

開發人員計畫政策

(若無另行公告，即自 2026 年 5 月 27 日起生效)

打造全球最受信賴的應用程式與遊戲來源

因為您的創新精神，促成了今日我們共同獲得的成果；不過，維繫這些成果仍需要您善盡責任。《開發人員計畫政策》和《[開發人員發行協議](#)》可確保我們能持續透過 Google Play，為超過十億名使用者提供全世界最具創意和最值得信賴的應用程式。歡迎在下方瀏覽我們的相關政策。

違規內容

每天都有來自世界各地的使用者透過 Google Play 存取應用程式和遊戲。在提交應用程式前，請先想想您的應用程式是否適合在 Google Play 上架且符合當地法律規範。

危害兒童安全

如果應用程式未禁止使用者建立、上傳或發布會助長剝削或虐待未成年人的內容，Google Play 會立即予以下架。適用範圍包括任何兒少性虐待內容。如要檢舉 Google 產品上含有可能剝削未成年人的內容，請按一下「[檢舉濫用情形](#)」。如果您在其他網站或網頁上發現這類內容，請直接與您[所在國家/地區的有關當局](#) 聯絡。

我們禁止使用應用程式危害未成年人，包括但不限於使用應用程式鼓吹針對未成年人的掠奪性行為，例如：

- 針對未成年人的不當互動 (例如撫摸或愛撫)。
- 兒少性誘拐內容，例如與未成年人線上交友，並在線上或現實生活中達成與該名未成年人從事性接觸行為的目的，以及/或是交換色情圖像。
- 將未成年人性慾化的內容，例如描繪、鼓勵或宣傳兒少性虐待行為的圖像，或是以可能導致兒少性剝削的角度描繪未成年人。
- 性勒索 (例如實際取得或佯稱取得未成年人的私密圖片，並以此威脅或勒索)
- 販運未成年人的內容，例如宣傳或誘使未成年人進行商業性剝削行為。

一旦我們發現兒少性虐待內容，就會採取適當行動，包括通報國際失蹤及被剝削兒童保護中心。如果您認為某名未成年人可能或已經受到虐待、剝削或販運，請聯絡當地執法單位，並聯繫[這裡](#) 所列的兒少安全機構。

此外，我們也禁止兒童導向應用程式中出現成人主題，包括但不限於：

- 應用程式含有大量暴力和血腥畫面。
- 應用程式描繪或鼓勵有害和危險活動。

我們也不允許應用程式宣傳負面的身體意象或自我形象，包括基於娛樂目的描繪整形手術、減重和其他化妝修容行為的應用程式。

兒童安全標準政策

Google Play 要求社群和約會交友應用程式遵守兒童安全標準政策。

這類應用程式須符合下列條件：

- **具有公開標準：**應用程式須在公開標準中明確禁止兒少性虐待及剝削 (CSAE) 行為。公開標準包含應用程式的服務條款、社群規範或任何其他公開的使用者政策文件。
- **應用程式內設有意見回饋機制：**您必須自主認證，使用者可利用應用程式內部機制提出意見、疑慮或檢舉。

- **處理兒少性虐待內容：**您必須自主認證，當您獲知應用程式內存在兒少性虐待內容，就會根據您發布的標準和相關法律採取適當處置，包括但不限於移除該內容。
- **遵守《兒童安全法》：**您必須自主認證，您的應用程式遵守適用兒童安全法律和法規，包括但不限於設有專門流程，可將經過確認的兒少性虐待內容回報給[美國國家失蹤與受虐兒童援助中心](#)，或您[所在地區的相關機構](#)。
- **提供兒童安全聯絡窗口：**您的應用程式須提供指定聯絡窗口，萬一您的應用程式或平台中出現 CSAE 內容，Google Play 就會通知該窗口。這名代表須能協助說明違規處置和審查程序相關事宜，並在需要時採取相應行動。

如要進一步瞭解這些規定和配合方式，請參閱[說明中心文章](#)。

不當內容

為確保使用者在 Google Play 這個平台安全無慮且互相尊重，我們制定了一套標準，說明有害或不當的內容的定義並設下使用禁令。

色情內容和不雅用語

我們禁止應用程式納入或宣傳色情內容或不雅用語，包括情色作品，或者意圖撩撥性慾的任何內容或服務。此外，也禁止疑似鼓吹或招攬性交易的應用程式或應用程式內容。應用程式不得納入或宣傳與性掠奪行為相關的內容，或在未經同意下散布色情內容。就包含裸露的內容而言，如果主要用於教育、紀實、科學或藝術用途，而確實有納入或宣傳的必要，則不在此限。

目錄應用程式 (即本身為內容目錄，書籍/影片作品是其中部分內容的應用程式) 可以發行包含色情內容的書籍 (包括電子書和有聲書) 或影片作品，惟須符合下列條件：

- 包含色情內容的書籍/影片作品只占應用程式整體目錄的一小部分
- 應用程式不會主動宣傳含有色情內容的書籍/影片作品，而這些作品仍能依使用者的閱覽/觀看記錄顯示在推薦專區，或於一般價格促銷活動期間顯示
- 應用程式發行的書籍/影片作品不含危害兒童安全的色情內容，也不含適用法律定義為違法的任何其他色情內容
- 應用程式會保護未成年人，限制他們存取含有色情內容的書籍/影片作品

如果應用程式含有違反本政策的內容，但該內容在特定地區經認定並無不當，應用程式便可提供給當地使用者，不過仍無法提供給其他地區的使用者。

以下是常見的違規情況：

- 描繪色情裸露或性暗示意味濃厚姿勢的內容，其中主體為裸體、經模糊處理或衣著過少，且/或所穿衣物在適當公開場合中並不得體。
- 性愛行為或性暗示意味濃厚姿勢的描繪、動畫或插圖，或是對於身體部位的色情描繪。
- 描繪情趣用品、性愛指南、非法色情主題和戀物癖的內容，或是具有這些功能的內容。
- 猥褻或不雅內容，包括但不限於商店資訊或應用程式中，可能包含不雅用語、詆毀用語、煽情露骨文字或成人/色情關鍵字的內容。
- 描繪、描述或鼓吹人獸交的內容。
- 應用程式宣傳可能被解讀為提供/招攬性交易的性娛樂、伴遊服務或其他服務，包括但不限於援交或性協議，意即其中一方期待或暗示另一方提供金錢、禮物或財務支援 (「包養」)。
- 貶低或物化他人的應用程式 (例如聲稱能夠脫去或透視他人衣物)，即使標示為惡作劇或娛樂性質的應用程式亦屬違規。
- 試圖以情色角度威脅或剝削他人的內容或行為，例如偷拍、隱藏式攝影機、在未經同意下透過深偽或類似技術製作的色情內容，或是侵犯他人的內容。

仇恨言論

我們禁止應用程式針對個人或群體的種族、族裔、宗教、失能情況、年齡、國籍、服役狀態、性傾向、性別、性別認同、種姓、移民狀態或其他與系統性歧視或邊緣化相關的特質，鼓吹暴力行為或煽動仇恨情緒。

如果應用程式包含與納粹相關的 EDSA (教育、紀實、科學或藝術) 內容，在特定國家/地區可能會依當地法律和法規遭到封鎖。

以下是常見的違規情況：

- 聲稱受保護團體毫無人性、低人一等或活該被仇視的內容或言論。
- 應用程式包含指稱受保護團體具有負面特質 (例如惡毒、腐敗、邪惡等) 的仇恨言論、刻板印象或理論，或是明確主張/暗示該團體能構成威脅。
- 認為屬於受保護群體的成員應該被仇恨或歧視，並試圖鼓勵他人相信這個觀點的內容或言論。
- 宣傳仇恨象徵 (例如與仇恨團體相關的旗幟、符號、徽章、物品或行為) 的內容。

暴力內容

我們禁止任何應用程式呈現或助長無端引起的暴力行為或其他危險活動，但如果應用程式以遊戲方式呈現虛構的暴力畫面 (例如卡通、狩獵或釣魚)，則通常不在此限。

以下是常見的違規情況：

- 以圖像或敘述呈現寫實的暴力行為或以暴力威脅任何人物或動物安全的行為。
- 應用程式宣傳自殘行為、自殺、飲食失調、窒息遊戲，或是其他可能造成嚴重傷害或致死的行為。

暴力極端主義

我們禁止恐怖組織基於任何目的 (包括招募成員) 在 Google Play 發布應用程式。其他危險組織或群眾運動若參與、準備對平民施暴，或聲稱對此類行動負責，亦在禁止之列。

應用程式不得包含下列內容：涉及暴力極端主義；策劃、籌備或讚揚對平民施暴行為；發起恐怖行動、煽動暴力行為或讚揚恐怖攻擊。如果發布內容與暴力極端主義相關，但具有教育、紀實、科學或藝術用途，請務必提供相關資訊，協助使用者瞭解來龍去脈。

敏感事件

我們禁止應用程式利用具有重大社會、文化或政治影響的敏感事件，例如民事緊急事件、天災、公衛緊急事件、衝突、死亡或其他悲劇事件；亦禁止應用程式對於這類事件缺乏敏感性。如果應用程式的內容與敏感事件相關，但該內容具有 EDSA (教育、紀錄、科學或藝術) 方面的價值，或旨在讓使用者注意或關注敏感事件，則通常不在此限。

以下是常見的違規情況：

- 對於因自殺、濫用藥物、自然因素等情況而死亡的個人或群體缺乏同理心。
- 否認發生過有據可查的重大悲劇事件。
- 涉嫌利用敏感事件牟利，且對事件受害者未帶來明顯助益。

霸凌與騷擾行為

我們禁止應用程式納入威脅、騷擾或霸凌內容，也禁止應用程式助長這類行為。

以下是常見的違規情況：

- 霸凌國際衝突或宗教衝突的受害者。
- 內容意圖剝削他人，包括勒索、敲詐等。
- 透過張貼內容公開羞辱他人。

- 騷擾不幸事件的受害者或其親友。

危險產品

我們禁止應用程式助長炸藥、槍枝、彈藥或特定槍枝配件的銷售。

- 管制配件包括可將槍枝改裝成仿自動或全自動射擊槍枝的配件 (例如撞火槍托、加特林扳機、自動退殼阻鐵、改造工具組)，以及裝有超過 30 發彈藥的彈匣或彈鏈。

我們禁止應用程式提供炸藥、槍枝、彈藥、管制槍枝配件或其他武器的製造說明，包括將槍枝改造為全自動或仿自動射擊武器的說明。

大麻

我們禁止應用程式助長大麻或大麻製品的銷售，無論合法與否皆然。

以下是常見的違規情況：

- 讓使用者透過應用程式內購物車功能訂購大麻。
- 協助使用者安排大麻的運送或取貨事宜。
- 促銷含四氫大麻酚 (THC) 的產品，包括含 THC 的 CBD 油等產品。

菸草製品和酒精飲料

應用程式不得助長菸草製品或含尼古丁產品 (例如電子菸和尼古丁袋) 的銷售，也不得鼓勵非法或不當的飲酒、吸菸或尼古丁使用行為。

以下是常見的違規情況：

- 不得向未成年人描述/鼓吹使用或銷售菸酒。
- 不得暗示抽菸可提高社會、性、專業、智識或運動方面的地位。
- 不得以正面角度描述過量飲酒行為，包括以討喜的方式描述過量飲酒、狂飲或拚酒場面。
- 不得推銷、宣傳或主打菸草產品，包括顯示廣告、橫幅、類別，以及菸草產品販售網站的連結。
- 我們可能會在特定地區允許食品/雜貨運送應用程式有限度地販售菸草產品，但這類應用程式須落實年齡管制保護措施，例如要求送貨人員在交付產品時查驗身分證件。
- 我們可能允許販售標榜有尼古丁戒除輔助功效的產品，但前提是落實年齡管制保護措施。

年齡限制內容和功能

為維護兒童安全，避免他們接觸到疑似有害的內容，符合下方敘述的應用程式必須使用 [Play 管理中心的功能和工具來封鎖未成年人](#)：

1. 促成[現金交易賭博、遊戲和競賽](#)。
2. 以[媒合交友或約會對象](#)為核心功能的應用程式。如果應用程式並非以媒合交友或約會對象為核心功能，就不必封鎖未成年人，前提是必須採取適當的年齡管制保護措施，防止他們存取這類功能。

金融服務

我們禁止應用程式向使用者提供涉及詐騙或可能造成傷害的金融商品和服務。

本政策提到的「金融產品和服務」係指與金錢和加密貨幣管理或投資相關的產品和服務，包括個人化諮詢服務。

如果應用程式含有或宣傳金融商品和服務，您必須遵守應用程式發行國家/地區的各州或地方法規，例如按照當地法律規定加入特定揭露事項。

若應用程式包含任何金融功能，開發人員就必須在 [Play 管理中心](#) 填寫金融功能聲明表單。

二元期權

我們禁止應用程式向使用者提供二元期權交易功能。

貸款

個人信貸：我們所稱的「個人信貸」，是指單一人士、機構或實體提供給個人消費者的一次性借款，非用於分期購買固定資產或支付教育費用。申辦個人信貸的消費者必須瞭解貸款產品的品質、特點、費用、還款時程、風險和好處等相關資訊，才能準確判斷是否要申辦。

- 例子：個人信貸、發薪日貸款、點對點網路借貸和產權貸款
- 不屬於「個人信貸」的示例：房屋貸款、汽車貸款、循環信貸 (例如信用卡和個人信用額度等)

薪資預支：我們所稱的「薪資預支」(EWA) 貸款是一種金融服務，可讓個人預支一部分已經賺得，但雇主尚未支付的薪資。有別於傳統貸款，EWA 服務具有以下特徵：

- 還款機制：透過扣除薪資的方式，或是與使用者銀行帳戶綁定的自動支付交易來自動還款。即使自動支付交易失敗，也不必支付額外的利息、罰金或手續費。
- 收入型放貸：可貸款給使用者的金額不會超過目前支付期間已經賺取的薪資，確保他們無法憑藉未來的收入借款。
- 收費標準：EWA 服務不收利息，而是收取一筆低額固定費用，或是按百分比計算的交易手續費。合理的手續費應該是越低越好，而且公開透明，足以反映提供服務的實際成本，卻又不造成使用者的負擔，範圍可能介於每筆交易 \$1 到 \$5 美元，或是預支金額的 1–5%。
- 不致負債：EWA 服務通常不會向信用機構回報交易，確保不影響使用者的信用評分或導致他們長期背債。

如果應用程式提供個人信貸 (包括但不限於直接提供貸款、開發新客戶、為消費者和第三方放款人媒合)，開發人員就必須在 Play 管理中心將應用程式類別設為「財經」，並在應用程式中繼資料內揭露下列資訊：

- 最短和最長還款期限。
- 最高年利率 (APR)，通常包含利息、手續費和一年間的其他費用，或是依據當地法律計算出來的其他類似費率。
- 貸款總費用計算示例，包括本金和所有相關手續費。
- 隱私權政策，當中依照「金融服務」政策所述限制，完整揭露對於使用者個人和私密資料的存取、蒐集、使用及分享行為

應用程式不得宣傳必須在放款當日起 60 天 (或更短期限) 內還清借款的個人信貸 (這類貸款稱為「短期個人信貸」)。

如果應用程式提供薪資預支貸款服務 (包括但不限於直接提供貸款、開發新客戶、為消費者和第三方放款人媒合)，開發人員就必須在 Play 管理中心將應用程式類別設為「財經」，並在應用程式中繼資料內揭露下列資訊：

- 還款條款及細則
- 所有手續費，包括訂閱費用、交易手續費，以及所有其他與提供貸款相關的手續費。
- 貸款總費用計算示例，包括所有手續費。
- 隱私權政策，當中依照「金融服務」政策所述限制，完整揭露對於使用者個人和私密資料的存取、蒐集、使用及分享行為

我們必須能確認，您為證明自身能經營個人信貸業務所提供的執照或文件，與您的開發人員帳戶有所關聯。為確認您的帳戶遵循所有當地法律和法規，我們可能會要求您提供其他資訊或文件。

個人信貸應用程式、主要用途為協助取得個人信貸 (例如開發潛在客戶或媒合借貸雙方) 的應用程式、與信用額度、貸款或信用相關的應用程式 (貸款計算工具、貸款指南等) 以及薪資預支 (EWA) 應用程式，一律不得存取相片和聯絡人等私密資料，也無法要求下列權限：

- Read_external_storage
- Read_media_images

- Read_contacts
- Access_fine_location
- Read_phone_numbers
- Read_media_videos
- Query_all_packages
- Write_external_storage

若應用程式會利用私密資訊，或所用 API 會存取私密資訊，即須遵守其他限制和規定。如需更多資訊，請參閱[權限政策](#)。

高年利率個人信貸

美國禁止應用程式提供年利率 (APR) 36% 以上的個人信貸；在美國，提供個人信貸的應用程式必須顯示根據《[誠實貸款法](#)》(Truth in Lending Act，簡稱 TILA) 計算出來的最高年利率。

這項政策同樣適用於直接提供貸款的應用程式、待開發客戶產生應用程式，以及為消費者和第三方放款人媒合的應用程式。

各個國家/地區的規範

鎖定下列國家/地區的個人信貸應用程式必須符合其他規定，並在 [Play 管理中心](#) 的金融功能聲明表單中提供補充文件。在相關管轄區的適用範圍內，提供薪資預支貸款服務的應用程式必須遵守這些規定。請務必依照 Google Play 的要求提供額外資訊或文件，證明您遵守適用的監管和授權規定。

1. 印度

- 應用程式必須提交執照，並列在印度儲備銀行 (RBI) 「Digital lending apps (DLAs) deployed by Regulated Entities」(受監管機構所部署的數位借貸應用程式 (DLA)) 清單上，才能送交 Google Play 進行個人信貸應用程式審查（相關指南請見這篇[說明中心文章](#)）。
- 如果您未直接涉及放款活動，只是提供平台，方便已註冊的非銀行金融公司 (NBFC) 或銀行對使用者放款，則必須在聲明中如實反映這點。
 - 此外，請務必在應用程式說明中，醒目揭露所有已註冊的 NBFC 和銀行名稱。

2. 印尼

- 根據印尼金融服務監管局頒布的第 77/POJK.01/2016 號法令 (可能不時修訂)，如果應用程式涉及以資訊技術為基礎的金錢借貸服務，您必須提供有效執照的副本以供審查。

3. 菲律賓

- 凡是透過線上借貸平台 (OLP) 提供貸款的金融和放款公司，都必須向菲律賓證券交易委員會 (PSEC) 取得 SEC 註冊號碼和執照 (CA) 號碼。
 - 此外，請務必在應用程式說明中揭露您的公司名稱、商家名稱、PSEC 註冊號碼，以及金融/放款公司的經營執照 (CA)。
- 如果應用程式涉及以借貸為基礎的群眾募資活動 (例如點對點 (P2P) 借貸)，或是群眾募資規章制度 (CF 規則) 定義的活動，就必須透過已向 PSEC 註冊的 CF 中介機構處理交易。

4. 奈及利亞

- 數位放款機構 (DML) 必須遵循奈及利亞聯邦競爭暨消費者保護署 (FCCPC) 頒布的《2022 年數位貸款有限臨時監管/註冊架構和指南》(可能不時修訂) 及填寫相關表單，並獲得 FCCPC 提供的可驗證核准函。
- 貸款整合商必須提供數位借貸服務的相關文件和/或證明，以及每個 DML 合作夥伴的聯絡資料。

5. 肯亞

- 數位信貸提供者 (DCP) 應完成 DCP 註冊程序並獲得肯亞中央銀行 (CBK) 核發執照。您必須在聲明中提供 CBK 核發執照的副本。
- 如果您未直接涉及放款活動，只是提供平台，方便已註冊的 DCP 對使用者放款，則必須在聲明中如實反映這點，並提供每位合作夥伴的 DCP 執照副本。
- 我們目前只接受 CBK 官網上「數位信貸提供者目錄」(Directory of Digital Credit Providers) 所列實體的聲明和執照。

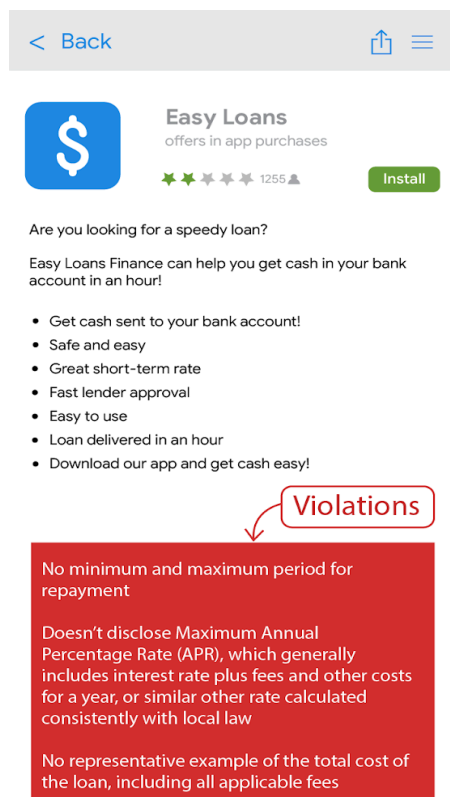
6. 巴基斯坦

- 每家非銀行金融公司 (NBFC) 放款機構只能發布一個數位借貸應用程式 (DLA)。如果開發人員試圖為單一 NBFC 發布多個 DLA，則開發人員帳戶和其他關聯帳戶可能會遭到終止。
- 您必須提交 SECP 核准證明，才能在巴基斯坦提供或協助取得數位借貸服務。此外，除了巴基斯坦法律和法規明確許可的少數幾種例外情況，我們一概不允許短期貸款應用程式。

7. 泰國

- 在泰國發布的個人信貸應用程式若貸款利率為 15% 以上，必須取得泰國銀行 (BoT) 或財政部 (MoF) 核發的有效執照。開發人員必須提供文件，證明有能力在泰國提供或協助辦理個人信貸。這份文件應包含：
 - 泰國銀行為個人信貸提供者/小額貸款金融機構核發的營業執照副本。
 - 泰國財政部為 Pico 或 Pico Plus 放款公司核發的 Pico Finance 營業執照副本。
- 所有鎖定泰國的個人信貸應用程式，都必須在 Google Play 商店資訊中顯示下列詳細資料：
 - 獲泰國銀行 (BoT) 或財政政策辦公室 (FPO) 核發執照的貸款服務供應商名稱。
 - 開發人員的法人名稱。
 - 最高利率和所有費用。
- 除了上述資訊，鎖定泰國的個人信貸應用程式若利率低於 15%，還必須包含下列資訊：
 - 聲明「此貸款服務供應商不受 BoT/FPO 監管」。

以下是常見的違規情況：



現金交易賭博內容、遊戲和競賽

我們允許符合特定條件的現金交易賭博應用程式、與現金交易賭博相關的廣告、結合遊戲化元素的會員方案，以及每日夢幻運動遊戲應用程式。

賭博應用程式

在遵守相關限制和 Google Play 所有政策的情況下，只要開發人員符合下列條件，即可在指定國家/地區提供讓使用者能夠或便於進行線上賭博的應用程式：[完成在 Google Play 發行賭博應用程式的申請程序](#)，

而且本身是這些國家/地區的官方核准業者，亦/或是向適當賭博主管機關登記立案的業者，並在當地持有所提供線上賭博產品的有效經營執照。

我們僅允許取得有效執照或授權的賭博應用程式提供下列類型的線上賭博產品

- 線上賭場遊戲
- 運動彩券
- 賽馬 (規範和執照皆與運動彩券有別)
- 彩券
- 每日夢幻運動遊戲

合格應用程式必須符合下列規定：

- 開發人員必須成功[完成申請程序](#)，才能在 Google Play 上發行這類應用程式；
- 應用程式必須符合發行國家/地區的所有適用法律和業界標準；
- 開發人員必須在應用程式發行的每個國家/地區/州別/領地取得有效賭博執照；
- 開發人員不得提供不屬於賭博執照範疇內的賭博產品；
- 應用程式必須防止未滿法定年齡的使用者使用；
- 應用程式必須防止不在開發人員賭博執照有效範圍 (國家/地區、州別/領地或其他地理區域) 內的使用者存取及使用；
- 應用程式「不得」以付費應用程式的形式，在 Google Play 上架供使用者購買，也不得使用 Google Play 應用程式內結帳功能；
- 應用程式必須能夠讓使用者從 Google Play 商店免費下載及安裝；
- 應用程式分級必須為 AO (僅限成人) 或 [IARC 的同等分級](#)；且
- 應用程式 (包括 Google Play 商店中的應用程式資訊) 必須清楚顯示關於理性賭博的說明資訊。

其他現金交易遊戲、競賽和錦標賽應用程式

如果應用程式不符合上述賭博應用程式資格規定，也並未加入下列「其他現金交易遊戲前測」，即不得提供讓使用者能夠或便於從事下列活動的內容或服務：利用現金 (包括付費購買的應用程式內產品) 下注、投注或參與活動，贏得具有實際貨幣價值的獎品。違規項目包括但不限於線上賭場、運動賽事投注、彩券，以及收取現金並提供現金或其他現實有價物品做為獎品的遊戲 (下方「遊戲化會員方案」規範所允許的方案不在此限)。

違規示例

- 遊戲提供以現金換取贏得實體或金錢獎勵的機會
- 應用程式的導覽元素或功能 (例如選單項目、分頁、按鈕、[WebView](#) 等) 含有「行動號召」，鼓動使用者以現金下注、投注或參與現金交易遊戲、競賽或錦標賽。例如，運用「立即下注！」、「立即註冊！」或「參加比賽！」之類的行動號召文字，邀請使用者參加有機會贏得獎金的錦標賽。
- 應用程式會收取或管理賭資、應用程式內貨幣、獎金或押金，讓使用者以此賭博或贏得實體獎勵或金錢獎勵。

其他現金交易遊戲前測

我們有時會在特定地區，針對某些類型的現金交易遊戲進行限時前測。如需詳細資訊，請參閱這個[說明中心](#)頁面。日本境內的線上夾娃娃遊戲前測將於 2023 年 7 月 11 日結束。自 2023 年 7 月 12 日起，線上夾娃娃遊戲應用程式可在全球的 Google Play 商店上架，惟須遵循適用法律和相關[規範](#)。

遊戲會員方案

在法律允許且不受其他賭博或遊戲授權規定限制的情況下，我們允許以真實獎品或等值物品來獎勵使用者的會員方案。但請注意，這類方案須符合下列 Play 商店資格規定：

所有應用程式 (遊戲 和非遊戲)：

- 會員方案的福利或獎勵必須明確附屬於應用程式中符合條件的付費交易 (這類交易必須是真實的獨立交易，以提供與會員方案無關的商品或服務為目的)，不得透過販售或任何形式的交換而取得，否則即違反現金交易賭博內容、遊戲和競賽政策的限制。
- 舉例來說，符合條件的付費交易不得有為加入會員方案而支付的費用或賭注，亦不可讓使用者以高於平常的價格購買商品或服務。

遊戲 應用程式：

- 會員點數、提供福利或獎品的獎勵，或與符合條件的付費交易相關聯的獎勵，僅能依照固定比率發放與兌換，且應用程式本身和會員方案的公開正式規則都必須明確標示這個比率。此外，使用者獲得的福利或兌換價值不得做為賭注或獎勵，也不得依遊戲表現或機率性結果予以加成。

非遊戲應用程式：

- 在符合下列條件的前提下，開發人員可以將會員點數或獎勵與競賽或機率性結果加以連結。會員方案的福利或獎勵與符合條件的付費交易相關聯，必須滿足以下要件：
 - 在應用程式中發布會員方案的正式規則。
 - 如果會員方案採用具有不確定性、機率性或隨機性的獎勵機制，須在正式條款中揭露以下項目：1) 透過固定機率發放獎勵的會員獎勵活動，應標明中獎機率，以及 2) 所有其他此類活動的抽選方式 (例如決定獎勵的變數)。
 - 如果會員方案提供抽獎、獨得獎金或其他類似形式的促銷活動，必須在正式條款中指明每次促銷活動的獲獎人數、參加活動的截止日期和獎勵發放日期。
 - 如果會員點數或獎勵是依照固定比率累計與兌換，應用程式本身和會員方案的正式條款中必須明確標示這個比率。

提供會員方案的 應用程式類型	遊戲會員方案 和變動獎勵	依固定比率/時間 表發放會員獎勵	須提供會員方案 的條款及細則	含有機率性元素的會員方案須在條款 及細則中揭露中獎機率或抽選方式
遊戲	不允許	允許	是	不適用 (遊戲應用程式的會員方案不得包含機率性元素)
非遊戲	允許	允許	是	是

在透過 Play 發行的應用程式中放送賭博或現金交易遊戲、競賽和錦標賽的廣告

我們允許應用程式放送宣傳賭博、現金交易遊戲、競賽和錦標賽的廣告，但前提是須符合下列條件：

- 應用程式和廣告 (包括廣告客戶) 必須遵守廣告放送地區的所有適用法律和業界標準；
- 廣告內容必須符合當地對於宣傳賭博相關產品和服務的所有適用廣告授權規定；
- 應用程式不得對已知未滿 18 歲的使用者顯示賭博廣告；
- 應用程式不得加入闔家適用計畫；
- 應用程式不得以未滿 18 歲的使用者為主要客層；
- 如要放送賭博應用程式 (定義如上) 廣告，在廣告到達網頁、宣傳的應用程式本身或其商店資訊中，必須清楚顯示關於理性賭博的說明資訊；
- 應用程式不得提供模擬賭博內容 (例如社交類賭場應用程式；包含虛擬吃角子老虎機的應用程式)；
- 應用程式不得提供賭博、現金交易遊戲、彩券或錦標賽的支援或附屬功能 (例如協助下注、付款、追蹤運動賽事比數/賠率/成績或管理參與資金的功能)；
- 應用程式內容不得宣傳賭博或現金交易遊戲、彩券或錦標賽服務，也不得將使用者導向這類服務。

只有符合本節所列全部規定的應用程式，才能放送有關賭博或現金交易遊戲、彩券或錦標賽的廣告。如果賭博應用程式 (定義如上) 或每日夢幻運動遊戲應用程式 (定義如下) 符合上方 1 至 6 條規定，亦可放送有關賭博或現金交易遊戲、彩券或錦標賽的廣告。

違規示例

- 應用程式是專為未滿法定年齡的使用者所設計，但放送宣傳賭博服務的廣告
- 模擬賭場遊戲宣傳或將使用者導向以現金下注的賭場

- 應用程式的主要用途是追蹤運動賽事賠率，但是其中含有連結至運動賽事投注網站的賭博廣告
- 應用程式放送的賭博廣告違反我們的[欺騙性廣告](#)政策，例如以按鈕、圖示或其他互動式應用程式內元素形式向使用者顯示的廣告

