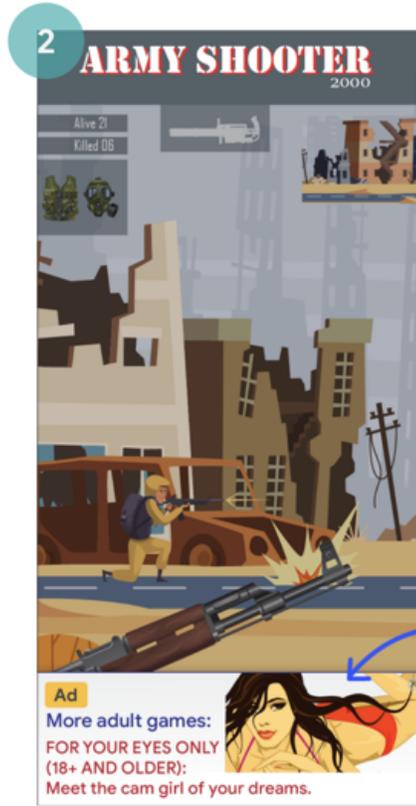
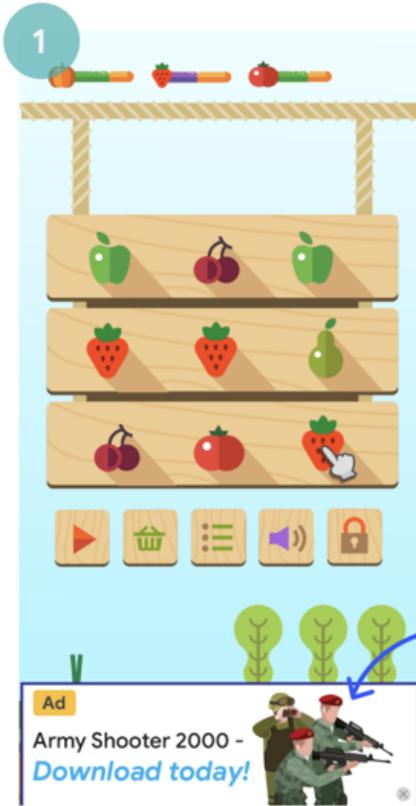


ब्यौरा: उपयोगकर्ता ऐप्लिकेशन से बाहर निकलने और होम स्क्रीन पर जाने की कोशिश करता है, लेकिन इसके बजाय, किसी विज्ञापन की वजह से ऐसा करने में रुकावट आ जाती है.

## ऐसे विज्ञापन जो सही नहीं हैं

आपके ऐप्लिकेशन में दिखाए गए विज्ञापन उन दर्शकों के लिए सही होने चाहिए जिनके लिए यह ऐप्लिकेशन बनाया गया है. भले ही, कॉन्टेंट हमारी नीतियों का पालन करता हो.

यहां आम तौर पर होने वाले उल्लंघन का उदाहरण दिया गया है:



- ① यह विज्ञापन, ऐप्लिकेशन के टारगेट दर्शकों (किशोरों) के लिए सही नहीं है (7+)
- ② यह विज्ञापन, ऐप्लिकेशन के टारगेट दर्शकों (वयस्कों) के लिए सही नहीं है (12+)

## Android विज्ञापन आईडी का इस्तेमाल

'Google Play सेवाएं' के वर्शन 4.0 में विज्ञापन और आंकड़े देने वालों के इस्तेमाल के लिए नए एपीआई और एक आईडी बनाया गया है. इस आईडी के इस्तेमाल की शर्तें नीचे दी गई हैं.

- इस्तेमाल. Android के विज्ञापन पहचानकर्ता का इस्तेमाल सिर्फ विज्ञापन और उपयोगकर्ता के आंकड़ों के लिए किया जाना चाहिए. हर बार आईडी एक्सेस करने पर, "पसंद के हिसाब से विज्ञापन से ऑफ्ट-आउट करने" या "दिलचस्पी के मुताबिक विज्ञापन से ऑफ्ट-आउट करने" की सेटिंग की स्थिति की पुष्टि की जानी चाहिए.
- व्यक्तिगत पहचान से जुड़ी जानकारी या दूसरे पहचानकर्ता से जुड़ना
  - विज्ञापन का इस्तेमाल: विज्ञापन पहचानकर्ता, विज्ञापन के मकसद के लिए डिवाइस पहचानकर्ता से लगातार नहीं जुड़ सकता. उदाहरण के लिए: SSAID, MAC का पता, IMEI वगैरह. विज्ञापन पहचानकर्ता, ऐप्लिकेशन इस्तेमाल करने वाले व्यक्ति की साफ़ तौर पर सहमति के बाद ही, व्यक्तिगत पहचान से जुड़ी जानकारी के साथ जुड़ सकता है.
  - आंकड़ों के तौर पर इस्तेमाल करने के लिए: विज्ञापन पहचानकर्ता ऐप्लिकेशन इस्तेमाल करने वाले व्यक्ति की साफ़ तौर पर सहमति के बाद ही, व्यक्तिगत पहचान से जुड़ी जानकारी या किसी डिवाइस पहचानकर्ता के साथ लगातार जुड़ सकता है. उदाहरण के लिए: SSAID, MAC का पता, IMEI वगैरह.
- ऐप्लिकेशन इस्तेमाल करने वाले लोगों ने जो चुना है उसके मुताबिक. अगर रीसेट किया जाता है, तो नए विज्ञापन पहचानकर्ता को उपयोगकर्ता की सहमति के बिना किसी पिछले विज्ञापन पहचानकर्ता से संपर्क या किसी पिछले विज्ञापन पहचानकर्ता से मिले हुए डेटा का इस्तेमाल नहीं करना चाहिए. साथ ही, आपको उपयोगकर्ता की "पसंद के हिसाब से विज्ञापन से ऑफ्ट आउट करने" या "दिलचस्पी के मुताबिक विज्ञापन से ऑफ्ट आउट करने" की सेटिंग के हिसाब से काम करना चाहिए. अगर किसी उपयोगकर्ता ने इस सेटिंग को चालू किया हुआ है, तो आप विज्ञापन उद्देश्यों के लिए उपयोगकर्ता प्रोफ़ाइल बनाने या पसंद को ध्यान में रखते हुए विज्ञापन बनाकर उपयोगकर्ताओं को टारगेट करने के लिए विज्ञापन पहचानकर्ता का इस्तेमाल नहीं कर सकते. जिन गतिविधियों की अनुमति दी गई है उनमें कॉन्टेंट के हिसाब से विज्ञापन, फ़्रीक्वेंसी कैपिंग, कन्वर्ज़न ट्रैकिंग, रिपोर्टिंग और सुरक्षा, और धोखाधड़ी की पहचान करना शामिल है.
- ऐप्लिकेशन इस्तेमाल करने वाले लोगों के लिए साफ़ तौर पर जानकारी देनी चाहिए. विज्ञापन पहचानकर्ता का संग्रह, इस्तेमाल, और इन शर्तों को पूरा करने के वादे को ऐप्लिकेशन इस्तेमाल करने वाले व्यक्ति के सामने कानूनी रूप से सही निजता नोटिस के रूप में ज़ाहिर किया जाना चाहिए. निजता मानकों के बारे में ज़्यादा जानकारी के लिए, कृपया हमारे [ऐप्लिकेशन इस्तेमाल करने वाले व्यक्ति के डेटा](#) की नीति देखें.

- इस्तेमाल करने की शर्तों को मानना विज्ञापन पहचानकर्ता का इस्तेमाल सिर्फ़ इन शर्तों के मुताबिक ही किया जा सकता है। इसमें वह पक्ष भी शामिल है जिसके साथ आप इसे कारोबार के दौरान शेयर कर सकते हैं। Google Play पर अपलोड या प्रकाशित किए गए सभी ऐप्लिकेशन को किसी भी विज्ञापन मकसद के लिए, किसी दूसरे डिवाइस पहचानकर्ता के बदले विज्ञापन आईडी (डिवाइस पर उपलब्ध होने पर) का इस्तेमाल करना होगा।

## परिवार के लिए विज्ञापन कार्यक्रम

अगर आप अपने ऐप्लिकेशन में विज्ञापन दिखाते हैं और आपके ऐप्लिकेशन के टारगेट किए जाने वाले दर्शकों में सिर्फ़ बच्चे शामिल हैं, जैसा कि [परिवार नीति](#) में बताया गया है, तो आपको Google Play की नीतियों के हिसाब से खुद प्रमाणित किया हुआ विज्ञापन SDK टूल इस्तेमाल करना होगा। साथ ही, इसे विज्ञापन SDK टूल प्रमाणित करने की नीचे दी गई ज़रूरी शर्तों के मुताबिक होना चाहिए। अगर आपके ऐप्लिकेशन का टारगेट बच्चे और बड़े दोनों हैं, तो आपको उम्र तय करने के तरीके लागू करने होंगे। साथ ही, यह पक्का करना होगा कि बच्चों को दिखाए जाने वाले विज्ञापन, खुद प्रमाणित किए हुए विज्ञापन SDK टूल से ही मिले हों। 'परिवार के लिए बनाए गए' कार्यक्रम में मौजूद ऐप्लिकेशन के लिए ज़रूरी है कि वे सिर्फ़ खुद प्रमाणित किए हुए विज्ञापन SDK टूल का इस्तेमाल करें।

Google Play के प्रमाणित विज्ञापन SDK टूल की ज़रूरत सिर्फ़ तब होती है, जब आप अपने विज्ञापन SDK टूल का इस्तेमाल बच्चों को विज्ञापन दिखाने के लिए करते हैं। यहां बताई गई परिस्थितियों में Google Play पर, विज्ञापन SDK टूल को खुद को प्रमाणित करने की ज़रूरत नहीं होती। हालांकि, इस बात को पक्का करने की ज़िम्मेदारी अब भी आपकी है कि विज्ञापन का कॉन्टेंट और डेटा इकट्ठा करने के तरीके Play की [ऐप्लिकेशन इस्तेमाल करने वाले की डेटा नीति](#) और [परिवार नीति](#) का पालन करते हों:

- इन-हाउस विज्ञापन से SDK टूल का इस्तेमाल करके, आप अपने ऐप्लिकेशन या दूसरी मालिकाना हक वाली मीडिया और प्रचार के लिए बेची जाने वाली चीज़ों को मैनेज करने के लिए SDK टूल का इस्तेमाल करते हैं
- विज्ञापन देने वालों के साथ प्रत्यक्ष डील करना, जिसमें आप इन्वेंट्री मैनेजमेंट के लिए SDK टूल का इस्तेमाल करते हैं

विज्ञापन SDK टूल प्रमाणित करने के लिए ज़रूरी शर्तें

- तय करें कि किस तरह के विज्ञापन और व्यवहार आपत्तिजनक हैं। साथ ही, विज्ञापन SDK टूल की शर्तों या नीतियों के मुताबिक उन पर पाबंदी लगाएं। आपत्तिजनक विज्ञापन और व्यवहार तय करते समय Play की डेवलपर कार्यक्रम नीतियों का पालन करना ज़रूरी है।
- अपने विज्ञापन क्रिएटिव को रेटिंग देने का एक तरीका बनाएं। यह तरीका उम्र के हिसाब से बने अलग-अलग ग्रुप के मुताबिक हो। इन ग्रुप में, 'सभी के लिए' और 'वयस्क' दोनों तरह के ग्रुप शामिल होने चाहिए। रेटिंग देने का तरीका, Google के उस तरीके के मुताबिक होना चाहिए जो वह SDK टूल को, पसंद बताने के लिए नीचे दिया गया फ़ॉर्म भरते समय देता है।
- प्रकाशकों को हर अनुरोध या हर ऐप्लिकेशन के आधार पर, विज्ञापन देने के लिए बच्चों को ध्यान में रखते हुए व्यवहार/बर्ताव का अनुरोध करने दें। इस तरह के बर्ताव को लागू कानूनों और नियमों, जैसे कि [यूएस चिल्ड्रेन ऑनलाइन प्राइवसी एंड प्रोटेक्शन ऐक्ट \(कोपा\)](#) और [ईयू \(यूरोपीय संघ\) जनरल डेटा प्रोटेक्शन रेगुलेशन \(जीडीपीआर\)](#) के मुताबिक होना चाहिए। Google Play को दर्शकों की पसंद को ध्यान में रखकर बनाए गए विज्ञापन, पसंद के हिसाब से बनाए गए विज्ञापन, और बच्चों को ध्यान में रखते हुए व्यवहार/बर्ताव के तौर पर फिर से मार्केटिंग को बंद करने के लिए SDK टूल की ज़रूरत होती है।
- प्रकाशकों को ऐसे विज्ञापन फ़ॉर्मेट चुनने की अनुमति दें जो [Play की परिवार के हिसाब से विज्ञापन और कमाई करने की नीति](#) का पालन करते हों और [शिक्षकों की अनुमति वाले ऐप्लिकेशन के कार्यक्रम](#) की ज़रूरी शर्तें पूरी करते हों।
- पक्का करें कि जब रीयल-टाइम बोली-प्रक्रिया का इस्तेमाल बच्चों को विज्ञापन दिखाने के लिए किया जाए, तो क्रिएटिव की समीक्षा की जाए। साथ ही, बोली लगाने वालों को निजता बनाए रखने के बारे में संकेत दिए जाएं।
- Google को इस बात की पुष्टि करने के लिए ज़रूरी जानकारी दें कि विज्ञापन SDK टूल प्रमाणित होने के लिए सभी ज़रूरी शर्तों को पूरा करता है, इस तरह की जानकारी नीचे दिए गए [पसंद बताने वाले फ़ॉर्म](#) में दी गई है। साथ ही, बाद में मांगी जाने वाली किसी भी जानकारी के लिए समय पर जवाब दें।

*ध्यान दें: विज्ञापन SDK टूल में ऐसे विज्ञापन देने की सुविधा होनी चाहिए जो बच्चों से जुड़े सभी ज़रूरी कानूनों और नियमों का पालन करती है। साथ ही, ये नियम और कानून उनके प्रकाशकों पर लागू होते हैं।*

बच्चों के लिए विज्ञापन दिखाते समय, इसकी सुविधा देने वाले प्लैटफ़ॉर्म के लिए मीडिएशन (मध्यस्थता) की शर्तें:

- यह पक्का करने के लिए कि मीडिएशन से दिखाए जाने वाले सभी विज्ञापन इन शर्तों को पूरा करते हों, सिर्फ़ Google Play से प्रमाणित विज्ञापन SDK टूल का इस्तेमाल करें या सुरक्षा के ज़रूरी उपाय लागू करें; और
- विज्ञापन की रेटिंग और बच्चों को ध्यान में रखते हुए व्यवहार/बर्ताव दिखाने के लिए मीडिएशन प्लैटफ़ॉर्म को ज़रूरी जानकारी दें।

डेवलपर यहां [खुद को प्रमाणित करने वाले विज्ञापन SDK टूल की सूची](#) देख सकते हैं।

इसके साथ ही, डेवलपर **पसंद बताने वाला फ़ॉर्म** भी उन विज्ञापन SDK टूल के साथ शेयर कर सकते हैं जो खुद को प्रमाणित करना चाहते हैं।

## स्टोर पेज और प्रचार

आपका ऐप्लिकेशन किसको दिखेगा और उसका प्रचार किस तरह हुआ है, इन बातों का स्टोर की क्वालिटी पर काफ़ी असर पड़ता है। स्पैम वाले स्टोर पेज, हल्की क्वालिटी वाला प्रचार, और Google Play पर आर्टिफ़िशियल तरीके से लोगों तक ऐप्लिकेशन पहुंचाने (दिखाने) की कोशिशों से बचें।

## ऐप्लिकेशन का प्रचार

हम ऐसे किसी ऐप्लिकेशन को अनुमति नहीं देते जो सीधे तौर पर या किसी और तरीके से लोगों या डेवलपर के साथ धोखाधड़ी करते हैं या उन्हें नुकसान पहुंचाते हैं। इसके अलावा, फ़ायदा लेने के लिए गलत तरीकों से भी प्रचार करने की अनुमति नहीं है। इसमें ऐसे ऐप्लिकेशन शामिल हैं जो इन तरीकों को अपनाते हैं:

- वेबसाइट, ऐप्लिकेशन या अन्य प्रॉपर्टी पर धोखाधड़ी करने वाले विज्ञापनों का इस्तेमाल करना। इनमें ऐसी सूचनाएं भी शामिल हैं जो सिस्टम की सूचना और चेतावनी जैसी ही होती हैं।
- प्रचार या इंस्टॉल कराने के ऐसे तरीके जो उपयोगकर्ताओं को Google Play पर ले जाते हैं या उपयोगकर्ताओं को कार्रवाई की सूचना दिए बिना ही ऐप्लिकेशन डाउनलोड कर देते हैं।
- एसएमएस सेवाओं से अनचाहा प्रचार करना।

यह पक्का करना आपकी ज़िम्मेदारी है कि कोई भी विज्ञापन नेटवर्क कंपनी या आपके ऐप्लिकेशन के सहयोगी इन नीतियों का पालन करते हों। साथ ही, प्रचार करने के लिए किसी भी पाबंदी वाले तरीके का इस्तेमाल नहीं करते हों।

## मेटाडेटा

हम उन ऐप्लिकेशन को अनुमति नहीं देते जिनमें गुमराह करने वाला, गलत तरीके से फ़ॉर्मेट किया गया, बिना किसी जानकारी वाला, ग़ैर-ज़रूरी, हद से ज़्यादा या गलत मेटाडेटा शामिल होता है। इनमें ऐप्लिकेशन की जानकारी, डेवलपर का नाम, शीर्षक, आइकॉन, स्क्रीनशॉट, और प्रमोशन की इमेज भी शामिल होती हैं। इसमें इनके अलावा, और भी चीज़ें शामिल हो सकती हैं डेवलपर को अपने ऐप्लिकेशन के बारे में साफ़ तौर पर और सही तरीके से लिखी जानकारी देनी चाहिए। हम ऐप्लिकेशन के बारे में दी गई जानकारी में, उन टेस्टीमोनियल को शामिल करने की अनुमति नहीं देते जिन्हें किसी व्यक्ति ने पहचान छिपाकर लिखा हो या जिन्हें लिखने वाले के बारे में कुछ पता न हो।

यहां बताई गई ज़रूरी शर्तों के अलावा, Play की खास डेवलपर नीतियों के लिए आपको मेटाडेटा की और भी जानकारी देने की ज़रूरत हो सकती है।

यहां आम तौर पर होने वाले उल्लंघनों के कुछ उदाहरण दिए गए हैं:

× RescueRover

The best way to find a new furry friend!

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

1 -----  
See how much our users love us:

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

2 -----  
It's the #1 app after Pet Rescue Saga, but in real life!

50% cooler and 100% faster than FidoFinder

3 -----  
You can see black dogs, brown dogs, white dogs, big dogs, medium dogs, small dogs, dog leashes, dog training books, dog bowls, dog toys, dog accessories. dog, dogs, rescue, shelter, animal, pet, pets, adopt, foster, puppy, puppies, dogs including:  
1) golden retriever  
2) labradoodle  
3) poodle  
4) chihuahua  
5) akita  
6) pug  
7) rottweiler



- ① बिना एट्रिब्यूशन या बिना पहचान वाले उपयोगकर्ता टेस्टीमोनियल
- ② ऐप्लिकेशन या ब्रैंड के डेटा की तुलना
- ③ वर्ड ब्लॉक और वर्टिकल/हॉरिज़ॉन्टल वर्ड लिस्ट

यहां आपके स्टोर पेज में मौजूद गलत टेक्स्ट, इमेज या वीडियो के कुछ उदाहरण दिए गए हैं:

- ऐसी तस्वीरें या वीडियो जिनमें यौन भावना को भड़काने वाला अश्लील कॉन्टेंट शामिल होता है. उन अश्लील इमेज से बचें जिनमें स्तन, कूल्हे, जननांग या ऐसा ही कोई दूसरा आकर्षित करने वाला अंग या कॉन्टेंट शामिल हो. भले ही, उसे तस्वीर के तौर पर दिखाया गया हो या असल रूप में.
- ऐप्लिकेशन के स्टोर पेज पर ऐसी भाषा का इस्तेमाल करना जो गाली-गलौज से भरी हो, अश्लील हो या आम तौर पर लोगों के लिए सही न हो.
- ऐप्लिकेशन आइकॉन, प्रचार से जुड़ी इमेज या वीडियो में खास तौर पर दिखाया गया दिल दहलाने वाला कॉन्टेंट.
- दवाओं के गैरकानूनी इस्तेमाल को दिखाना. यहां तक कि EDSA (शिक्षा, डॉक्यूमेंट्री, विज्ञान या कला) कॉन्टेंट को भी सभी दर्शकों की सुविधा के हिसाब से स्टोर पेज में शामिल किया जाना चाहिए.

यहां कुछ सबसे सही तरीके दिए गए हैं:

- अपने ऐप्लिकेशन की सबसे अच्छी बातों को हाइलाइट करें. दिलचस्प और मज़ेदार जानकारी शेयर करें, ताकि लोगों को यह पता चल सके कि आपके ऐप्लिकेशन में क्या खास है.
- पक्का करें कि आपके ऐप्लिकेशन का शीर्षक और ब्यौरा, ऐप्लिकेशन के फ़ंक्शन के बारे में सही जानकारी देता हो.
- दोहराए जाने वाले या बेवजह के कीवर्ड या रेफ़रंस का इस्तेमाल करने से बचें.
- अपने ऐप्लिकेशन की जानकारी कम और आसान शब्दों में दें. कम शब्दों में जानकारी का मकसद, खास तौर पर छोटे डिसप्ले वाले डिवाइस पर बेहतरीन उपयोगकर्ता अनुभव देना है. हद से ज़्यादा लंबे, ब्यौरे, गलत फ़ॉर्मेट या दोहराई जाने वाली जानकारी से, इस नीति का उल्लंघन हो सकता है.

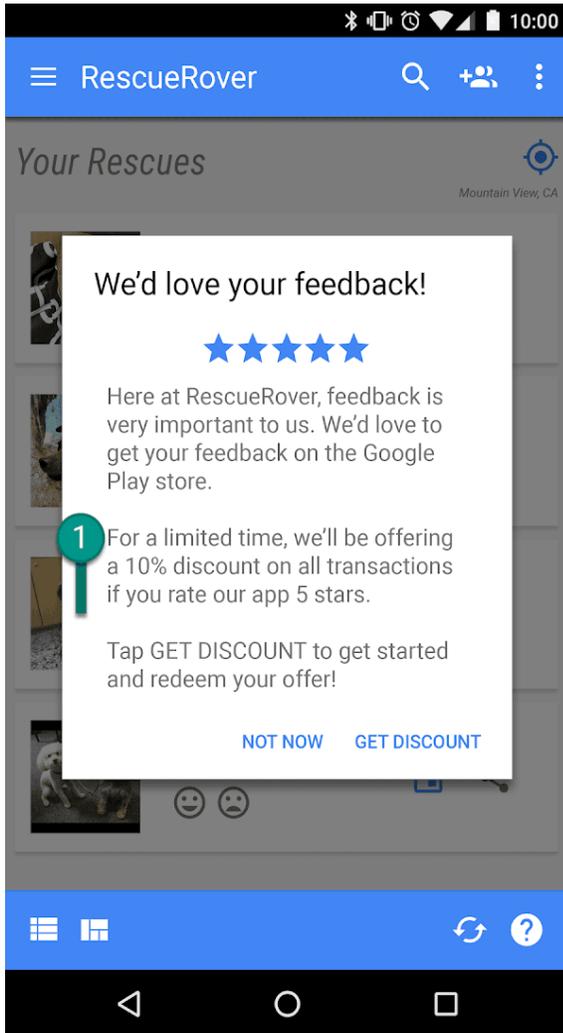
- ध्यान रखें कि आपका स्टोर पेज, आम दर्शक के हिसाब से होना चाहिए. अपने स्टोर पेज में गलत टेक्स्ट, इमेज या वीडियो के इस्तेमाल से बचें. साथ ही, ऊपर बताए गए दिशा-निर्देशों का पालन करें.

## ऐप्लिकेशन इस्तेमाल करने वाले व्यक्ति की रेटिंग, समीक्षाएं, और इंस्टॉल की संख्या

डेवलपर को Google Play में किसी भी ऐप्लिकेशन के प्लेसमेंट में बदलाव करने की कोशिश नहीं करनी चाहिए. इसमें धोखाधड़ी या कोई फ़ायदा देकर कराए गए इंस्टॉल, समीक्षाएं और रेटिंग जैसे अवैध तरीकों से, प्रॉडक्ट रेटिंग, समीक्षाएं या इंस्टॉलेशन की संख्याओं को बढ़ाना शामिल है. हालांकि, यह इन ही चीज़ों तक सीमित नहीं है.

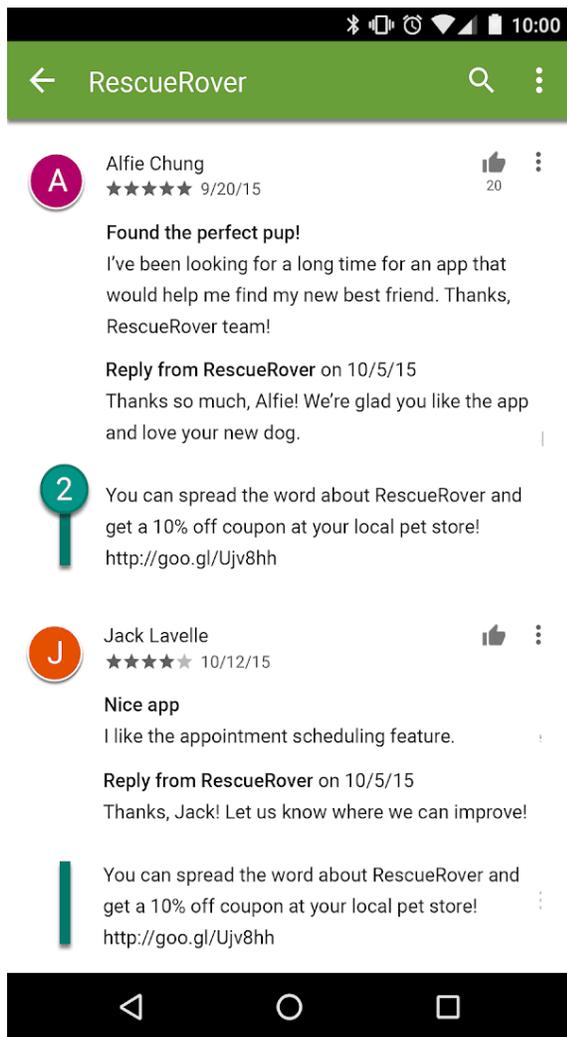
यहां आम तौर पर होने वाले उल्लंघनों के कुछ उदाहरण दिए गए हैं:

- फ़ायदा देते हुए, उपयोगकर्ताओं से अपने ऐप्लिकेशन को रेट करने के लिए कहना:



① ① यह सूचना उपयोगकर्ताओं को ज़्यादा रेटिंग के बदले में छूट ऑफ़र करती है.

- Google Play पर ऐप्लिकेशन के प्लेसमेंट को प्रभावित करने के लिए बार-बार रेटिंग सबमिट करना.
- आपत्तिजनक कॉन्टेंट वाली समीक्षाएं सबमिट करना या इस्तेमाल करने वाले को ऐसी समीक्षाएं सबमिट करने के लिए बढ़ावा देना, जिनमें सहयोगी, कूपन, गेम के कोड, ईमेल पते या वेबसाइट और अन्य ऐप्लिकेशन के लिंक शामिल होते हैं:



② यह समीक्षा इस्तेमाल करने वालों को एक कूपन का ऑफ़र देकर RescueRover ऐप्लिकेशन का प्रचार करने के लिए बढ़ावा देती है।

रेटिंग और समीक्षाएं ऐप्लिकेशन की गुणवत्ता के मानदंड हैं। इस्तेमाल करने वाले ऐसे ऐप्लिकेशन की पुष्टि करने और इसके ज़रूरी होने के लिए रेटिंग और समीक्षाओं पर निर्भर करते हैं। यहां इस्तेमाल करने वालों की समीक्षाओं के जवाब देने के लिए सबसे सही तरीके दिए गए हैं:

- अपने जवाब में उपयोगकर्ता की टिप्पणियों में उठाई गई समस्याओं को हल करने पर ध्यान दें, न कि ज़्यादा रेटिंग की मांग करें।
- सहायता पता या अक्सर पूछे जाने वाले सवालों के पेज जैसे उपयोगी संसाधनों को शामिल करें।

## कॉन्टेंट रेटिंग

Google Play पर कॉन्टेंट रेटिंग इंटरनेशनल एज रेटिंग कोअलिशन (आईएआरसी) देता है और इसे ऐप्लिकेशन इस्तेमाल करने वाले लोगों को स्थानीय रूप से सभी ज़रूरी कॉन्टेंट रेटिंग देने में डेवलपर की सहायता करने के लिए डिज़ाइन किया गया है। आईएआरसी के क्षेत्रीय विभाग ऐसे दिशा-निर्देश बनाए रखते हैं जिनका इस्तेमाल ऐप्लिकेशन में कॉन्टेंट के समझदारी लेवल को तय करने के लिए किया जाता है। हम Google Play पर बिना कॉन्टेंट रेटिंग वाले ऐप्लिकेशन को अनुमति नहीं देते हैं।

## कॉन्टेंट रेटिंग का इस्तेमाल किस तरह किया जाता है

कॉन्टेंट रेटिंग का इस्तेमाल उपभोक्ताओं, खासकर अभिभावकों को ऐप्लिकेशन में संभावित रूप से मौजूद आपत्तिजनक कॉन्टेंट की जानकारी देने के लिए किया जाता है। ये कुछ जगहों पर आपके कॉन्टेंट को फ़िल्टर करने या कुछ लोगों तक इस तरह के कॉन्टेंट की पहुंच को रोकने में मदद करते हैं, जहां भी कानूनी तौर पर ऐसा करना ज़रूरी होता है। साथ ही, यह इस बात का पता लगाने में भी मदद करते हैं कि आपका ऐप्लिकेशन खास डेवलपर प्रोग्राम की ज़रूरी शर्तों को पूरा करता है या नहीं।

## कॉन्टेंट रेटिंग किस तरह दी जाती हैं

कॉन्टेंट रेटिंग पाने के लिए, आपको [Play Console में रेटिंग से जुड़े सवालों की सूची](#) भरनी होगी। इसमें यह पूछा जाता है कि आपके ऐप्लिकेशन का कॉन्टेंट कैसा है। सवालों की सूची में दिए गए जवाबों के मुताबिक, आपके ऐप्लिकेशन को अलग-अलग रेटिंग देने वाले विभागों की तरफ से कॉन्टेंट रेटिंग दी जाएगी। आपके ऐप्लिकेशन के कॉन्टेंट को गलत तरीके से पेश करने की वजह से ऐप्लिकेशन को हटाया जा सकता है या उस पर कुछ देर के लिए रोक लगाई जा सकती है। इसलिए, कॉन्टेंट रेटिंग से जुड़े सवालों की सूची में सही जवाब देना ज़रूरी है।

अपने ऐप्लिकेशन को “बगैर रेटिंग वाला” सूची में शामिल होने से रोकने के लिए, आपको Play Console में सबमिट किए गए हर नए ऐप्लिकेशन की कॉन्टेंट रेटिंग से जुड़े सवालों की सूची पूरी करना ज़रूरी है। साथ ही, ऐसा करना Google Play पर पहले से मौजूद सभी ऐप्लिकेशन के लिए भी ज़रूरी है।

अगर आप अपने ऐप्लिकेशन के कॉन्टेंट या सुविधाओं में ऐसे बदलाव करते हैं जिनसे रेटिंग के सवालों की सूची में दिए गए जवाबों पर असर पड़ता है, तो आपको Play Console में कॉन्टेंट रेटिंग से जुड़े सवालों की नई सूची सबमिट करनी होगी।

अलग-अलग [रेटिंग देने वाले विभागों](#) के बारे में ज़्यादा जानकारी पाने और कॉन्टेंट रेटिंग से जुड़े सवालों की सूची को पूरा करने का तरीका जानने के लिए [सहायता केंद्र](#) पर जाएं।

## रेटिंग से जुड़ी अपील

अगर आप अपने ऐप्लिकेशन को मिली रेटिंग से सहमत नहीं हैं, तो आप अपने प्रमाणपत्र ईमेल में दिए गए लिंक का इस्तेमाल करके सीधे आईएआरसी रेटिंग देने वाले विभाग में अपील कर सकते हैं।

## समाचार

ऐसा ऐप्लिकेशन जो Play Console (“समाचार ऐप्लिकेशन”) पर खुद के “समाचार” ऐप्लिकेशन होने का दावा करता है उसे इन सभी ज़रूरी शर्तों को पूरा करना होगा।

ऐसे समाचार ऐप्लिकेशन जिनका इस्तेमाल करने के लिए किसी व्यक्ति को सदस्यता लेने की ज़रूरत होती है, तो उन ऐप्लिकेशन की खरीदारी से पहले लोगों को ऐप्लिकेशन के अंदर मौजूद कॉन्टेंट की झलक दिखानी चाहिए।

समाचार ऐप्लिकेशन के लिए ज़रूरी है कि वे:

- समाचार प्रकाशक और इनमें योगदान देने वालों के मालिकाना हक से जुड़ी जानकारी दें। इसके अलावा, इसमें और भी जानकारी शामिल हो सकती है। जैसे- आपके ऐप्लिकेशन में प्रकाशित किए गए समाचार की आधिकारिक वेबसाइट, प्रकाशक की मान्य और पुष्टि की जा सकने वाली संपर्क जानकारी, और हर लेख के असली प्रकाशक का नाम।
- साथ ही, ऐप्लिकेशन के अंदर किसी पेज या वेबसाइट पर साफ़ तौर पर संपर्क जानकारी को लेबल किया गया हो और जो आसानी से मिल जाए (उदाहरण के लिए, उसे होम पेज में सबसे नीचे या साइट नेविगेशन बार में लिंक किया गया हो)। इसके अलावा, इसमें समाचार प्रकाशक की मान्य संपर्क जानकारी होनी चाहिए जिसमें कम से कम उसका ईमेल पता और फ़ोन नंबर शामिल हो।

कृपया ध्यान दें कि सोशल मीडिया ख़ातों के लिंक, प्रकाशक की संपर्क जानकारी के तौर पर काफ़ी नहीं हैं। इसके अलावा, ऐसे ऐप्लिकेशन जिनमें मुख्य रूप से यूज़र जनरेटेड कॉन्टेंट होता है (उदाहरण के लिए, सोशल मीडिया ऐप्लिकेशन) उन्हें खुद के समाचार ऐप्लिकेशन होने का दावा नहीं करना चाहिए।

समाचार ऐप्लिकेशन के लिए ज़रूरी है कि:

- उनमें स्पेलिंग या व्याकरण से जुड़ी गड़बड़ियां न हों,
- सिर्फ़ स्टैटिक कॉन्टेंट (उदाहरण के लिए, कई महीने पुराना कॉन्टेंट) न हो
- उनका मुख्य मकसद अफ़िलिएट मार्केटिंग या विज्ञापन से होने वाली आय न हो।

कृपया ध्यान दें कि जब तक समाचार ऐप्लिकेशन का मुख्य मकसद प्रॉडक्ट और सेवाओं को बेचना या विज्ञापन से होने वाली आय जनरेट करना न हो, तब तक *हो सकता है कि वे ऐप्लिकेशन कमाई करने के लिए विज्ञापन और मार्केटिंग के अन्य तरीकों का इस्तेमाल करें।*

ऐसे समाचार ऐप्लिकेशन जो प्रकाशन के अलग-अलग स्रोतों से कॉन्टेंट इकट्ठा करते हैं उन्हें ऐप्लिकेशन में प्रकाशित होने वाले कॉन्टेंट के स्रोत के बारे में साफ़ तौर पर जानकारी देनी चाहिए। साथ ही, हर एक स्रोत को समाचार नीति की ज़रूरी शर्तों को पूरा करना चाहिए।

## बुनियादी सुविधाएं और स्पैम

कम से कम, ऐप्लिकेशन के ज़रिए उपयोगकर्ताओं को बुनियादी सुविधाओं के साथ-साथ बेहतर अनुभव देना चाहिए. जिन ऐप्लिकेशन का मकसद लोगों या Google Play को सिर्फ़ स्पैम भेजना होता है उनका कैटलॉग सही तरीके से बड़ा नहीं होता. ऐसा उन ऐप्लिकेशन के साथ भी होता है जो अचानक बंद हो जाते हैं या इस तरह से काम करते हैं कि ऐप्लिकेशन इस्तेमाल करने वाले व्यक्ति को अच्छा अनुभव नहीं मिल पाता.

## स्पैम

हम ऐसे ऐप्लिकेशन को अनुमति नहीं देते जो ऐप्लिकेशन इस्तेमाल करने वाले लोगों को या Google Play को स्पैम भेजते हैं. जैसे: वे ऐप्लिकेशन जो लोगों को अनचाहे मैसेज भेजते हैं या ऐसे ऐप्लिकेशन जो बार-बार एक ही चीज़ दिखाते हैं या जिनकी क्वालिटी हल्की होती है.

## मैसेज स्पैम

हम ऐसे ऐप्लिकेशन को अनुमति नहीं देते जो इस्तेमाल करने वाले व्यक्ति को कॉन्टेंट और चुने हुए लोगों की पुष्टि करने की सुविधा दिए बिना, उनकी तरफ़ से एसएमएस, ईमेल या अन्य मैसेज भेजते हैं.

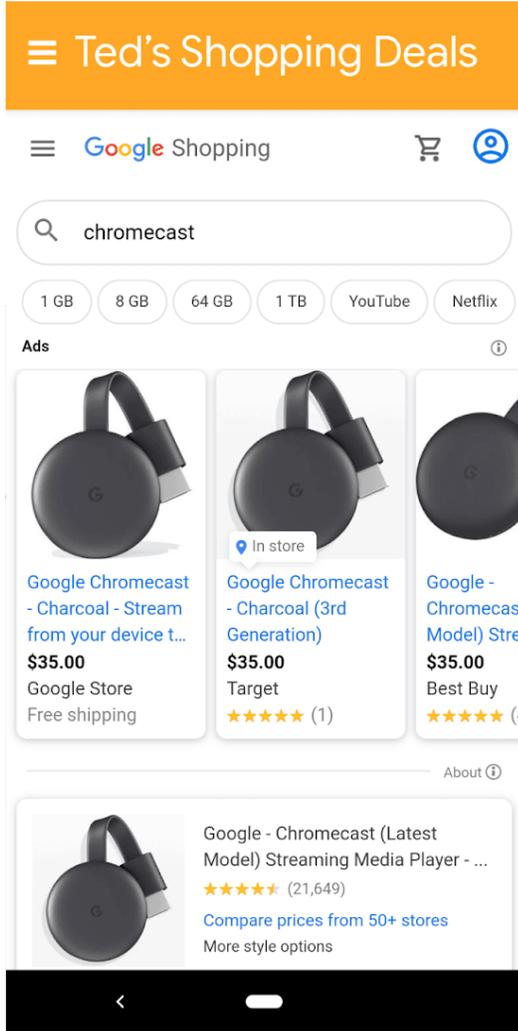
## वेबव्यू और उससे जुड़े स्पैम

हम ऐसे ऐप्लिकेशन को अनुमति नहीं देते जिनका मुख्य मकसद अफ़िलिएट ट्रैफ़िक को किसी वेबसाइट पर भेजना या किसी वेबसाइट का वेबव्यू उस वेबसाइट के मालिक या एडमिन की मंजूरी के बिना दिखाना हो.

यहां आम तौर पर होने वाले उल्लंघनों के कुछ उदाहरण दिए गए हैं:

- ऐसा ऐप्लिकेशन जिसका मुख्य मकसद रेफ़रल ट्रैफ़िक को किसी वेबसाइट पर भेजना होता है, ताकि उस वेबसाइट पर इस्तेमाल करने वाले व्यक्ति के साइन-अप या खरीदारी करने से क्रेडिट पा सके.

- ऐसे ऐप्लिकेशन जिनका मुख्य मकसद अनुमति के बिना किसी वेबसाइट का वेबव्यू दिखाना होता है:



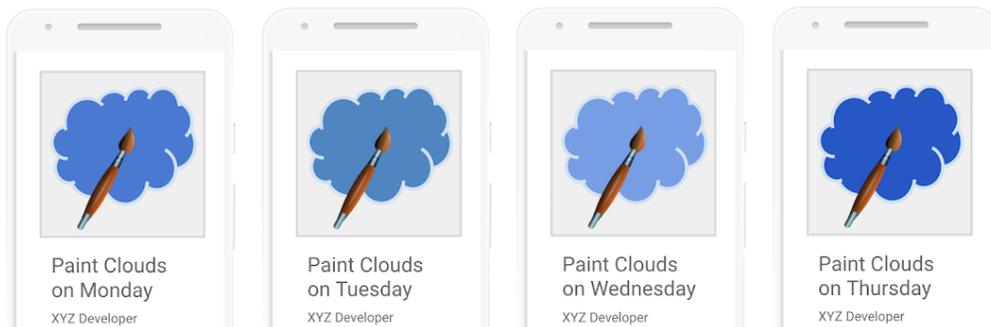
इस ऐप्लिकेशन का नाम "Ted's Shopping Deals" है और यह सामान्य तौर पर Google Shopping का वेबव्यू दिखाता है.

## बार-बार एक ही तरह का कॉन्टेंट

हम ऐसे ऐप्लिकेशन को अनुमति नहीं देते जो Google Play पर पहले से मौजूद दूसरे ऐप्लिकेशन के जैसा ही अनुभव देते हों. ऐप्लिकेशन ऐसे होने चाहिए जो सबसे अलग कॉन्टेंट या सेवाएं देकर लोगों के लिए फ़ायदेमंद साबित हों.