每日夢幻運動遊戲 (DFS) 應用程式

我們允許符合當地適用法律定義的每日夢幻運動遊戲 (DFS) 應用程式，但前提是須符合下列條件：

- 應用程式 1) 只在美國發行，或 2) 符合上列適用於美國以外國家/地區的賭博應用程式規定，並完成申請程序；
- 開發人員必須成功完成 [DFS 應用程式申請程序](#) 並獲得許可，才能在 Play 上發行這類應用程式；
- 應用程式必須符合發行國家/地區的所有適用法律和業界標準；
- 應用程式必須防止未滿法定年齡的使用者透過應用程式進行投注或金錢交易；
- 應用程式「不得」以付費應用程式的形式，在 Google Play 上架供使用者購買，也不得使用 Google Play 應用程式內結帳功能；
- 應用程式必須能夠讓使用者從 Play 商店免費下載及安裝；
- 應用程式分級必須為 AO (僅限成人) 或 [IARC 的同等分級](#)；
- 應用程式 (包括 Google Play 商店中的應用程式資訊) 必須清楚顯示關於理性賭博的說明資訊；
- 在發行應用程式的美國州份或領地，應用程式須符合所有適用法律和業界標準；
- 在某些美國州份和領地中，開發人員必須依當地規定取得有效的每日夢幻運動遊戲應用程式執照；
- 如果開發人員在特定美國州份或領地中，並未依規定持有每日夢幻運動遊戲應用程式執照，則必須防止該地區使用者存取應用程式；且
- 在每日夢幻運動遊戲應用程式並不合法的美國州份或領地中，開發人員必須防止該地區使用者存取應用程式。

非法活動

我們禁止任何應用程式助長或宣傳非法活動。

以下是常見的違規情況：

- 方便買賣禁藥。
- 描述/鼓吹未成年人使用或銷售藥物或是菸酒。
- 說明如何種植或製造禁藥。

使用者自製內容

使用者原創內容 (UGC) 是指內容由使用者提供給應用程式，且至少有部分應用程式使用者能看見或存取。

如果應用程式含有或主打使用者原創內容 (包括專門將使用者導向使用者原創內容平台的瀏覽器或用戶端)，就必須持續實行有效完善的使用者原創內容審核機制：

- 要求使用者先接受應用程式的使用條款和/或使用政策，才能建立或上傳使用者原創內容。
- 根據《Google Play 開發人員計畫政策》定義不當內容和行為，並在應用程式的使用條款或使用政策中禁止這類內容和行為。
- 依據應用程式內的使用者原創內容類型，以合理且一致的方式實行使用者原創內容審核機制，包括在應用程式中提供檢舉及封鎖不當使用者原創內容和使用者的系統，並適時處理受檢舉的使用者原創內容或使用者。不同的使用者原創內容體驗需要不同審核機制，例如：
 - 如果應用程式主打使用者原創內容，且透過使用者驗證或離線註冊等方式識別特定一群使用者 (比如專門在某間學校或公司使用的應用程式等等)，就必須在應用程式中提供檢舉內容與使用者的功能。
 - 如有支援與特定使用者 1:1 互動的使用者原創內容功能 (例如即時訊息、標記、提及他人等等)，應用程式中必須提供封鎖使用者的功能。

- 如果應用程式讓使用者存取向大眾公開的使用者原創內容 (比如社群網路應用程式和網誌應用程式)，必須在應用程式中導入檢舉使用者/內容與封鎖使用者的功能。
- 如果是擴增實境 (AR) 應用程式，使用者原創內容審核機制 (包括應用程式內的檢舉系統) 必須涵蓋不當的 AR 使用者原創內容 (例如煽情露骨的 AR 圖像)，以及敏感 AR 錨定地點 (比如將 AR 內容的錨定地點設在軍事基地等管制區域，或是設在 AR 錨定會對地產業主造成問題的私有地產)。
- 採取保護措施，防止有人藉由鼓勵不當的使用者行為在應用程式內營利。

附隨性的色情內容

如果出現色情內容的使用者原創內容應用程式符合以下條件，相關色情內容即屬於「附隨性」色情內容：

(1) 主要讓使用者存取非色情內容，且 (2) 不會主動宣傳或推薦色情內容。違反適用法律的色情內容以及[危害兒童安全](#)的內容，都不屬於「附隨性」色情內容，且一律受到禁止。

若使用者原創內容應用程式符合下列所有規定，即可包含附隨性色情內容：

- 篩選器會自動隱藏這類內容，而且使用者至少要執行兩項操作才能完全停用這類篩選器 (例如隱藏在模糊處理的插頁後方，或是未停用「安全搜尋」就不會出現在畫面上)。
- 採用年齡審查系統，例如[非誘導性年齡選擇畫面](#)或適用法律定義的適當系統，明確禁止兒童 (依[家庭政策](#)定義) 使用應用程式。
- 開發人員依[內容分級政策](#)規定，在應用程式的內容分級問卷中正確作答與使用者自製內容相關的題目。

如果應用程式的主要用途是提供不當的使用者自製內容，Google Play 會予以下架。同樣地，如果應用程式的主要用途最終演變為存放不當的使用者原創內容，或是因為含有大量這類內容而廣為使用者所知，Google Play 也會將其下架。

以下是常見的違規情況：

- 宣傳煽情露骨的使用者自製內容，包括實作或允許主要在鼓勵分享不當內容的付費功能。
- 含有使用者自製內容 (UGC) 但並未適當過濾威脅、騷擾或霸凌行為 (尤其是針對未成年人) 的應用程式。
- 文章、註解或應用程式內相片的主要目的在於騷擾他人或是虐待、惡意攻擊或揶揄特定人士
- 應用程式含有不當內容，遭到使用者多次檢舉而未處理。

健康狀況相關內容和服務

應用程式不得向使用者提供有害健康的內容和服務。

如果您的應用程式包含或者會宣傳健康狀況相關內容和服務，請務必確保該應用程式遵循適用法律和法規。

健康與醫療應用程式

如果您的應用程式功能包含提供健康相關功能或資訊，或有非健康功能需要存取健康資料，即須遵守現有的《Google Play 開發人員計畫政策》，包括「[隱私權、欺騙行為和裝置濫用情形](#)」政策。另外，亦須滿足下列條件：

- **在 Play 管理中心完成聲明：**
 - 所有開發人員都必須前往 Play 管理中心的「應用程式內容」頁面 (依序點選「監控及改善」>「政策」>「應用程式內容」)，填寫健康應用程式聲明表單。填寫方式請見[本文](#)。
- **符合隱私權政策與醒目揭露事項規定：**
 - 您的應用程式必須在 Play 管理中心的指定欄位張貼隱私權政策連結，並在應用程式內提供該政策的連結或內文。如「[資料安全性](#)」專區規範所述，請確保隱私權政策位於有效、公開且存取權不受地理位置限制的網址，不是以 PDF 顯示，而且不開放編輯。
 - 應用程式的隱私權政策和應用程式內任何揭露事項，皆必須完整揭露存取、蒐集、使用及分享[使用者個人或私密資料](#)的方式，而不是只公布上述「資料安全性」專區揭露的資料。若應用程式包含受[危險或執行階段權限](#)管理的功能或資料，即必須遵守所有適用的[醒目揭露事項與同意聲明規定](#)。
 - 健康應用程式不得索取無助核心功能執行的權限，亦須移除未使用的權限。如要瞭解涉及健康私密資料的權限，請參閱「[健康應用程式政策涉及哪些權限](#)」一節。

- 如果本質上不是健康應用程式，但提供健康相關功能，也會存取健康資料，即須符合健康應用程式政策規範。諸如提供保險服務的應用程式，以及蒐集使用者活動資料來推進遊戲進程的遊戲應用程式等等，都必須向使用者清楚指出核心功能與蒐集健康相關資料之間的關聯。應用程式的隱私權政策必須清楚說明這項資料用途限制規定。
- **符合醫療保健功能規定：**
 - 應用程式不得提供誤導性或可能有礙健康的醫療保健相關功能。
 - 若應用程式需連接外部硬體或裝置 (例如血糖儀) 才能執行醫療功能，說明中即須明確揭露此類額外硬體需求，且不得暗示沒有所需外部硬體時，仍可獨立運作。
 - 若應用程式需使用裝置感應器 (例如鏡頭) 提供健康功能，說明中須載明裝置相容性資訊。例如，只靠裝置感應器提供血氧儀功能的應用程式，就必須適當揭露哪些裝置型號支援此功能。
 - 如果應用程式因屬於醫療器材而受到監管，則須提出相關聲明，亦須填寫[本文](#)所述的必要資訊。Google Play 會註明這類應用程式為「醫療器材」。應用程式因屬於醫療器材而受到監管，即須配合要求，提出獲得相關主管機關批准、授權或認證的證明。至於其他健康與醫療應用程式，則須在相關說明中加入清楚的免責事項，表明本身不是醫療器材，非用於診斷、治療、治癒或預防任何疾病。
 - 應用程式也必須提醒使用者，如需醫療建議、診斷或治療，應諮詢專業醫護人員。

- **符合其他規定：**

如果您的健康應用程式屬於下列任一類，即須遵守相應規範：

- **政府相關健康應用程式：**如果政府或已獲認可的醫療照護機構授權您開發及發行相關應用程式，您必須透過[提前告知表單](#)提交資格證明。
- **患者接觸追蹤/健康狀態應用程式：**如果您提供的是患者接觸追蹤和/或健康狀態應用程式，請在 Play 管理中心選取「疾病預防與公共衛生」，並透過上述提前告知表單提供必要資訊。
- **人體研究應用程式：**應用程式在進行健康相關人體研究時，必須遵守所有規定和法規，包括但不限於取得參與者的知情同意；若參與者未成年，則須取得其家長或監護人的同意。健康狀態研究應用程式亦須通過機構審查委員會 (IRB) 和/或同等的獨立倫理委員會核准，符合豁免條件者不在此限。此類核准證明必須依要求提供。

若要進一步瞭解健康與醫療應用程式，請參閱「[健康應用程式類別和其他資訊](#)」一文。

「健康資料同步」平台資料

透過「健康資料同步」平台權限存取的資料屬於使用者的個人和私密資料，相關權限使用行為必須遵循[使用者資料](#) 政策，亦須遵循[其他規定](#) 。

處方藥

我們禁止應用程式協助買賣未經醫師開立處方的處方藥物。

未經核可的物質

Google Play 禁止應用程式宣傳或銷售未經核可的物質，即使是聲稱合法的物質亦然。

以下是常見的違規情況：

- 這份[違禁藥品與營養補給品摘錄清單](#) 上的所有項目。
- 含麻黃的產品。
- 含有與減重/控制體重相關的人類絨毛膜性腺激素 (hCG) 產品，或是搭配同化類固醇宣傳促銷的 hCG 產品。
- 含有效藥劑成分或危險成分的草本和營養補給品。
- 不實或具誤導性的醫療保健聲明，包括在聲明中暗示產品擁有與處方藥或管制藥品相等的療效。
- 未經政府核可的產品，但其宣傳手法暗示該產品安全無虞或能夠有效預防、治癒或治療特定病症。
- 受任何政府或管制行動/警告規範的產品。

- 名稱與未經核可的藥品、營養補給品或管制藥品相似而可能造成混淆的產品。

若要進一步瞭解 Google 會監管哪些未經核可或具誤導性的藥品與營養補給品，請前往 www.legitscript.com 。

健康不實資訊

我們禁止應用程式包含違背現有醫療共識，或可能對使用者造成傷害的誤導性健康聲明。

以下是常見的違規情況：

- 關於疫苗的誤導性聲明，例如疫苗可以改變一個人的 DNA。
- 提倡有害、未經核准的療法。
- 提倡其他有害健康的做法，例如迴轉治療。



(1) 這個應用程式的醫療或保健相關聲明 (治癒癌症) 具有誤導性。

付款 - 臨床醫療服務

如果交易內容涉及受法規監管的臨床醫療服務，不得使用 Google Play 帳單系統。如需更多資訊，請參閱「[瞭解 Google Play 付款政策](#)」。

區塊鏈內容

隨著區塊鏈技術持續迅速發展，我們致力提供一個平台，讓開發人員透過創新來拓展業務，並為使用者打造更豐富、沉浸感更強的體驗。

本政策提到的區塊鏈內容是指區塊鏈上受保護的代幣化數位資產。如果應用程式含有區塊鏈內容，開發人員就必須遵守這些規定。

加密貨幣交易平台和軟體錢包

加密貨幣的購買、保存或兌換程序，應透過法定管轄區內獲得認證的服務執行。

您也必須遵守應用程式發行國家/地區的適用法規，並避免在禁止您產品與服務的地方發布應用程式。Google Play 可能會要求您提供額外資訊或文件，證明自身遵循任何適用的監管或授權規定。

如要進一步瞭解特定國家/地區的相關規定，請參閱這篇[說明中心](#)文章。

加密貨幣挖礦

我們禁止應用程式在裝置上挖掘加密貨幣，但允許應用程式從遠端控管加密貨幣的挖掘作業。

關於發行代幣化數位資產的資訊公開規定

如果應用程式販售代幣化數位資產，或是讓使用者取得這類資產，開發人員必須前往 Play 管理中心的「應用程式內容」頁面，在金融功能聲明表單中聲明相關資訊。

建立應用程式內產品時，您必須在產品詳細資料中指出該產品代表這類資產。如需詳細指引，請參閱「[建立應用程式內產品](#)」一文。

您不得宣傳或美化可能透過遊戲或交易活動賺取的任何收益。

NFT 遊戲化機制適用的額外規定

根據 Google Play「[現金交易賭博內容、遊戲和競賽](#)」政策規定，整合 NFT 等代幣化數位資產的賭博應用程式應完成申請程序。

如有任何其他應用程式不符合賭博應用程式資格規定，而且未加入[其他現金交易遊戲前測](#)，便不得接受以具有貨幣價值的任何物品，換取有機會獲得價值不明的 NFT。使用者購買的 NFT 應該在遊戲中消耗掉或用掉，以便提升使用者體驗，或是協助使用者推進遊戲。NFT 不得用於賭博或下注，換取有機會贏得具實際貨幣價值的獎勵，包括其他 NFT。

以下是常見的違規情況：

- 應用程式販售 NFT 套裝組合，但未揭露 NFT 的具體內容和價值。
- 付費制的社交類賭場遊戲 (例如老虎機) 提供 NFT 做為獎勵。

AI 產生的內容

隨著開發人員對生成式 AI 模式的應用日益廣泛，您或許會將這些模型整合至自己的應用程式，從而促進參與並改善使用者體驗。Google Play 希望協助確保 AI 產生的內容對所有使用者安全無虞，並整合使用者意見，推動負責任的創新發展。

AI 產生的內容

AI 產生的內容是生成式 AI 模型依使用者提示詞建立的內容，例如：

- 文字對話生成式 AI 聊天機器人 (與聊天機器人互動是應用程式的主要特色)
- AI 依文字、圖片或語音提示詞生成的圖片或影片

為保障使用者安全，在 Google Play 的[政策涵蓋範圍](#)內，使用 AI 生成內容的應用程式必須遵守現有的 Google Play 開發人員計畫政策，包括禁止與防止生成[違規內容](#)，例如[助長剝削或虐待未成年人的內容](#)，以及會導致[欺騙行為](#)的內容。

如需有關生成式 AI 應用程式安全防護之業界最佳做法的資源，請參閱[說明中心](#)文章。

使用 AI 生成內容的應用程式須內建回報或檢舉功能，讓使用者不必離開應用程式，就能向開發人員回報或檢舉令人反感的內容。開發人員應利用使用者回報的資訊，改進應用程式的內容過濾和管理機制。

智慧財產

我們禁止任何應用程式或開發人員帳戶侵犯他人的智慧財產權 (包括商標、版權、專利、商業機密和其他專屬權利)。此外，我們也禁止任何應用程式鼓吹或誘導使用者侵犯智慧財產權。

如果有人針對疑似侵犯版權的行為發出明確通知，我們會做出回應。如需更多資訊，或想依據《數位千禧年著作權法》(DMCA) 提出申訴，請參閱我們的[版權程序](#)。

如要針對在應用程式內銷售或宣傳仿冒商品的行為提出申訴，請提出[仿冒申訴通知](#)。

如果您是商標擁有者，當您認為 Google Play 上的某個應用程式已侵犯您的商標權時，建議您直接與該應用程式的開發人員聯絡，解決侵權疑慮。如果您與對方無法達成共識，請使用[這份表單](#) 提出商標申訴。

如果您有書面文件可證明您已取得授權，能夠在自己的應用程式或商店資訊中使用第三方的智慧財產 (例如品牌名稱、標誌、圖片和影片資源)，請在提交應用程式前[先與 Google Play 團隊聯絡](#)，確保我們不會將該應用程式誤判為違反智慧財產權規定而予以拒絕。

未經授權使用受版權保護的內容

我們禁止任何應用程式侵犯版權。即使開發人員對受版權保護的內容做出修改，仍可能違反規定。如要使用受版權保護的內容，開發人員必須提供相關權利證明。

如需使用受版權保護的內容來展示應用程式功能，請務必謹慎行事。一般而言，最安全的做法就是建立原創內容。

以下是常見的違規情況：

- 音樂專輯、電玩遊戲和書籍的封面圖片。
- 電影、電視或電玩遊戲的行銷圖片。
- 出自漫畫、卡通、電影、音樂 MV 或電視節目的畫作或圖片。
- 大專院校球隊和職業球隊的標誌。
- 從公眾人物的社交媒體帳戶中取得的相片。
- 公眾人物的專業圖片。
- 難以與受版權保護的原作區分的重製作品或同人作品。
- 從受版權保護的內容中擷取音訊片段，透過內建音效集播放的應用程式。
- 公有領域外書籍的全文重製作品或翻譯作品。

鼓吹侵犯版權的行為

我們禁止任何應用程式誘導或鼓吹使用者侵犯版權。發布應用程式之前，請先檢查應用程式有沒有以任何形式鼓吹侵犯版權的行為，並視需要尋求法律建議。

以下是常見的違規情況：

- 在未經授權的情況下，讓使用者將受版權保護的內容下載到本機的串流應用程式。
- 違反適用版權法，鼓吹使用者串流播放及下載受版權保護的作品 (包括音樂和影片) 的應用程式：



- ① 應用程式資訊中的說明文字鼓吹使用者未經授權下載受版權保護的內容。
- ② 應用程式資訊中的螢幕截圖鼓吹使用者未經授權下載受版權保護的內容。

侵犯商標權

我們禁止任何應用程式侵犯他人商標權。商標是用於識別商品或服務來源的字詞、符號或兩者的組合。取得商標權後，商標擁有者即具備將商標用於特定商品或服務的專屬權利。

商標侵權是指不當使用或未經授權使用相同或是相似的商標，而可能對產品來源造成混淆的行為。如果您的應用程式使用他人商標，且使用方式可能造成混淆，我們會將該應用程式停權。

仿冒商品

我們禁止應用程式銷售或宣傳仿冒商品。仿冒商品帶有與正品商標相同或幾可亂真的商標/標誌，這類商品會仿製正版產品的品牌特徵，讓消費者誤信仿冒品就是如假包換的正版商品。

隱私權、欺騙行為和裝置濫用情形

Google 致力保障使用者隱私權，以及提供安全無虞的使用環境。我們嚴禁所有具有欺騙或惡意性質的應用程式，以及所有濫用或不當使用任何網路、裝置或個人資料的應用程式。

使用者資料

您必須公開說明自己如何處理使用者資料，例如向使用者蒐集的資訊或自行蒐集的使用者資料，包括裝置資訊。也就是說，您必須揭露應用程式存取、蒐集、使用、處理及分享使用者資料的行為，而且資料使用範圍僅限已揭露且符合政策的用途。請注意，在處理使用者個人和私密資料時，也必須遵守下方「使用者個人及私密資料」一節所列的其他規定。除了這項 Play 開發人員計畫政策和其他相關政策外，也請務必隨時遵守您提供產品或服務時所在司法管轄區內，適用的隱私和資料保護法律。舉例來說，如果您的服務對象是歐盟使用者，請注意，法國資料保護主管機關 (CNIL) 採用了行動環境內[個人資料保護最佳做法指導原則](#)，建議您多加參考。

如果您在應用程式中加入了第三方程式碼 (例如 SDK)，請務必確認應用程式中所用的第三方程式碼，以及該第三方對於應用程式中使用使用者資料的處理方式，皆符合《Google Play 開發人員計畫政策》，包括使用與揭露規定。舉例來說，您必須確保 SDK 供應商不會販售應用程式中的使用者個人和私密資料。無論使用者資料是在傳送至伺服器後轉移，還是透過在應用程式中嵌入第三方程式碼的方式轉移，都適用這項規定。

使用者個人及私密資料

🔑 完整 政策

使用者的個人和私密資料包括但不限於個人識別資訊、財務和付款資訊、驗證資訊、電話簿、聯絡人、[裝置位置資訊](#)、簡訊和通話相關資料、[健康資料](#)、[「健康資料同步」平台資料](#)、裝置中其他應用程式的清單、麥克風和相機資料，以及其他具私密性的裝置或使用資料。如果您的應用程式會處理使用者的個人和私密資料，請務必遵守下列規定：

- 透過應用程式存取、蒐集、使用及分享使用者的個人和私密資料的行為，只限於提供合乎一般使用者預期的應用程式和服務功能，以及符合政策的用途：
 - 如果應用程式還會利用使用者的個人和私密資料來放送廣告，就必須遵守 Google Play 的 [「廣告」政策](#)。
 - 如需轉移資料至 [服務供應商](#)，或基於履行合法政府要求、遵守適用法律等法律因素，或涉及併購或收購的情況下，在依法給予使用者充分通知後，您亦能轉移資料。
- 以安全無虞的方式處理使用者的所有個人和私密資料，包括使用新型密碼編譯法 (例如 HTTPS) 傳輸資料。
- 存取 [Android 權限](#) 保護的資料前，盡可能使用執行階段權限要求。
- 不販售使用者的個人和私密資料。
 - 「販售」是指出於金錢考量而與 [第三方](#) 交換使用者的個人或私密資料，或將使用者的個人或私密資料轉移給第三方。
 - 使用者自行轉移個人和私密資料的行為 (例如，使用者利用應用程式的功能將檔案轉移給第三方，或是使用者選擇使用研究專用的應用程式) 不算販售資料。

🔍 考量重點

Do	Don't
Have a valid privacy policy in both the app's store listing and within the app itself.	Don't provide misleading or inaccurate information about your data practices.
Disclose your data collection and sharing practices in the Play Console's Data safety section.	Don't collect data that is not critical to your app's core purpose.
Obtain clear, affirmative user consent before collecting any personal or sensitive data.	Don't sell personal and sensitive user data.
Protect all user data with appropriate security measures, including modern cryptography for data in transit.	Don't violate child safety policies. If your app is for children, you must comply with the Google Play Families policy, which includes specific rules for handling user data.
Only collect and use data that is necessary for your app's functionality.	Don't collect data without the user's consent or manipulate them into giving it.
Allow account deletion. This must be available both in-app and on an external web resource.	Don't neglect account deletion. Provide a clear and easy way for users to delete their accounts and data. Account freezing is not a valid substitute.

醒目揭露事項與同意聲明規定

📄 政策 摘要

Google Play 政策對處理個人或裝置私密資料有嚴格要求，特別是出乎使用者意料收集或使用資料的情況 (例如在背景收集資料)。徵求任何權限或同意之前，請務必先在應用程式內顯眼、容易進入的位置提供一看就懂的揭露聲明，

詳述資料的存取、收集、使用及分享行為。之後，您必須允許使用者主動完成獨立操作來明確表示同意，確保他們已經知情才做出選擇。

🕒 完整 政策

如果應用程式存取、蒐集、使用或分享使用者個人和私密資料的行為，可能不在使用相關產品或功能的使用者的合理預期範圍內 (例如，在使用者未使用應用程式期間，於背景蒐集資料)，請務必遵守下列規定：

醒目揭露事項：您必須在應用程式中載明揭露事項，清楚說明應用程式存取、蒐集、使用及分享資料的行為。這份應用程式內揭露事項必須符合下列規定：

- 必須隨附於應用程式中，不能只出現在應用程式說明或網站中。
- 必須在正常使用應用程式時就能顯示，不需要讓使用者透過選單或設定頁面操作才能查看。
- 必須說明存取或蒐集的資料類型。
- 必須說明使用和/或分享資料的方式。
- 不得僅列載於隱私權政策或服務條款中；且
- 不得包含在與個人和私密資料蒐集行為無關的其他揭露事項中。

同意聲明和執行階段權限：如果應用程式需要徵詢使用者同意或索取執行階段權限，必須先顯示符合本政策規定的揭露事項，隨後再提出這類要求。應用程式徵詢使用者同意時，必須符合下列規定：

- 同意聲明對話方塊必須以清楚明確的方式呈現。
- 應用程式必須要求使用者做出確認動作，例如輕觸項目表示接受，或勾選核取方塊。
- 不得將使用者離開揭露事項的操作 (包括輕觸其他位置關閉揭露事項，或輕觸返回/主畫面按鈕) 視為同意。
- 不得使用會自動關閉或設有期限的訊息來取得使用者同意。
- 必須獲得使用者許可才能開始蒐集或存取使用者的個人和私密資料。

如果應用程式基於其他法律依據 (例如歐盟 GDPR 規定的正當利益)，會在未經使用者同意的情況下處理其個人和私密資料，就必須遵守所有適用法律要求，並對使用者適當揭露此事，包括提供本政策規定的應用程式內揭露事項。

為配合政策規定，建議您視需要參考下方的醒目揭露事項範例格式：

- 「為提供 [功能]，[這個應用程式] 會蒐集/傳輸/同步處理/儲存 [資料類型]，[資料使用情境]。」
- 範例：「為提供健身追蹤功能，Fitness Funds 會蒐集位置資料，即使在應用程式關閉或未使用時也一樣；而且還會把上述資料用來支援廣告放送。」
- 範例：「為提供聯絡人整理功能，Call buddy 會蒐集、讀取及寫入通話記錄資料，甚至在未使用的狀態下也會進行這些作業。」

如果應用程式整合了第三方程式碼 (例如 SDK)，並預設以該程式碼蒐集使用者的個人和私密資料，請在收到 Google Play 要求後的 2 週內 (或 Google Play 指定的更長期限內) 提供充分證據，表明應用程式符合本政策的「醒目揭露事項與同意聲明」規定，而且透過第三方程式碼存取、蒐集、使用或分享資料的行為亦符合規定。

以下是常見的違規情況：

- 應用程式蒐集裝置位置資訊，但未醒目揭露哪些功能會使用這類資料，以及/或者指出應用程式在背景的使用情形。
- 應用程式透過執行階段權限要求存取資料，卻沒有先醒目揭露資料的用途。
- 應用程式存取使用者的已安裝應用程式清單，但未根據上述「隱私權政策」、「資料處理」及「醒目揭露事項與同意聲明」規定將這些資料視為個人或私密資料。
- 應用程式存取使用者的電話簿或通訊錄資料，但未根據上述「隱私權政策」、「資料處理」及「醒目揭露事項與同意聲明」規定將這些資料視為個人或私密資料。
- 應用程式記錄使用者的螢幕畫面，但未根據這項政策將此資料視為個人或私密資料。
- 應用程式蒐集裝置位置資訊，但未按照上述規定詳盡揭露資料用途及徵得使用者同意。

- 應用程式會基於追蹤、研究或行銷等目的，在背景使用受限制權限，但未按照上述規定詳盡揭露權限用途及徵得使用者同意。
- 應用程式使用的 SDK 會蒐集使用者的個人和私密資料，但是處理這些資料的方式不符合「使用者資料」政策，以及存取權、資料處理 (包括禁止銷售) 和醒目揭露事項與同意聲明規定。

請參閱這篇文章，進一步瞭解醒目揭露事項與同意聲明規定。

個人和私密資料存取限制

政策摘要

Google Play 針對處理財務、聯絡人或永久 ID 資料的應用程式設有特定限制。首先，開發人員嚴禁公開揭露財務資訊或政府核發的身分證件號碼，且禁止未經授權發布私人聯絡人資訊。此外，專為兒童設計的應用程式必須使用經過核准的 SDK。若應用程式涉及將永久 ID 與其他資料連結，其用途應僅限於特定的電話通訊或企業管理，並須向使用者清楚揭露相關資訊。請詳閱完整政策內容，確保符合規範。

完整政策

除了上述規範以外，請參閱下表，瞭解特定活動需遵守的相關規定。

活動	規定
您的應用程式會處理財務、付款資訊或身分證字號	應用程式不得公開揭露任何與財務或付款活動相關的使用者個人資料和私密資料，或是任何身分證字號。
您的應用程式會處理非公開的電話簿或聯絡人資訊	我們不允許在未經授權的情況下擅自發布或揭露使用者非公開的聯絡資訊。
您的應用程式具有防毒或安全防護功能 (例如防毒、防惡意軟體或安全性相關功能)	應用程式必須提供隱私權政策，搭配應用程式內的揭露事項，清楚說明應用程式蒐集及傳輸的使用者資料內容、這些資料的用途和分享對象類型。
您的應用程式以兒童做為目標對象	應用程式不得納入未獲核准用於兒童導向服務的 SDK。如果想瞭解完整的政策內容和規定，請參閱 為兒童和家庭設計應用程式 。
您的應用程式會蒐集或連結永久裝置 ID (例如 IMEI、IMSI、SIM 卡序號等)	我們禁止將永久裝置 ID 連結至使用者的其他個人和私密資料，或是可重設的裝置 ID，但下列情況不在此限： • 進行與 SIM 識別資訊連結的電話通訊 (例如：連結至電信業者帳戶的 Wi-Fi 通話)。 • 在裝置擁有者模式下執行企業裝置管理應用程式。 請務必按照使用者資料政策 中的規定對使用者明確揭露這類用途。 如需瞭解其他專屬 ID，請參考這項資源。 如需瞭解 Android 廣告 ID 的其他指南，請參閱廣告政策。

考量重點

Do	Don't
Handle contacts securely.	Don't publicly disclose any financial information or government ID numbers.
Ensure any SDKs used in child-directed apps are approved for that purpose.	Don't disclose sensitive data publicly. Do not make financial data or government IDs public.
Disclose data use for security apps. If your app has anti-virus or security features, its privacy policy must clearly explain all data collection and sharing.	Don't publish or share people's non-public contacts without authorization.
Only link persistent identifiers (like IMEI) to other user data for specific telephony or enterprise management purposes.	Don't use unapproved SDKs for children's apps. Do not include unapproved SDKs in apps targeting children.
Disclose use of identifiers. All permitted uses of persistent identifiers must be prominently disclosed to	Don't link identifiers unnecessarily. Avoid linking persistent identifiers to other user data unless for the

資料安全性專區

政策摘要

Google Play 要求完整公開說明您的應用程式所收集的使用者資料，以及這些資料的用途。您必須在 Play 管理中心，為每款應用程式填寫並維持正確的「資料安全性」專區內容，詳述資料收集、使用及分享情形 (包括應用程式中任何 SDK 的相關行為)。此專區中的資訊必須與您應用程式的隱私權政策揭露事項一致。這些資訊會顯示在您應用程式的 Google Play 「資料安全性」專區，協助使用者瞭解您會如何處理其資料，讓他們做出明智的選擇。請詳閱完整政策內容，確保符合規範。

完整 政策

所有開發人員必須在每個應用程式中提供清楚正確的資料安全性專區，詳述蒐集、使用和分享使用者資料的行為。開發人員應負責確保隱私權標籤正確無誤，並即時更新相關資訊。在適用情況下，資料安全性專區中的內容必須與應用程式隱私權政策中的揭露事項保持一致。

如要進一步瞭解如何建置「資料安全性」專區，請參閱[這篇文章](#)。

考量重點

Do	Don't
Share your privacy policy in Play Console and within the app itself.	Don't attempt to hide data collection or usage from users.
Provide prominent and accessible in-app data disclosure and obtain user consent via affirmative action when required. Affirmative action means that the user must complete an action in order to indicate that they agree. Update regularly information in your app's Data safety section and your privacy policy as you change how your app handles user data.	Don't request device permissions before users have provided their consent.
Verify data handling procedures of all third parties (SDKs). This is an important opportunity to audit your app, know your code, and what you integrate into it. Many SDKs share their data practices on Play SDK Index.	Don't use auto-dismissing consent popups when affirmative action is required to obtain user consent.