यहां आम तौर पर होने वाले उल्लंघनों के कुछ उदाहरण दिए गए हैं:

- कोई मूल कॉन्टेंट या उसमें कुछ नया जोड़े बिना दूसरे ऐप्लिकेशन से कॉन्टेंट की नकल करना.
- इसके अलावा, ऐसे कई सारे ऐप्लिकेशन बनाना जिनका काम करने का तरीका, कॉन्टेंट, और ऐप्लिकेशन को इस्तेमाल करने का अनुभव बहुत ही मिलता-जुलता हो. अगर इनमें से हर ऐप्लिकेशन पर कम कॉन्टेंट है, तो डेवलपर को सभी कॉन्टेंट के लिए एक ही ऐप्लिकेशन बनाना चाहिए.



## विज्ञापन के लिए बनाए गए ऐप्लिकेशन

हम ऐसे ऐप्लिकेशन को अनुमति नहीं देते जिनका मुख्य मकसद विज्ञापन दिखाना है।

यहां आम तौर पर होने वाले उल्लंघनों के कुछ उदाहरण दिए गए हैं:

- ऐसे ऐप्लिकेशन जिन पर इस्तेमाल करने वाले व्यक्ति की हर कार्रवाई के बाद, पेज पर अचानक दिखने वाले विज्ञापन आ जाते हैं। इनमें क्लिक, स्वाइप वगैरह शामिल हैं। इसमें इनके अलावा, और भी चीजें शामिल हो सकती हैं।

## कम से कम सुविधाएं

पक्का करें कि आपका ऐप्लिकेशन भरोसेमंद, दिलचस्प, और इस्तेमाल करने वाले व्यक्ति को बेहतर अनुभव देता हो।

यहां आम तौर पर होने वाले उल्लंघनों के कुछ उदाहरण दिए गए हैं:

- ऐसे ऐप्लिकेशन जिन्हें बेवजह बनाया गया है या जिनमें कोई सुविधा नहीं है

## अधूरी सुविधाएं

हम ऐसे ऐप्लिकेशन को अनुमति नहीं देते जो बीच में रुक जाते हैं, ज़बरदस्ती बंद हो जाते हैं, फ्रीज़ हो जाते हैं या फिर असामान्य तरीके से काम करते हैं।

यहां आम तौर पर होने वाले उल्लंघनों के कुछ उदाहरण दिए गए हैं:

- ऐसे ऐप्लिकेशन जो इंस्टॉल नहीं होते
- ऐसे ऐप्लिकेशन जो इंस्टॉल तो होते हैं, लेकिन लोड नहीं होते
- ऐसे ऐप्लिकेशन जो लोड तो होते हैं, लेकिन काम नहीं करते

## दूसरे प्रोग्राम

Android के दूसरे अनुभवों के लिए डिज़ाइन किए गए और Google Play पर उपलब्ध ऐप्लिकेशन को इस नीति केंद्र में बताई गई कॉन्टेंट की नीतियों का पालन करना होगा। इसके अलावा, उन पर प्रोग्राम के लिए खास तौर पर बनी ज़रूरी नीतियां भी लागू हो सकती हैं। यह तय करने के लिए नीचे दी गई सूची की समीक्षा करें कि क्या इनमें से कोई नीति आपके ऐप्लिकेशन पर लागू होती है।

## Android Instant Apps

हमारा मकसद है कि Android Instant Apps के साथ उपयोगकर्ता को शानदार और बिना रुकावट वाले अनुभव मिलें। साथ ही, निजता और सुरक्षा के सबसे ऊंचे मानकों का पालन भी किया जाए। हमारी नीतियां इस तरह से बनाई गई हैं कि वे इस मकसद को पूरा करने में मददगार हों।

Google Play से Android Instant Apps को लोगों तक पहुंचाने के लिए, डेवलपर को सभी [Google Play की डेवलपर कार्यक्रम नीतियों](#) का पालन करना होगा। इनके अलावा, नीचे दी गई नीतियों का भी पालन करना होगा।

## पहचान

लॉगिन की सुविधा देने वाले इंस्टैंट ऐप्लिकेशन में, डेवलपर को [पासवर्ड के लिए Smart Lock](#) की सुविधा जोड़नी होगी।

## लिंक देकर मदद करना

Android Instant Apps के डेवलपर के लिए ज़रूरी है कि वे अपने ऐप्लिकेशन में दूसरे ऐप्लिकेशन के लिंक सही तरीके से शामिल करें। अगर डेवलपर के इंस्टैंट ऐप्लिकेशन या इंस्टॉल किए गए ऐप्लिकेशन में ऐसे लिंक मौजूद हैं जो लोगों को किसी इंस्टैंट ऐप्लिकेशन तक ले जा सकते हैं, तो डेवलपर को अपने ऐप्लिकेशन के [वेबव्यू](#) में दूसरे लिंक नहीं दिखाने चाहिए। डेवलपर के लिए ज़रूरी है कि वह ऐसे तरीके इस्तेमाल करने के बजाय, लोगों को उस इंस्टैंट ऐप्लिकेशन तक भेजे।

## तकनीकी जानकारी

डेवलपर को Android Instant Apps से जुड़ी उन तकनीकी बातों और ज़रूरी शर्तों का पालन करना होगा जिनके बारे में Google ने बताया है। इनमें समय-समय पर बदलाव भी हो सकते हैं। [हमारे सार्वजनिक दस्तावेज़](#) में मौजूद जानकारी और ज़रूरी शर्तें भी इनमें शामिल हैं।

## ऐप्लिकेशन इंस्टॉल करने की सुविधा का ऑफ़र देना

इंस्टैंट ऐप्लिकेशन, उपयोगकर्ता को इंस्टॉल करने लायक ऐप्लिकेशन ऑफ़र कर सकता है, लेकिन यह इंस्टैंट ऐप्लिकेशन का मुख्य मकसद नहीं होना चाहिए। इंस्टॉल करने का ऑफ़र देते समय, डेवलपर को:

- मटीरियल डिज़ाइन वाला "ऐप्लिकेशन डाउनलोड करें" आइकॉन और इंस्टॉल करने वाले बटन के लिए, "इंस्टॉल करें" लेबल इस्तेमाल करना चाहिए।
- अपने इंस्टैंट ऐप्लिकेशन में, किसी ऐप्लिकेशन को इंस्टॉल करने के दो या तीन से ज़्यादा अनुरोध शामिल नहीं करने चाहिए।
- लोगों को किसी ऐप्लिकेशन को इंस्टॉल करने का अनुरोध दिखाने के लिए, बैनर या विज्ञापन जैसी दूसरी तकनीक का इस्तेमाल नहीं करना चाहिए।

इंस्टैंट ऐप्लिकेशन के बारे में ज़्यादा जानकारी और UX से जुड़े दिशा-निर्देश [ऐप्लिकेशन इस्तेमाल करने वाले व्यक्ति को बेहतर अनुभव देने के सबसे सही तरीके](#) पर जा कर देखे जा सकते हैं।

## डिवाइस की स्थिति में बदलाव करना

Instant Apps को उपयोगकर्ता के डिवाइस में ऐसे बदलाव नहीं करने चाहिए जो इंस्टैंट ऐप्लिकेशन के सत्र के समय से ज़्यादा देर तक बने रहें। उदाहरण के लिए, इंस्टैंट ऐप्लिकेशन उपयोगकर्ता का वॉलपेपर नहीं बदल सकते हैं या कोई होमस्क्रीन विजेट नहीं बना सकते हैं।

## ऐप्लिकेशन कैसा दिखेगा

डेवलपरों को यह पक्का करना चाहिए कि उपयोगकर्ताओं को इंस्टैंट ऐप्लिकेशन इस तरह दिखाई दें, कि उपयोगकर्ता को हर समय यह पता रहे कि उसके डिवाइस पर इंस्टैंट ऐप्लिकेशन चल रहा है।

## डिवाइस पहचानकर्ता

Instant Apps ऐसे डिवाइस पहचानकर्ता एक्सेस करने पर पाबंदी लगाते हैं जो (1) इंस्टैंट ऐप्लिकेशन चलना बंद होने के बाद भी बने रहते हैं और (2) जिन्हें उपयोगकर्ता फिर से सेट नहीं कर सकता है। नीचे इनके उदाहरण दिए जा रहे हैं, लेकिन ये इन ही तक सीमित नहीं हैं:

- बिल्ड सीरियल
- किसी भी नेटवर्किंग चिप के Mac पते
- IMEI, IMSI

अगर फ़ोन नंबर रनटाइम अनुमति के दौरान मिला है, तो Instant Apps उसे एक्सेस कर सकते हैं। डेवलपर को इन पहचानकर्ताओं या दूसरे किसी भी तरीके का उपयोग करके, उपयोगकर्ता को फ़िंगरप्रिंट करने की कोशिश नहीं करनी चाहिए।

## नेटवर्क ट्रैफ़िक

इंस्टैंट ऐप्लिकेशन में चलने वाले नेटवर्क ट्रैफ़िक को एचटीटीपीएस जैसे किसी TLS प्रोटोकॉल का इस्तेमाल करके एन्क्रिप्ट (सुरक्षित) किया जाना ज़रूरी है।

## परिवार

Google Play, डेवलपर के लिए ऐसा बेहतरीन प्लैटफ़ॉर्म मुहैया कराता है जहां वे अपना कॉन्टेंट दिखाकर बता सकें कि वह अच्छी क्वालिटी का, हर उम्र के मुताबिक, और पूरे परिवार के हिसाब से सही है। किसी ऐप्लिकेशन को 'परिवार के लिए बनाए गए' कार्यक्रम में सबमिट करने से पहले या फिर बच्चों को टारगेट करने वाला ऐप्लिकेशन 'Google Play स्टोर' में सबमिट करने से पहले, यह तय करना आपकी ज़िम्मेदारी है कि आपका ऐप्लिकेशन बच्चों के लिए सही है और सभी संबंधित कानूनों का पालन करता है।

Academy for App Success पर जाएं और परिवार से जुड़ी प्रोसेस के बारे में जानें। साथ ही, आप इसकी इंटरैक्टिव चेकलिस्ट भी देख सकते हैं।

# बच्चों और परिवार के लिए ऐप्लिकेशन बनाना

परिवारों की ज़िंदगी बेहतर बनाने के टूल के तौर पर टेक्नोलॉजी का इस्तेमाल बढ़ता जा रहा है। अभिभावक अपने बच्चों से शेयर करने के लिए सुरक्षित और अच्छी क्वालिटी का कॉन्टेंट खोज रहे हैं। हो सकता है कि आप खास तौर पर बच्चों के लिए ऐप्लिकेशन बना रहे हों या फिर आपका ऐप्लिकेशन ऐसा हो जो उनका ध्यान खींचता हो। Google Play यह पक्का करने में आपकी मदद करना चाहता है कि आपका ऐप्लिकेशन सभी उपयोगकर्ताओं के लिए सुरक्षित है, जिसमें परिवार भी शामिल हैं।

अलग-अलग जगह भाषा और परिस्थितियों में "बच्चे" शब्द का मतलब अलग हो सकता है। आप अपने कानूनी सलाहकार से पूछ सकते हैं कि आपके ऐप्लिकेशन पर किस तरह की कानूनी जवाबदेही और/या उम्र से जुड़ी पाबंदी लागू हो सकती है। आपका ऐप्लिकेशन कैसा है इस बारे में आपसे बेहतर कोई नहीं जानता। इसलिए, हम आप पर भरोसा करके यह पक्का करना चाहते हैं कि Google Play पर मौजूद ऐप्लिकेशन परिवारों के लिए सुरक्षित हों।

खास तौर पर, बच्चों के लिए बनाए गए ऐप्लिकेशन को 'परिवार के लिए बनाए गए' कार्यक्रम में हिस्सा लेना चाहिए। अगर आपका ऐप्लिकेशन बच्चों और बड़ों, दोनों तरह के दर्शकों को टारगेट करता है, तब भी आप 'परिवार के लिए बनाए गए' कार्यक्रम में हिस्सा ले सकते हैं। 'परिवार के लिए बनाए गए' कार्यक्रम में ऑफ्ट-इन करने वाले सभी लोगों को [शिक्षकों से मंजूरी मिले ऐप्लिकेशन वाले कार्यक्रम](#) के लिए रेट किया जा सकता है। हालांकि, हम गारंटी नहीं दे सकते कि आपका ऐप्लिकेशन शिक्षकों से मंजूरी मिले ऐप्लिकेशन वाले कार्यक्रम में शामिल होगा। अगर आप 'परिवार के लिए बनाए गए' कार्यक्रम में हिस्सा नहीं लेते हैं, तब भी आपको नीचे दी गई Google Play की परिवार के लिए बनाई गई नीति का पालन करना होगा। साथ ही, आपको [Google Play डेवलपर कार्यक्रम की नीतियों](#) और [डेवलपर वितरण अनुबंध](#) का भी पालन करना होगा।

## Play Console से जुड़ी ज़रूरी शर्तें

### [टारगेट ऑडियंस और कॉन्टेंट](#)

ऐप्लिकेशन प्रकाशित करने से पहले, आपको Google Play Console के [टारगेट ऑडियंस और कॉन्टेंट](#) सेक्शन में जाकर उम्र समूहों की सूची में से अपनी टारगेट ऑडियंस को चुनना होगा। भले ही, आपने Google Play Console में किसी भी उम्र समूह को टारगेट ऑडियंस के तौर पर चुना हो, लेकिन अगर आप अपने ऐप्लिकेशन में ऐसी तस्वीरों और शब्दों को शामिल करते हैं जिन्हें बच्चों को टारगेट करने वाला माना जा सकता है, तो इसका असर आपकी दी गई जानकारी के आकलन पर दिख सकता है। यह आकलन Google Play करता है, ताकि पक्का हो सके कि टारगेट ऑडियंस के बारे में आपने जो जानकारी दी है वह सही है या नहीं। Google Play को यह अधिकार है कि वह ऐप्लिकेशन के बारे में आपकी दी गई जानकारी की समीक्षा कर सके। समीक्षा के बाद यह तय किया जाता है कि अपनी टारगेट ऑडियंस के बारे में आपने जो जानकारी दी है वह सही है या नहीं।

अगर आप ऐसी टारगेट ऑडियंस चुनते हैं जिनमें सिर्फ वयस्क शामिल हैं, लेकिन Google को पता चलता है कि यह सही नहीं है, क्योंकि आपका ऐप्लिकेशन बच्चों और वयस्कों दोनों को टारगेट कर रहा है। ऐसे में आपके पास यह बताने का विकल्प होगा कि आपका ऐप्लिकेशन बच्चों को टारगेट नहीं करता है। इसके लिए आपको एक चेतावनी लेबल लगाने की सहमति देनी होगी।

आपको अपने ऐप्लिकेशन की टारगेट ऑडियंस के लिए एक से ज़्यादा उम्र समूह तभी चुनने चाहिए, जब आपने ऐप्लिकेशन को उन चुने हुए उम्र समूह के लोगों को ध्यान में रखकर बनाया हो। साथ ही, आप पक्के तौर पर यह जानते हों कि आपका ऐप्लिकेशन उनके लिए पूरी तरह सही है। उदाहरण के लिए, अगर आपका ऐप्लिकेशन शिशुओं, छोटे बच्चों, और प्री-स्कूल में पढ़ने वाले बच्चों के लिए है, तो उम्र समूह को टारगेट करते समय "पांच साल और उससे कम" उम्र का समूह ही चुनना चाहिए। अगर आपका ऐप्लिकेशन स्कूल के किसी खास लेवल के लिए बनाया गया है, तो वह उम्र समूह चुनें जो उस स्कूल लेवल के लिए सबसे सही हो। आपको वयस्कों और बच्चों, दोनों को शामिल करने वाला उम्र समूह तभी चुनना चाहिए, जब वाकई आपका ऐप्लिकेशन सभी उम्र के लोगों के लिए हो।

### [टारगेट ऑडियंस और कॉन्टेंट सेक्शन के अपडेट](#)

आप जब चाहें, Google Play Console के टारगेट ऑडियंस और कॉन्टेंट सेक्शन में जाकर, अपने ऐप्लिकेशन की जानकारी को अपडेट कर सकते हैं। 'Google Play स्टोर' पर यह जानकारी दिखाने से पहले [ऐप्लिकेशन अपडेट](#) करना ज़रूरी है। हालांकि, आप Google Play Console के इस सेक्शन में जो भी बदलाव करेंगे उनकी समीक्षा ऐप्लिकेशन अपडेट सबमिट किए जाने से पहले भी यह देखने के लिए की जा सकती है कि वे नीति का पालन करते हैं या नहीं।

हमारा सुझाव है कि अगर आप अपने ऐप्लिकेशन के टारगेट उम्र समूह में बदलाव करते हैं या फिर इन-ऐप्लिकेशन खरीदारी या विज्ञापनों की शुरुआत करते हैं, तो अपने मौजूदा दर्शकों को इसकी जानकारी दें। ऐसा करने के लिए, आप ऐप्लिकेशन के स्टोर पेज के "नया क्या है" सेक्शन का या फिर इन-ऐप्लिकेशन सूचनाओं का इस्तेमाल कर सकते हैं।

**Play Console** में गलत तरीके से पेश करना

'टारगेट ऑडियंस और कॉन्टेंट' सेक्शन के साथ ही, Play Console में आपके ऐप्लिकेशन के बारे में किसी जानकारी को गलत तरीके से पेश करने की वजह से आपका खाता हटाया या निलंबित किया जा सकता है। इसलिए, सही जानकारी देना ज़रूरी है।

## परिवार नीति से जुड़ी ज़रूरी शर्तें

अगर आपके ऐप्लिकेशन के टारगेट ऑडियंस में बच्चे भी शामिल हैं, तो आपको आगे दी गई ज़रूरतों का पालन करना चाहिए। इन शर्तों को पूरा नहीं करने पर ऐप्लिकेशन को हटाया या निलंबित किया जा सकता है।

- ऐप्लिकेशन का कॉन्टेंट: आपके ऐप्लिकेशन का ऐसा कॉन्टेंट जिसे बच्चे एक्सेस कर सकते हैं, उसे बच्चों के लिए सही होना चाहिए।
- Google Play Console में सवालियों के जवाब: आपको Google Play Console में अपने ऐप्लिकेशन से जुड़े सवालों के सही जवाब देने चाहिए। साथ ही, अपने ऐप्लिकेशन में कोई भी बदलाव होने पर उन जवाबों को अपडेट करना चाहिए।
- विज्ञापन: अगर आपका ऐप्लिकेशन बच्चों को या ऐसे लोगों को विज्ञापन दिखाता है जिनकी उम्र के बारे में पता नहीं है, तो आप:
  - ऐसे लोगों को विज्ञापन दिखाने के लिए, सिर्फ [Google Play से प्रमाणित किए गए विज्ञापन SDK टूल](#) का इस्तेमाल करें;
  - यह पक्का करें कि उन लोगों को दिखाए गए विज्ञापनों में, पसंद के हिसाब से विज्ञापन (ऑनलाइन ब्राउज़िंग व्यवहार के हिसाब से अलग-अलग लोगों को टारगेट करके दिखाए जाने वाले विज्ञापन) या रीमार्केटिंग (किसी ऐप्लिकेशन या वेबसाइट के साथ पिछले इंटरैक्शन के आधार पर अलग-अलग लोगों को टारगेट करने वाले विज्ञापन) शामिल नहीं हो;
  - यह पक्का करें कि उन लोगों को दिखाए गए विज्ञापनों का कॉन्टेंट बच्चों के लिए सही हो;
  - यह पक्का करें कि उन लोगों को दिखाए गए विज्ञापनों में ऐसा कॉन्टेंट है जो परिवार के लिए बनाए गए विज्ञापन फ़ॉर्मेट की शर्तें पूरी करता है; और
  - यह भी पक्का करें कि बच्चों को विज्ञापन दिखाने से जुड़े सभी कानूनी नियमों और उद्योग मानकों का पालन हो।
- डेटा इकट्ठा करना: आपको अपने ऐप्लिकेशन में, बच्चों से मिली किसी भी तरह की [निजी और संवेदनशील जानकारी](#) को इकट्ठा करने के बारे में बताना चाहिए। इसमें, आपके ऐप्लिकेशन में इस्तेमाल किए गए एपीआई और SDK टूल की मदद से ली जाने वाली जानकारी भी शामिल है। बच्चों से मिली संवेदनशील जानकारी में, माइक्रोफ़ोन और कैमरा सेंसर का डेटा, पहचान की पुष्टि करने की जानकारी, डिवाइस का डेटा, Android आईडी, विज्ञापन देखने का डेटा, और विज्ञापन आईडी की जानकारी के अलावा, और भी चीज़ें शामिल हैं।
- एपीआई और SDK टूल: आपको यह पक्का करना होगा कि आपका ऐप्लिकेशन हर एपीआई और SDK टूल को सही तरीके से लागू करे।
  - सिर्फ बच्चों को टारगेट करने वाले ऐप्लिकेशन में ऐसा एपीआई या SDK टूल नहीं होना चाहिए जिसे बच्चों से जुड़ी सेवाओं में इस्तेमाल करने की मंजूरी न मिली हो। इसमें, Google साइन-इन (या किसी Google खाते से जुड़ी डेटा एक्सेस करने वाली कोई भी अन्य Google API सेवा), Google Play गेम सेवाएं, और पुष्टि करने और अनुमति देने के लिए OAuth टेक्नोलॉजी का इस्तेमाल करने वाली कोई भी दूसरी एपीआई सेवा शामिल है।
  - जो ऐप्लिकेशन बच्चों और बड़ों, दोनों को टारगेट करते हैं उन्हें ऐसे एपीआई या SDK टूल इस्तेमाल नहीं करने चाहिए जिन्हें बच्चों के लिए बनी सेवाओं में इस्तेमाल करने की मंजूरी नहीं मिली है। इन टूल को [न्यूट्रल एज स्क्रीन](#) के साथ ही इस्तेमाल किया जा सकता है। इसके अलावा, अगर इन टूल का इस्तेमाल इस तरीके से किया जा रहा हो कि इनसे बच्चों से मिला डेटा इकट्ठा न हो, तो भी इन्हें इस्तेमाल किया जा सकता है। उदाहरण के लिए, Google साइन-इन की सुविधा को विकल्प के तौर पर देना। जिन ऐप्लिकेशन का टारगेट बच्चे और बड़े, दोनों तरह के दर्शक हैं उन्हें ऐसे एपीआई या SDK टूल से लोगों को साइन इन या कॉन्टेंट एक्सेस करने के लिए नहीं कहना चाहिए जिन्हें बच्चों के लिए बनी सेवाओं में इस्तेमाल की मंजूरी नहीं मिली है।
- निजता नीति: आपको अपने ऐप्लिकेशन के स्टोर पेज पर, ऐप्लिकेशन की निजता नीति के बारे में बताने वाला लिंक देना चाहिए। जब तक ऐप्लिकेशन 'स्टोर' में मौजूद हो, तब तक यह लिंक हमेशा रहना चाहिए। साथ ही, इसे किसी ऐसी निजता नीति से जोड़ा जाना चाहिए जो आपके ऐप्लिकेशन के डेटा संग्रह करने और उसके इस्तेमाल के साथ दूसरी चीज़ों की सही जानकारी देती हो।
- खास पाबंदियां:
  - अगर आपके ऐप्लिकेशन में ऑगमेंटेड रिएलिटी (एआर) का इस्तेमाल किया जाता है, तो आपको एआर सेक्शन लॉन्च होते ही एक सुरक्षा चेतावनी शामिल करनी होगी। चेतावनी में नीचे दी गई जानकारी शामिल होनी चाहिए:
    - माता-पिता के निरीक्षण की अहमियत के बारे में सही मैसेज।
    - असली दुनिया के असली खतरों से सजग रहने का रिमाइंडर (उदाहरण के लिए, अपने आस-पास होने वाली चीज़ों के बारे में सजग रहना)।
  - आपके ऐप्लिकेशन को ऐसे डिवाइस के इस्तेमाल करने की ज़रूरत नहीं पड़नी चाहिए जिसके लिए यह सलाह दी गई हो कि बच्चे इसका इस्तेमाल न करें। (उदाहरण के लिए, Daydream, Oculus)
- कानून का पालन: आपको यह पक्का करना होगा कि आपका ऐप्लिकेशन और इसमें इस्तेमाल होने वाले सभी एपीआई या SDK टूल, [अमेरिका में लागू बच्चों की ऑनलाइन निजता और संरक्षण नियम \(कोपा\)](#), [ईयू \(यूरोपीय संघ\) में लागू सामान्य डेटा से जुड़े सुरक्षा कानून \(जीडीपीआर\)](#) के

साथ-साथ, अन्य लागू कानून या नियम का पालन करते हों।

यहां आम तौर पर होने वाले उल्लंघनों के कुछ उदाहरण दिए गए हैं:

- ऐसे ऐप्लिकेशन जो अपने स्टोर पेज में बच्चों के लिए खेल का प्रचार करते हैं, लेकिन ऐप्लिकेशन का कॉन्टेंट सिर्फ वयस्कों के लिए सही होता है।
- ऐसे ऐप्लिकेशन जो एपीआई को सेवा की ऐसी शर्तों के साथ लागू करते हैं जो बच्चों के लिए बने ऐप्लिकेशन में इनके इस्तेमाल पर पाबंदी लगाती हैं।
- ऐसे ऐप्लिकेशन जिनमें शराब, तंबाकू के बारे में बढ़ा-चढ़ाकर बताया जाता है या ऐसे केमिकल या दवाइयों का बखाना किया जाता है जो आपके शरीर को नुकसान पहुंचा सकती हैं और जिन पर सरकार का कंट्रोल होता है।
- ऐसे ऐप्लिकेशन जिनमें असली या नकली जुआ शामिल होता है।
- ऐसे ऐप्लिकेशन जिनमें हिंसा, खून खराबे या चौंकाने वाला ऐसा कॉन्टेंट शामिल है जो बच्चों के लिए सही नहीं है।
- डेटिंग सेवाएं देने वाले या ऐसे ऐप्लिकेशन जो सेक्शुअल या शादीशुदा ज़िंदगी से जुड़ी सलाह देते हैं।
- ऐसे ऐप्लिकेशन जिनमें उन वेबसाइटों के लिंक होते हैं जो Google Play की [डेवलपर कार्यक्रम नीतियों](#) का उल्लंघन करने वाले कॉन्टेंट को पेश करते हैं।
- ऐसे ऐप्लिकेशन जो बच्चों को बड़ों के लिए बनाए गए विज्ञापन दिखाते हैं। जैसे: हिंसक कॉन्टेंट, सेक्शुअल कॉन्टेंट, जुआ खेलने से जुड़ा कॉन्टेंट। बच्चों के लिए विज्ञापन, इन-ऐप्लिकेशन खरीदारी, और व्यावसायिक कॉन्टेंट पर Google Play की नीतियों के बारे में ज़्यादा जानकारी के लिए कृपया [परिवार के लिए विज्ञापन और कमाई करने की नीतियां](#) देखें।

## परिवार के लिए बनाए गए कार्यक्रम

खास तौर पर, बच्चों के लिए बनाए गए ऐप्लिकेशन को 'परिवार के लिए बनाए गए' कार्यक्रम में हिस्सा लेना चाहिए। अगर आपका ऐप्लिकेशन बच्चों और परिवारों के साथ ही, सभी उम्र के लिए बनाया गया है, तो आप भी इस कार्यक्रम में हिस्सा लेने के लिए आवेदन कर सकते हैं।

कार्यक्रम में शामिल होने के लिए स्वीकार किए जाने से पहले, आपके ऐप्लिकेशन को [Google Play डेवलपर कार्यक्रम की नीतियों](#) और [डेवलपर डिस्ट्रिब्यूशन एग्रीमेंट](#) की शर्तों को पूरा करना होगा। साथ ही, परिवार नीति और परिवार के लिए बनाए गए कार्यक्रम की सभी ज़रूरी शर्तों को भी पूरा करना होगा।

इस कार्यक्रम में अपने ऐप्लिकेशन को शामिल कराने की प्रोसेस के बारे में ज़्यादा जानने के लिए, [यहां](#) क्लिक करें।