隱私權政策

政策摘要

為提升使用者信任感和隱私權，Google Play 要求所有應用程式提供可在應用程式內取得的完整隱私權政策，同時在 Play 管理中心顯示相關連結。這項政策必須準確地揭露應用程式如何存取、收集、使用及分享所有類型的使用者和裝置資料。若應用程式提供帳戶建立功能，您也必須為使用者提供清楚且容易操作的帳戶刪除方式。重要的是，一旦收到帳戶刪除要求，您必須刪除所有相關聯的使用者資料，而不僅僅是凍結帳戶。

完整 政策

所有應用程式都必須在 Play 管理中心的指定欄位張貼隱私權政策連結，並在應用程式內提供該政策的連結或內文。這份隱私權政策連同應用程式內的所有揭露事項，必須完整說明您的應用程式如何存取、蒐集、使用及分享使用者資料，而非僅附上「資料安全性」專區揭露的資料。其中必須包括：

- 開發人員資訊和隱私權問題的聯絡窗口或諮詢機制。

- 應用程式存取、蒐集、使用與分享的使用者個人和私密資料類型說明，並附帶個人或私密資料的分享對象。
- 使用者個人和私密資料的安全處理程序。
- 開發人員的資料保留和刪除政策。
- 明確標示的隱私權政策 (例如在標題中列出「隱私權政策」)。

應用程式在 Google Play 商店資訊中提及的實體名稱 (例如開發人員、公司) 必須出現在隱私權政策中，或是應用程式名稱必須出現在隱私權政策中。即使應用程式不會存取使用者的任何個人和私密資料，仍須提交隱私權政策。

請確保您的隱私權政策位於有效、公開且存取權不受地理位置限制的網址，不是以 PDF 顯示，而且不開放編輯。

考量重點

Do	Don't
Ensure your comprehensive privacy policy is linked in Play Console.	Don't omit any user or device data handling from your privacy policy.
Make your privacy policy accessible from within the app.	Don't fail to include required app/company identification in the privacy policy.
Accurately disclose all data access, collection, use, and sharing in the policy.	Don't present account freezing as a substitute for deletion.
Include your app name and company details in the policy.	Don't create any difficulties or hidden steps for users deleting their account.
Implement a clear, accessible process for user account deletion.	Don't fail to permanently delete all user data upon account deletion.
Upon account deletion, ensure all associated user data is deleted.	Don't neglect to complete and maintain the Data safety section accurately.
Ensure your privacy policy is globally accessible.	

帳戶刪除規定

政策 摘要

為遵守 Google Play 政策並尊重使用者資料自主權，凡提供帳戶建立功能的應用程式，皆須提供易於辨識的帳戶刪除選項。必須讓使用者無論從您的應用程式內，或從外部透過指定網路資源，都能使用此選項。當使用者要求刪除帳戶時，您必須刪除所有相關聯的使用者資料；僅凍結帳戶並不足夠。請確保刪除程序清晰且順暢無阻，並在隱私權政策中詳實說明任何必要的資料保留規範。

完整 政策

如果您的應用程式允許使用者從中建立帳戶，也必須允許使用者可要求刪除本人帳戶。當使用者想從應用程式內部和外部 (例如前往您的網站)，刪除應用程式帳戶時，必須輕易就能找到啟動選項。請務必在 Play 管理中心的指定網址表單欄位，輸入這項網路資源的連結。

依使用者的要求刪除應用程式帳戶時，必須一併刪除與該帳戶關聯的使用者資料。停用、「凍結」或暫時禁用應用程式帳戶不等同於刪除帳戶。如果出於保護安全、預防詐欺或遵循法規等正當理由，而需要保留特定資料，請務必向使用者清楚說明資料保留做法，例如將這類做法加入隱私權政策。

如要進一步瞭解有關刪除帳戶的政策規定，請參閱這篇[說明中心](#)文章。如果想詳細瞭解如何更新資料安全性表單，可以瀏覽這篇[文章](#)。

考量重點

Do	Don't
Offer a clear account deletion option within your app.	Don't fail to provide both an in-app and external deletion method.
Provide an accessible external web resource for account deletion.	Don't create any hidden patterns or undue rigor in the deletion process.
Ensure the user process for deletion is straightforward and free of obstacles.	Don't use account freezing as a substitute for deletion.
Upon user request, delete <i>all</i> data associated with their account.	Don't fail to delete <i>all</i> associated user data upon account deletion request.
Clearly disclose any necessary (e.g. regulatory compliance) data retention in your privacy policy.	Don't provide broken or outdated links to the external deletion resource page.
Ensure your deletion resources clearly reference your app/service.	Don't omit necessary data retention information from your privacy policy.

應用程式組 ID 的使用方式

政策摘要

The App Set ID is intended to support essential non-ads use cases such as analytics and fraud prevention. It must not be used for ads personalization and ads measurement or associated with personally-identifiable information or other device identifiers (for example, Android Advertising ID). You must be transparent, so disclose any collection and usage of App Set ID to users in a legally adequate privacy notification. Please review the full policy to ensure compliance.

完整政策

為支援分析和詐欺防範等基本用途，Android 將導入一種新的 ID。這類 ID 的使用條款如下。

- **使用方式：**應用程式組 ID 不得用於廣告個人化和廣告評估目的。
- **與個人識別資訊或其他 ID 之間的關聯：**應用程式組 ID 不得基於廣告目的與任何 Android ID (例如 AAID) 建立連結，或與任何個人和私密資料建立連結。
- **資訊公開和同意聲明：**應用程式組 ID 的蒐集和使用行為，以及遵守這些條款的承諾，必須透過具有充分法律效力的隱私權聲明 (包括您的隱私權政策) 向使用者揭露。在適用情況下，您必須依法取得使用者的有效同意聲明。如要進一步瞭解 Google 的隱私權標準，請參閱我們的[使用者資料政策](#)。

考量重點

Do	Don't
Use the App Set ID for essential functions such as analytics and fraud prevention.	Don't use the App Set ID for personalized ads or ad measurement.
Disclose the collection and usage of the App Set ID in a legally adequate privacy notification and your privacy policy.	Don't link the App Set ID to any Android identifiers or personal and sensitive user data for advertising purposes.
Obtain legally valid consent from users where required before collecting and using App Set ID.	Don't omit from your privacy policy. You must be transparent about the use of the App Set ID.

歐盟-美國、英國和瑞士資料隱私架構

政策摘要

如果您的應用程式會處理來自歐洲經濟區、英國或瑞士使用者的個人資料，則須遵守當地的隱私權和資料保護法律。除了應徵得使用者同意外，亦須保護這類資料免遭濫用。此外，您有義務監控自身的合規情況；若無法符合要求，應立即通知 Google。請詳閱完整政策內容，確保符合規範。

完整 政策

存取、使用或處理由 Google 提供的個人資料時，如果這些資訊來自歐洲經濟區、英國或瑞士，而且可直接或間接識別個人身分 (以下簡稱「歐盟個人資料」)，請務必：

- 遵守關於隱私權、資料安全和資料保護的所有適用法律、指令、規章和規定；
- 僅依據「歐盟個人資料」相關當事人同意之用途來存取、使用或處理「歐盟個人資料」；
- 採取適當的組織措施和技術措施來保護歐盟個人資料，以免發生遺失、遭到濫用、擅自/非法存取、揭露、變更和毀損的情況；以及
- 如《[Google 控管者與控管者資料保護條款](#)》所述，依據[資料隱私架構原則](#) 或相關轉移機制之規定，提供同等級的防護。

請務必定期確認您是否遵守上述規定。一旦無法達成 (或極有可能無法達成) 這些條件，您必須立即傳送電子郵件到 data-protection-office@google.com 通知我們，並且馬上停止處理歐盟個人資料，或採取合理、適當的措施來恢復應有的防護等級。

考量重點

Do	Don't
Adhere to all applicable privacy, data security, and data protection laws (e.g., GDPR).	Don't ignore privacy laws, as failing to comply with applicable laws is a policy violation.
Only access and use personal data for purposes consistent with user consent.	Don't access or process personal data for any purpose that a user has not consented to.
Implement technical and organizational measures to secure EU Personal Information.	Don't avoid insecurely handling personal data, which could lead to loss or misuse.
If you are unable to meet these conditions, you must immediately notify Google's data-protection-office@google.com and take corrective action.	Don't fail to notify Google. If you can't comply with these conditions, you must inform Google immediately.
Regularly monitor compliance, ensuring you consistently meet these conditions, especially following regulatory or legal updates to applicable policies.	Don't sell or transfer user data without meeting all legal and policy requirements.

存取機密資訊的權限和 API

如要求會存取私密資訊的權限和 API，則這類要求應讓使用者覺得合理且有必要。您只能要求使用必要的權限和 API 來存取私密資訊，以便應用程式能夠執行在 Google Play 商店資訊中所宣傳的現有功能或服務。請勿將存取使用者/裝置私密資訊的權限或 API 用於未揭露、未提供或遭禁止的功能或用途。您不得販售透過存取私密資訊的權限或 API 所取得的個人或私密資料，亦不得基於促銷目的分享這類資料。

若要藉由存取私密資訊的權限和 API 取得資料，請在相關情境下透過漸進式要求提出，讓使用者瞭解應用程式要求該權限的原因。這類資料只能用於使用者同意的用途。如果您之後想將資料用於其他用途，則必須徵詢使用者，確認使用者同意用於這些其他用途。

受限制權限

受限制權限是指歸為[危險](#)、[特殊](#)、[簽署](#) 或如下文所述的權限；除了上述規範外，這類權限也適用下列額外的規定和限制：

- 透過受限制權限存取的使用者或裝置資料，將視為使用者的個人和機密資料，適用「[使用者資料](#)」政策規定。
- 如果使用者拒絕授予受限制權限，您必須尊重他們的決定，而且不得操控或強迫使用者同意授予任何非關鍵的權限。對於不授予機密權限的使用者，您必須在合理範圍內提供使用者其他選項。舉例來說，當使用者限制應用程式存取通話記錄時，讓他們能夠手動輸入電話號碼。
- 我們嚴禁以違反 Google Play「[惡意軟體](#)」政策（包括[進階權限濫用行為](#)）的方式使用權限。

部分受限制權限可能適用下列額外的規定。這些限制旨在保護使用者的隱私權。如果應用程式提供的功能極具吸引力或相當重要，且必須獲得受限制權限後才能運作，並無其他替代方案，那麼我們可能會允許少數特例。我們會審查申請成為特例的案例，評估其在隱私權或安全性方面可能對使用者造成的影響。

受限制權限 (可使用最低限度的替代方案)

系統選擇器和替代方案 (例如 [Sharesheet](#)) 能協助開發人員在開發應用程式時，優先考量使用者隱私。處理相片、影片、聯絡人，以及其他由受限制權限控管的個人私密資料，應遵循隱私維護最佳做法。唯有在採用了最小權限範圍的替代方案，但仍不足以提供核心功能時，應用程式才能要求並具備下列私密資訊權限。詳情請參閱[說明中心](#)。

相片和影片權限

所有使用者相片都是個人私密資料，適用「[使用者資料](#)」政策。

如果系統選擇器 (例如 [Android 相片挑選工具](#)) 無法滿足應用程式提供核心功能的需求，指定 Android 13 以上版本 (API 級別 33 以上) 的應用程式才能要求 [READ_MEDIA_IMAGES](#) 和 [READ_MEDIA_VIDEO](#) 權限。倘若應用程式仍要求 [READ_MEDIA_IMAGES](#) 和 [READ_MEDIA_VIDEO](#) 權限，就必須提交 Play 管理中心聲明，指出存取 Google 相簿的需求，以及 Android 相片挑選工具 (或替代方案) 不敷使用的原因。

簡訊和通話記錄權限

簡訊和通話記錄為使用者的個人和私密資料，相關權限適用[個人及私密資訊](#) 政策規定和下列規範：

受限制權限	規定
通話記錄權限群組 (例如 READ_CALL_LOG 、 WRITE_CALL_LOG 、 PROCESS_OUTGOING_CALLS)	應用程式必須由使用者主動註冊為裝置預設的通話或助理處理常式。
簡訊權限群組 (例如 READ_SMS 、 SEND_SMS 、 WRITE_SMS 、 RECEIVE_SMS 、 RECEIVE_WAP_PUSH 、 RECEIVE_MMS)	應用程式必須由使用者主動註冊為裝置預設的簡訊或助理處理常式。

如果應用程式不具備預設簡訊、通話或助理處理常式的功能，就不得在資訊清單 (包括資訊清單內的預留位置文字) 中宣告要使用上述權限。此外，應用程式必須由使用者主動註冊為預設的簡訊、通話或助理處理常式，才能提示使用者授予這些權限；一旦應用程式不再是預設處理常式，則須立即停止使用該權限。如要瞭解允許的用途和例外狀況，請造訪[這個說明中心網頁](#)。

應用程式只能將權限 (及其衍生資料) 用於提供經過核准的應用程式核心功能。核心功能是指應用程式的主要用途，可能不只一種，而且全都必須是應用程式說明中著重介紹及主打的功能。如果沒有核心功能，應用程式就會「毀損」或無法運作。您只能基於提供應用程式核心功能或服務的目的，傳輸、分享或授權使用這類資料，不得將資料用於任何其他用途 (例如改善其他應用程式或服務、放送廣告或是行銷)。您不得透過其他方法 (包括其他權限、API 或第三方來源) 產生資料，卻將來源註明為通話記錄或簡訊相關權限。

位置存取權

[裝置位置資訊](#) 為使用者的個人和私密資料，適用[個人和私密資訊](#) 政策、[背景位置資訊](#)政策及下列規範：

- 如果應用程式提供現有功能或服務時，不再需要使用受到位置存取權 (例如 [ACCESS_FINE_LOCATION](#)、[ACCESS_COARSE_LOCATION](#)、[ACCESS_BACKGROUND_LOCATION](#)) 保護的資料，就不得存取這類資料。
- 您不得單純為了放送廣告或進行分析，要求使用者提供位置存取權。如果應用程式將這類資料的使用範圍擴及廣告放送，則須遵循我們的[廣告政策](#)。
- 應用程式僅可要求最低限度的必要權限 (即概略位置/前景存取權，而非精細位置/背景存取權)，以提供需要使用位置資訊的現有功能或服務，且使用者應合理預期為了享有該功能或服務，應用程式需取得所要求層級的位置資訊。舉例來說，如果應用程式要求或存取背景位置資訊，但理由缺乏說服力，我們可能會拒絕。
- 背景位置資訊只能用在與應用程式核心功能相關、並有益於使用者的功能。

僅具備前景存取權 (例如「使用時」存取權) 的應用程式可透過前景服務權限存取位置資訊，前提是相關位置資訊使用情形符合下列條件：

- 當使用者在應用程式中執行操作後，應用程式才開始使用位置資訊；以及
- 達到使用者執行操作的目的後，應用程式便立即停止使用位置資訊。

專為兒童設計的應用程式必須遵守[閨家適用](#) 政策。

若要進一步瞭解相關政策規定，請參閱[這篇說明文章](#)。

「所有檔案存取權」權限

使用者裝置上的檔案和目錄屬性為使用者的個人和私密資料，適用[個人和私密資訊](#) 政策規定和下列規範：

- 只有在攸關功能是否得以運作的情況下，應用程式才能要求存取裝置儲存空間，且若非基於重要的使用者導向功能考量，亦不得代表任何第三方要求存取裝置儲存空間。
- 在搭載 R 以上版本的 Android 裝置上，應用程式必須具備 [MANAGE_EXTERNAL_STORAGE](#) 權限，才能管理共用儲存空間的存取權。如果應用程式以 R 版本為指定目標，並且要求取得共用儲存空間 (「所有檔案存取權」) 的廣泛存取權，則必須在發布前通過適當的存取權審查。假使應用程式獲准使用這項權限，就必須明確提示使用者前往「特殊應用程式存取權」設定，為應用程式啟用「所有檔案存取權」。若要進一步瞭解 R 版本的相關規定，請參閱這篇[說明文章](#)。

套件 (應用程式) 瀏覽權限

從裝置查詢到的已安裝應用程式清單為使用者的個人和機密資料，適用[個人和機密資訊](#) 政策規定和下列規範：

如果應用程式的核心用途是啟動、搜尋裝置上的其他應用程式，或是與這些應用程式交互運作，或許可以取得瀏覽裝置上其他已安裝應用程式的適當權限，如下所示：

- **大範圍的應用程式瀏覽權限：**有大範圍的瀏覽權限，代表應用程式能夠查看裝置上已安裝的許多應用程式 (套件)。
 - 如果應用程式是指定 [30 以上的 API 級別](#) 為目標，那麼只有在應用程式需要知道裝置上的任何或所有應用程式，並且/或是與這些應用程式互通才能正常運作時，才能透過 [QUERY_ALL_PACKAGES](#) 取得大範圍的安裝版應用程式瀏覽權限。
 - 如果應用程式可以基於更有[針對性的套件瀏覽權限宣告](#) 運作 (例如查詢特定套件並進行互動，而非索取大範圍瀏覽權限)，就不得使用 [QUERY_ALL_PACKAGES](#)。
 - 如果應用程式使用其他方法獲取的權限，類似於與 [QUERY_ALL_PACKAGES](#) 權限相關聯的大範圍瀏覽權限，則該權限同樣僅限用於提供面向使用者的核心功能，以及與透過該方法發現的應用程式交互運作。
 - 請參閱這篇[說明中心文章](#)，瞭解 [QUERY_ALL_PACKAGES](#) 權限可用於哪些用途。
- **有限的應用程式瀏覽權限：**所謂有限的瀏覽權限，是指應用程式利用更有針對性 (而非「大範圍抓取」) 的方法查詢特定應用程式 (例如查詢應用程式資訊清單宣告提及的特定應用程式)，所以只會存取最低限度

的資料。如果應用程式是以符合政策規定的方式與所查詢的應用程式互相運作，或是管理這類應用程式，就能使用這個查詢方法。

- 如果應用程式需要裝置上已安裝應用程式清單的瀏覽權限，則目的必須與應用程式為使用者提供的核心用途或核心功能直接相關。

我們一律禁止基於數據分析或廣告營利目的，出售或[分享](#)透過 Play 所發行應用程式查詢到的應用程式清單資料。

Accessibility API

Accessibility API 不得用於下列用途：

- 未經使用者同意即變更使用者設定，或是不讓使用者停用或解除安裝任何應用程式/服務，但如果家長或監護人透過家長監護應用程式進行授權，或者獲得授權的管理員透過企業管理軟體進行授權，則不在此限。
- 規避 Android 內建的平台安全控制項、隱私控制項及通知；或
- 以涉及欺騙或違反《Google Play 開發人員計畫政策》的方式，變更或利用使用者介面。

Accessibility API 不應用於以下用途，也不接受以下請求：

- 遠端通話錄音
- 由應用程式自主發起、規劃及執行動作或決定

Accessibility API 的使用情形必須列載於 Google Play 商店資訊中。

IsAccessibilityTool 規範

如果應用程式的核心功能旨在直接協助身心障礙者，可以使用 **IsAccessibilityTool**，以適當方式將應用程式公開標示為無障礙工具應用程式。

如果應用程式不符合 **IsAccessibilityTool** 使用資格，就不得使用這個標記，且必須遵循「[使用者資料](#)」政策中的醒目揭露事項與同意聲明規定，因為使用者對於應用程式中的無障礙相關功能，可能並不知情。

應用程式在執行必要功能時，必須盡可能採用範圍較限縮的 [API 和權限](#) 來取代 Accessibility API。

如要進一步瞭解違禁用途與 IsAccessibilityTool 使用指南，請參閱這篇 [AccessibilityService API](#) 說明中心文章。

「要求安裝套件」權限

若應用程式取得 **REQUEST_INSTALL_PACKAGES** 權限，即可要求安裝應用程式套件。如要使用這項權限，應用程式的核心功能必須包括：

- 傳送或接收應用程式套件。
- 讓使用者啟動應用程式套件的安裝程序。

許可的功能包括：

- 瀏覽或搜尋網頁
- 支援附件的通訊服務
- 分享、傳輸或管理檔案
- 管理企業裝置
- 備份與還原
- 裝置間遷移/手機間轉移
- 將手機與穿戴式裝置或 IoT 裝置 (例如智慧手錶或智慧型電視) 保持同步的隨附應用程式

核心功能是指應用程式的主要用途，連同構成這項核心功能的其他功能，全都必須是應用程式說明中著重介紹及主打的功能。

REQUEST_INSTALL_PACKAGES 權限不得用於執行自我更新、修改或與資產檔案中的其他 APK 組合，唯裝置管理用途不在此限。所有更新或套件安裝作業都必須遵循 Google Play「[裝置與網路濫用行為](#)」政策規定，並須由使用者執行。

人體感應器權限

感應器測量人體生理徵象 (例如心率、血氧濃度和皮膚溫度) 而取得的資料，將視為使用者個人私密資料。應用程式若要求存取這些資料，必須遵守[使用者資料政策](#)和[健康應用程式政策](#)所述的規定。手機、平板電腦和 Wear OS 裝置等所有板型規格若要求 android.permission.BODY_SENSORS 和 android.permission.BODY_SENSORS_BACKGROUND 這兩項權限，也適用上述規定。

從 Android 16 開始，特定資料類型將改用精細、更保護隱私的 android.permissions.health.* 權限 (例如 android.permission.health.READ_HEART_RATE、android.permission.health.READ_OXYGEN_SATURATION、android.permission.health.READ_SKIN_TEMPERATURE)，取代之前廣泛的 BODY_SENSORS 權限。

應用程式如果鎖定 Android 16 以上版本，對於之前要求 BODY_SENSORS 的 API，現在必須使用上述的特定權限。詳情請參閱「[行為變更：指定 Android 16 以上版本的應用程式](#)」這個頁面。

所有對人體感應器權限 (舊版和新版精細權限) 的要求都會經過審查，確保這類個人私密資料的預期用途能讓使用者直接受益，與許可用途一致。許可用途主要涉及健身與保健追蹤功能 (例如即時監控訓練狀況)、病況監控、健康研究 (經適當核准)，或增強穿戴式裝置隨附應用程式功能。

如需完整政策指南 (包括違禁用途、合規用途和詳細規定)，請參閱「[Android Health 權限：指南與常見問題](#)」一文。

「Android 健康資料同步」權限

「[健康資料同步](#)」是一個 Android 平台，可讓健康與健身應用程式在統合的生態系統內儲存和共享相同的裝置資料。此外，這個平台也方便使用者集中管理設定，控制哪些應用程式能讀取及寫入健康與健身資料，例如健康記錄，內容可能包括病史、診斷結果、療程、用藥和檢驗結果等臨床資料，這些資料則是取自醫療服務提供者/機構，或透過支援的第三方保健平台取得。

「健康資料同步」支援讀取及寫入[各種類型的資料](#)，如步數、體溫和健康記錄等。

透過「健康資料同步」權限存取的資料，屬於使用者的個人和私密資料，適用[使用者資料政策](#)規定。如果應用程式符合健康應用程式的資格，或有健康相關功能並會存取健康資料 (包括「健康資料同步」資料)，亦須遵守[健康應用程式政策](#)。

請參閱這篇 [Android 開發人員指南](#)，瞭解如何開始使用「健康資料同步」。如要求存取「健康資料同步」資料類型，並查看其他常見問題，請參閱「[Android Health 權限：指南與常見問題](#)」一文。

透過 Google Play 發行的應用程式須符合下列政策規定，才能讀取及/或寫入「健康資料同步」資料。

適當存取及使用「健康資料同步」

「健康資料同步」平台只能依據適用政策、條款及細則使用，僅限用於本政策載明的核准用途。也就是說，您的應用程式或服務必須符合任一核准用途，才能要求取得相應權限。

核准的用途包括健身與保健、獎勵、健身指導、企業健康、醫療照護、健康研究及遊戲。應用程式獲准用於上述用途後，不得另外用於未揭露或未經許可的用途。

應用程式或服務必須要有一或多項功能的用途是有益使用者健康與健身，才能要求取得「健康資料同步」權限。以下是符合規定的功能：

- 應用程式或服務允許使用者**直接記錄、回報、監控和/或分析**自己的體能活動、睡眠情形、心理健康狀況、營養資訊、健康測量值、體徵描述，以及/或者其他與健康或健身相關的描述、健康記錄和測量值。
- 應用程式或服務允許使用者在裝置上**儲存自己的體能活動、睡眠情形、心理健康狀況、營養資訊、健康測量值、體徵描述、健康記錄**，以及/或者其他與健康或健身相關的描述和測量值，並與符合這些用途的其他裝置端應用程式共用自身資料。

- 應用程式或服務可讓使用者管理慢性疾病、醫療或照護支援狀況。

「健康資料同步」平台的使用情形不得違反本政策，或是其他適用的「健康資料同步」政策或條款及細則，相關規定如下：

- 如果可以合理預期在應用程式、環境或活動中使用「健康資料同步」或相關故障可能導致人員傷亡、環境或財物毀損，則不得將「健康資料同步」用於開發或納入這類應用程式、環境或活動 (例如建造或運行核子設施、飛航控制系統、維生系統或武器)。
- 不得使用無頭應用程式存取透過「健康資料同步」取得的資料。應用程式必須在應用程式匣、裝置應用程式設定、通知圖示等處清楚顯示可辨識的圖示。
- 如果應用程式在不相容裝置或平台之間同步處理資料，就不得與「健康資料同步」一起使用。
- 「健康資料同步」不得連結兒童專用的應用程式、服務或功能。
- 採取合理的適當措施保護所有使用「健康資料同步」的應用程式或系統，以免發生未經授權或非法存取、使用、毀損、遺失、變更或揭露的狀況。

您將「健康資料同步」平台和來自本平台的資料用於預定用途時，同樣有責任確保這些行為遵守任何適用的法規或法律要求。舉例來說，如果您是受到《健康保險流通與責任法案》所規範，且位於涵蓋範圍內的實體或商業夥伴，則當存取及使用來自「健康資料同步」平台的資訊時，就必須遵守適用規定。同理，如果您是受到歐盟使用者《一般資料保護規則》(GDPR) 所規範的開發人員，就必須履行 GDPR 所賦予的義務。這些法律和法規可能會要求您先履行額外協議 (例如業務合作協議或資料處理協議)，再與涉及活動處理的相關實體共用資料。此外，應用程式開發人員也必須判斷自己在進行活動時，是否需要履行這類協議。收到要求時，開發人員必須向 Google 提供這類協議或履行協議的證據。

除非 Google 為特定 Google 產品或服務提供的標籤或資訊有所註明，否則針對將「健康資料同步」平台資料用於任何目的 (尤其是研究、健康或醫療用途) 之行為，Google 一概不予背書，亦不保證這類資料的準確性。對於從「健康資料同步」平台取得資料後加以使用的行為，Google 不承擔任何責任。

使用限制

存取和使用「健康資料同步」資料時，須遵守特定限制：

- 資料只能用於提供或提升適當用途，或者應用程式使用者介面顯示的適當功能。
- 使用者資料須經使用者明確同意，才能基於下列目的轉移給第三方：維護安全 (例如調查濫用行為)、遵守適用法律或法規，或完成合併/收購事宜。
- 禁止以人為方式存取使用者資料，但若此類行為係已取得使用者明確同意、符合安全目的、基於法規遵循目的，或者是依法律要求匯總資料以供內部營運之用，則不在此限。
- **您不得出於任何其他目的轉移、使用或出售「健康資料同步」資料，包括：**
 - 將使用者資料轉移或出售給第三方，例如廣告平台、數據經紀人或任何資訊經銷商。
 - 為廣告放送目的使用、轉移或出售使用者資料，包括放送個人化廣告或按照興趣顯示廣告。
 - 為確認使用者的信用度或貸款目的使用、轉移或出售使用者資料。
 - 將使用者資料轉移、出售，或以其他方式，與可能定義為醫療器材的產品或服務搭配使用；如果該醫療器材應用程式符合所有適用法規，包含取得相關監管機構 (例如美國食品藥物管理局) 的必要授權或核准，可將「健康資料同步」資料用於預定用途，且經過使用者明確同意，則不在此限。
 - 為任何目的或以任何方式，轉移、出售或使用涉及受保護健康資訊 (如《健康保險流通與責任法案》所定義) 的使用者資料；如果是由使用者採取上述動作，且符合《健康保險流通與責任法案》規範的情況，則不在此限。