कार्यक्रम की ज़रूरी शर्तें

परिवार के लिए बनाए गए कार्यक्रम में हिस्सा लेने वाले सभी ऐप्लिकेशन का और उनमें शामिल विज्ञापन का कॉन्टेंट ऐसा होना चाहिए जो बच्चों के लिए सही और उनके काम का हो। साथ ही, इन ऐप्लिकेशन को नीचे दी गई सभी ज़रूरी शर्तें भी पूरी करनी होंगी। 'परिवार के लिए बनाए गए' कार्यक्रम में स्वीकार किए गए ऐप्लिकेशन को कार्यक्रम की सभी ज़रूरी शर्तों का पालन करना होगा। Google Play किसी भी ऐप्लिकेशन को 'परिवार के लिए बनाए गए' कार्यक्रम के लिए गलत पाए जाने पर, उसे खारिज कर सकता है, हटा सकता है या निलंबित कर सकता है।

परिवार के लिए बनाए गए कार्यक्रम की ज़रूरी शर्तें

1. ऐप्लिकेशन को ईएसआरबी (एंटरटेनमेंट सॉफ़्टवेयर रेटिंग बोर्ड) से 'सभी' या 'सभी 10+' या इसके बराबर रेटिंग मिलनी चाहिए।
2. आपको Google Play Console की कॉन्टेंट रेटिंग वाली सवालियों की सूची में, इस बात की सही जानकारी देनी चाहिए कि ऐप्लिकेशन के कॉन्टेंट और उसे इस्तेमाल करने वाले लोगों की एक-दूसरे तक किस तरह पहुंच है। इसमें यह जानकारी भी शामिल है कि क्या:
  - ऐप्लिकेशन इस्तेमाल करने वाले लोग जानकारी एक्सेस कर सकते हैं या उसे शेयर कर सकते हैं;
  - आपका ऐप्लिकेशन उपयोगकर्ताओं की जानकारी तीसरे पक्षों के साथ शेयर करता है; और
  - आपका ऐप्लिकेशन उपयोगकर्ता की मौजूदा जगह की जानकारी अन्य उपयोगकर्ताओं के साथ शेयर करता है।
3. अगर आपका ऐप्लिकेशन [Android Speech API](#) का इस्तेमाल करता है, तो उसके `RecognizerIntent.EXTRA_CALLING_PACKAGE` को `PackageName` पर सेट किया जाना चाहिए।
4. ऐप्लिकेशन को सिर्फ [Google Play से प्रमाणित किए गए विज्ञापन SDK टूल](#) का इस्तेमाल करना चाहिए।
5. खास तौर पर, बच्चों के लिए बनाए गए ऐप्लिकेशन, जगह की जानकारी की अनुमतियां नहीं मांग सकते।
6. ब्लूटूथ कनेक्शन का अनुरोध करते समय ऐप्लिकेशन के लिए, [कंपैनियन डिवाइस मैनेजर \(सीडीएम\)](#) का इस्तेमाल करना ज़रूरी है। हालांकि, अगर आपका ऐप्लिकेशन ऐसे डिवाइस ऑपरेटिंग सिस्टम वर्शन को टारगेट करता है जो कंपैनियन डिवाइस मैनेजर (सीडीएम) के साथ काम नहीं करते, तो यह ज़रूरी नहीं है।

यहां कुछ ऐसे सामान्य ऐप्लिकेशन के उदाहरण दिए गए हैं जिन्हें कार्यक्रम में हिस्सा लेने की अनुमति नहीं है:

- ऐसे ऐप्लिकेशन जिन्हें 'ईएसआरबी सभी' रेटिंग दी गई है, लेकिन उनमें जुए के कॉन्टेंट से जुड़े विज्ञापन शामिल हैं
- अभिभावकों या देखभाल करने वालों के लिए बने ऐप्लिकेशन (उदाहरण के लिए, स्तनपान कराने की गतिविधि ट्रैक करने वाला ऐप्लिकेशन, डेवलपर गाइड)
- माता-पिता के लिए गाइड या डिवाइस मैनेज करने वाले ऐसे ऐप्लिकेशन जिनका इस्तेमाल सिर्फ़ माता-पिता या देखभाल करने वाले लोग ही कर सकते हैं
- ऐप्लिकेशन, जो ऐसे ऐप्लिकेशन आइकॉन और लॉन्चर आइकॉन का इस्तेमाल करते हैं जो बच्चों के लिए सही नहीं हैं

## कैटगरी

अगर आपको परिवार के लिए बनाए गए कार्यक्रम में हिस्सा लेने की मंजूरी दी गई है, तो आप खास तौर पर परिवारों के लिए बनी दूसरी कैटगरी चुन सकते हैं जिसमें आपके ऐप्लिकेशन की जानकारी दी जाती है। यहां परिवार के लिए बनाए गए कार्यक्रम में हिस्सा लेने वाले ऐप्लिकेशन के लिए मौजूद कैटगरी दी गई हैं:

ऐक्शन और रोमांच: ऐक्शन वाले ऐप्लिकेशन/गेम जिनमें आसान रेटिंग गेम से लेकर परी कथा के रोमांच तक सब कुछ शामिल है। साथ ही, ऐसे ऐप्लिकेशन और गेम भी हैं जिन्हें रोमांच पैदा करने के मकसद से बनाया गया है।

दिमाग लगाने वाले गेम: ऐसे गेम जिनमें गेम खेलने वाले व्यक्ति को सोचना पड़ता है। इनमें पहेलियां, मिलान करने वाले गेम, सवाल-जवाब, और दूसरे गेम शामिल हैं जो याददाश्त, काबिलीयत या तर्क को चुनौती देते हैं।

क्रिएटिविटी: ऐसे ऐप्लिकेशन और गेम जो क्रिएटिविटी को बढ़ावा देते हैं। इनमें ड्रॉइंग, पेंटिंग, कोर्डिंग, और दूसरे ऐप्लिकेशन और गेम शामिल हैं जिनमें आप चीज़ें बना सकते हैं।

शिक्षा: ऐसे ऐप्लिकेशन और गेम जिन्हें कुछ विशेषज्ञों (उदाहरण के लिए, शिक्षकों, सिखाने में महारत रखने वालों, शोध करने वालों) से मिली जानकारी की मदद से बनाया गया है, ताकि सीखने का बढ़ावा मिल सके। इनमें शैक्षणिक, सामाजिक-भावनात्मक, शारीरिक, और रचनात्मक तरीके से सीखना शामिल है। साथ ही, बुनियादी जीवन कौशल, तर्क के साथ सोचना, और समस्याएं सुलझाने से जुड़ी शिक्षा भी शामिल है।

संगीत और वीडियो: संगीत या वीडियो वाले ऐसे ऐप्लिकेशन और गेम जिनमें इंस्ट्रुमेंट सिम्युलेशन वाले ऐप्लिकेशन से लेकर वीडियो और म्यूज़िकल ऑडियो कॉन्टेंट मुहैया कराने वाले ऐप्लिकेशन तक सब कुछ शामिल है।

किरदार निभाना: ऐसे ऐप्लिकेशन और गेम जिनमें गेम खेलने वाला या ऐप्लिकेशन को इस्तेमाल करने वाला व्यक्ति कोई किरदार निभा सकता है। जैसे: शेफ़, देखभाल करने वाले, राजकुमार/राजकुमारी, फ़ायर फ़ाइटर, पुलिसकर्मी या किसी काल्पनिक किरदार की भूमिका निभाना।

## विज्ञापन और कमाई करना

नीचे दी गई नीतियां किसी भी तरह के विज्ञापन (जिसमें आपके ऐप्लिकेशन और तीसरे पक्षों के लिए विज्ञापन शामिल हैं), इन-ऐप्लिकेशन खरीदारी के ऑफ़र या किसी भी दूसरे व्यावसायिक कॉन्टेंट (जैसे कि पेड प्रॉडक्ट प्लेसमेंट) पर लागू होती हैं, जिन्हें ऐप्लिकेशन इस्तेमाल करने वाले लोगों को मुहैया कराया जाता है। इन लोगों पर 'परिवार नीति' और/या 'परिवार के लिए बनाए गए' कार्यक्रम की ज़रूरी शर्तें लागू होती हैं। इन ऐप्लिकेशन में दिखाए जाने वाले सभी तरह के विज्ञापन, इन-ऐप्लिकेशन खरीदारी के ऑफ़र, और व्यावसायिक कॉन्टेंट को इन पर लागू होने वाले सभी कानूनों और नियमों (इनमें खुद लागू किए गए नियम या उद्योग से जुड़े दिशा-निर्देश शामिल हैं) का पालन करना ज़रूरी है।

Google Play के पास व्यावसायिक फ़ायदे के लिए बहुत ज़्यादा आक्रामक विज्ञापन दिखाने वाले ऐप्लिकेशन को खारिज करने या हटाने का अधिकार होता है।

विज्ञापन फ़ॉर्मेट की ज़रूरी शर्तें

विज्ञापनों और इन-ऐप्लिकेशन खरीदारी के ऑफ़र देने वाले कॉन्टेंट को गुमराह करने वाला नहीं होना चाहिए। साथ ही, उन्हें इस तरह से डिज़ाइन किया जाए कि बच्चे अनजाने में क्लिक न करें। नीचे दी गई चीज़ों पर पाबंदी है:

- परेशान करने वाले विज्ञापन में ऐसे विज्ञापन शामिल हैं जो पूरी स्क्रीन को घेर लेते हैं या सामान्य इस्तेमाल में रुकावट डालते हैं और विज्ञापन हटाने का तरीका भी सही से नहीं बताते हैं। (उदाहरण के लिए, [विज्ञापन वॉल](#))
- ऐसे विज्ञापन जो ऐप्लिकेशन के सामान्य इस्तेमाल या गेम खेलने में रुकावट डालते हैं और इन्हें पांच सेकंड के बाद बंद भी नहीं किया जा सकता। ऐसे विज्ञापन जो ऐप्लिकेशन के सामान्य इस्तेमाल या गेम खेलने में रुकावट नहीं डालते हैं, लेकिन ये पांच सेकंड के बाद भी चलते रहते हैं (जैसे कि विज्ञापन से जुड़ा हुआ वीडियो कॉन्टेंट)।

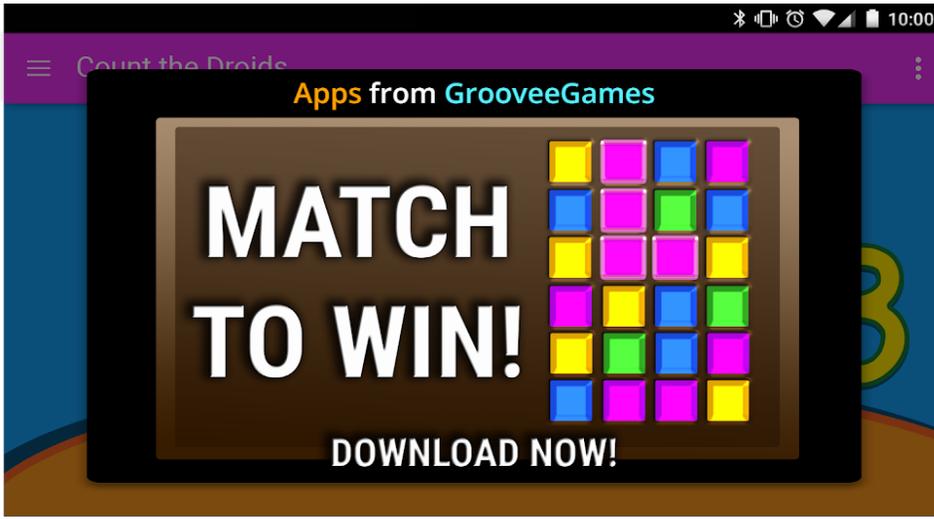
- पेज पर अचानक दिखने वाले विज्ञापन या इन-ऐप्लिकेशन खरीदारी के ऐसे ऑफ़र जो ऐप्लिकेशन लॉन्च होते ही दिखते हैं
- पेज पर एक से ज़्यादा विज्ञापन प्लेसमेंट (उदाहरण के लिए, ऐसे बैनर विज्ञापन जो एक प्लेसमेंट में एक से ज़्यादा ऑफ़र दिखाते हैं या एक से ज़्यादा बैनर या वीडियो विज्ञापन दिखाते हैं, जिसकी अनुमति नहीं है).
- ऐसे विज्ञापन या इन-ऐप्लिकेशन खरीदारी के ऑफ़र जिनकी आपके ऐप्लिकेशन के कॉन्टेंट से साफ़ तौर पर अलग पहचान नहीं की जा सकती
- विज्ञापन के दर्शकों की संख्या बढ़ाने या इन-ऐप्लिकेशन खरीदारी को बढ़ाने के लिए, भावनात्मक रूप से गुमराह करने या चौंकाने वाले तरीकों का इस्तेमाल करना
- इन-ऐप्लिकेशन खरीदारी करने के लिए, वर्चुअल गेम के सिक्कों और असली पैसों के बीच फ़र्क न दिखाना

यहां विज्ञापन फ़ॉर्मेट के आम तौर पर होने वाले उल्लंघनों के कुछ उदाहरण दिए गए हैं

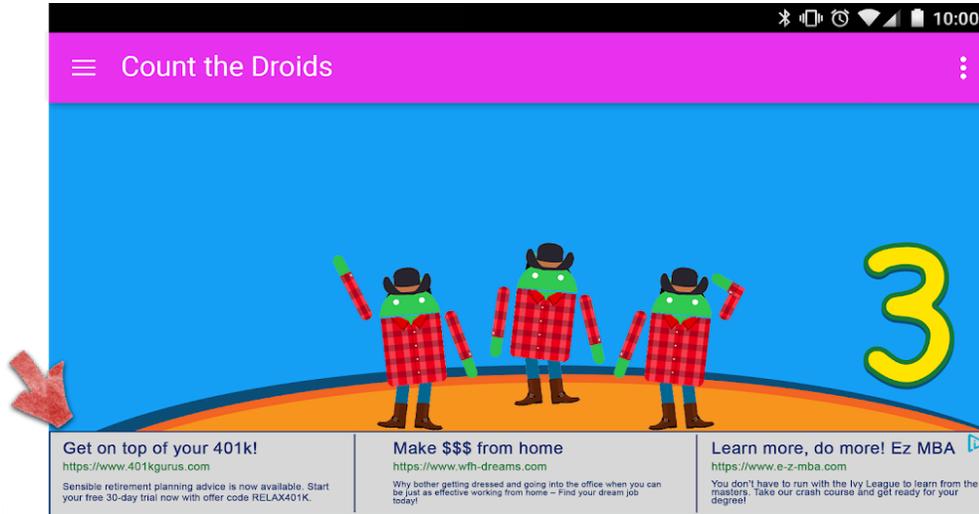
- ऐसे विज्ञापन जो ऐप्लिकेशन इस्तेमाल करने वाले व्यक्ति की पहुंच से तब दूर हो जाते हैं, जब वह उन्हें बंद करने की कोशिश करता है
- ऐसे विज्ञापन जिनके शुरू होने के पांच (5) सेकंड बाद भी, ऐप्लिकेशन इस्तेमाल करने वाले व्यक्ति को विज्ञापन हटाने का तरीका नहीं बताया जाता, जैसा कि नीचे दिए गए उदाहरण में दिखाया गया है:



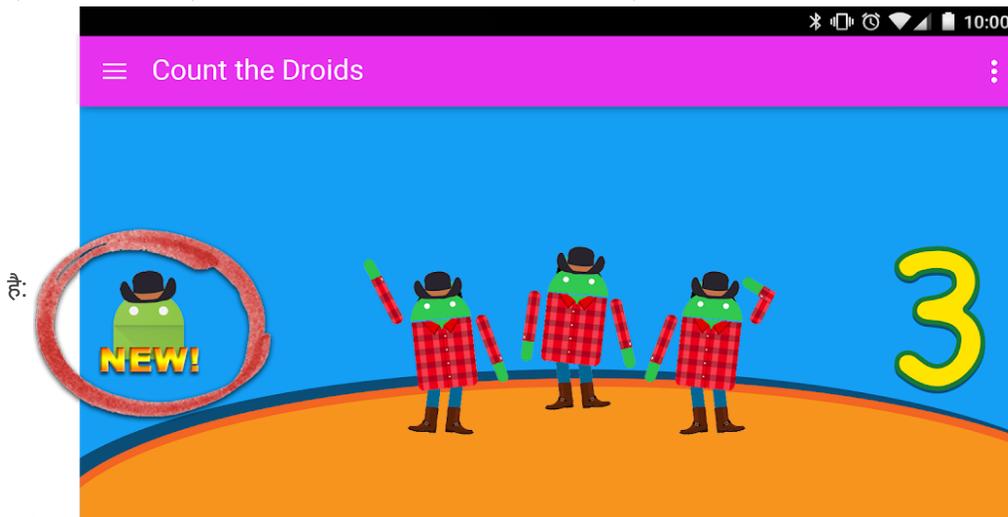
- ऐसे विज्ञापन जो ऐप्लिकेशन इस्तेमाल करने वाले व्यक्ति को विज्ञापन हटाने का तरीका साफ़ तौर पर बताए बिना, डिवाइस की पूरी स्क्रीन या उसके ज़्यादातर हिस्से पर दिखने लगते हैं, जैसा कि नीचे दिए गए उदाहरण में दिखाया गया है:



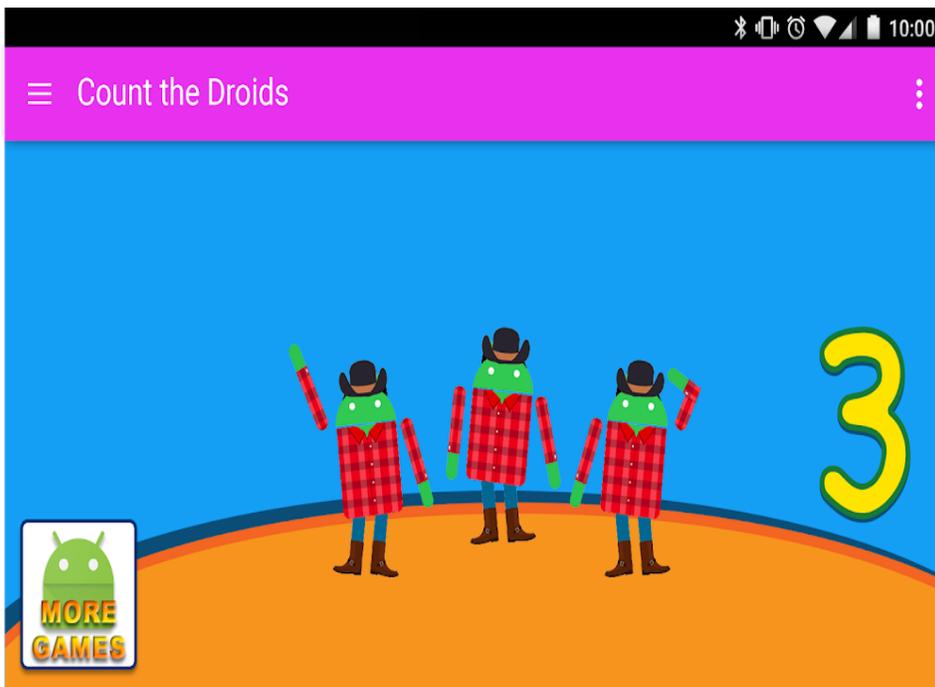
- एक से ज़्यादा ऑफ़र दिखाने वाले बैनर विज्ञापन. इनका उदाहरण नीचे दिखाया गया है:



- ऐसे विज्ञापन जिन्हें ऐप्लिकेशन इस्तेमाल करने वाला व्यक्ति गलती से ऐप्लिकेशन का कॉन्टेंट समझ सकता है. इनका उदाहरण नीचे दिखाया गया



- ऐसे बटन या विज्ञापन जो आपके 'Google Play स्टोर' के अन्य पेज का प्रचार करते हैं, लेकिन जिन्हें ऐप्लिकेशन के कॉन्टेंट से अलग नहीं पहचाना जा सकता है. इनका उदाहरण नीचे दिखाया गया है:



यहां ऐसे गलत विज्ञापन कॉन्टेंट के कुछ उदाहरण दिए गए हैं जो बच्चों को नहीं दिखाना चाहिए।

- आपत्तिजनक मीडिया कॉन्टेंट: टीवी शो, फ़िल्में, म्यूजिक एल्बम या किसी भी अन्य तरह के मीडिया आउटलेट के विज्ञापन जो बच्चों के लिए ठीक नहीं हैं।
- आपत्तिजनक वीडियो गेम और डाउनलोड करने लायक सॉफ़्टवेयर: डाउनलोड करने लायक सॉफ़्टवेयर और इलेक्ट्रॉनिक वीडियो गेम के विज्ञापन जो बच्चों के लिए सही नहीं हैं।
- पाबंदी वाली नशीली दवाएं या नुकसान पहुंचाने वाली चीज़ें: शराब, तंबाकू, पाबंदी वाली नशीली दवाएं या नुकसान पहुंचाने वाली किसी और चीज़ के विज्ञापन।
- जुआ: असली में जुआ खेलने जैसा अनुभव देने वाले विज्ञापन, प्रतियोगिता या लॉटरी के प्रचार, भले ही उसमें शामिल होने के लिए कोई शुल्क न मांगा जाए।
- वयस्क और अश्लील रूप से सेक्शुअल ऐक्ट दिखाने वाला कॉन्टेंट: ऐसे विज्ञापन जिनमें यौन, अश्लील रूप से सेक्शुअल ऐक्ट दिखाने वाला, और मैच्योर कॉन्टेंट हो।
- डेटिंग या संबंध: डेटिंग या वयस्क संबंध वाली साइटों के लिए बने विज्ञापन
- हिंसा से जुड़ा कॉन्टेंट: ऐसे विज्ञापन जिनमें हिंसा से जुड़ा और दिल दहलाने वाला ऐसा कॉन्टेंट हो जो बच्चों के लिए सही न हो।

### विज्ञापन SDK टूल

अगर आप अपने ऐप्लिकेशन में विज्ञापन दिखाते हैं और आपकी टारगेट ऑडियंस में सिर्फ़ बच्चे शामिल हैं, तो आपको [Google Play से प्रमाणित विज्ञापन SDK टूल](#) का इस्तेमाल करना होगा। अगर आपके ऐप्लिकेशन की टारगेट ऑडियंस बच्चे और वयस्क दोनों हैं, तो आपको स्क्रीन से जुड़े हुए मानकों का पालन करना चाहिए, जैसे कि [न्यूट्रल एज स्क्रीन](#)। साथ ही, यह पक्का करना चाहिए कि बच्चों को दिखाए जाने वाले विज्ञापनों में Google Play के प्रमाणित विज्ञापन SDK टूल का इस्तेमाल हो। 'परिवार के लिए बनाए गए' कार्यक्रम में मौजूद ऐप्लिकेशन के लिए ज़रूरी है कि वे सिर्फ़ खुद प्रमाणित किए हुए विज्ञापन SDK टूल का इस्तेमाल करें।

ज़रूरी शर्तों के बारे में जानने और मंजूरी पा चुके SDK टूल की मौजूदा सूची देखने के लिए, कृपया [परिवार के लिए विज्ञापन कार्यक्रम की नीति](#) देखें।

अगर आप AdMob का इस्तेमाल करते हैं, तो उनके प्रॉडक्ट के बारे में ज़्यादा जानकारी के लिए [AdMob सहायता केंद्र](#) देखें।

यह पक्का करना आपकी ज़िम्मेदारी है कि आपका ऐप्लिकेशन विज्ञापनों, इन-ऐप्लिकेशन खरीदारी, और व्यावसायिक कॉन्टेंट से जुड़ी सभी ज़रूरी शर्तों को पूरा करता हो। विज्ञापन SDK टूल देने वाले (वालों) की कॉन्टेंट नीतियों और विज्ञापन देने के तौर-तरीकों के बारे में ज़्यादा जानने के लिए, उनसे संपर्क करें।

Google Play 'परिवार के लिए बनाए गए' कार्यक्रम में हिस्सा लेने वाले ऐप्लिकेशन में इन-ऐप्लिकेशन खरीदारी के लिए फिर से मंजूरी देगा. इस तरीके से यह पक्का करने में मदद मिलती है कि वित्तीय रूप से ज़िम्मेदार पक्ष ही खरीदारी को मंजूरी दे रहे हैं, न कि बच्चे.

## नीति उल्लंघन ठीक करने के तरीके

नीति उल्लंघन को मैनेज करने के बजाय, उससे बचना हमेशा बेहतर होता है. हालांकि, नीति का उल्लंघन होने पर, यह हमारी ज़िम्मेदारी होती है कि हम डेवलपर को यह बताएं कि वे अपने ऐप्लिकेशन को नीतियों के हिसाब से कैसे बना सकते हैं. अगर आपको [कोई उल्लंघन दिखता है](#) या [उल्लंघन को मैनेज करने](#) के बारे में आपके सवाल हैं, तो कृपया हमें बताएं.

## नीति का कवरेज

आपके ऐप्लिकेशन में जो भी कॉन्टेंट दिखाया जाता है या जिससे वह जुड़ा हुआ है उस पर Google Play की नीतियां लागू होती हैं. इसमें, ऐप्लिकेशन इस्तेमाल करने वाले लोगों को दिखाए जाने वाले विज्ञापन शामिल हैं. साथ ही, किसी भी तरह का यूजर जनरेटेड कॉन्टेंट जिसे ऐप्लिकेशन होस्ट करता है या जिससे यह जुड़ा हुआ है उस पर भी ये नीतियां लागू होती हैं. इसके अलावा, ये नीतियां आपके डेवलपर खाते के ऐसे किसी भी कॉन्टेंट पर लागू होती हैं जो Google Play में सार्वजनिक रूप से दिखता है. इसमें डेवलपर का नाम और सूची में शामिल आपकी डेवलपर वेबसाइट का लैंडिंग पेज भी शामिल है.

हम ऐसे किसी ऐप्लिकेशन को मंजूरी नहीं देते हैं जो उपयोगकर्ताओं को उनके डिवाइस पर दूसरे ऐप्लिकेशन इंस्टॉल करने की अनुमति देते हैं. कुछ ऐप्लिकेशन लोगों को दूसरे ऐप्लिकेशन, गेम या सॉफ्टवेयर का ऐक्सेस उन्हें इंस्टॉल किए बिना ही दे देते हैं और साथ ही, तीसरे पक्ष की दी हुई सुविधाएं और उनसे जुड़े अनुभव भी देते हैं. ऐसे ऐप्लिकेशन के लिए यह पक्का करना ज़रूरी है कि वे जिस कॉन्टेंट का ऐक्सेस देते हैं वह [Google Play की नीतियों](#) के मुताबिक हो. साथ ही, उस पर नीति की अन्य समीक्षाएं भी लागू हो सकती हैं.

इन नीतियों में बताई गई शर्तों का वही मतलब है जैसा [डेवलपर वितरण अनुबंध \(DDA\)](#) में बताया गया है. इन नीतियों और DDA का पालन करने के अलावा, ज़रूरी है कि आपके ऐप्लिकेशन का कॉन्टेंट हमारे [कॉन्टेंट रेटिंग से जुड़े दिशा-निर्देश](#) के मुताबिक रेट किया जाए.

हम ऐसे ऐप्लिकेशन या ऐप्लिकेशन के कॉन्टेंट को अनुमति नहीं देते जो Google Play नेटवर्क में उपयोगकर्ता के भरोसे को कम करता है. Google Play में किसी ऐप्लिकेशन को शामिल करना या हटाना, कुछ बातों के मुताबिक तय किया जाता है. इनमें नुकसान पहुंचाने वाले या बुरे बर्ताव और यौन शोषण के अलावा, और भी चीज़ें शामिल हो सकती हैं. हम ऐप्लिकेशन और डेवलपर के हिसाब से शिकायतें, समाचार रिपोर्टिंग, पहले हुए उल्लंघनों की जानकारी, और ऐप्लिकेशन इस्तेमाल करने वाले लोगों की शिकायतों, सुझाव या राय की मदद से बुरा बर्ताव होने के खतरे की पहचान करते हैं. साथ ही, इसके लिए हम लोकप्रिय ब्रैंड, उससे जुड़े लोगों की जानकारी, और अन्य एसेट जैसी चीज़ों का इस्तेमाल भी करते हैं. इनमें इनके अलावा, और भी चीज़ें शामिल हो सकती हैं.