最小範圍

您只能索取為實現產品功能或服務的必要權限，這類權限要求應只針對所需的具體資料提出。

資訊透明且準確的通知與控制系統

「健康資料同步」會處理健康與健身資料，包括個人和私密資訊。開發人員必須透過詳盡的隱私權政策，就資料相關做法提供清楚且容易找到的揭露聲明，內容包括：

- 如實表明要求存取使用者資料的應用程式或服務名稱。

- 提供清楚準確的資訊，說明應用程式存取、要求及/或蒐集的資料類型。這些資料必須與應用程式中提供的面向使用者功能或建議相關。
- 說明資料用途和/或共用方式：如果您基於某原因要求存取資料，但也會將資料用於次要目的，則所有用途都必須揭露。
- 使用者說明文件，讓他們瞭解如何在應用程式中管理及刪除資料，以及停用及/或刪除帳戶會對資料產生哪些影響。
- 說明如何以安全方式處理使用者個人和私密資料，包括使用新型密碼編譯法 (例如 HTTPS) 傳輸資料。

如需進一步瞭解應用程式連結至「健康資料同步」的規定，請參閱這篇[說明中心文章](#)。

VPN 服務

VpnService 是應用程式擴充及建構其專屬 VPN 解決方案的基礎類別。只有使用 VpnService 並將 VPN 做為核心功能的應用程式，可以建立指向遠端伺服器的安全裝置級通道。例外狀況包括核心功能需要遠端伺服器的應用程式，例如：

- 家長監護和企業管理應用程式。
- 追蹤應用程式使用情況。
- 裝置安全性應用程式 (例如防毒、行動裝置管理服務、防火牆)。
- 網路相關工具 (例如遠端存取)。
- 網頁瀏覽應用程式。
- 由電信業者發布，需要利用 VPN 功能來提供電話或連線服務的應用程式。

VpnService 不得用於下列用途：

- 在未提供醒目揭露事項，也未徵得使用者同意的情況下，蒐集使用者的個人和私密資料。
- 基於營利目的重新導向或操控來自裝置上其他應用程式的使用者流量 (例如重新導向廣告流量，使之流經使用者所在國家/地區以外的國家/地區)。

使用 VpnService 的應用程式必須符合下列規定：

- 在 Google Play 商店資訊中註明 VpnService 的使用情形。
- 必須加密從裝置傳送到 VPN 通道端點的資料。
- 遵循所有《[開發人員計畫政策](#)》，包括[廣告詐欺](#)、[權限](#) 和 [惡意軟體](#) 政策。

精確鬧鐘權限

USE_EXACT_ALARM 是一項即將推出的新權限，作用是針對以 Android 13 (API 級別 33) 以上版本為目標的應用程式，授予[精確鬧鐘功能](#) 的存取權。

USE_EXACT_ALARM 是一項受限制權限，只有當應用程式的核心功能支援精確鬧鐘需求，應用程式才能宣告這項權限。要求這項受限制權限的應用程式必須接受審查，若是應用程式不符合使用限制條件，就禁止在 Google Play 發布

精確鬧鐘權限的使用限制

只有在應用程式為使用者提供的核心功能需要精確計時的操作時，應用程式才必須使用

USE_EXACT_ALARM 功能，例如：

- 應用程式是鬧鐘或計時器應用程式。
- 應用程式是會顯示活動通知的日曆應用程式。

如果您需要將精確鬧鐘功能用於上述以外的用途，則應評估能否選擇使用 **SCHEDULE_EXACT_ALARM** 做為替代方案。

如果要進一步瞭解精確鬧鐘功能，請參閱這篇[開發人員指南](#)。

全螢幕意圖權限

對指定 Android 14 (目標 API 級別 34) 以上版本為目標的應用程式來說，[USE_FULL_SCREEN_INTENT](#) 是一項**特殊的應用程式存取權限**。只有在應用程式核心功能屬於以下需要高度優先通知的類別時，系統才會自動授予應用程式 [USE_FULL_SCREEN_INTENT](#) 的使用權限：

- 設定鬧鐘
- 接聽電話或視訊通話

要求這項權限的應用程式必須接受審查，若是應用程式不符合上述條件，系統就不會自動授予這項權限。在此情況下，應用程式必須要求使用者授予 [USE_FULL_SCREEN_INTENT](#) 使用權限。

提醒您，每當使用 [USE_FULL_SCREEN_INTENT](#) 權限時，都必須遵守所有 [Google Play 開發人員政策](#)，包括**行動垃圾軟體**、**裝置與網路濫用行為**，以及**廣告**政策。全螢幕意圖通知不得干擾、中斷、損害或以未經授權的方式存取使用者的裝置。此外，應用程式亦不得干擾裝置運作或其他應用程式。

如要進一步瞭解 [USE_FULL_SCREEN_INTENT](#) 權限，請前往[說明中心](#)。

Age Signals API 和使用者資料

這項政策定義了您使用 [Age Signals API](#) 的條件，該 API 可存取使用者的敏感個資，也就是年齡和家長同意聲明。

透過 Age Signals API 存取的資料，只能用於確保應用程式履行**適用的法律和監管義務**，例如在應用程式內提供適齡體驗。

我們嚴禁將這些資料用於下列用途，包括但不限於：

- 廣告、行銷或個人化用途，例如放送指定廣告
- 資料分析、使用者剖析或商業智慧
- 基於任何理由將資料販售、分享或轉移給任何第三方，但法律嚴格要求的情況除外

裝置與網路濫用行為

我們禁止任何應用程式干擾、中斷、損害或以未經授權的方式存取使用者的裝置、其他裝置或電腦、伺服器、網路、應用程式設計介面 (API) 或服務，包括但不限於裝置上的其他應用程式、任何 Google 服務或授權電信業者的網路。

在 Google Play 發布的應用程式必須符合預設的 Android 系統最佳化需求，詳細內容請參閱《[Google Play 核心應用程式品質指南](#)》。

經由 Google Play 發行的應用程式，除了透過 Google Play 的更新機制以外，不得以任何方式自行修改、取代或更新版本。同樣地，應用程式不得自 Google Play 以外的來源下載可執行程式碼 (例如 dex、JAR、.so 檔案)。這項限制不適用於在虛擬機器或解譯器中執行，並透過這種方式間接存取 Android API 的程式碼 (例如 WebView 或瀏覽器中的 JavaScript)。

使用 JavaScript、Python、Lua 等編譯語言的應用程式或第三方案式碼 (例如 SDK) 若在執行階段載入 (例如未附在應用程式套件中)，不得允許可能違反 Google Play 政策規定的情形。

我們禁止會導入或利用安全漏洞的程式碼。請查看[應用程式安全性提升計畫](#)，掌握我們為開發人員提供的最新安全性問題資訊。

違反「裝置與網路濫用情形」政策的常見案例：

- 應用程式封鎖或干擾其他顯示廣告的應用程式。
- 應用程式提供遊戲作弊功能，影響其他應用程式的遊戲玩法。
- 應用程式協助使用者入侵服務、軟體/硬體或規避安全保護措施，或是提供相關操作說明。
- 應用程式存取/使用特定服務或 API 的方式，違反了服務條款。
- 應用程式**不符合列入許可清單的條件**，且試圖略過**系統電源管理機制**。

- 應用程式為第三方提供 Proxy 服務；不過如果這是應用程式為使用者提供的主要核心用途，則不構成違規。
- 應用程式或第三方案式碼 (例如 SDK) 會從 Google Play 以外的來源下載可執行程式碼，例如 dex 檔案或原生程式碼。
- 應用程式未經使用者同意，擅自在裝置上安裝其他應用程式。
- 應用程式透過連結或其他方式發布或安裝惡意軟體。
- 應用程式或第三方案式碼 (例如 SDK) 內含 WebView 並加入了 JavaScript 介面，會載入不安全的網頁內容 (例如 http:// 網址) 或從不安全的來源取得未驗證的網址 (例如透過不受信任的意圖取得的網址)。
- 應用程式使用[全螢幕意圖權限](#)，強制使用者與干擾性廣告或通知互動。
- 應用程式為了從其他應用程式擷取使用者活動或身分資料，而規避[Android 沙盒保護措施](#)。

前景服務使用方式

前景服務權限可確保應用程式適當運用面向使用者的前景服務。如果您的應用程式指定 Android 14 以上版本為目標，請務必為應用程式中使用的每項前景服務指定有效的前景服務類型，並聲明適合該類型的前景服務權限。舉例來說，如果應用程式的用途需要地圖的地理位置偵測功能，您必須在應用程式資訊清單中聲明 [FOREGROUND_SERVICE_LOCATION](#) 權限。

前景服務的使用情形必須符合以下條件，應用程式才能聲明這類權限：

- 提供的功能與應用程式核心功能相關，而且有益於使用者
- 由使用者啟動，或使用者可察覺，例如播放歌曲音訊、投放媒體內容到其他裝置、發送清楚明確的使用者通知，或者依使用者要求將相片上傳至雲端
- 可由使用者終止或停止
- 如果系統中斷或延遲服務，會造成不良的使用者體驗，或導致使用者預期的功能無法正常運作 (例如使用者必須能立即開始通話，不受系統延遲)
- 只在完成工作所需的期間執行

下列前景服務用途不受上述條件約束：

- 前景服務類型 [systemExempted](#) 或 [shortService](#)
- 前景服務類型 [dataSync](#) (僅限使用 [Play Asset Delivery](#) 功能時)

如要進一步瞭解前景服務的使用方式，請參閱[這篇文章](#)。

User-Initiated Data Transfer Jobs

只有在 [User-Initiated Data Transfer Jobs](#) API 的使用方式符合以下條件時，應用程式才能使用這個 API：

- 由使用者啟動
- 用於網路資料轉移工作
- 只在完成資料轉移所需的期間執行

如要進一步瞭解 User-Initiated Data Transfer Jobs API 的使用方式，請參閱[這篇文章](#)。

FLAG_SECURE 相關規定

[FLAG_SECURE](#) 是應用程式程式碼中聲明的顯示標記，用於表明 UI 含有機密資料，而且這些資料只限在使用應用程式時透過安全途徑使用。這個標記的作用是防止這類資料顯示在螢幕截圖中，並避免使用者透過不安全的裝置查看這類資料。如果應用程式內容不應在應用程式或使用者裝置以外的地方播送、查看或以其他方式傳輸，開發人員就會聲明這個標記。

為了保障安全和隱私權，所有在 Google Play 發行的應用程式都必須尊重其他應用程式的 [FLAG_SECURE](#) 聲明。這意味著，應用程式不得協助略過其他應用程式中的 [FLAG_SECURE](#) 設定，亦不得建立相關應對措施。

符合[無障礙工具](#) 條件的應用程式可以豁免此規定，前提是此類應用程式不會傳輸、儲存或快取受 FLAG_SECURE 保護的內容，以致這些內容能夠在使用者裝置外的地方存取。

執行裝置端 Android 容器的應用程式

裝置端的 Android 容器應用程式能模擬基礎 Android 作業系統的全部或局部環境。這些環境可能無法提供完整的 [Android 安全防護功能](#)，所以開發人員可以選擇加入安全環境資訊清單標記，藉此向裝置端的 Android 容器表明，這些容器不得在模擬的 Android 環境中運作。

安全環境資訊清單標記

[REQUIRE_SECURE_ENV](#) 是可在應用程式資訊清單中宣告的標記，用於指出應用程式不得在裝置端的 Android 容器中執行。為了保障安全和隱私權，提供裝置端 Android 容器的應用程式必須依循任何宣告此標記的應用程式，以及：

- 查看要在裝置端 Android 容器中載入的應用程式資訊清單，確認是否含有此標記。
- 不得在裝置端 Android 容器中載入宣告此標記的應用程式。
- 不得做為 Proxy，亦即不得在裝置上攔截或呼叫 API，讓應用程式看似已安裝在容器中。
- 不得協助略過標記，亦不得建立相關應對措施，例如載入舊版應用程式，藉此略過現有應用程式的 REQUIRE_SECURE_ENV 標記。

如要進一步瞭解這項政策，請前往[說明中心](#)。

欺騙行為

我們禁止應用程式企圖欺騙使用者或助長欺騙行為，包括但不限於遭判定為功能不實的應用程式。應用程式必須就其功能，在中繼資料的各個部分提供正確的相關揭露事項、說明和圖片/影片。此外，應用程式不得試圖模仿作業系統或其他應用程式的功能或警告。如要對裝置設定做出變更，必須事先告知使用者並徵得同意，同時確保使用者能復原變更。

誤導聲明

我們禁止任何應用程式在說明、名稱、圖示和螢幕截圖等部分中納入不實或具有誤導性的資訊或聲明。

以下是常見的違規情況：

- 應用程式功能標示不實，或是未提供清楚正確的功能說明：
 - 應用程式在說明訊息和螢幕截圖中宣稱為賽車遊戲，實際上卻是使用汽車圖片的益智方塊遊戲。
 - 應用程式標榜提供防毒功能，但事實上僅以文字指示說明如何移除病毒。
- 應用程式所標榜的功能實際上無法執行 (例如驅蟲應用程式)，即使以惡作劇、假功能或笑話的方式呈現亦然。
- 應用程式分類不當，包括但不限於應用程式分級或應用程式類別不當的情況。
- 應用程式含有明顯欺騙或不實的內容，可能干擾投票程序，或與選舉結果相關。
- 應用程式謊稱與特定政府機關有關聯，或是未獲適當授權即提供或協助使用者取得政府服務。
- 應用程式謊稱是知名實體的官方應用程式。舉例來說，如未取得必要權限或權利，應用程式不得使用「小賈斯汀官方應用程式」這類名稱。



(1) 應用程式標榜的功能 (以手機做為酒測器) 實際上無法執行。

以欺騙手段變更裝置設定

我們禁止任何應用程式在未經使用者同意的情況下，擅自變更使用者裝置的設定或功能 (應用程式本身內容除外)。裝置設定和功能涵蓋系統和瀏覽器的設定、書籤、捷徑、圖示、小工具，以及應用程式在主畫面中的顯示方式。

此外，我們也禁止下列情事：

- 應用程式經使用者同意修改裝置的設定或功能，但未提供簡單易用的變更復原選項。
- 應用程式或廣告基於廣告或為第三方提供服務的目的，修改裝置的設定或功能。
- 應用程式誤導使用者移除或停用第三方應用程式，或是誤導使用者修改裝置的設定或功能。
- 應用程式鼓勵或誘導使用者移除或停用第三方應用程式，或是修改裝置的設定或功能 (具公信力的安全性服務不受此限)。

助長欺騙行為

我們禁止應用程式協助使用者誤導他人，或者提供涉及欺騙行為的功能，包括但不限於產生或協助產生身分證件、身分證字號、護照、文憑、信用卡、銀行帳戶和駕照。應用程式必須就本身的功能和/或內容提供正確的揭露事項、名稱、說明和圖片/影片，其運作方式也必須合乎使用者預期。

只有在使用者必須擁有額外應用程式資源 (例如遊戲資產) 才能使用應用程式的情況下，才可提供這類資源讓使用者下載。下載資源必須符合所有 Google Play 政策規定，而且應用程式必須在開始下載前提示使用者，並明確揭露下載內容大小。

即使應用程式聲明其用途為「惡作劇」、「純屬娛樂性質」(或其他類似用語)，仍須符合我們的政策規定。

以下是常見的違規情況：

- 應用程式模仿其他應用程式或網站，藉此誘騙使用者洩漏個人資訊或驗證資訊。
- 應用程式在未經相關人士或實體同意的情況下，呈現或顯示未經驗證或現實中的電話號碼、聯絡人、地址或個人識別資訊。
- 應用程式的核心功能會因使用者的地理位置、裝置參數或其他使用者資料而有所差異，但其商店資訊中並未向使用者清楚告知這些差異。
- 應用程式在更新版本後有大幅變更，但並未告知使用者 (例如列載於「[新功能](#)」部分) 及更新商店資訊。
- 應用程式在審查期間試圖修改或模糊化其行為。
- 採用內容傳遞聯播網 (CDN) 的應用程式進行下載作業，但在下載前並未提示使用者及揭露下載大小。

經過操弄的媒體內容

我們禁止應用程式宣傳或協助製作不實或具誤導性的資訊或聲明，包括透過圖像、音訊、影片和/或文字傳達的資訊或聲明。若經確認，應用程式會宣傳或持續傳播明顯具有誤導性或欺騙性的圖像、影片和/或文字，並可能會造成與敏感事件、政治、社會議題或其他公共事務相關的傷害，則也在禁止之列。

合乎公眾利益、圖像明顯屬於人造、媒體內容經過操弄但附帶面向使用者的免責事項或浮水印，或顯然是為了嘲諷或搞笑模仿的情況，則不在此限。

經過操弄的媒體內容必須遵守現行的 Google Play 開發人員政策，包括不得出現[違規內容](#)政策所禁止的內容。

以下是常見的違規情況：

- 應用程式在商店資訊中，利用敏感事件中的公眾人物或媒體內容來宣傳媒體修改功能。
- 應用程式能修改媒體片段，加入真實新聞媒體的名稱或標誌來模仿新聞廣播，但未附帶清楚的免責事項或浮水印。
- 應用程式的唯一目的是製作媒體內容來誤導他人。



(1) 該應用程式讓使用者可以修改媒體片段來模仿新聞廣播，並在片段中加入名人或公眾人物，且不會加上浮水印。

行為資訊公開

對使用者而言，應用程式功能應清楚明瞭。請勿在應用程式中加入任何隱藏、未使用或未記錄的功能。我們禁止以任何手段規避應用程式審查。為確保使用者安全、系統完整性及合乎政策規定，應用程式可能必須提供其他詳細資料。

不實陳述或行為

我們禁止應用程式或開發人員帳戶有以下行為：

- 冒用任何個人或機構的身分，或是不實陳述或隱瞞擁有權或主要目的。
 - 從事刻意誤導使用者的活動。包括但不限於不實陳述或隱瞞來源國家/地區，以及向其他國家/地區的使用者發送內容。
 - 在應用程式內容涉及政治、社會議題或公眾議題的情況下，與其他應用程式、網站、開發人員或帳戶合作，藉此隱瞞/不實陳述開發人員或應用程式的身分或其他相關詳細資料。
-

Google Play 的目標 API 等級政策

為了帶給使用者安全可靠的使用體驗，Google Play 要求**所有應用程式**必須符合下列目標 API 級別：

新應用程式和應用程式更新所指定的 Android API 級別，「必須」是 Android 作業系統最新主版本發布後一年內所推出。如果新應用程式和應用程式更新不符合此規定，未來將無法透過 Play 管理中心提交。

Google Play 現有的應用程式若未更新，而且未採用在 Android 最新主版本發布後兩年內所推出的 API 級別，新使用者就無法從搭載較新版 Android 作業系統的裝置上取得該應用程式。先前曾經從 Google Play 安裝該應用程式的使用者則不受影響，仍然可以透過該應用程式支援的 Android 作業系統版本，繼續在裝置上尋找、重新安裝及使用該應用程式。

如需尋求技術建議，瞭解如何符合目標 API 級別的規定，請參閱[遷移指南](#)。

如需瞭解明確時程和例外狀況，請參閱這篇[說明中心文章](#)。

在應用程式中使用 SDK

當您在應用程式中加入 SDK，就有責任確保 SDK 的第三方程式碼和相關做法不會造成應用程式違反《Google Play 開發人員計畫政策》。您必須瞭解應用程式使用的 SDK 會如何處理使用者資料，也要確實掌握這些 SDK 使用的權限、蒐集的資料類型和原因。

SDK 規定

應用程式開發人員經常會利用第三方程式碼 (例如 SDK) 在自家應用程式中整合重要的功能和服務。在應用程式中加入 SDK 時，您不僅要確保使用者的安全，也要防止應用程式因此出現安全漏洞。在本部分中，我們會介紹現有的一些隱私權和安全性規定在 SDK 應用方面的規範，以及這些規定如何協助開發人員將 SDK 安全整合到應用程式中。

當您在應用程式中加入 SDK，就有責任確保 SDK 的第三方程式碼和相關做法不會造成應用程式違反《Google Play 開發人員計畫政策》。您必須瞭解應用程式使用的 SDK 會如何處理使用者資料，也要確實掌握這些 SDK 使用的權限、蒐集的資料類型和原因。提醒您，SDK 蒐集及處理使用者資料的行為必須符合應用程式在這方面的政策規定。

為確保您使用的 SDK 不會違反政策規定，請充分閱讀並理解下列政策，並留意下方與 SDK 相關的一些規定：

使用者資料政策

您必須公開說明自己如何處理使用者資料，例如您向使用者蒐集的資訊或您自行蒐集的使用者相關資訊，包括裝置資訊。也就是說，您必須揭露應用程式存取、蒐集、使用、處理及分享使用者資料的行為，而且

資料使用範圍僅限已揭露且符合政策的用途。

如果您在應用程式中加入第三方程式碼 (例如 SDK)，請務必確保應用程式中所用的第三方程式碼，以及該第三方對於應用程式中使用者資料的處理方式，符合《Google Play 開發人員計畫政策》，包括使用與揭露規定。舉例來說，您必須確保 SDK 供應商不會販售從應用程式中取得的使用者個人和私密資料。無論使用者資料是在傳送至伺服器後轉移，還是透過在應用程式中嵌入的第三方程式碼轉移，都適用這項規定。

使用者的個人和私密資料

- 應用程式和服務只能為了滿足使用者對其功能及法規遵循的合理期待，而存取、蒐集、使用及分享透過應用程式取得的使用者個人和私密資料：
 - 如果應用程式還會利用使用者的個人和私密資料來放送廣告，就必須遵守 Google Play 的廣告政策。
- 以安全無虞的方式處理使用者的所有個人和私密資料，包括使用新型密碼編譯法 (例如 HTTPS) 傳輸資料。
- 存取 Android 權限保護的資料前，盡可能使用執行階段權限要求。

使用者個人和私密資料的販售行為

不販售使用者的個人和私密資料。

- 「販售」是指出於金錢考量而與第三方交換使用者的個人或私密資料，或將這類資料轉移給第三方。
 - 使用者自行轉移個人和私密資料的行為 (例如，使用者利用應用程式的功能將檔案轉移給第三方，或是使用者選擇使用研究專用的應用程式) 不算販售資料。

醒目揭露事項與同意聲明規定

如果應用程式存取、蒐集、使用或分享使用者個人和私密資料的行為，可能不在使用者運用該產品或功能時的合理預期範圍內，請務必遵守[使用者資料政策](#)的醒目揭露事項與同意聲明規定。

如果應用程式整合了第三方程式碼 (例如 SDK)，並預設以該程式碼蒐集使用者的個人和私密資料，請務必在收到 Google Play 要求後的 2 週內 (或 Google Play 指定的更長期限內) 提供充分證據，表明應用程式符合本政策的「醒目揭露事項與同意聲明」規定，而且透過第三方程式碼存取、蒐集、使用或分享資料的行為亦符合規定。

切記，使用第三方程式碼 (例如 SDK) 時，您必須確保這不會導致應用程式違反[使用者資料政策](#)。

請參閱這篇[說明中心文章](#)，進一步瞭解醒目揭露事項與同意聲明規定。

SDK 導致的違規問題示例

- 應用程式中的 SDK 會蒐集使用者的個人和私密資料，但是處理這些資料的方式違反使用者資料政策，以及存取權、資料處理 (包括禁止銷售) 和醒目揭露事項與同意聲明規定。
- 應用程式整合的 SDK 預設會蒐集使用者的個人和私密資料，因而違反本政策的醒目揭露事項與同意聲明規定。
- 應用程式中的 SDK 聲稱只會將蒐集到的使用者個人和私密資料用於提供反詐欺和反濫用功能，但實際上也會基於廣告或數據分析目的與第三方分享資料。
- 應用程式所含的 SDK 會傳送使用者安裝套件的資訊，不符合醒目揭露事項和/或[隱私權政策規範](#)。
 - 另請參閱[行動垃圾軟體政策](#)。

其他個人和私密資料存取規定

下表列出了各種活動的相關規定。

活動	規定
應用程式蒐集或連結永久裝置 ID (例如 IMEI、IMSI、SIM 卡序號等)	永久裝置 ID 不得連結至使用者的其他個人和私密資料，或是可重設裝置 ID，但下列目的不在此限： - 會辨識 SIM 卡資訊的電話通訊行為 (例如與電信業者帳戶連結的 Wi-Fi 通話)。 - 在裝置擁有者模式下執行企業裝置管理應用程式。 請務必按照使用者資料政策中的規定，對使用者明確揭露這類用途。 如需瞭解其他專屬 ID，請參考這項資源。 如需查看 Android 廣告 ID 的其他規範，請參閱廣告政策。
您的應用程式以兒童做為目標對象	應用程式只能包含完成自主認證、用於兒童導向服務的 SDK。如想瞭解完整的政策內容和規定，請參閱「 家庭版自主認證廣告 SDK 計畫 」一文。

SDK 導致的違規問題示例

- 應用程式使用的 SDK 會連結 IMEI 和位置資訊
- 應用程式中的 SDK 會出於廣告或數據分析目的，將 Android 廣告 ID (AAID) 連結至永久裝置 ID。
應用程式使用的 SDK 會出於數據分析目的，將 AAID 與電子郵件地址相連結。

「資料安全性」專區

所有開發人員均須針對旗下每個應用程式提供清楚正確的「資料安全性」專區，詳述蒐集、使用和分享使用者資料的行為。這包括揭露透過應用程式所用的第三方案庫或 SDK 蒐集與處理使用者資料的行為。開發人員應負責確保相關標示正確無誤，並即時更新資訊。在適用情況下，此專區中的內容必須與應用程式隱私權政策中的揭露事項保持一致。

如要進一步瞭解如何完成「資料安全性」專區的設定，請參閱這篇[說明中心文章](#)。

請參閱[使用者資料政策](#)全文。

存取機密資訊的權限和 API 政策

如果您需要使用的權限和 API 會存取機密資訊，則這類要求對使用者而言必須具備合理性。您只能要求使用必要的權限和 API 來存取機密資訊，以便應用程式能夠執行在 Google Play 商店資訊中所宣傳的現有功能或服務。請勿將存取使用者/裝置機密資訊的權限或 API 用於未揭露、未提供或遭禁止的功能或用途。您不得販售透過存取機密資訊的權限或 API 所取得的個人或機密資料，亦不得基於促銷目的分享這類資料。

請參閱[存取機密資訊的權限和 API 政策](#)全文。

SDK 導致的違規行為示例

- 應用程式所含的 SDK 會在背景索取位置資訊，用於受到禁止/未經揭露的用途。
- 應用程式所含的 SDK 未經使用者同意，擅自傳輸 read_phone_state Android 權限衍生的 IMEI

裝置與網路濫用行為政策

我們的惡意軟體政策十分簡單，就是為包括 Google Play 商店在內的 Android 生態系統和使用者裝置阻絕任何惡意行為 (即惡意軟體) 侵擾。秉持這個基本原則，我們致力為使用者及其 Android 裝置提供安全的 Android 生態系統。

惡意軟體是指任何可能將使用者、使用者的資料或裝置暴露在風險中的程式碼。惡意軟體包括但不限於可能有害的應用程式 (PHA)、二進位檔或架構修改內容。目前已知有木馬程式、網路釣魚、間諜軟體應用程式等類別，而我們還在持續更新及增加新類別。

本政策規定也適用於應用程式包含的第三方案式碼 (例如 SDK)。

請參閱[惡意軟體政策](#)全文。

SDK 導致的違規行為示例

- 應用程式所含的 SDK 程式庫來自散布惡意軟體的供應商。
- 應用程式違反 Android 權限模型，或從其他應用程式竊取憑證 (例如 OAuth 權杖)。
- 應用程式濫用功能，讓使用者無法將其解除安裝或停止。
- 應用程式停用 SELinux。
- 應用程式所含的 SDK 會透過存取裝置資料取得進階權限，並用於未經揭露的用途，因此違反 Android 權限模型。
- 應用程式所含的 SDK 程式碼會誘騙使用者訂閱或購買內容，並將費用併入電信帳單。

未經使用者授權即取得裝置 Root 權限的權限提升應用程式，會被歸為取得 Root 權限的應用程式。

間諜軟體

間諜軟體是帶有惡意的應用程式、程式碼或行為，會蒐集、竊取或分享使用者/裝置資料，而這些動作與符合政策規定的功能無關。

若惡意程式碼或程式行為疑似會監視使用者，或是未充分告知使用者或徵得同意即洩漏資料，亦可視為間諜軟體。

請參閱[間諜軟體政策](#)全文。

例如，SDK 導致的間諜軟體違規行為包括但不限於：

- 應用程式使用的 SDK 會傳輸語音或電話錄音資料，但此種作為與符合政策規範的應用程式功能無關。
- 應用程式內含惡意的第三方程式碼 (例如 SDK)，會以使用者無法預期的方式，將裝置上的資料傳輸至他處，而且/或者執行此作業時，未充分告知使用者或徵得同意。

行動垃圾軟體政策

確保行為公開透明並清楚揭露相關資訊

所有程式碼的行為都必須合乎對使用者所做的承諾。應用程式必須提供所標榜的所有功能，且不得讓使用者產生混淆。

違規示例：

- 廣告詐欺
- 社交工程

保護使用者資料

請清楚公開揭露對於使用者個人和機密資料的存取、蒐集、使用及分享行為。運用使用者資料時，必須遵循所有相關適用的使用者資料政策，並採取所有預防措施來保護資料。

違規示例：

- 資料蒐集 (另請參閱「[間諜軟體](#)」)
- 受限制權限的濫用行為

請參閱[行動垃圾軟體政策](#)全文。

裝置與網路濫用行為政策

我們禁止任何應用程式干擾、中斷、損害或以未經授權的方式存取使用者的裝置、其他裝置或電腦、伺服器、網路、應用程式設計介面 (API) 或服務，包括但不限於裝置上的其他應用程式、任何 Google 服務或授權電信業者的網路。

如果應用程式或第三方程式碼 (例如 SDK) 會在執行階段載入 JavaScript、Python、Lua 等解譯語言 (例如未封裝於應用程式中)，則不得允許可能違反 Google Play 政策規定的行為。

我們禁止會導入或利用安全漏洞的程式碼。請查看「[應用程式安全性提升計畫](#)」，掌握我們為開發人員提供的最新安全性問題資訊。

請參閱[裝置與網路濫用行為政策](#)全文。

SDK 導致的違規行為示例

- 應用程式為第三方提供 Proxy 服務；不過如果這是應用程式面向使用者的主要核心用途，則不構成違規。
- 應用程式所含的 SDK 會從 Google Play 以外的來源下載可執行程式碼，例如 dex 檔案或原生程式碼。
- 應用程式所含的 SDK 包含已加入 JavaScript 介面的 WebView，而且 JavaScript 介面會載入不受信任的網路內容 (例如 http:// 網址)，或載入從不受信任的來源取得的未驗證網址 (例如透過不受信任的意圖取得的網址)。
- 應用程式所含的 SDK 包含用於更新自身 APK 的程式碼。
- 應用程式所含的 SDK 會透過不安全的連線下載檔案，導致使用者暴露在安全風險中。

- 應用程式使用的 SDK 含有會從 Google Play 以外的不明來源下載或安裝應用程式的程式碼。
- 應用程式所含的 SDK 會使用前景服務，但沒有適當用途。
- 應用程式所含的 SDK 會基於政策許可原因使用前景服務，但資訊清單並未聲明此事。

欺騙行為政策

我們禁止應用程式企圖欺騙使用者或助長欺騙行為，包括但不限於遭判定為功能不實的應用程式。應用程式必須就其功能，在中繼資料的各個部分提供正確的相關揭露事項、說明和圖片/影片。此外，應用程式不得試圖模仿作業系統或其他應用程式的功能或警告。如要對裝置設定做出變更，必須事先告知使用者並徵得同意，同時確保使用者能復原變更。

請參閱[欺騙行為政策](#)全文。

行為公開透明

對使用者而言，應用程式功能應清楚明瞭。請勿在應用程式中加入任何隱藏、未使用或未記錄的功能。我們禁止以任何手段規避應用程式審查。為確保使用者安全、系統完整性及合乎政策規定，應用程式可能必須提供其他詳細資料。

SDK 引發的違規行為示例

- 應用程式所含的 SDK 會以某些手段規避應用程式審查。

SDK 造成違規行為通常與哪些 Google Play 開發人員政策相關？

為協助您確保應用程式使用的第三方案式碼遵守《Google Play 開發人員計畫政策》，請參閱下列政策全文：

- [使用者資料政策](#)
- [存取機密資訊的權限和 API](#)
- [裝置與網路濫用行為政策](#)
- [惡意軟體](#)
- [行動垃圾軟體](#)
- [家庭版自主認證廣告 SDK 計畫](#)
- [廣告政策](#)
- [欺騙行為](#)
- [Google Play 開發人員計畫政策](#)

儘管與上述政策相關的問題更常見，但也要留意，不合規範的程式碼同樣可能造成應用程式違反其他政策。請務必閱讀並及時瞭解所有政策條文，因為各位身為應用程式開發人員，有責任確保 SDK 在處理應用程式資料時遵守政策規定。

如需瞭解詳情，請造訪[說明中心](#)。

惡意軟體

我們的惡意軟體政策十分簡單，就是為包括 Google Play 商店在內的 Android 生態系統和使用者裝置阻絕任何惡意行為 (即惡意軟體) 侵擾。秉持這個基本原則，我們致力為使用者及其 Android 裝置提供安全的 Android 生態系統。

惡意軟體是指任何可能將使用者、使用者的資料或裝置暴露在風險中的程式碼。惡意軟體包括但不限於可能有害的應用程式 (PHA)、二進位檔或架構修改內容。目前已知有木馬程式、網路釣魚、間諜軟體應用程式等類別，而我們還在持續更新及增加新類別。

本政策規定也適用於應用程式包含的第三方案式碼 (例如 SDK)。

雖然惡意軟體有多種類型和不同的破壞能力，但目的通常不出以下幾項：

- 破壞使用者裝置的完整性。

- 取得使用者裝置的控制權。
- 讓攻擊者能夠透過遙控操作，存取、使用或以其他方式利用受感染的裝置。
- 在未充分告知使用者並徵得同意的情況下，將裝置上的個人資料或憑證傳輸至他處。
- 從受感染的裝置散布垃圾內容或指令，影響其他裝置或網路。
- 詐騙使用者。

應用程式、二進位檔或架構修改內容，即使原始目的並無惡意，也可能有害並因此產生惡意行為。這是因為應用程式、二進位檔或架構修改內容可能會因為各種變數，產生迥異的運作情況。所以，有些應用程式可能對某個 Android 裝置有害，但對另一個 Android 裝置卻不會造成任何風險。舉例來說，假設有應用程式利用已淘汰的 API 進行惡意行為，這對搭載 Android 最新版本的裝置不會產生任何影響；但對搭載 Android 較舊版本的裝置可能會造成危害。如果應用程式、二進位檔或架構修改內容對部分或所有 Android 裝置和使用者造成明確風險，就會被舉報為惡意軟體或 PHA。

下方的惡意軟體類別反映出我們的基本理念，也就是使用者應該瞭解自己裝置的運用情形，並且推廣安全的生態系統，打造健全的創新流程和穩當的使用者體驗。

詳情請前往 [Google Play 安全防護](#) 網站。

後門

程式碼讓有心人士以遙控的方式，對裝置執行不必要且可能有害的作業。

這類作業可能包括在未經使用者同意即自動執行後，會導致應用程式、二進位檔或架構修改內容被歸為其他惡意軟體類別的行為。一般來說，「後門」是指會導致裝置上發生可能有害作業的情況，並不完全符合帳單詐欺或商業間諜軟體等惡意行為的定義。因此，在某些情況下，Google Play 安全防護會將某幾種後門視為安全漏洞。

帳單詐欺

程式碼會以蓄意欺瞞的方式自動向使用者收費。

行動帳單詐欺分為簡訊詐欺、電話詐欺和話費詐欺三種形式。

簡訊詐欺

程式碼未經使用者同意就擅自傳送付費簡訊，藉此向使用者收費；或隱藏揭露協議、電信業者發送的收費通知簡訊或確認訂閱簡訊，企圖掩蓋簡訊活動。

有些程式碼即使在技術上會揭露簡訊傳送行為，但仍會帶入其他縱容簡訊詐欺行為的操作。這包括對使用者隱藏揭露協議的部分內容、使揭露協議內容無法閱讀，以及依據特定條件阻絕電信業者向使用者發送收費通知簡訊或確認訂閱簡訊。

電話詐欺

程式碼會在未經使用者同意的情況下擅自撥打付費電話，藉此向使用者收費。

話費詐欺

程式碼會透過電信費帳單誘騙使用者訂閱或購買內容。

話費詐欺涵蓋各種收費行為 (付費簡訊和付費電話除外)，例如電信代扣、無線應用程式通訊協定 (WAP) 和手機通話額度轉移。WAP 詐欺是最猖獗的一種話費詐欺，手法包括誘騙使用者點擊以透明隱形 WebView 形式載入的按鈕。一旦使用者採取相應動作，就會啟動週期性訂閱，而確認簡訊或電子郵件通常會遭到攔截，以防使用者發現這類金融交易。

追蹤軟體

出於監控目的，從裝置中蒐集使用者的個人或機密資料，並將資料傳輸至第三方 (企業或其他個人) 的程式碼。

應用程式必須提供充分明確的醒目揭露事項，並依[使用者資料政策](#) 規定徵求同意。

監控應用程式規範

專為監控其他個人而設計及行銷的應用程式 (例如協助家長監控孩子的應用程式，或是用於監控個別員工的企業管理應用程式) 必須完全符合下述規定才能上架，而且不得用於追蹤其他使用者 (例如配偶)，不論對方是否知情或同意，抑或應用程式是否會向對方顯示長駐通知。這類應用程式必須在資訊清單檔案中使用 IsMonitoringTool 中繼資料標記，適當地標示本身為監控應用程式。

監控應用程式必須符合以下規定：

- 應用程式不得做為間諜或祕密監視用途的工具。
- 應用程式不得隱藏或偽裝追蹤行為，也不得使用誤導手法欺騙裝置使用者，意圖隱瞞這項功能。
- 應用程式必須提供專屬識別圖示，而且在運作期間一律必須向使用者顯示常駐通知。
- 應用程式必須在 Google Play 商店說明中揭露監控或追蹤功能。
- 應用程式以及 Google Play 上的應用程式資訊不得提供任何方式來啟用或存取違反上述條款的功能 (例如連結到 Google Play 商店以外的違規 APK)。
- 應用程式必須符合任何適用法律。您必須自行負責確認應用程式在目標地區的合法性。

如需更多資訊，請參閱說明中心的「[使用 IsMonitoringTool 標記](#)」一文。

阻斷服務 (DoS)

程式碼會在使用者不知情的情況下執行阻斷服務 (DoS) 攻擊，或是涉及對其他系統和資源進行分散式 DoS 攻擊。

舉例來說，藉由傳送大量 HTTP 要求導致遠端伺服器負載超量，就屬於這種情況。

惡意下載工具

程式碼本身不會造成危害，但會下載其他 PHA。

程式碼如果符合下列條件，就可能是惡意下載工具：

- 我們有理由相信，這類程式碼是有人士為了散播 PHA 而編寫，其中不是含有已經下載的 PHA，就是含有可能下載並安裝應用程式的程式碼；或者
- 據觀察最少下載了 500 個應用程式，而且其中至少有 5% 是 PHA (相當於下載 25 個 PHA)。

我們不會將符合下列條件的主流瀏覽器和檔案分享應用程式視為惡意下載工具：

- 只在使用者互動時下載內容；而且
- 所有 PHA 下載作業都是在使用者同意後才執行。

對 Android 以外的平台有威脅

程式碼對 Android 以外的平台有威脅。

這類應用程式不會對 Android 使用者或裝置造成危害，但包含對其他平台可能有害的元件。

網路詐騙

程式碼會假裝來自可信任的來源，要求取得使用者驗證憑證或帳單資訊，然後將這些資料傳送給第三方。如果程式碼會攔截傳輸中的使用者憑證，也屬於這個類別。

常見的網路詐騙目標包括銀行憑證、信用卡號碼，以及社交網路和遊戲的線上帳戶憑證。

進階權限濫用行為

程式碼會破壞應用程式沙箱、取得進階權限，或是變更或停用安全性相關核心功能的存取權，藉此影響系統的完整性。

相關示例包括：

- 應用程式違反 Android 權限模型，或從其他應用程式竊取憑證 (例如 OAuth 憑證)。
- 應用程式濫用功能，讓使用者無法將其解除安裝或停止。
- 應用程式停用 SELinux。

未經使用者授權即取得裝置 Root 權限的權限提升應用程式，會被歸為取得 Root 權限的應用程式。

勒索軟體

程式碼會取得裝置或裝置上資料的部分或廣泛控管權，並要求使用者付款或執行特定動作以取回控管權。

部分勒索軟體會將裝置上的資料加密，並要求使用者付款以解密資料，以及/或者利用裝置管理員功能，讓一般使用者無法將其移除。相關示例包括：

- 鎖定使用者的裝置，並要求使用者付款以取回控管權。
- 加密裝置上的資料，並聲稱使用者須付款才可解密資料。
- 利用裝置政策管理員功能，禁止使用者將其移除。

針對隨裝置發布的程式碼，如果其主要用途是要分擔裝置管理工作，只要確實符合安全鎖定與管理的要求，並已向使用者充分揭露相關資訊及徵得同意，就不會被歸為勒索軟體。

取得 Root 權限

程式碼會取得裝置的 Root 權限。

用於取得 Root 權限的程式碼有惡意與非惡意之分。舉例來說，非惡意的應用程式會在取得裝置的 Root 權限前事先通知使用者，也不會另外執行符合其他 PHA 類別而可能有害的動作。

惡意應用程式則不會在取得裝置的 Root 權限前事先通知使用者，或是會在事先通知使用者後另外執行符合其他 PHA 類別的動作。

垃圾內容

程式碼會向使用者的聯絡人傳送垃圾訊息，或使用裝置轉發垃圾電子郵件。

間諜軟體

間諜軟體是帶有惡意的應用程式、程式碼或行為，會蒐集、竊取或分享使用者/裝置資料，而且這些資料與符合政策規定的功能無關。

若惡意程式碼或行為疑似會監視使用者，或是未充分告知使用者或徵得同意即洩漏資料，亦可視為間諜軟體。

舉例來說，間諜軟體違規行為包括但不限於：

- 錄音或對通話錄音
- 竊取應用程式資料
- 應用程式內含惡意的第三方程式碼 (例如 SDK)，會以使用者無法預期的方式，將裝置上的資料傳輸至他處，以及/或是未充分告知使用者或徵得同意

所有應用程式亦須完全遵守《Google Play 開發人員計畫政策》的規定，包括使用者和裝置資料政策，例如[行動垃圾軟體](#)、[使用者資料](#)、[存取私密資訊的權限](#)和[API](#)及[SDK 規定](#)。

木馬程式

程式碼看起來無害 (例如宣稱純粹是遊戲的遊戲)，但會對使用者執行不當動作。

這個類別通常會與其他 PHA 類別併用。木馬程式包含無害的部分和隱藏的有害部分，例如在使用者不知情的情況下，擅自在背景從使用者的裝置傳送付費簡訊的遊戲。

有關不常見應用程式的附註

針對少見的新型應用程式，如果 Google Play 安全防護所擁有的相關資訊不足，無法確定該應用程式是否安全無虞，就會將其歸為不常見的應用程式。這不一定表示該應用程式有害，但在未經過進一步審查的情況下，也無法確定其安全無虞。

有關後門類別的附註

後門惡意軟體類別是以程式碼的行為做為歸類依據。只有在所產生的行為經自動執行後，會導致其本身被歸為其他惡意軟體類別的程式碼，才屬於後門惡意軟體。舉例來說，如果應用程式會動態載入程式碼，且動態載入的程式碼會擷取簡訊，我們就會將該應用程式歸為後門惡意軟體。

不過，如果應用程式會任意執行程式碼，且我們沒有任何理由認為執行這個程式碼是為了做出惡意行為，則會將該應用程式判定為有安全漏洞 (而非歸為後門惡意軟體)，並要求開發人員進行修補。

風險軟體

這是指應用程式會透過各種規避技術，向使用者提供虛假或與預期不同的功能。這類應用程式會偽裝成合法的應用程式或遊戲，在應用程式商店中看似對使用者無害，實際上卻利用模糊處理、動態載入程式碼或偽裝等技術，顯示潛在的有害內容。

風險軟體與其他 PHA 類別類似 (特別是木馬程式)，主要差別在於掩蓋惡意活動的技術不同。

冒用他人身分

我們禁止應用程式冒用他人身分 (例如假冒其他開發人員、公司或實體) 或模仿其他應用程式，藉此誤導使用者。請勿不實暗示您的應用程式與他人相關或已獲他人授權。請務必小心，不要使用可能會誤導使用者的應用程式圖示、說明、名稱或應用程式內元素，讓使用者誤會您的應用程式與他人或其他應用程式有關聯。

以下是常見的違規情況：

- 開發人員不實暗示與其他公司/開發人員/實體/機構有關聯。



① 應用程式顯示的開發人員名稱，不實暗示該應用程式與 Google 之間有正式關聯。

- 應用程式的圖示和名稱不實暗示與其他公司/開發人員/實體/機構有關聯。

✓		
✗	①	②

① 應用程式使用國徽，讓使用者誤以為其與政府有關聯。

② 應用程式複製企業實體的標誌，不實暗示是該企業的官方應用程式。

- 應用程式名稱和圖示與現有的其他產品或服務過於相似，可能造成使用者誤解。

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

✓		
✗	① 	② 

① 應用程式在圖示中使用熱門加密貨幣網站的標誌，暗示這是應用程式的官方網站。

② 應用程式在圖示中複製知名電視節目的角色和標題，讓使用者誤以為應用程式與該電視節目有關。

- 應用程式不實聲稱是知名實體的官方應用程式。舉例來說，如未取得必要權限或權利，應用程式不得使用「小賈斯汀官方應用程式」這類名稱。
- 應用程式違反《[Android 品牌宣傳指南](#)》。

如要查看「冒用他人身分」政策的常見問題，請見[這篇](#)說明中心文章。

行動垃圾軟體

Google 深信，只要以使用者為中心，一切就會水到渠成。我們在[軟體原則](#)和《[垃圾軟體政策](#)》中提供了一般性建議，說明何種條件的軟體可提供良好的使用者體驗。這項政策的制定依據為《Google 垃圾軟體政策》，其中大致歸納了 [Android 生態系統](#)和 Google Play 商店的適用原則。違反這些原則的軟體都可能對使用者體驗造成負面影響，而我們會採取適當措施保護使用者。

如《[垃圾軟體政策](#)》所述，我們發現大部分的垃圾軟體都具備下列一或多項基本特性：

- 具有欺騙性，承諾其根本達不到的訴求與用途。
- 試圖誘騙使用者安裝軟體，或者暗藏在其他程式的安裝程序中。
- 未向使用者表明軟體所有主要和重要的功能。
- 以意想不到的方式影響使用者的系統。
- 在使用者不知情的情況下收集或傳輸私人資訊。
- 以不安全的處理方式收集或傳輸私人資訊 (例如不透過 HTTPS 傳輸)
- 與其他軟體一起綁定提供，但使用者並不知情。

在行動裝置上，軟體指的是應用程式、二進位檔、架構修改內容等形式的程式碼。為了杜絕對軟體生態系統有害或對使用者體驗造成干擾的軟體，我們會針對違反這些原則的程式碼採取適當措施。

以下規範以《垃圾軟體政策》為基礎，將行動軟體也納入該政策的適用範圍。與《垃圾軟體政策》一樣，我們會持續修訂這項《行動垃圾軟體政策》來因應新型濫用行為。

確保行為公開透明並清楚揭露相關資訊

所有程式碼的行為都必須合乎對使用者所做的承諾。應用程式必須提供所標榜的所有功能，且不得讓使用者產生混淆。

- 應用程式應清楚說明其功能和用途。
- 請向使用者明確說明應用程式會進行哪些系統變更，並讓使用者查看並核准所有重要的安裝選項和異動。
- 軟體不得向使用者顯示不實的裝置狀態，例如宣稱系統有重大安全性問題或遭到病毒感染。
- 請勿利用無效活動來提高廣告流量和/或轉換次數。
- 我們禁止應用程式冒用他人身分 (例如假冒其他開發人員、公司或實體) 或模仿其他應用程式，以藉此誤導使用者。請勿不實暗示您的應用程式與他人相關或已獲他人授權。

違規示例：

- 廣告詐欺
- 社交工程

保護使用者資料與隱私權

請清楚公開揭露對於使用者個人和私密資料的存取、蒐集、使用及分享行為。運用使用者資料時，必須遵循所有相關適用的使用者資料政策，並採取所有預防措施來保護資料。

所有應用程式須完全遵守《Google Play 開發人員計畫政策》的規定，包括使用者和裝置資料政策，例如[使用者資料](#)、[存取私密資訊的權限](#)和 [API](#)、[間諜軟體](#)及 [SDK 規定](#)。

- 不得要求或欺騙使用者關閉裝置安全保護措施，例如 Google Play 安全防護。舉例來說，您不得以關閉 Google Play 安全防護為條件，向使用者提供額外的應用程式功能或獎勵。

請勿影響行動體驗

您應為使用者提供直接明瞭的操作體驗，根據使用者做出的明確選擇，提供相應的服務或內容。應用程式應向使用者明確呈現其價值主張，且不得影響其所標榜或理應提供的使用者體驗。

- 請勿以非預期的方式向使用者顯示廣告，包括影響或干擾裝置功能的可用性，或是在未獲使用者充分同意的情況下，於觸發廣告的應用程式環境以外的地方顯示廣告，而且不讓使用者輕易關閉廣告，也未明確指出廣告是從何而來。
- 應用程式不得干擾其他應用程式或裝置的可用性。
- 解除安裝相關資訊 (如適用) 應清楚明確。
- 行動軟體不得模仿裝置作業系統或其他應用程式的提示，也不得隱藏其他應用程式或作業系統所發出的快訊，特別是向使用者告知作業系統有所變更的快訊。

違規示例：

- 干擾性廣告
 - 未經授權使用或仿製系統功能
-

惡意下載工具

程式碼本身不是垃圾軟體，但是會下載其他行動垃圾軟體 (MUwS)。

如果程式碼符合下列任一條件，就可能是惡意下載工具：

- 我們有理由相信，程式碼是有人心人士為了散播 MUwS 而編寫，而且已經下載 MUwS，或是含有可能下載並安裝應用程式的程式碼。
- 觀察程式碼至少執行 500 次應用程式下載作業後，確認下載的應用程式至少有 5% 是 MUwS (相當於 25 次 MUwS 下載)。

我們不會將符合下列兩項條件的主流瀏覽器和檔案分享應用程式視為惡意下載工具：

- 不在與使用者無互動的情況下啟動下載；以及
 - 所有軟體下載作業都是在使用者同意後才執行。
-

廣告詐欺

我們嚴禁廣告詐欺行為。如果產生的廣告互動是要欺騙廣告聯播網，讓廣告聯播網誤信流量確實是因使用者感興趣而產生，就屬於廣告詐欺行為 (這是一種[無效流量](#))。廣告詐欺可能是因開發人員以不允許的方式導入廣告而產生，例如顯示隱藏的廣告、自動點擊廣告、變更或修改資訊，以及利用非人為動作 (自動尋檢程式、機器人等) 或人為活動企圖產生無效廣告流量。無效流量和廣告詐欺行為會對廣告客戶、開發人員與使用者造成負面影響，並長久導致他們對行動廣告生態系統失去信任。

以下是常見的違規情況：

- 應用程式顯示使用者看不到的廣告。

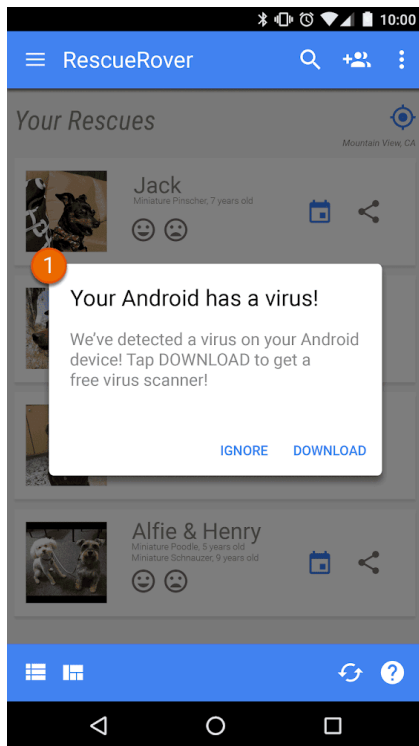
- 應用程式在非出於使用者意願的情況下自動點擊廣告，或產生對等的網路流量來誘騙系統給予點擊功勞。
 - 應用程式傳送假的安裝歸因點擊以獲得收益，但實際上該次安裝並非源自傳送者的網路。
 - 使用者已離開應用程式的介面，但應用程式仍彈出廣告。
 - 應用程式對於廣告空間的陳述不實，例如應用程式向廣告聯播網表示是在 iOS 裝置上運作，但實際上是在 Android 裝置上運作；或是應用程式針對營利的套件使用不實的套件名稱。
-

未經授權使用或仿製系統功能

我們禁止任何應用程式或廣告模仿或干擾系統功能，例如通知或警告。系統性的通知僅限用於應用程式主要功能，例如航空公司應用程式的特惠活動通知，或是遊戲內的商品促銷通知。

以下是常見的違規情況：

- 利用系統通知或快訊放送的應用程式或廣告：



- ① 應用程式透過本身顯示的系統通知放送廣告。

如要查看更多廣告相關示例，請參閱[廣告政策](#)。

社交工程

我們禁止應用程式假冒成其他應用程式，藉此誘騙使用者信以為真，做出原本要對可信任應用程式執行的動作。

營利與廣告

Google Play 支援各種營利策略，包括付費發布、應用程式內產品、訂閱功能和廣告營利模式，致力為開發人員和使用者提供優質服務。為確保使用者能獲得最佳體驗，請務必遵守以下政策。

付款

1. 如果開發人員透過 Google Play 提供付費的應用程式下載內容，必須採用 Google Play 結帳系統向使用者收取這類交易款項。
2. 在 Google Play 發行的應用程式，若提供需要/可付費取得的應用程式內功能或服務 (包括任何應用程式功能、數位內容或商品，統稱「應用程式內購」)，必須以 Google Play 結帳系統收取這類交易款項，但適用第 3 節、第 8 節或第 9 節規定的情況除外。

舉例來說，須使用 Google Play 結帳系統的應用程式功能或服務，包括但不限於下列應用程式內購項目：

- 商品 (例如虛擬貨幣、額外生命、額外遊戲時間、附加道具、角色和顯示圖片/虛擬化身)
- 訂閱服務 (例如健身、遊戲、交友、教育、音樂、影片、服務升級和其他內容訂閱服務)
- 應用程式功能或內容 (例如應用程式的無廣告版本，或是免費版沒有的新功能)
- 雲端軟體和服務 (例如資料儲存服務、企業效率提升軟體和財務管理軟體)

3. Google Play 帳單系統不得用於下列情況：

- a. 付款的主要目的是：

- 購買或租用實體商品 (例如食品雜貨、服飾、家居用品和電子產品)。
- 購買實體服務 (例如交通運輸服務、清潔服務、機票、健身房會籍、餐點外送服務和現場活動票券)。
- 以匯款方式繳清信用卡帳單或水電瓦斯費帳單 (例如有線電視和電信服務帳單)。

- b. 點對點付款、網路拍賣和免稅捐款等類型的付款。

- c. 支付讓使用者便於從事線上賭博行為的內容或服務 (請見「[現金交易賭博內容、遊戲和競賽](#)」政策中「[賭博應用程式](#)」一節的說明)。

- d. 支付 Google [付款中心內容政策](#) 不接受的產品類別。

注意：在部分市場中，販售實體商品和/或服務的應用程式可以使用 Google Pay。詳情請參閱 [Google Pay 開發人員網頁](#)。

4. 除了第 3 節、第 8 節和第 9 節所述情況外，應用程式不得將使用者導向 Google Play 結帳系統以外的付款方式。違禁行為包括但不限於透過以下管道將使用者導向其他付款方式：

- Google Play 中的應用程式資訊。
- 應用程式中針對可購買內容刊登的宣傳廣告。
- 應用程式內的網頁畫面、按鈕、連結，訊息、廣告或其他行動號召內容。
- 從應用程式內的使用者介面流程 (包括帳戶建立流程或註冊流程) 將使用者導向 Google Play 結帳系統以外的付款方式。

5. 應用程式內虛擬貨幣只能在購得虛擬貨幣的應用程式或遊戲內使用。

6. 開發人員必須向使用者清楚說明應用程式、應用程式內付費功能、付費訂閱項目的條款和定價。應用程式內定價必須與使用者在 Play 帳款服務介面中看到的定價一致。在 Google Play 中，如果您的產品說明提及需收取特定或額外費用的應用程式內功能，則必須在應用程式資訊中明確告知使用者這類功能需付費才能使用。

7. 如果應用程式和遊戲提供透過購買交易隨機取得虛擬商品的機制 (包括但不限於「虛擬寶箱」)，必須在使用者購買前或即將交易時，及時清楚揭露這些商品的中獎機率。

8. 如果目標使用者位於[符合資格的國家/地區/區域](#)，且開發人員已加入[適用計畫](#)，並同意遵守額外條款和計畫規範，即可在應用程式內提供其他結帳系統。

9. 如果開發人員已加入適用計畫，並同意附加條款和[計畫規範](#)，便可[依計畫規範](#)，將位於符合資格國家/地區/區域的使用者導向應用程式外部內容。

注意：如要查看這項政策的相關時程和常見問題，請造訪[說明中心](#)。

廣告

為了確保使用者能享有良好的體驗，我們會將廣告的內容、目標對象、使用者體驗、運作方式、安全性和隱私防護納入考量。考量範圍涵蓋應用程式包含的廣告及關聯內容，這些內容必須一併遵循所有其他 Google Play 政策。如果您想透過兒童應用程式在 Google Play 賺取收益，就必須遵守額外規定。

您也可以進一步瞭解[這個頁面](#)的「商店資訊與宣傳」政策，包括我們如何處理[欺騙性宣傳行為](#)。

廣告內容

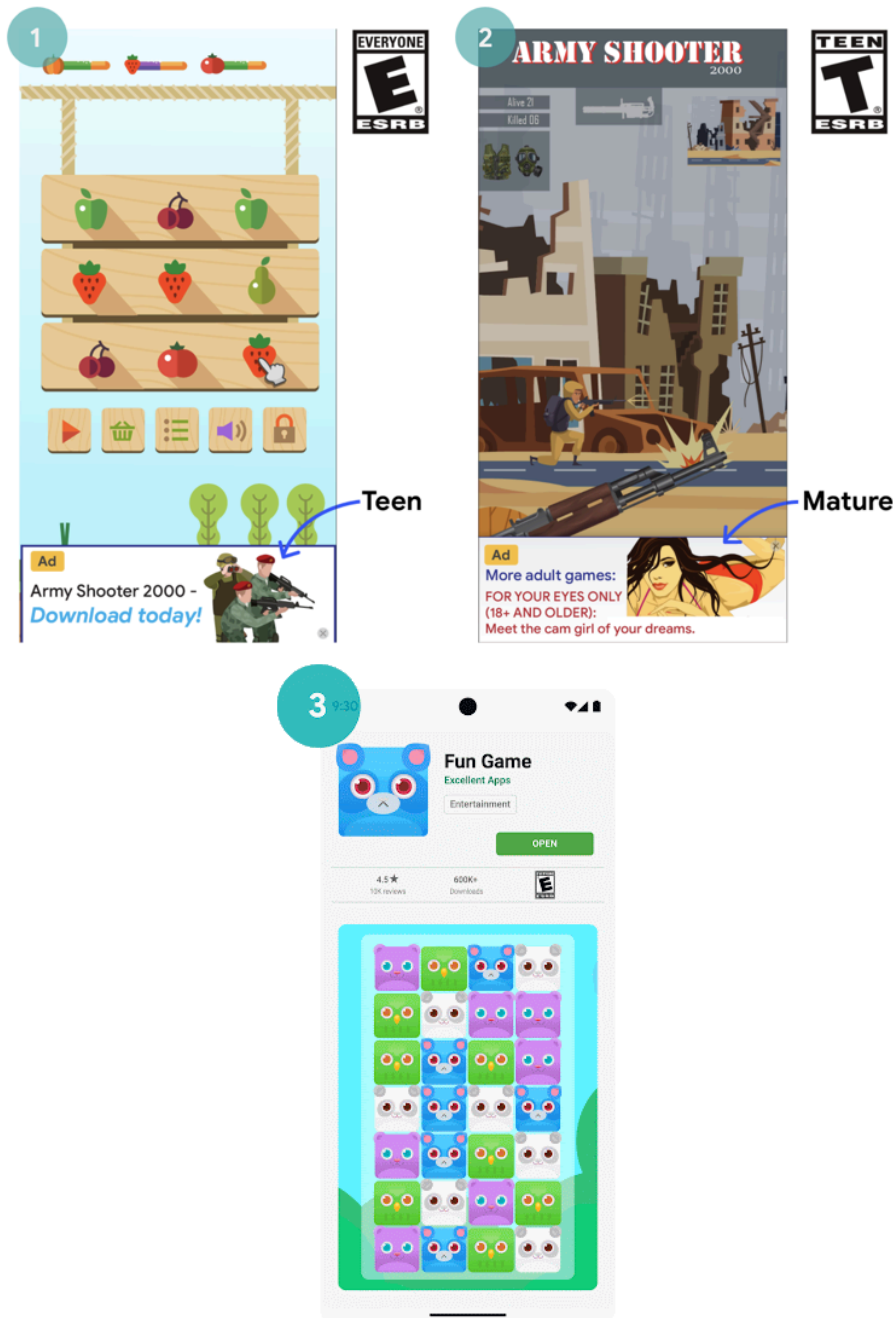
應用程式包含的廣告和關聯內容必須遵循「[違規內容](#)」政策。如果應用程式是[賭博](#)應用程式，也必須符合額外規定。