## Google Play Protect के काम करने का तरीका

जब आप ऐप्लिकेशन को इंस्टॉल करते हैं, तब Google Play Protect उनकी जांच करता है. यह समय-समय पर आपका डिवाइस भी स्कैन करता है. नुकसान पहुंचा सकने वाला कोई ऐप्लिकेशन मिलने पर, यह ये काम कर सकता है:

- आपको सूचना भेज सकता है. ऐप्लिकेशन हटाने के लिए सूचना और उसके बाद 'अनइंस्टॉल करें' पर टैप करें.
- ऐप्लिकेशन को तब तक के लिए बंद कर सकता है, जब तक कि आप इसे अनइंस्टॉल नहीं कर देते.
- ऐप्लिकेशन को अपने-आप हटा सकता है. ज़्यादातर मामलों में, अगर किसी नुकसान पहुंचाने वाले ऐप्लिकेशन के होने का पता चलता है, तो आपको सूचना मिलेगी कि ऐप्लिकेशन को हटा दिया गया है.

## मैलवेयर सुरक्षा कैसे काम करती है

आपके डिवाइस को नुकसान पहुंचाने वाले तीसरे पक्ष के सॉफ्टवेयर, यूआरएल, और सुरक्षा से जुड़ी दूसरी समस्याओं से बचाव करने के लिए Google को यह जानकारी मिल सकती है:

- आपके डिवाइस के नेटवर्क कनेक्शन की जानकारी
- ऐसे यूआरएल की जानकारी जो आपके डिवाइस को नुकसान पहुंचा सकते हैं
- आपके डिवाइस पर Google Play या दूसरे स्रोतों से इंस्टॉल किए गए ऐप्लिकेशन और ऑपरेटिंग सिस्टम.

आपको Google से, किसी ऐसे ऐप्लिकेशन या यूआरएल के बारे में चेतावनी मिल सकती है जो शायद सुरक्षित न हो. अगर Google को लगता है कि डिवाइस, डेटा या लोगों के लिए ऐप्लिकेशन या यूआरएल सुरक्षित नहीं है, तो वह उसे हटा सकता है या इंस्टॉल होने से रोक सकता है.

आप अपने डिवाइस की सेटिंग में जाकर इन सुरक्षाओं में से कुछ को बंद करना चुन सकते हैं. हालांकि, Google को Google Play से इंस्टॉल किए गए ऐप्लिकेशन के बारे में जानकारी मिलनी जारी रह सकती है. साथ ही, आपके डिवाइस पर दूसरे स्रोतों से इंस्टॉल किए गए ऐप्लिकेशन की सुरक्षा समस्याओं के लिए जांच करना जारी रह सकता है. इसकी जानकारी Google को नहीं भेजी जाएगी.

निजता से जुड़ी चेतावनियां आपको कैसे मिलती हैं

अगर 'Google Play स्टोर' से किसी ऐप्लिकेशन को हटाया जाता है, तो Google Play Protect आपको इस बारे में चेतावनी भेजेगा. ऐसा इसलिए किया जाता है, क्योंकि ऐप्लिकेशन आपकी निजी जानकारी एक्सेस करने की कोशिश कर सकता है और चेतावनी मिलने पर आप ऐप्लिकेशन को अनइंस्टॉल कर सकते हैं.

## नीति उल्लंघन ठीक करने की प्रोसेस

अगर आपका ऐप्लिकेशन हमारी किसी नीति का उल्लंघन करता है, तो हम सही कार्रवाई करेंगे, जैसा कि नीचे बताया गया है. इसके अलावा, हम जो कार्रवाई करेंगे उसकी जानकारी आपको ईमेल से भेज देंगे. साथ ही, अगर आपको लगता है कि हमने गलत कार्रवाई की है, तो हम अपील करने का तरीका बताएंगे.

कृपया ध्यान दें कि हो सकता है कि निकालने की प्रक्रिया या प्रशासनिक नोटिस, आपके ऐप्लिकेशन या व्यापक ऐप्लिकेशन कैटलॉग के हर नीति उल्लंघन को न दिखाए. डेवलपर किसी भी फ़्लैग की गई नीति के मुद्दे को पता करने और उसे ठीक करने के लिए ज़िम्मेदार हैं और वह यह ध्यान से देख लें कि उनके ऐप्लिकेशन का बाकि बचा हिस्सा पूरी तरह से नीति का पालन करता हो. आपके सभी ऐप्लिकेशन में नीति उल्लंघन को हल न कर पाने पर, नीति उल्लंघन के तरीके ठीक करने के तहत कार्रवाई हो सकती है.

इन नीतियों या [डेवलपर वितरण अनुबंध](#) (DDA) से बार-बार होने वाले या गंभीर उल्लंघनों के नतीजे के बाद व्यक्तिगत या Google Play डेवलपर खाते से मिलते-जुलते खातों को खत्म कर दिया जाएगा. जैसे कि मैलवेयर, धोखाधड़ी, और उपयोगकर्ता या डिवाइस को नुकसान पहुंचाने वाले ऐप्लिकेशन.

## नीति उल्लंघन ठीक करने के लिए कार्रवाईयां

नीति उल्लंघन ठीक करने की अलग-अलग कार्रवाईयां, आपके ऐप्लिकेशन पर अलग-अलग असर डाल सकती हैं. नीचे दिए गए सेक्शन में उन कार्रवाईयां की जानकारी दी गई है जो Google Play कर सकता है. साथ ही, यह जानकारी भी दी गई है कि इन कार्रवाईयां का आपके ऐप्लिकेशन या Google Play डेवलपर खाते पर क्या असर पड़ेगा. [इस वीडियो](#) में पूरी जानकारी दी गई है.

### खारिज करना

- समीक्षा के लिए सबमिट किया गया नया ऐप्लिकेशन या ऐप्लिकेशन अपडेट Google Play पर उपलब्ध नहीं होगा.
- अगर किसी मौजूदा ऐप्लिकेशन के अपडेट को खारिज किया गया था, तो अपडेट से पहले प्रकाशित किया गया वर्शन अब भी Google Play पर मौजूद रहेगा.
- खारिज होने का असर, खारिज हुए ऐप्लिकेशन के मौजूदा स्टोर पेज, उपयोगकर्ता इंस्टॉल, आंकड़े, और रेटिंग देखने की सुविधा पर नहीं पड़ता.
- खारिज होने से आपके Google Play डेवलपर खाते की स्थिति पर असर नहीं होता है.

ध्यान दें: खारिज किए गए ऐप्लिकेशन को तब तक दोबारा सबमिट करने की कोशिश न करें, जब तक आप नीतियों के उल्लंघन को ठीक नहीं कर लेते हैं.

### हटाना

- ऐप्लिकेशन और उसके पहले का कोई भी ऐसा वर्शन जिसे Google Play से हटा दिया गया है, लोगों के डाउनलोड करने के लिए उपलब्ध नहीं होगा.
- ऐप्लिकेशन को हटा दिया गया है. इसलिए, लोग ऐप्लिकेशन के स्टोर पेज, मौजूदा उपयोगकर्ता इंस्टॉल, आंकड़े, और रेटिंग नहीं देख पाएंगे. हटाए गए ऐप्लिकेशन में नीति का पालन करने वाला अपडेट करने पर जानकारी वापस आ जाएगी.

- जब तक Google Play नीति का पालन करने वाले वर्शन को मंजूरी नहीं देता, तब तक लोग इन-ऐप्लिकेशन खरीदारी या इन-ऐप्लिकेशन बिलिंग की सुविधा का फ़ायदा नहीं ले सकते.
- ऐप्लिकेशन को कई बार हटाने से उस पर रोक लगा सकते हैं, लेकिन इसका असर आपके Google Play डेवलपर खाते की स्थिति पर तुरंत नहीं पड़ता.

ध्यान दें: हटाए गए ऐप्लिकेशन को तब तक दोबारा प्रकाशित करने की कोशिश न करें, जब तक आप सभी नीतियों के उल्लंघन को ठीक नहीं कर लेते हैं.

## निलंबन

- ऐप्लिकेशन और उसके पहले का कोई भी ऐसा वर्शन जिसे Google Play से हटा दिया गया है, लोगों के डाउनलोड करने के लिए उपलब्ध नहीं होगा.
- नीति के बहुत खराब या एक से ज़्यादा बार उल्लंघन होने के साथ ही, कई बार खारिज होने या हटाने से ऐप्लिकेशन निलंबित हो सकता है.
- ऐप्लिकेशन को निलंबित कर दिया गया है. इसलिए, लोग ऐप्लिकेशन के स्टोर पेज, मौजूदा उपयोगकर्ता इंस्टॉल, आंकड़े, और रेटिंग नहीं देख पाएंगे. निलंबित ऐप्लिकेशन के लिए नीति का पालन करने वाला अपडेट करने पर जानकारी वापस आ जाएगी.
- अब आप निलंबित ऐप्लिकेशन का APK या ऐप्लिकेशन बंडल का इस्तेमाल नहीं कर सकते.
- जब तक Google Play नीति का पालन करने वाले वर्शन को मंजूरी नहीं देता, तब तक लोग इन-ऐप्लिकेशन खरीदारी या इन-ऐप्लिकेशन बिलिंग की सुविधा का फ़ायदा नहीं ले पाएंगे.
- निलंबन को आपके Google Play डेवलपर खाते की अच्छी स्थिति के खिलाफ़ हमला माना जाता है. एक से ज़्यादा बार निलंबित होने पर आपका Google Play डेवलपर खाता और उससे जुड़े खाते बंद किए जा सकते हैं.

ध्यान दें: किसी निलंबित ऐप्लिकेशन को तब तक दोबारा प्रकाशित करने की कोशिश न करें, जब तक Google Play आपसे ऐसा करने के लिए न कहे.

## ऐप्लिकेशन किसको दिखेगा, यह सीमित करना

- Google Play पर आपके ऐप्लिकेशन को खोजे जाने पर पाबंदी लगा दी गई है. आपका ऐप्लिकेशन Google Play पर उपलब्ध रहेगा और ऐप्लिकेशन के 'Play स्टोर' में दिए सीधे लिंक के साथ लोग इसे एक्सेस कर सकते हैं.
- ऐप्लिकेशन किसको दिखेगा, यह सीमित करने से आपके Google Play डेवलपर खाते की स्थिति पर असर नहीं पड़ता.
- ऐप्लिकेशन किसको दिखेगा, यह सीमित करने से लोगों के ऐप्लिकेशन के मौजूदा स्टोर पेज, उपयोगकर्ता इंस्टॉल, आंकड़े, और रेटिंग देखने की सुविधा पर असर नहीं पड़ता.

## खाता बंद कर देना

- जब आपका डेवलपर खाता बंद कर दिया जाता है, तो आपकी सूची के सभी ऐप्लिकेशन को Google Play से हटा दिया जाएगा और आप नए ऐप्लिकेशन प्रकाशित नहीं कर पाएंगे. इसका मतलब यह भी है कि Google Play डेवलपर से जुड़े हुए सभी खातों को भी हमेशा के लिए निलंबित कर दिया जाएगा.
- अगर आपको नीति का कई बार निलंबन या गंभीर उल्लंघन करने की वजह से निलंबित किया जाता है, तो आपका Play Console खाता बंद किया जा सकता है.
- बंद किए गए खाते को ऐप्लिकेशन से हटा दिया गया है. इसलिए, लोग ऐप्लिकेशन के स्टोर पेज, मौजूदा उपयोगकर्ता इंस्टॉल, आंकड़े, और रेटिंग नहीं देख पाएंगे.

ध्यान दें: आप जिस नए खाते को खोलने की कोशिश करेंगे उसे भी बंद कर दिया जाएगा (डेवलपर रजिस्ट्रेशन शुल्क रिफ़ंड किए बिना). इसलिए, जब आपका कोई दूसरा खाता बंद कर दिया गया हो, तो कृपया किसी नए Play Console खाते के लिए रजिस्टर करने की कोशिश न करें.

## नीति के उल्लंघनों को मैनेज करना और उनकी शिकायत करना

## How to handle a policy violation on Go...



### ऐप्लिकेशन पर नीति उल्लंघन ठीक करने के तरीके की कार्रवाई के खिलाफ़ अपील करना

अगर कोई गड़बड़ी हुई हो और हमें पता चले कि आपका ऐप्लिकेशन Google Play कार्यक्रम नीतियों और डेवलपर वितरण अनुबंध का उल्लंघन नहीं करता है, तो हम ऐप्लिकेशन बहाल करेंगे. अगर आपने नीतियों की ध्यान से समीक्षा की है और आपको लगता है कि हमारे फ़ैसले में गड़बड़ी हुई है, तो कृपया अपील करने के लिए नीति उल्लंघन ठीक करने के तरीके बताने वाले ईमेल में नीचे दिए गए निर्देशों का पालन करें.

### दूसरे संसाधन

अगर आपको किसी उपयोगकर्ता पर लागू कार्रवाई या रेटिंग/टिप्पणी से जुड़ी ज़्यादा जानकारी चाहिए, तो आप नीचे दिए गए कुछ संसाधनों को देख सकते हैं या [Google Play सहायता केंद्र](#) पर हमसे संपर्क कर सकते हैं. हालांकि, हम आपको कानूनी सलाह नहीं दे सकते हैं. अगर आपको कानूनी सलाह चाहिए, तो कृपया कानूनी सलाहकार से संपर्क करें.

- [ऐप्लिकेशन की पुष्टि और अपील करना](#)
- [नीति उल्लंघन की शिकायत करना](#)
- [खाता बंद किए जाने या ऐप्लिकेशन हटाए जाने के बारे में Google Play से संपर्क करना](#)
- [साफ़ तौर पर चेतावनी](#)
- [आपत्तिजनक ऐप्लिकेशन और टिप्पणियों की शिकायत करना](#)
- [मेरा ऐप्लिकेशन Google Play से हटा दिया गया है](#)
- [Google Play डेवलपर खाता बंद होने की वजह समझना](#)

### और मदद चाहिए?

आगे दिए गए कदमों को आजमाएं:

हमसे संपर्क करें

हमें ज़्यादा जानकारी दें और हम आपकी पूरी मदद करेंगे