內容不當的廣告

應用程式內顯示的廣告和相關優惠 (例如宣傳下載其他應用程式的廣告) 必須符合應用程式的[內容分級](#)，即使內容本身在其他方面符合我們的政策也是如此。

以下是常見的違規情況：

- 廣告不符合應用程式內容分級



- ① 這則廣告的目標對象為青少年，不符合應用程式內容分級 (所有人)
- ② 這則廣告的目標對象為成人，不符合應用程式內容分級 (青少年)
- ③ 廣告內容 (宣傳下載成人應用程式) 不符合放送該廣告的遊戲應用程式的內容分級 (所有人)

家庭版廣告規定

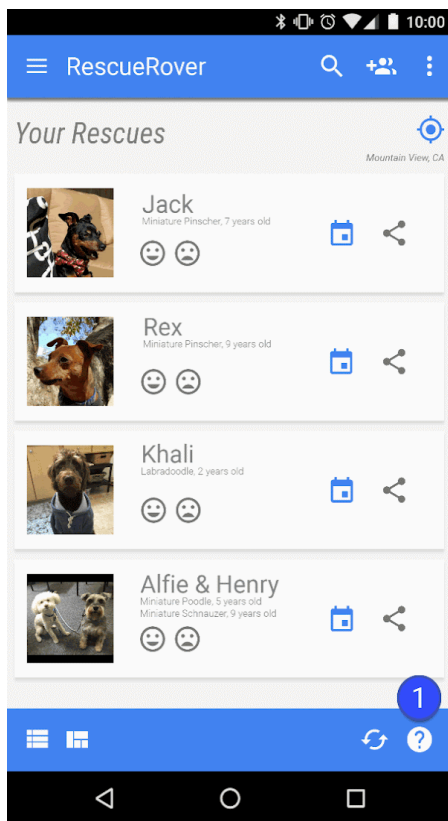
如果您想透過兒童應用程式在 Google Play 賺取收益，請務必確保該應用程式符合家庭版「廣告和營利」政策規定。

欺騙性廣告

廣告不得模仿或仿冒任何應用程式功能的使用者介面，例如作業系統的通知或警告。您必須讓使用者能輕易分辨廣告出自哪個應用程式。

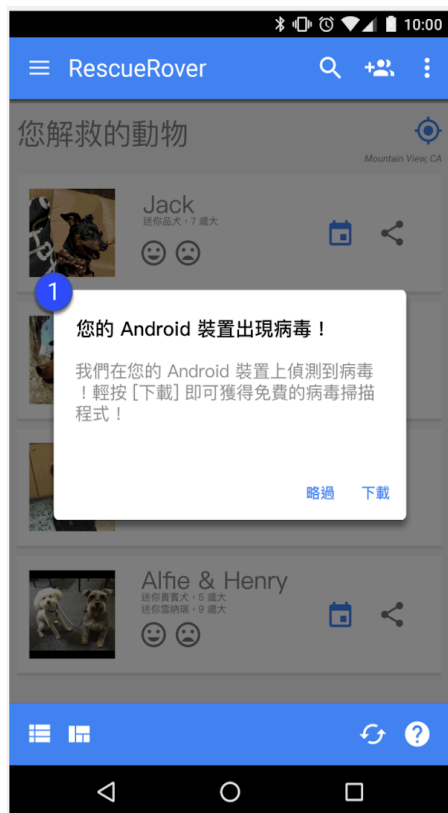
以下是常見的違規情況：

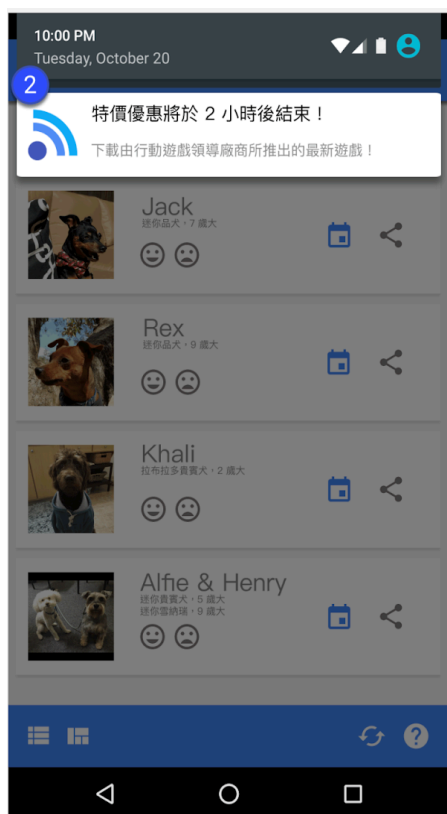
- 模仿特定應用程式使用者介面的廣告：



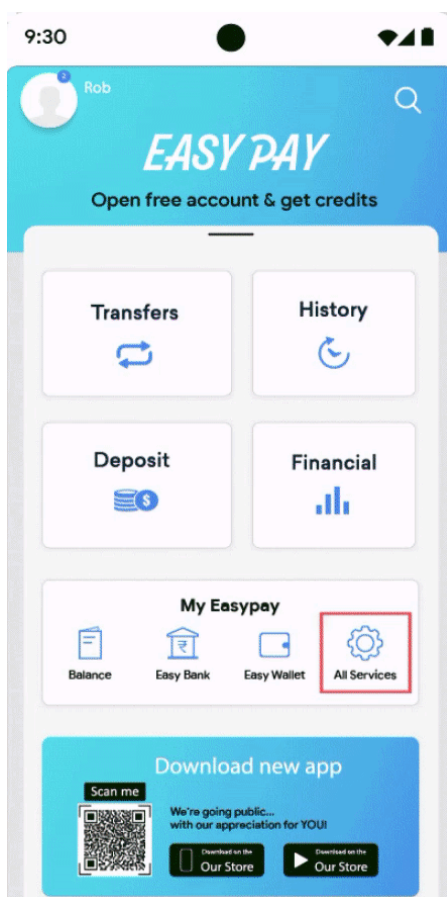
① 這款應用程式中的問號圖示是廣告，會將使用者導向外部到達網頁。

- 仿冒系統通知的廣告：





① ② 以上是仿冒不同系統通知的廣告示例。



① 上方示例中的功能專區雖然看起來與其他功能類似，但實際上只會將使用者導向一或多則廣告。

干擾性廣告

干擾性廣告是指以異常方式對使用者顯示廣告，可能導致使用者無意間點按廣告，或是影響、干擾裝置功能的可用性。

應用程式不得強迫使用者以點按廣告或提供個人資訊 (用於廣告目的) 的方式換取完整體驗。廣告 (包括重疊廣告、分享元件功能或小工具化廣告單元) 只能顯示在放送廣告的應用程式中，不得干擾其他應用程式、廣告或裝置運作，包括系統或裝置的按鈕和連接埠。如果應用程式顯示會干擾正常使用行為的廣告，開發人員必須讓使用者能在不損及任何權益的情況下輕易關閉廣告。

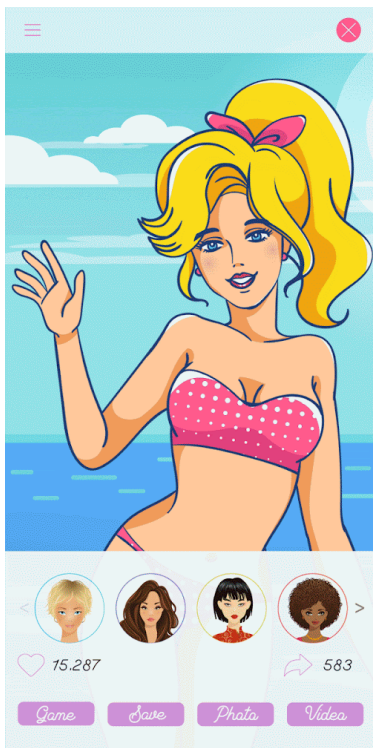
以下是常見的違規情況：

- 廣告占據整個螢幕畫面或干擾正常使用行為，且未提供明確的關閉方式：

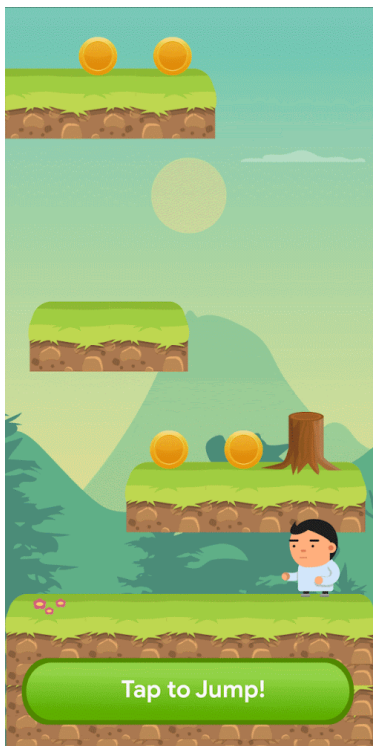


① 廣告未顯示關閉按鈕。

- 廣告使用假的關閉按鈕，或突然顯示在使用者會點按的其他應用程式功能區域，藉此強迫使用者點閱：

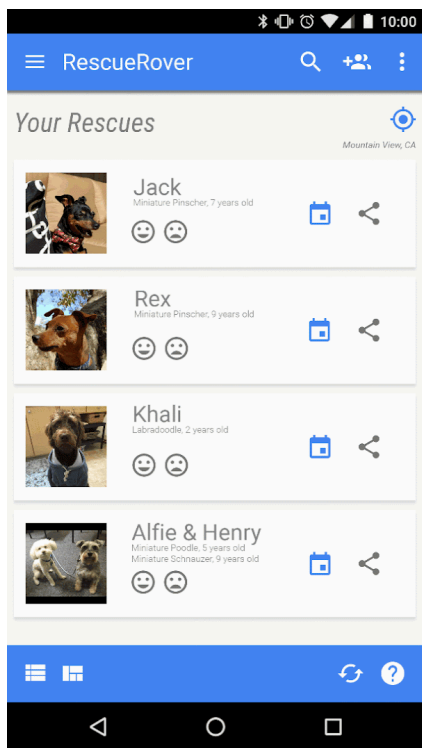


① 廣告使用假的關閉按鈕。



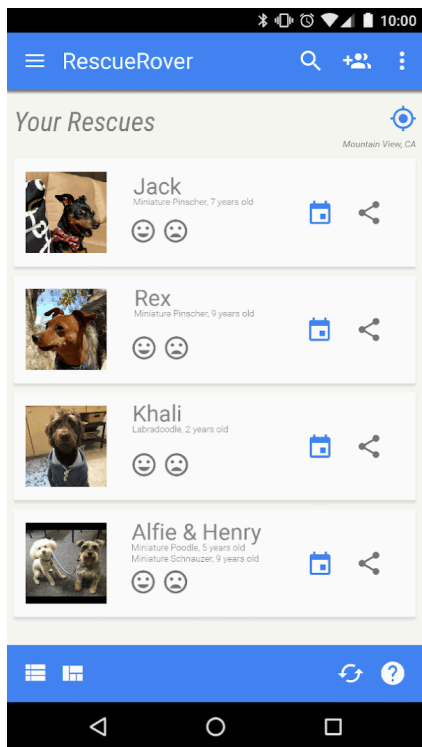
② 廣告突然顯示在使用者會點按的應用程式功能區域。

- 在放送廣告的應用程式外顯示廣告：



① 使用者從這個應用程式切換至主畫面，廣告就突然出現在主畫面上。

- 在使用者輕觸主畫面按鈕或專為退出應用程式設計的其他功能後放送廣告：



① 使用者嘗試退出應用程式並切換至主畫面，但操作過程因廣告而中斷。

優質廣告體驗

開發人員必須遵守下列廣告規範，確保使用者在使用 Google Play 應用程式時獲得優質體驗。不得透過以下這些非預期的方式顯示廣告：

- 禁止以非預期的方式 (通常是在使用者選擇做其他事時) 顯示任何格式 (影片、GIF、靜態等) 的全螢幕插頁式廣告。
- 禁止在遊戲中的某個關卡或內容片段開始時顯示廣告。

- 禁止在應用程式的載入畫面 (啟動畫面) 之前顯示全螢幕影片插頁式廣告。
- 禁止任何格式的全螢幕插頁式廣告在顯示 15 秒後無法關閉。使用者選擇開啟或不會干擾使用者操作 (例如在遊戲應用程式的得分畫面後出現) 的全螢幕插頁式廣告可以持續顯示超過 15 秒時間。

這項政策不適用於使用者明確選擇開啟的獎勵廣告 (例如開發人員明確提供給使用者觀看，用來換取解鎖特定遊戲功能或內容片段等獎勵的廣告)，也不適用於不會干擾使用者正常使用應用程式或玩遊戲的營利和廣告內容 (例如包含整合式廣告的影片內容、非全螢幕橫幅廣告)。

以上規範是參照[廣告體驗提升標準 - 行動應用程式體驗](#) 規範所制定。如要進一步瞭解廣告體驗提升標準，請造訪[廣告體驗提升聯盟](#)。

以下是常見的違規情況：

- 在遊戲過程中或內容片段開始時無預期出現的廣告 (例如，在使用者點選某個按鈕後，以及點選按鈕的預期效果出現前)。由於使用者原本是要玩遊戲或查看相應內容，所以這些廣告對他們來說很出乎意料。

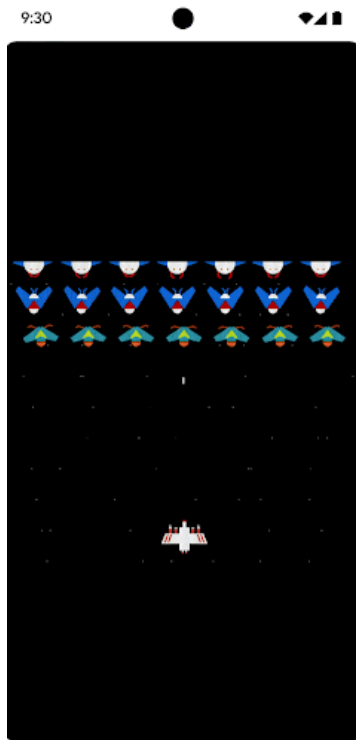


- ① 在遊戲關卡開始時突然出現的靜態廣告。



② 在內容片段開始時突然出現的影片廣告。

- 在遊戲過程中出現，而且無法在 15 秒後關閉的全螢幕廣告。



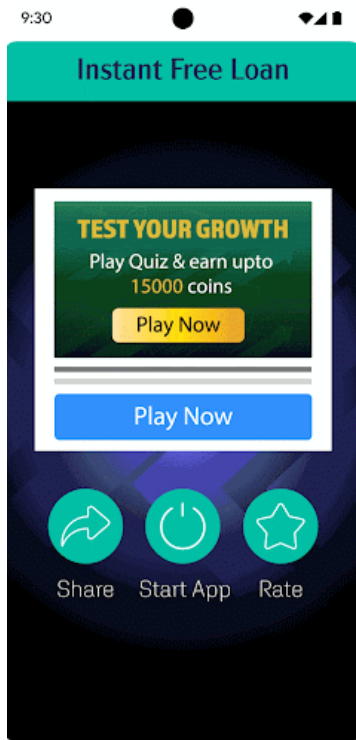
① 在遊戲過程中顯示插頁式廣告，而且未在 15 秒後提供略過廣告的選項。

廣告用途

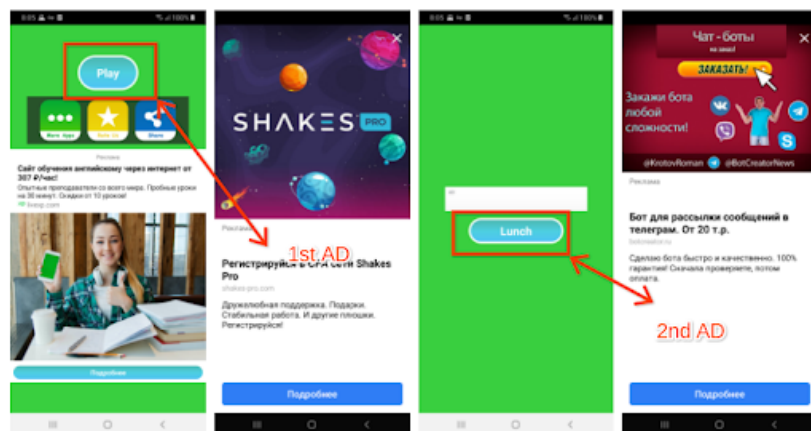
我們禁止應用程式重複顯示會干擾使用者操作應用程式及在應用程式中執行作業的插頁式廣告。

以下是常見的違規情況：

- 在使用者操作 (包括但不限於點擊、滑動等) 後連續放送插頁式廣告的應用程式。



① 第一個應用程式內頁面有多個互動按鈕。當使用者點選「Start app (啟動應用程式)」來使用應用程式，畫面上就會彈出插頁式廣告。使用者在關閉該廣告後返回了應用程式，接著點選「Service (服務)」來使用服務，結果出現了另一則插頁式廣告。



② 第一個頁面上只有「Play (開始遊戲)」按鈕，就是在引導使用者點選這個按鈕。當使用者點選後按鈕，畫面上出現了插頁式廣告。使用者在關閉廣告後又點選了唯一顯示的「Launch (啟動)」按鈕，結果出現了另一則插頁式廣告。

利用螢幕鎖定功能營利

除了專為螢幕鎖定功能開發的應用程式之外，其他應用程式不得提供透過裝置鎖定畫面營利的廣告或功能。

廣告詐欺

我們嚴禁廣告詐欺行為。詳情請參閱「[廣告詐欺](#)」政策。

將位置資料用於廣告

如果應用程式有權使用裝置位置資料，且會進一步使用該資料放送廣告，除須遵循[個人和機密資訊](#)政策的規範外，還須符合下列規定：

- 應用程式須在隱私權政策中向使用者明確揭露將使用或收集裝置的位置資料，並會依此放送廣告，且須提供相關廣告聯播網的隱私權政策連結。
- 根據[位置存取權](#)政策規定，要求位置存取權的目的僅限於執行應用程式中現有的功能或服務，如果廣告是唯一目的，則不得要求使用者授予權限。

Android 廣告 ID 的使用方式

Google Play 服務 4.0 版導入了最新 API 和廣告 ID，可供廣告及分析服務供應商使用。這類 ID 的使用條款如下。

- **使用方式。**Android 廣告 ID (AAID) 只能用於放送廣告及分析使用者數據。每次存取廣告 ID 時，「停用按照興趣顯示的廣告」或「停用廣告個人化」設定的狀態都必須經過驗證。
- **與個人識別資訊或其他 ID 之間的關聯。**
 - 廣告用途：廣告 ID 不得基於任何廣告目的與永久裝置 ID (例如 SSAID、MAC 位址、IMEI 等) 建立關聯，只能在經使用者明確同意的情況下與個人識別資訊建立連結。
 - 分析用途：不得基於任何分析目的，將廣告 ID 與個人識別資訊建立連結，或與任何永久裝置 ID (例如 SSAID、MAC 位址、IMEI 等) 建立關聯。如需瞭解有關永久裝置 ID 的其他規範，請參閱[使用者資料政策](#)。
- **尊重使用者的選擇。**
 - 廣告 ID 經過重設後，在未經使用者明確同意下，新 ID 不得與舊 ID 本身或其衍生資料建立連結。
 - 您的廣告放送方式必須符合使用者的「停用按照興趣顯示的廣告」或「停用廣告個人化」設定。如果使用者啟用上述設定，您就不得使用廣告 ID 建立放送廣告所需的設定檔，或針對使用者放送個人化廣告。允許使用的功能包括內容相關廣告、展示頻率上限、轉換追蹤、報表與安全性，以及詐騙偵察。
 - 如果使用者在新裝置上刪除 Android 廣告 ID，系統就會移除這組 ID。屆時若嘗試存取這組 ID，就會收到一串零。沒有廣告 ID 的裝置不得與連結或衍生自舊廣告 ID 的資料建立連結。
- **善盡告知責任：**廣告 ID 的蒐集和使用行為，以及遵守這些條款的相關義務，必須透過符合法律規範的隱私權聲明向使用者揭露。如要進一步瞭解 Google 的隱私權標準，請參閱我們的[使用者資料](#) 政策。
- **遵守使用條款。**使用廣告 ID 時，請務必遵守《Google Play 開發人員計畫政策》；如果因業務需求與任何第三方分享廣告 ID，對方同樣必須遵守這些條款。如果裝置上有廣告 ID，上傳或發布至 Google Play 的應用程式必須使用這個 ID 放送廣告，不得使用其他裝置 ID。

詳情請參閱「[使用者資料](#)」政策。

訂閱

開發人員不得對應用程式中的任何訂閱服務或內容，提供會誤導使用者的資訊。如果應用程式含有宣傳廣告、啟動畫面和訂閱方案選擇畫面，請務必在當中清楚傳達訊息。應用程式在使用者購物時 (包含應用程式內商品或訂閱方案)，不得採取欺騙或操弄的手段。您提供的[訂閱福利](#)必須完全符合實際情況，相關訂閱方案的任何環節不得有不實陳述。

您必須提供公開透明的優惠資訊，包括清楚且明確揭露優惠條款、訂閱費用、帳單週期、自動續訂條款、應用程式是否必須訂閱才能使用，以及其他與訂閱方案相關的重要資訊。這些資訊應可直接查看，不需要使用者額外執行操作。

訂閱項目必須在訂閱期間持續或定期為使用者帶來價值，不得用於提供實際上只會讓使用者享有一次福利的內容 (例如 SKU 僅提供一筆應用程式內抵免額/貨幣，或者只能使用一次的遊戲強化道具)。您的訂閱項目可提供獎勵或促銷紅利，但這些內容必須與訂閱期間持續或定期產生的價值相輔相成。若產品並未持續或定期貢獻價值，就必須設為[應用程式內商品](#)，而非[訂閱產品](#)。

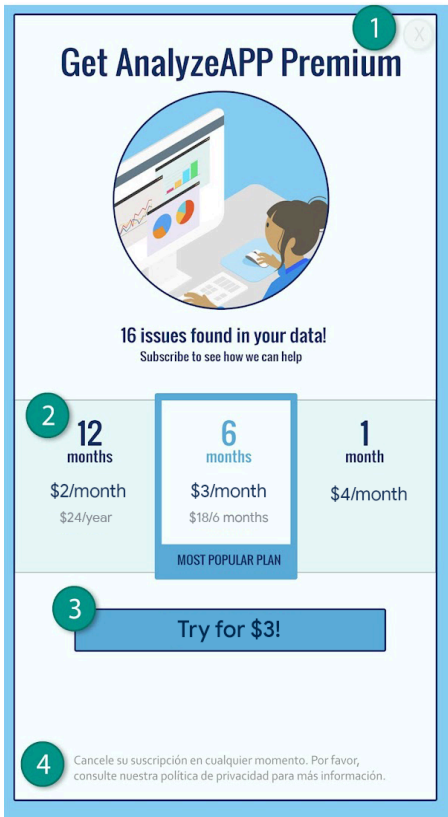
您不得掩飾或不當描述一次性福利，讓使用者誤以為這是訂閱項目。如果在使用者購買訂閱方案後，將方案修改為一次性產品 (例如取消、不再提供或盡可能縮減定期產生的價值)，亦屬違規。

以下是常見的違規情況：

- 未告知使用者：按月訂閱項目每個月會自動續訂並收費。
- 按年訂閱項目，卻用很顯眼的月費標示價格。

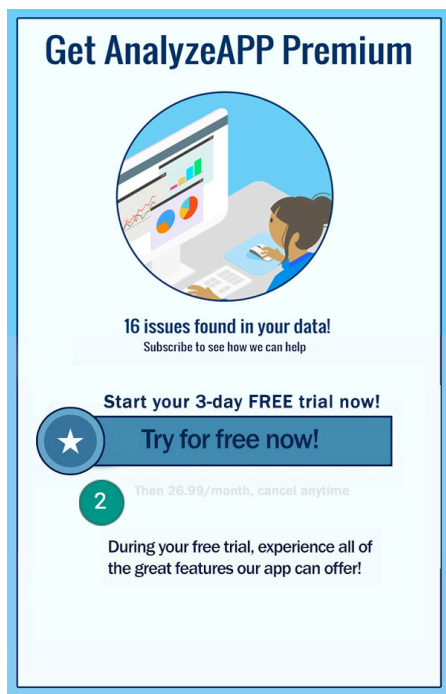
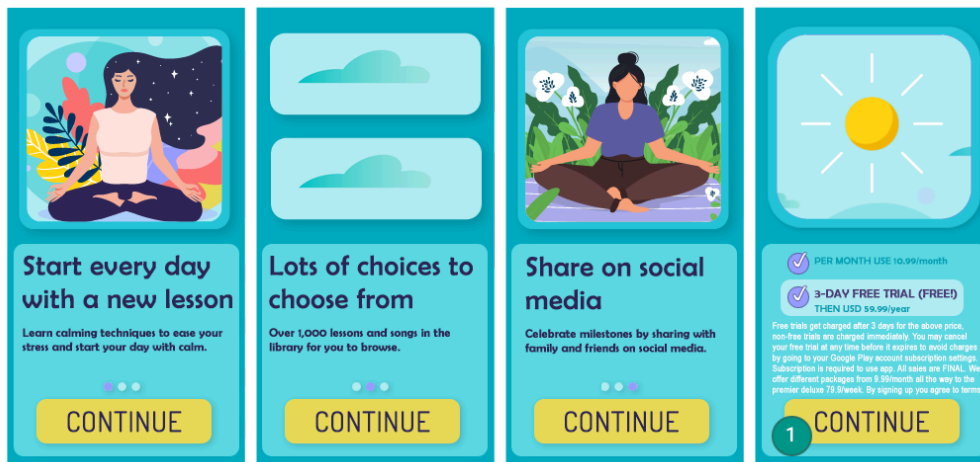
- 訂閱項目的定價資訊和條款僅有部分內容完成本地化。
- 應用程式內宣傳廣告並未清楚說明，使用者不需訂閱也能存取內容 (如適用)。
- SKU 名稱未準確表達訂閱項目的性質，例如名稱中包含「免費試用」或「免費享有 3 天付費會員資格」，實際上系統卻會自動針對訂閱項目定期收費。
- 購買流程中有多個畫面會引導使用者意外點選訂閱按鈕。
- 訂閱項目未持續或定期貢獻價值，例如在訂閱期間首月先提供 1,000 個寶石，後續幾個月卻將福利縮減為 1 個寶石。
- 要求使用者必須申請自動續訂才能享有一次性福利，以及在使用者購買後未經當事人要求就取消訂閱項目。

示例 1：



- ① 關閉按鈕不存在或不明顯，使用者可能不清楚可以直接使用功能，而不必接受訂閱優惠。
- ② 優惠刻意凸顯每月分攤下來的費用，而不是列出使用者實際須支付的金額。他們可能不清楚在訂閱當下就必須支付六個月的費用。
- ③ 優惠只顯示新用戶優惠價，因此使用者可能不清楚在新用戶優惠期結束後，系統會自動向他們收取多少費用。
- ④ 優惠不合規定，不像條款及細則，優惠用語和幣別未根據使用者所在國家/地區進行本地化，導致他們不清楚優惠的完整細節。

示例 2：



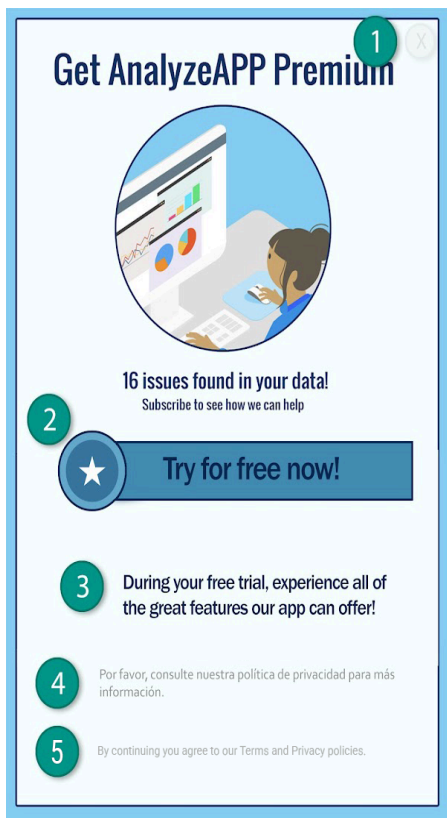
- ① 需要反覆點選同一個按鈕區，導致使用者不小心按下最後的「繼續」按鈕而訂閱。
- ② 試用期結束後須支付的費用不明顯，導致使用者誤以為是免付費方案。

免費試用與新用戶優惠

在使用者註冊訂閱方案前：您必須如實清楚敘述優惠條款，包括可存取內容或服務的時限、定價和說明。請務必向使用者說明免付費試用轉換為付費訂閱的方式和時間、付費訂閱費用，以及不想轉換時可如何取消。

以下是常見的違規情況：

- 優惠內容未清楚說明免費試用期限或新用戶優惠效期。
- 優惠內容未清楚說明優惠期結束後，系統會自動為使用者註冊付費訂閱項目。
- 優惠內容未清楚說明使用者可直接存取內容，不必申請試用（如有）。
- 優惠定價和條款未完全本地化。



- ① 關閉按鈕不存在或不明顯，使用者可能不清楚可以不必接受訂閱優惠，直接使用功能。
- ② 優惠強調免費試用，因此使用者可能不清楚在試用期結束後，系統會自動向他們收取費用。
- ③ 優惠未註明試用期，因此使用者可能不清楚可免費存取訂閱內容的期間。
- ④ 優惠不合規定，不像條款及細則，優惠用語言和幣別需根據使用者所在國家/地區進行本地化，導致他們不清楚優惠的完整細節。
- ⑤ 優惠未清楚說明免費試用期結束後，不想繼續付費訂閱的取消方式。

訂閱管理、退訂及退款

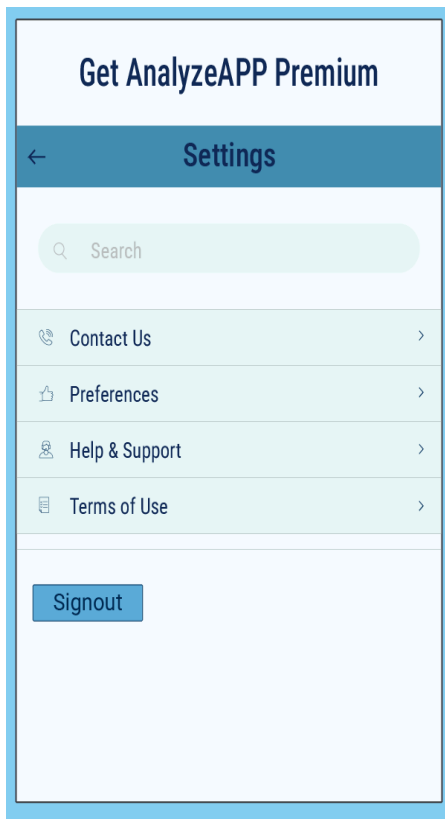
如果您在應用程式中販售訂閱內容，請務必確保應用程式明確揭露使用者可以如何管理訂閱內容或取消訂閱。您也必須在應用程式中提供方便在線上取消訂閱的做法。如要符合這項規定，您可以在應用程式的帳戶設定 (或相應頁面) 中加入：

- Google Play 訂閱中心的連結 (若為採用 Google Play 結帳系統的訂閱方案)；以及/或是
- 直接進入取消程序的途徑。

我們的一般政策規定，如果使用者取消了透過 Google Play 帳單系統購買的訂閱內容，無論在哪一天退訂，他們在當前帳單週期的剩餘期間內仍能繼續取得訂閱內容，所以無法獲得當前帳單週期的退款。使用者取消訂閱的動作會在下一個帳單週期生效。部分國家/地區的使用者可根據適用法律立即取消訂閱，並收到按比例退還的款項。

您是內容或權限的提供者，可以直接向使用者訂定更有彈性的退款政策。訂閱、退訂和退款政策如有異動，您有責任通知使用者，並確保合乎適用法律。

以下是常見的違規情況：



應用程式的帳戶設定或對應頁面，缺少用來管理和取消訂閱的連結。

家庭自我認證廣告 SDK 計畫

如果您的應用程式會放送廣告，而且僅指定兒童 (依[家庭政策](#) 的定義) 為目標對象，那麼您使用的廣告 SDK 版本一律必須經過自我認證符合 Google Play 政策，包括下方的家庭自我認證廣告 SDK 規定。

如果應用程式同時以兒童和年齡較大的使用者為目標對象，您必須確保向兒童放送的廣告全都來自通過自我認證的廣告 SDK 版本，可採取的做法包括使用非誘導性年齡選擇畫面。

請注意，您有責任確保應用程式中使用的每個 SDK 版本 (包括完成自我認證的廣告 SDK 版本) 均符合所有適用的政策、當地法律和法規。Google 無法聲明或保證廣告 SDK 在自我認證程序中提供的資訊完全準確。

只有在應用程式會使用廣告 SDK 向兒童放送廣告的情況下，您才必須使用家庭自我認證廣告 SDK。以下是廣告 SDK 可免除向 Google Play 進行自我認證的情況。不過，您仍有責任確保廣告內容和資料蒐集做法符合 Google Play 的[使用者資料政策](#) 和[家庭政策](#) 規定：

- 在版位自用廣告中，使用 SDK 來管理您的應用程式或其他自有媒體和商品間的交叉宣傳內容。
- 與廣告客戶進行直接交易時，將 SDK 用於廣告空間管理。

家庭自我認證廣告 SDK 規定

- 定義何謂不當廣告內容和行為，並在廣告 SDK 的條款或政策中禁止這類內容和行為。這些定義應符合《Google Play 開發人員計畫政策》。
- 制定一套將廣告素材依適當年齡層進行分級的方法，級別至少要包含適合「所有人」和「成人」。分級法必須與 Google 為填寫以下意願調查表的供應商所提供的 SDK 分級法一致。
- 允許發布商依個別要求或個別應用程式，針對廣告放送提出兒童導向內容要求。這類內容必須遵守適用的法律及法規，例如美國《[兒童網路隱私保護法 \(COPPA\)](#)》和歐盟《[一般資料保護規則 \(GDPR\)](#)》的規定。Google Play 規定廣告 SDK 不得在兒童導向內容中顯示個人化廣告、按照興趣顯示廣告及進行再行銷。
- 允許發布商選取符合 Google Play [家庭版廣告與營利政策](#) 的廣告格式，並遵守[教師認可評估計畫](#) 的規定。

- 使用即時出價功能對兒童放送廣告時，請確保放送的廣告素材已通過審核，並將隱私權指標套用至出價工具。
- 向 Google 提供充分的資訊 (例如提交測試版應用程式和下方[意願調查表](#) 中所列的資訊)，驗證廣告 SDK 符合所有自我認證政策規定，並在 Google 後續要求提供任何資訊時及時回覆；比如，您可能需要提供新版本，用於驗證廣告 SDK 版本符合所有自我認證規定。
- 進行[自我認證](#)，確保所有新版本符合最新的《Google Play 開發人員計畫政策》，包括《家庭政策》規定。

注意：家庭自我認證廣告 SDK 在放送廣告時，必須遵守所有可能適用於其發布商的兒童相關法令和法規。

如要進一步瞭解如何將廣告素材加上浮水印及提供測試版應用程式，請參閱[這篇文章](#)。

以下是向兒童放送廣告時，放送平台須遵守的中介服務規定：

- 僅使用家庭自我認證廣告 SDK，或採取必要的保護措施，確保透過中介服務放送的所有廣告均符合相關規定。
- 傳送必要的資訊至中介平台，指明廣告內容分級和任何適用的兒童導向內容。

開發人員可以按[這裡](#) 瀏覽家庭自我認證廣告 SDK 清單，並查看相關廣告 SDK 有哪些特定版本已通過自我認證，可用於闔家適用應用程式。

此外，開發人員可以將這份[意願調查表](#) 提供給有意完成廣告 SDK 自我認證的供應商。

商店資訊與宣傳

應用程式的宣傳方式和能見度對於商店品質大有影響。請避免在商店資訊中使用垃圾內容，或進行品質低劣的促銷活動，也不得以人為方式提高應用程式在 Google Play 中的能見度。

應用程式宣傳廣告

任何直接或間接涉及欺騙性行為，或是會對使用者或開發人員產業環境造成傷害的宣傳手法 (例如廣告)，都不得出現在應用程式中，我們也禁止應用程式從這類活動中直接或間接受益。但凡宣傳手法的行為或內容違反《開發人員計畫政策》規定，即視同具欺騙性或危害性。

以下是常見的違規情況：

- 在網站、應用程式或其他資源 (包括模擬系統通知或快訊的訊息) 中透過[欺騙性](#) 的廣告進行宣傳。
- 以[煽情露骨](#) 的廣告將使用者導向應用程式的 Google Play 商店資訊進行下載。
- 利用不當宣傳或安裝手法，在未告知使用者的情況下，將對方重新導向至 Google Play 或是下載應用程式。
- 透過簡訊服務散布來路不明的宣傳內容。
- 在應用程式名稱、圖示或開發人員名稱中加入文字或圖片，用於指出在商店的表現或排名、表明價格或促銷資訊，或者暗示與現有 Google Play 計畫的關係。

您有責任確保與自家應用程式相關的廣告聯播網、關係企業或廣告均遵守這些政策。

中繼資料

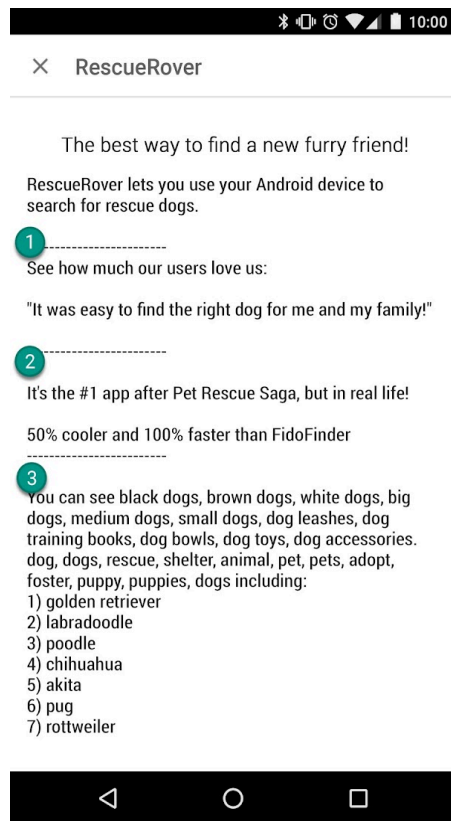
應用程式說明可協助使用者瞭解應用程式的功能和用途。我們禁止應用程式使用誤導性、格式錯誤、非敘述性、不相關、大量或不當的中繼資料，包括但不限於應用程式說明、開發人員名稱、應用程式名稱、圖示、螢幕截圖和宣傳圖片。開發人員必須提供清楚完善的應用程式說明，且不得在應用程式說明中加入未註明來源或匿名的使用者推薦文。

對使用者而言，您的應用程式名稱、圖示和開發人員名稱十分有助於他們找到及瞭解您的應用程式。請勿在這些中繼資料元素中使用表情符號或重複的特殊字元。除了品牌名稱外，請避免使用全大寫字母。應用程式圖示不得使用具誤導性的標誌或符號，例如：在沒有新訊息的情況下出現指明新訊息的圓點標誌，或是在與下載內容無關的應用程式中顯示下載/安裝符號。應用程式名稱長度上限為 30 個字元。請勿在應用

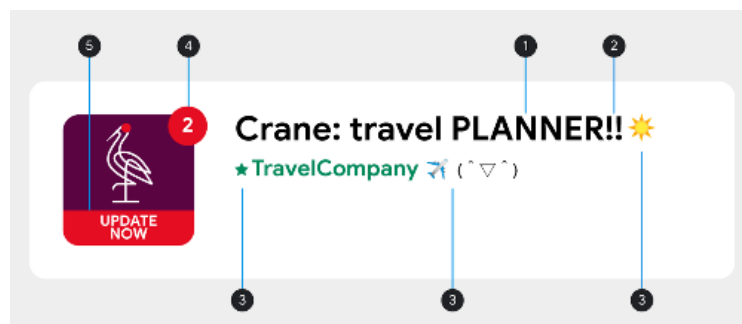
程式名稱、圖示或開發人員名稱中加入文字或圖片，用於指出在商店的表現或排名、表明價格或促銷資訊，或者暗示與現有 Google Play 計畫的關係。

除了此處提及的規定外，您可能還必須依特定 Google Play 開發人員政策的規定提供其他中繼資料資訊。

以下是常見的違規情況：



- ① 未註明來源或匿名的使用者推薦文
- ② 多個應用程式或品牌的資料比較
- ③ 文字方塊和直向/橫向字詞清單



- ① 不屬於品牌名稱的部分使用全大寫字母
- ② 與應用程式無關的特殊字元序列
- ③ 使用表情符號 (包含日文表情符號) 和特殊字元
- ④ 具誤導性的符號
- ⑤ 具誤導性的文字

- 表明商店成效或排名的圖片或文字，例如「年度應用程式」、「第 1 名」、「20XX 年 Play 精選」、「熱門」、獲獎圖示等



It's Magic - #1 in magic games

Top Free Games.
4.5 ★



Music Player - Best of Play

Super Play.
4.5 ★



Jackpot - Best Slot Machine

Slot Games.
4.5 ★



Rewards Game

RT Games.
3.5 ★

- 表明價格或促銷資訊的圖片或文字，例如「10% 折扣」、「\$50 美元現金回饋」、「限時免費」等



O Basket - \$50 Cashback

Digital Brand.
4.5 ★



Gmart - On Sale For Limited Time

Shop Limited.
4.3 ★



Fish Pin- Free For Limited Time Only

Entertainment Play.
4.5 ★



Golden Slots Fever: Free 100

Gamepub Play.
4.2 ★

- 表明 Google Play 計畫的圖片或文字，例如「編輯精選」、「新上架」等



Build Roads - New Game

KDG Games.
3.5 ★



Robot Game - Editor's choice

Entertainment Games.
4.5 ★

以下列舉商店資訊中禁用的不當文字、圖片或影片：

- 包含性暗示內容的圖像或影片。請避免使用含乳房、臀部、生殖器等帶有性挑逗意味的圖像，或者透過繪圖或真實影像呈現以戀物角度描繪的身體部位或內容。
- 在應用程式的商店資訊中使用不雅、粗俗或其他不適合一般大眾的用語。
- 包含大量暴力內容的應用程式圖示、宣傳圖片或影片。
- 描述違法使用藥品的內容。商店資訊中呈現的內容必須適合各年齡層的目標對象，即使是 EDSA (教育、紀錄、科學或藝術) 內容亦然。

以下例示幾種最佳做法：

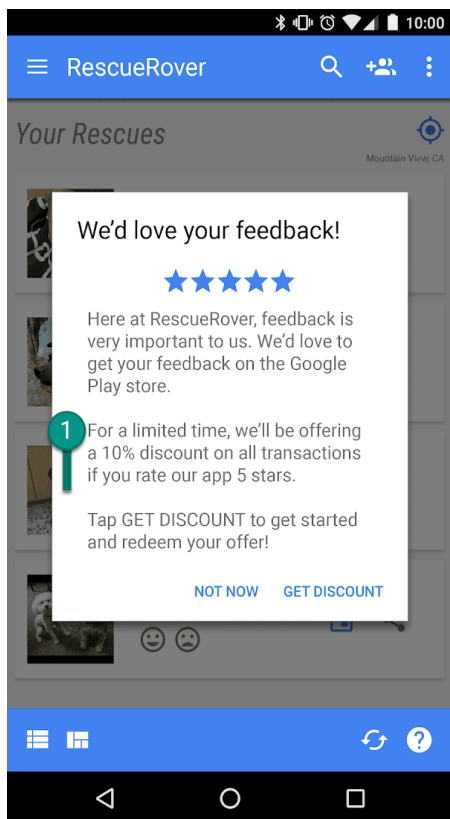
- 凸顯應用程式的優點，說明您的應用程式有何有趣和令人期待之處，協助使用者瞭解您應用程式的特點為何。
 - 確認應用程式的名稱和說明可以如實表達應用程式的功能。
 - 避免使用重複或不相關的關鍵字或提及其他無關的內容。
 - 應用程式的說明務求簡潔明瞭。簡短一點的說明往往能讓使用者覺得更容易閱讀，對於螢幕較小的裝置而言尤其如此。文字過於冗長、太過詳盡、格式不當或是內容重複，都可能會違反這項政策。
 - 提醒您，商店資訊應適合一般大眾瀏覽。請避免在商店資訊中加入不當文字、圖片或影片，並遵守上述規範。
-

使用者評分、評論與安裝次數

開發人員不得試圖操控任何應用程式在 Google Play 的顯示位置，包括但不限於以不正當手段，為產品評分、評論或安裝次數灌水，例如製造不實的評論和評分、透過獎勵條件換取評論及評分，或者應用程式的主要功能是利誘使用者安裝其他應用程式。

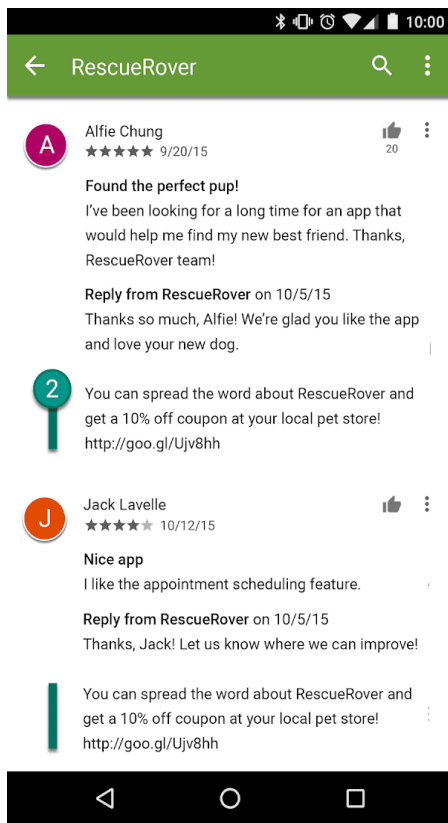
以下是常見的違規情況：

- 以獎勵為誘因，吸引使用者為您的應用程式評分：



① 這則通知向使用者提供折扣優惠，換取良好評分。

- 冒充使用者重複提交評分，影響應用程式在 Google Play 的顯示位置。
- 自行提交或鼓吹使用者提交含有不當內容的評論，包括關係企業、優待券、遊戲代碼、電子郵件地址或網站/其他應用程式的連結。



② 這則評論透過提供優惠券，鼓勵使用者宣傳 RescueRover 應用程式。

評分和評論是衡量應用程式品質的基準，必須真實且具有關聯性，對使用者而言才具有參考價值。以下列舉回應使用者評論的一些最佳做法：

- 請務必針對導致使用者如此評論的問題本身給予回覆，請勿要求使用者給予更高的評分。
- 加入實用資源的參考資訊，例如支援團隊電子郵件地址或常見問題的網頁。

內容分級

Google Play 採用**國際年齡分級聯盟 (IARC)** 的分級機制，與各地制度對應，方便開發人員向當地使用者說明相應的分級辦法。各地 IARC 機關負責制定規範，用以判斷應用程式內容的適合年齡；沒有內容分級的應用程式不得在 Google Play 上架。請注意，應用程式中所有廣告內容的年齡分級均不得明顯高於應用程式主要內容。詳情請參閱「**不當廣告**」政策。

內容分級機制的用途

內容分級是用來告知消費者 (特別是家長) 特定應用程式中可能含有不當內容，同時也可協助我們依法針對特定地區或特定使用者過濾或封鎖您的內容，以及評估您的應用程式是否符合特殊開發人員計畫資格。

內容分級指派方式

如要取得內容分級，您必須填寫 **Play 管理中心** 的**內容分級問卷**，說明您應用程式的內容性質。系統會根據您的問卷填答內容，從多間分級機構的機制中找出相符內容分級，再指派給您的應用程式。如果對應用程式的內容有任何不實描述，可能會導致應用程式遭到下架或停權，因此請務必據實回答內容分級問卷中的問題。

為了避免系統將您的應用程式列為「未分級」，您必須為應用程式填寫內容分級問卷；不論是提交到 Play 管理中心的應用程式，還是在 Google Play 上架的應用程式，都包括在內。我們會將沒有內容分級的應用程式從 Play 商店下架。

如果應用程式內容或功能有異動，會改變您在內容分級問卷的填答內容，請前往 [Play 管理中心](#) 重新提交內容分級問卷。

指派給應用程式的內容分級取決於應用程式內容，而非消費者協議或廣告等其他功能和做法。如有其他視年齡而定的注意事項 (例如特定年齡的隱私權實務規範)，您必須負責通知使用者。

如需更多問卷相關資訊，請前往 [說明中心](#) 瞭解各區的不同 [分級機構](#)，以及如何填寫分級問卷。

內容分級申訴

如果您不認同您的應用程式獲派的分級，可以使用分級認證電子郵件中提供的連結，直接向 IARC 分級機構提出申訴。

新聞與雜誌

所有新聞與雜誌應用程式，都必須在 Google Play 管理中心完成自我聲明。

這類應用程式的特徵如下：

- 在 Google Play 管理中心聲明本身為「新聞」或「雜誌」應用程式；或
- 在 Google Play 商店中歸類為「新聞與雜誌」，且在應用程式名稱、圖示、開發人員名稱或說明中，描述本身屬於「新聞」或「雜誌」類

如要進一步瞭解「新聞」或「雜誌」應用程式的資格條件，請見「[新聞和新聞相關應用程式的規定](#)」一文。

此外，新聞與雜誌應用程式也必須：

- 提供新聞與雜誌文章的來源，包括但不限於每篇文章的原始出版商或作者。
 - 定期更新本身內容 (不能用靜態內容)。
 - 為使用者提供清楚又簡單的管道，讓他們能取得新聞與雜誌應用程式的最新聯絡資訊。
 - 為使用者提供清楚的資訊，說明第三方內容的發布來源 (例如由新聞與雜誌集結應用程式提供)。
 - 讓使用者可以先預覽應用程式內容再購買 (如需入會或訂閱)。
 - 確保主要目的不是聯盟行銷或廣告收益。
-

垃圾內容、功能和使用者體驗

應用程式應至少提供使用者所需的基本功能和內容，帶來愉快的使用者體驗。如果應用程式會異常終止、出現不符合正常使用者體驗的其他行為，或者只會對使用者/Google Play 發布垃圾內容，則我們認為增列這類應用程式並無意義。

垃圾內容

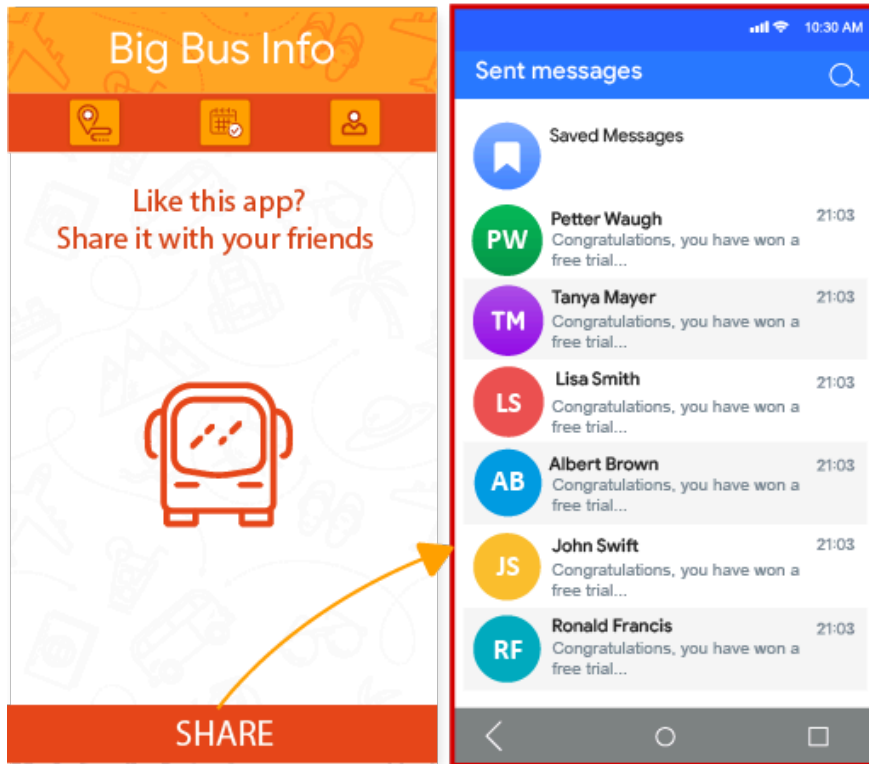
我們禁止應用程式向使用者或在 Google Play 中發布垃圾內容；舉例來說，應用程式不得擅自向使用者傳送重複或劣質的內容。

垃圾訊息

我們禁止任何應用程式在未經使用者確認內容和收件者的情況下，擅自以使用者名義傳送簡訊、電子郵件或其他訊息。

以下是常見的違規情事：

- 如果使用者按下 [分享] 按鈕，這款應用程式不會先讓使用者確認內容和收件者，而會直接以使用者的名義傳送簡訊：

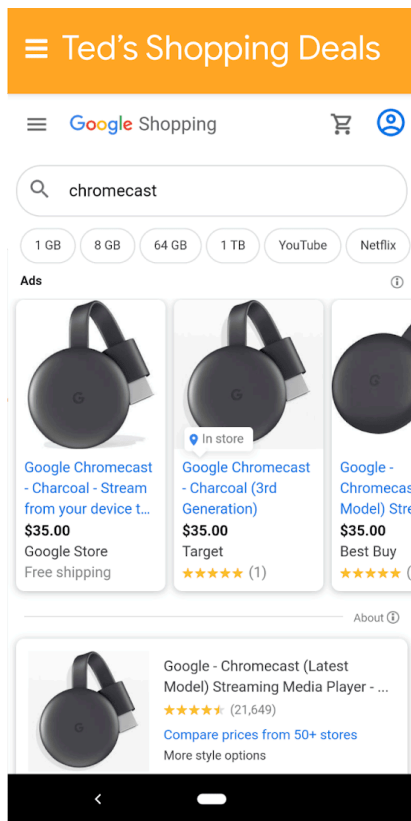


垃圾流量和關聯企業垃圾內容

我們禁止任何應用程式在未經網站擁有者或管理員許可的情況下，專門為網站吸引關聯流量或提供網站的網頁畫面。

以下是常見的違規情況：

- 專門為網站吸引參照連結網址流量，進而就使用者在該網站的訂閱或消費行為獲取功勞的應用程式。
- 在未經許可的情況下，專門提供網站網頁畫面的應用程式：



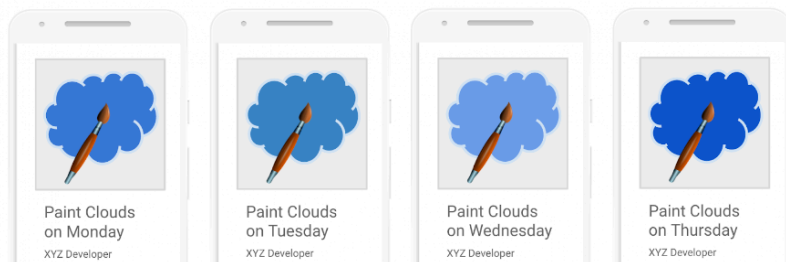
① 這款應用程式的名稱為「阿泰的購物優惠」，但其中只提供 Google 購物的網頁畫面。

重複內容

我們禁止應用程式單純提供與其他 Google Play 既有應用程式相同的功能。應用程式必須打造獨特的內容或服務，為使用者帶來價值。

以下是常見的違規情況：

- 複製其他應用程式的內容，而未添加任何原創內容或價值。
- 製作多款擁有高度相似功能、內容和使用者體驗的應用程式。如果這些應用程式都只有少量內容，開發人員應考慮將所有內容整合在單一應用程式中。



功能、內容和使用者體驗

應用程式應提供穩定可靠、引人入勝且操作順暢的使用者體驗。應用程式若會異常終止、不具備行動應用程式應有的基本實用功能、缺乏吸引人的內容，或出現不符合正常良好使用者體驗的其他行為，就不得在 Google Play 上架。

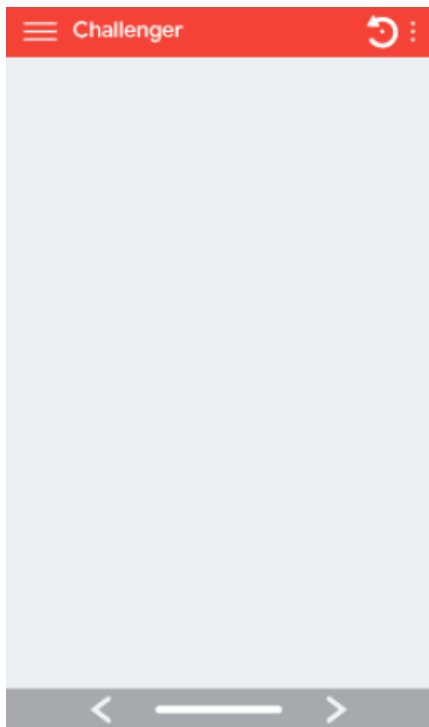
有限功能與內容

應用程式不得僅提供有限功能與內容。

以下是常見的違規情事：

- 應用程式呈現靜態內容且缺少專屬功能，比如只能顯示文字或開啟 PDF 檔案

- 應用程式只有極少內容，未提供吸引人的使用者體驗，例如單一桌布應用程式
- 應用程式沒有任何功能或功用

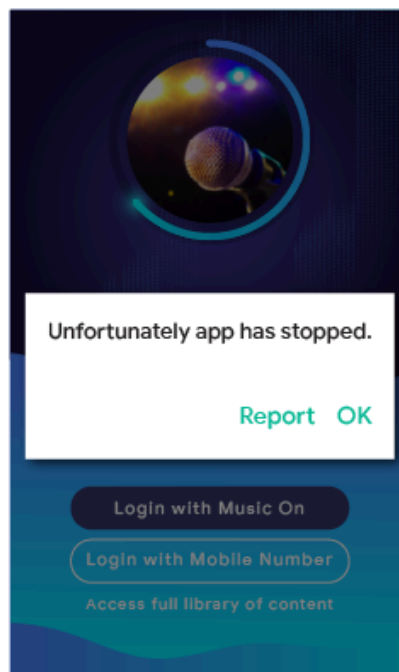
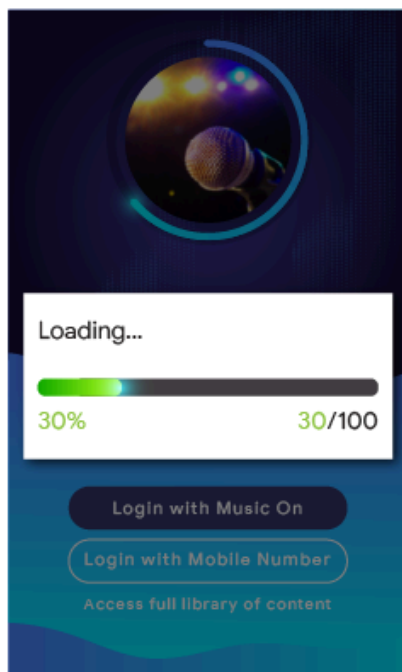


功能異常

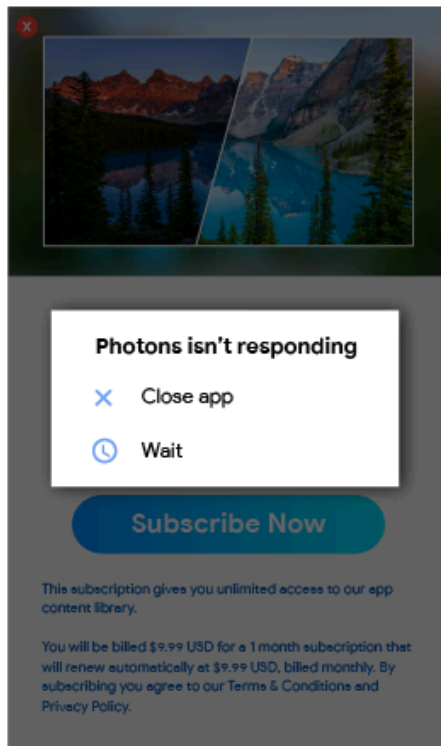
我們不允許應用程式持續出現當機、強制關閉、卡住或其他功能異常的情況。

以下是常見的違規情況：

- 應用程式無法安裝
- 應用程式安裝後無法載入



- 應用程式載入後沒有回應



其他計畫

如果開發人員透過 Google Play 發布了其他類型的 Android 應用程式，那麼除了政策中心所載的其他內容政策外，還可能必須遵守相關計畫的政策規定。請務必查看下方清單，確認您的應用程式是否應符合其中任何政策的規定。

Android 免安裝應用程式

Android 免安裝應用程式的開發宗旨是創造令人滿意而沒有障礙的使用體驗，同時仍提供最高標準的隱私權和安全性保障。設立相關政策的用意，就是為了達成這個目標。

如果開發人員選擇透過 Google Play 發布 Android 免安裝應用程式，就必須遵守下列政策及所有其他《[Google Play 開發人員計畫政策](#)》。

身分識別

如果免安裝應用程式包含登入功能，開發人員就必須在其中整合[密碼專用 Smart Lock](#)。

支援連結

開發人員必須讓自己的 Android 免安裝應用程式能夠正確連結到其他應用程式。如果開發人員的免安裝應用程式或需安裝應用程式所包含的連結可以開啟某個免安裝應用程式，則必須將使用者導向至該免安裝應用程式，而非採用其他顯示方式 (例如擷取 [WebView](#) 中的連結)。

技術規格

開發人員必須採用 Google 制定的 Android 免安裝應用程式技術規格並遵守相關規定，包含[公開說明文件](#)中明列的規範 (相關內容可能不時修訂)。

提供應用程式安裝功能

免安裝應用程式可為使用者提供該應用程式的安裝版本，但不得以此為主要目的。開發人員提供安裝功能時必須遵守下列規範：

- 在安裝按鈕上使用[質感設計的「取得應用程式」圖示](#) 以及「安裝」標籤。
- 免安裝應用程式中的暗示性安裝提示不得超過 2 到 3 次。
- 不得透過橫幅或其他類似廣告的技術向使用者顯示安裝提示。

如需免安裝應用程式的其他詳細資料以及使用者體驗指南，請參閱[使用者體驗最佳做法](#) 。

變更裝置狀態

免安裝應用程式不得在工作階段外變更使用者的裝置狀態。舉例來說，免安裝應用程式不得變更使用者的桌布，也不能建立主畫面小工具。

應用程式持續顯示

開發人員必須確保免安裝應用程式開啟後會持續顯示在畫面上，讓使用者確知自己的裝置正在執行免安裝應用程式。

裝置 ID

免安裝應用程式不得存取符合下列條件的裝置 ID：(1) 在免安裝應用程式停止執行後仍然有效，且 (2) 無法由使用者重設。相關例子包括但不限於：

- Build Serial
- 任何網路晶片的 Mac 位址
- IMEI、IMSI

免安裝應用程式可透過執行階段權限取得電話號碼。開發人員不得試圖運用這些 ID 或以其他方式追蹤使用者。

網路流量

對於從免安裝應用程式產生的對外網路流量，必須使用傳輸層安全標準 (TLS) 通訊協定 (例如 HTTPS) 進行加密。

Android 表情符號政策

我們的表情符號政策旨在推廣多元包容且一致的使用者體驗。為了達成這個目標，凡是在 Android 12 或以上版本中執行的應用程式，都必須支援最新版的[萬國碼 \(Unicode\) 表情符號](#) 。

如果應用程式在 Android 12 或以上版本中執行，而且使用預設 Android 表情符號，沒有任何自訂導入項目，便已使用最新版萬國碼 (Unicode) 表情符號。

如果應用程式在 Android 12 或以上版本中執行，而且已導入自訂表情符號 (包括由第三方程式庫提供者)，當新的萬國碼 (Unicode) 表情符號推出後，應用程式就必須在 4 個月內完整支援最新版萬國碼 (Unicode)。

請參閱這份[指南](#) ，瞭解如何支援新式表情符號。

家庭

Google Play 為開發人員提供能夠推動成長的平台，方便他們展示優質且適合全家使用的內容。在將應用程式提交至閹家適用計畫，或將兒童導向應用程式提交至 Google Play 商店之前，您必須負責確保應用程式適合兒童使用，且符合所有相關法律的規定。

[前往 App 開發學習中心進一步瞭解閹家適用計畫的政策規定，並查看互動式檢查清單。](#)

Google Play 家庭政策

如今有越來越多家庭利用科技來豐富家庭生活，而家長也在尋找安全優質的內容來與子女分享。您的應用程式可能是專為兒童設計，也可能只會吸引他們注意。Google Play 希望協助您確保應用程式闔家適用，讓所有使用者都能安心使用。

不同地區和背景對「兒童」一詞的定義不盡相同。請務必諮詢您的法律顧問，以正確判斷應用程式適用的義務和/或年齡限制。您最清楚應用程式的運作方式，為確保 Google Play 上的應用程式適合全家使用，我們需要您協力配合。

凡是遵守 Google Play「家庭」政策的應用程式，皆可選擇接受[教師認可評估計畫](#)評分，但我們不保證您的應用程式一定能加入教師認可評估計畫。

Play 管理中心規定

目標對象和內容

發布應用程式前，您必須前往 Google Play 管理中心的[目標對象和內容](#) 部分，從提供的年齡層清單中選取應用程式的目標對象。無論您在 Google Play 管理中心選擇的選項為何，只要您的應用程式包含可視為兒童導向的圖像和術語，就可能影響 Google Play 針對您聲明的目標對象所給予的評估結果。Google Play 有權自行審核您提供的應用程式資訊，以判斷您揭露的目標對象是否正確。

如要選擇多個年齡層做為應用程式的目標對象，您必須確保應用程式是專為所選年齡層的使用者設計，且確實適合這些使用者。舉例來說，如果是專為嬰幼兒和學齡前兒童設計的應用程式，就只能選取「5 歲以下」這個年齡層做為目標對象。如果您的應用程式是專為特定年級的學童設計的，請選擇最能代表該年級的年齡層。只有在應用程式確實是為所有年齡層的使用者設計時，才能選擇包含成人和兒童的年齡層。

更新「目標對象和內容」部分

您隨時可以在 Google Play 管理中心的「目標對象和內容」部分更新應用程式的資訊，相關資訊要等您[提交應用程式更新](#) 後才會顯示在 Google Play 商店中。不過，在您提交應用程式更新之前，Google 可能會先行審查您在 Google Play 管理中心的這個部分變更的任何內容，確認是否符合政策規定。

如果您變更了應用程式的目標對象年齡層，或開始使用廣告或應用程式內購機制，強烈建議您透過應用程式商店資訊頁面的「新功能」部分或應用程式內通知，向使用者告知這些異動內容。

在 Play 管理中心提供不實描述

如果您在 Play 管理中心為應用程式提供的資訊有任何不實陳述 (包括「目標對象和內容」部分的資訊)，可能會導致應用程式遭到下架或停權，因此請務必據實提供資訊。

《家庭政策》規定

如果您的應用程式目標對象包含兒童，請務必遵守下列規定，否則可能會導致應用程式遭到下架或停權。

- 應用程式內容：**應用程式中可供兒童存取的內容不得為兒童不宜內容。如果應用程式含有非全球適用的內容，但該內容經認定為適合特定地區的兒童使用者，則應用程式可在當地 ([限定地區](#)) 上架，但仍無法提供給其他地區的使用者。
- 應用程式功能：**如未取得網站擁有者或管理員的許可，應用程式不得僅提供網站的網頁畫面，或專門為網站吸引關聯流量。
- 提供給 Play 管理中心的回覆：**您必須在 Play 管理中心據實回答有關應用程式的問題，如果應用程式有變更，也必須依異動內容更新答案。這包括但不限於在「目標對象和內容」部分、「資料安全性」專區和 IARC 內容分級問卷中，據實回答應用程式相關問題。
- 資料相關做法：**如果您的應用程式會向兒童蒐集任何[個人與機密資訊](#) (包括透過應用程式呼叫或使用的 API 和 SDK 蒐集資訊)，您必須揭露這項行為。兒童的機密資訊包括但不限於驗證資訊、麥克風和相機感應器資料、裝置資料、Android ID，以及廣告使用資料。您也必須確保應用程式遵守下列[資料相關做法](#)：
 - 僅以兒童為目標對象的應用程式不得傳輸 Android 廣告 ID (AAID)、SIM 卡序號、版本序號、BSSID、MAC、SSID、IMEI 和/或 IMSI。

- 如果目標對象僅限兒童的應用程式指定 API 級別 33 以上的 Android 版本，則不得要求 AD_ID 權限。
- 如果應用程式的目標對象涵蓋兒童和成人，則不得傳輸從兒童或年齡不詳使用者處獲得的 AAID、SIM 卡序號、版本序號、BSSID、MAC、SSID、IMEI 和/或 IMSI。
- 不得透過 Android API 的 TelephonyManager 要求裝置電話號碼。
- 僅以兒童為目標對象的應用程式不得要求位置存取權，亦不得蒐集、使用及傳輸**精確位置**資訊。
- 應用程式在要求取得藍牙權限時，必須使用[隨附裝置管理工具 \(CDM\)](#)，但如果應用程式僅適用於不支援 CDM 的裝置作業系統 (OS) 版本，則不在此限。

5. API 和 SDK：您必須確保應用程式採用適當方式導入 API 和 SDK。

- 僅以兒童為目標對象的應用程式，不得包含未獲准用於兒童導向服務的 API 或 SDK。
 - 舉例來說，如果是會使用 OAuth 技術進行驗證和授權的 API 服務，且相關服務條款指出其未獲准用於針對兒童的服務，就屬於上述情況。
- 如果應用程式的目標對象同時涵蓋兒童和年齡較大的使用者，則不得導入未獲准用於兒童導向服務的 API 或 SDK。但如果在這些 API 或 SDK 之前顯示了**非誘導性年齡選擇畫面**，或本身的導入方式不會蒐集兒童相關資料，則不在此限。如果應用程式的目標對象同時涵蓋兒童和年齡較大的使用者，也不得要求使用者透過未獲准用於兒童導向服務的 API 或 SDK 存取應用程式內容。

6. 擴增實境 (AR)：如果應用程式使用擴增實境技術，就必須在使用者進入擴增實境部分時立即顯示安全性警告，當中須包含下列資訊：

- 適當提醒家長在子女使用時善加監督。
- 提醒使用者留意現實環境中的危險因素 (例如注意周遭環境)。
- 應用程式不得要求使用不建議兒童操作的裝置 (例如 Daydream、Oculus)。

7. 社交應用程式與功能：如果應用程式可讓使用者分享或交換資訊，請務必在 Play 管理中心的[內容分級問卷](#)中據實揭露這些功能。

- 社交應用程式的主要訴求，是讓使用者能夠與廣大的用戶群分享任何形式的內容或進行交流。如果社交應用程式的目標對象包含兒童，在讓兒童使用者交換任何形式的媒體或資訊前，一律必須透過內部訊息提醒他們注意上網安全，以及線上互動會對現實生活帶來的風險。您也必須要求兒童使用者需通過成人驗證，才能交換個人資訊。
- 社交功能：如果應用程式的附加功能可讓使用者與廣大的用戶群分享任何形式的內容或進行交流，就屬於社交功能。只要應用程式的目標對象包含兒童，而且本身具備社交功能，那麼在讓兒童使用者交換任何形式的媒體或資訊前，一律必須透過內部訊息提醒他們注意上網安全，以及線上互動會對現實生活帶來的風險。您也必須讓成人能夠管理開放給兒童使用的社交功能，包括但不限於為兒童啟用/停用社交功能，或選取不同級別的功能。最後，您必須要求兒童使用者需通過成人驗證，才能使用交換個人資訊的功能。
- 成人驗證是一種用來確認使用者已成年的機制，其驗證方式必須避免兒童謊報年齡，以防他們存取應用程式中專為成人設計的部分。比如，要求提供成人的 PIN 碼、密碼、出生日期、電子郵件驗證資訊、附相片身分證件、信用卡或社會安全號碼 (SSN)，即屬於成人驗證機制。
- 如果社交應用程式的主要訴求是讓使用者與不認識的人聊天，就不能以兒童做為目標對象。例如：隨機配對聊天應用程式、約會交友應用程式、以兒童為中心的公開聊天室等等。

8. 法規遵循：您必須確保應用程式 (包括應用程式呼叫或使用的所有 API 或 SDK) 符合美國《[兒童網路隱私保護法](#)》(COPPA)、歐盟《[一般資料保護規則](#)》(GDPR) 和任何其他適用法律或法規。

以下是常見的違規情況：

- 應用程式在商店資訊頁面中鼓勵兒童使用，但應用程式內容卻僅適合成人。
- 應用程式實作的 API 依服務條款規定不可用於兒童導向應用程式。
- 應用程式美化使用酒精飲料、菸草製品或管制藥品的行為。
- 應用程式包含實際賭博或模擬賭博的內容。
- 應用程式含有兒童不宜的暴力、血腥或驚悚內容。
- 應用程式提供交友服務或性愛/婚姻建議。
- 應用程式包含網站連結，但該網站有違反 Google Play《[開發人員計畫政策](#)》的內容。

- 應用程式向兒童放送成人廣告 (例如暴力、色情、賭博內容)。

廣告和營利

如果您利用以兒童為目標對象的應用程式在 Google Play 營利，請務必確保您的應用程式符合下列家庭版廣告與營利規定。

下列政策適用於應用程式包含的任何營利和廣告內容，包括廣告、交叉宣傳 (針對您的應用程式和第三方應用程式)、應用程式內購優惠或任何其他商業內容 (例如付費產品置入性行銷)。此外，這類應用程式中所有的營利和廣告內容也必須遵循所有適用的法律和法規 (包括任何相關的自我規範或業界規範)。

對於過度強調商業策略的應用程式，Google Play 有權拒絕、下架或予以停權。

廣告規定

如果您的應用程式會向兒童或年齡不詳的使用者放送廣告，請務必遵守下列規定：

- 只使用 [Google Play 家庭自我認證廣告 SDK](#) 向這類使用者放送廣告。
- 確保向這類使用者放送廣告時，未採用依興趣顯示廣告的機制 (根據使用者的網路瀏覽行為，向具有特定特徵的個別使用者放送廣告) 或再行銷機制 (根據使用者的應用程式或網站互動記錄，向個別使用者放送廣告)。
- 確保向這些使用者放送的廣告內容適合兒童觀看。
- 確保向這些使用者放送的廣告符合家庭廣告格式規定。
- 確實遵守所有與兒童導向廣告相關的適用法規與業界標準。

廣告格式規定

應用程式中的營利和廣告內容不得具欺騙性，而且要避免使用兒童容易不慎點選的設計。

如果應用程式目標對象僅限兒童，即禁止下列行為；如果應用程式的目標對象涵蓋兒童和成人，則向兒童或年齡不詳的使用者放送廣告時，禁止下列行為：

- 顯示具干擾性的營利和廣告內容，包括會占據整個螢幕畫面或干擾正常使用，且未明確提供關閉方式的營利和廣告內容 (例如 [廣告牆](#))。
- 顯示會干擾正常使用應用程式或玩遊戲的營利和廣告內容 (包括獎勵廣告或使用者主動觀看的廣告)，而且無法在顯示 5 秒後關閉。
- 如果營利和廣告內容不會干擾使用者正常使用應用程式或玩遊戲，則可持續顯示超過 5 秒 (例如包含整合式廣告的影片內容)。
- 在應用程式啟動後隨即顯示插頁式營利和廣告內容。
- 在單一頁面中刊登多則廣告，比如運用橫幅廣告在單一刊登位置顯示多項優惠，或顯示多則橫幅廣告或影片廣告，都在禁止之列。
- 顯示不易與應用程式內容區分的營利和廣告內容，例如 Offerwall 和其他沉浸式廣告體驗。
- 運用聳動或煽情的手法，吸引使用者瀏覽廣告或購買應用程式內商品。
- 強迫使用者點閱欺騙性廣告，例如使用關閉按鈕觸發另一則廣告，或讓廣告突然出現在一般是用於點選其他功能的區域。
- 未區分使用虛擬遊戲幣和現金購買應用程式內商品的行為。

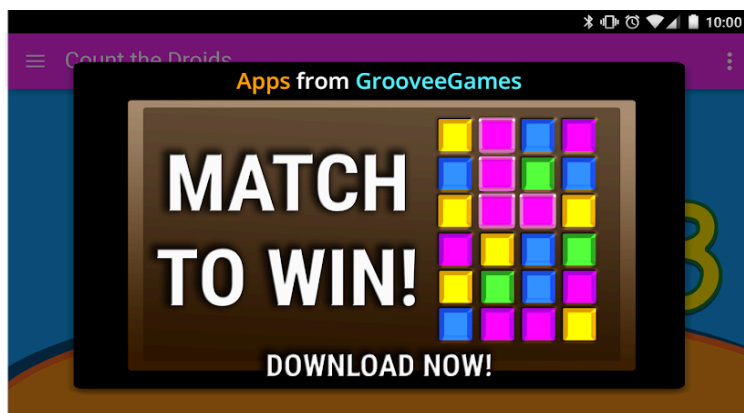
以下是常見的違規情況：

- 營利和廣告內容在使用者嘗試關閉時移到其他位置

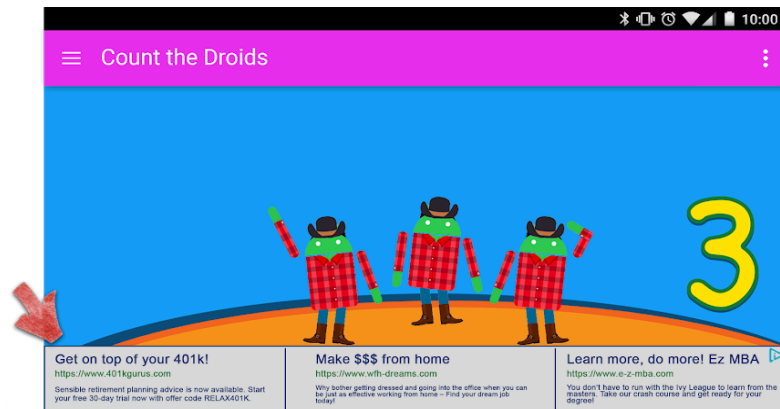
- 營利和廣告內容未在顯示五 (5) 秒後向使用者提供退出優惠畫面的方式，如下例所示：



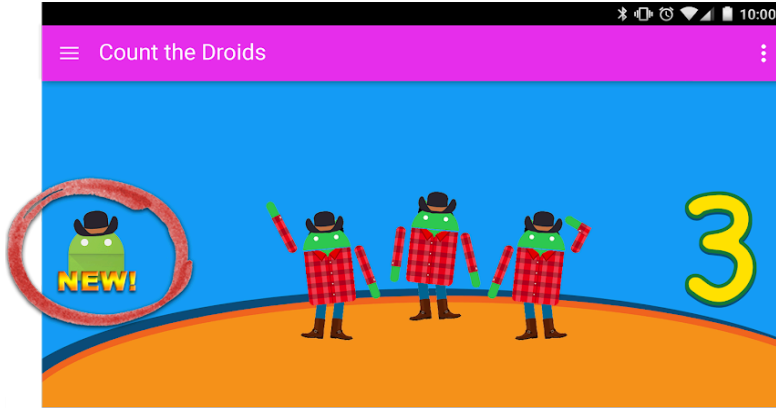
- 營利和廣告內容占據裝置螢幕的絕大部分畫面，且未提供明確的關閉方式，如下例所示：



- 橫幅廣告顯示多項優惠，如下例所示：

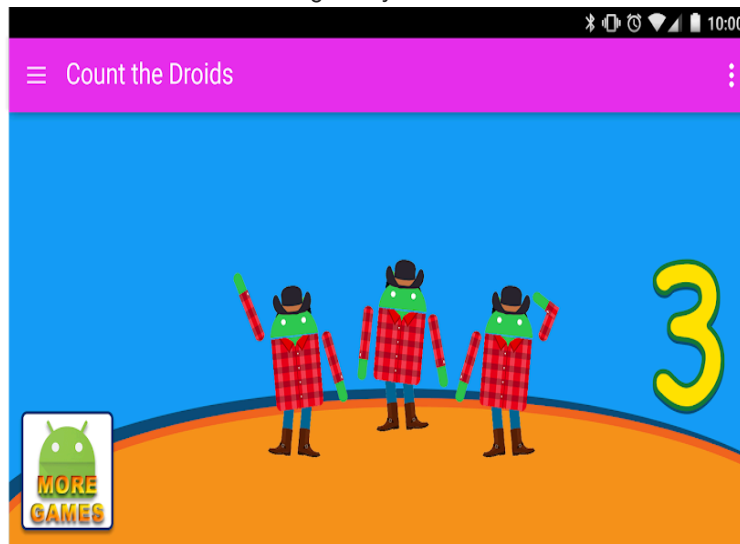


- 營利和廣告內容有可能會被使用者誤認為應用程式內容，如下例所示：



- 按鈕、廣告或其他營利內容是用於宣傳您的其他 Google Play 商店資訊，但難以與應用程式本身的內容

區分，如下例所示：



以下列舉一些不應向兒童放送的不當廣告內容。

- **不當的媒體內容：**廣告宣傳內容包含兒童不宜的電視節目、電影、音樂專輯或任何其他媒體。
- **不當的電玩遊戲與可下載軟體：**廣告宣傳內容包含兒童不宜的可下載軟體及電玩遊戲。
- **管制性或有害物品：**廣告宣傳內容包含酒精飲料、菸草製品、管制性藥物或任何其他有害物品。
- **賭博：**廣告宣傳內容包含模擬賭博、競賽或抽獎等促銷活動 (即使免費入場也包括在內)。
- **具有性暗示的成人內容：**廣告含有情色、性暗示和成人內容。
- **約會或交友：**關於約會或成人交友網站的廣告。
- **暴力內容：**廣告含有兒童不宜的暴力內容和血腥畫面。

廣告 SDK

如果您的應用程式會放送廣告，而且目標對象僅限兒童，則只能使用已加入[家庭自我認證廣告 SDK](#) 計畫的版本。如果應用程式的目標對象涵蓋兒童和成人，您必須採用年齡篩選措施 (例如[非誘導性年齡選擇畫面](#))，並確保向兒童放送的廣告全都來自已向 Google Play 完成自主認證的廣告 SDK 版本。

如需進一步瞭解這類規定，請造訪「[家庭自我認證廣告 SDK 計畫政策](#)」頁面；如要查看目前已加入家庭自我認證廣告 SDK 計畫的版本清單，請參閱[這篇文章](#)。

如果您是 AdMob 使用者，請前往 [AdMob 說明中心](#) 瞭解相關產品詳情。

您有責任確保應用程式符合與廣告、應用程式內購和商業內容相關的所有規定。如要瞭解特定廣告 SDK 供應商的內容政策和廣告做法，請與對方聯絡。

家庭版自主認證廣告 SDK 政策

Google Play 致力為兒童和家庭打造安全無虞的體驗，其中一項關鍵是確保兒童只會看到適合自身年齡的廣告，而且他們的資料均經過妥善處理。為了達到這個目標，我們要求廣告 SDK 和中介服務平台必須通過自主認證，確認這類 SDK 與平台提供適合兒童的內容，而且符合《[Google Play 開發人員計畫政策](#)》及 [Google Play 家庭政策](#)，包括[家庭版自主認證廣告 SDK 計畫規定](#)。

Google Play 家庭版自主認證廣告 SDK 計畫相當重要，開發人員可透過本計畫找出完成自主認證的廣告 SDK 或中介服務平台，進而瞭解哪些 SDK 或平台適用於專為兒童設計的應用程式。

如果您提供的 SDK 相關資訊 (包括[意願調查表](#) 的申請資料) 有任何不實描述，可能會導致 SDK 從家庭版自主認證廣告 SDK 計畫中移除或遭到停權，因此請務必據實提供資訊。

政策規定

如果您的 SDK 或中介服務平台所服務的應用程式已加入 Google Play 闔家適用計畫，請務必遵守所有 Google Play 開發人員政策，包括下列規定。若 SDK 或中介服務平台違反任何政策規定，就可能從家庭版自主認證廣告 SDK 計畫中移除或遭到停權。

您有責任確保自己的 SDK 或中介服務平台符合規範，因此請務必詳閱《[Google Play 開發人員計畫政策](#)》、[Google Play 家庭政策](#)和[家庭版自主認證廣告 SDK 計畫規定](#)。

1. 廣告內容：可供兒童存取的廣告內容必須適合兒童觀看。

- 您必須 (i) 定義不當的廣告內容和行為，並 (ii) 在條款或政策中禁止這類內容和行為。這些定義應符合《[Google Play 開發人員計畫政策](#)》。
- 您也必須制定一套將廣告素材依適當年齡層進行分級的方法，級別至少要包含適合「所有人」和「成人」。這套分級法必須與 Google 在供應商填寫[意願調查表](#) 後提供的 SDK 分級法一致。
- 使用即時出價功能向兒童放送廣告時，您必須確保廣告素材已通過審核且符合上述規定。
- 此外，也必須採用適當機制清楚標示廣告素材來自您的廣告空間，比如在素材中加入貴公司標誌或類似記號的浮水印。

2. 廣告格式：您必須確保向兒童使用者放送的所有廣告均遵循家庭版廣告格式規定，也必須允許開發人員選取符合 [Google Play 家庭政策](#) 的廣告格式。

- 廣告不得含有欺騙性內容，而且要避免易使兒童使用者不慎點選的設計。我們禁止以下列手法強迫使用者點選的欺騙性廣告：透過關閉按鈕觸發另一則廣告，或突然顯示在應用程式中通常供使用者點選其他功能的區域。
- 我們禁止干擾性廣告，這類廣告會涵蓋整個螢幕畫面或干擾正常使用，且未明確提供關閉方式的內容，例如廣告牆。
- 如果廣告會干擾正常使用應用程式或玩遊戲 (包括獎勵廣告或使用者主動觀看的廣告)，就必須在顯示 5 秒後提供關閉選項。
- 單一頁面不得有多個廣告刊登位置。比如，運用橫幅廣告在單一刊登位置顯示多項優惠，或顯示多則橫幅廣告或影片廣告，都在禁止之列。
- 廣告和應用程式內容之間必須有明顯區別。如果 Offerwall 和沉浸式廣告無法讓兒童使用者清楚辨識為廣告，即違反規定。
- 廣告不得利用聳動或煽情的手法吸引使用者觀看。

3. IBA/再行銷：您必須確保向兒童使用者放送的廣告未採用依興趣顯示廣告的機制或再行銷機制。依興趣顯示廣告是指根據使用者的網路瀏覽行為，向具有特定特徵的個別使用者放送廣告；再行銷則是根據使用者的應用程式或網站互動記錄，向個別使用者放送廣告。

4. 資料相關做法：您 (即 SDK 供應商) 必須開誠布公地說明自己如何處理使用者資料，例如蒐集的使用者相關資訊或取自使用者的資訊，包括裝置資訊。也就是說，您必須揭露 SDK 存取、蒐集、使用及分享資料的行為，而且資料使用範圍僅限揭露的用途。除了這些 Google Play 規定外，您亦須遵守適用的隱私權和資料保護法律。如果您的 SDK 會向兒童蒐集任何個人與私人資訊，請務必揭露這項行為。上述資訊包括但不限於驗證資訊、麥克風和相機感應器資料、裝置資料、Android ID 和廣告使用資料。

- 您必須允許開發人員依個別要求或個別應用程式，針對廣告放送行為提出兒童導向內容要求。這類內容必須遵循適用的法律及法規，例如美國《[兒童網路隱私保護法](#)》(COPPA) 和歐盟《[一般資料保護](#)

[規則》\(GDPR\)](#)。

- 根據 Google Play 規定，廣告 SDK 不得在兒童導向內容中放送個人化廣告、按照興趣顯示廣告及進行再行銷。
- 使用即時出價功能向兒童放送廣告時，您必須確保隱私權指標套用至出價工具。
- 您不得傳輸來自兒童或年齡不詳使用者的 AAID、SIM 卡序號、版本序號、BSSID、MAC、SSID、IMEI 和/或 IMSI。

5. **中介服務平台：**向兒童放送廣告時，您必須遵守下列規定：

- 僅使用家庭版自主認證廣告 SDK，或採取必要保護措施，確保透過中介服務放送的所有廣告均符合相關規定。
- 傳送必要的資訊至中介服務平台，指明廣告內容分級和任何適用的兒童導向內容。

6. **自主認證和法規遵循：**您必須向 Google 提供充分資訊 (例如 [意願調查表](#) 所列資訊)，驗證廣告 SDK 符合所有自主認證政策規定。相關做法包括但不限於：

- 針對您的 SDK 或中介服務平台，提供英文版的服務條款、隱私權政策和發布商整合指南。
- 提交[測試版應用程式](#)。此應用程式須採用符合規定的最新版廣告 SDK，本身是建構完成的可執行 Android APK，並且用到該 SDK 的所有功能。以下是測試版應用程式規定：
 - 提交的應用程式必須是建構完成的可執行 Android APK，且專為手機板型規格所設計。
 - 採用的廣告 SDK 必須是符合 Google Play 政策的最新版本，或即將發布的版本。
 - 必須使用您廣告 SDK 的所有功能，包括呼叫廣告 SDK 來擷取及顯示廣告。
 - 在要求廣告素材時，必須能完全存取相應廣告聯播網中所有即時/放送中的廣告空間。
 - 必須不受地理位置限制。
 - 如果您廣告空間的目標對象包含各年齡層使用者，那麼測試版應用程式必須能夠分辨不同要求，判斷廣告素材應取自完整廣告空間，還是適合兒童或所有年齡層的廣告空間。
 - 除非受到非誘導性年齡選擇畫面所控管，否則不得僅放送廣告空間中的特定廣告。

7. 如果收到後續訊息，要求您提供進一步資訊，請務必及時回覆，並[自主認證](#) 所有新發布的版本都符合最新《Google Play 開發人員計畫政策》，包括家庭政策規定。

8. **法規遵循：**家庭版自主認證廣告 SDK 在放送廣告時，必須遵守其發布商可能適用的所有兒童相關法令和法規。

- 您必須確保自己的 SDK 或中介服務平台符合[美國《兒童網路隱私保護法》\(COPPA\)](#)、[歐盟《一般資料保護規則》\(GDPR\)](#) 和任何其他適用法律或法規。

注意：「兒童」一詞在不同地區和語境可能有不同涵義。請務必諮詢您的法律顧問，以正確判斷應用程式適用的義務和/或年齡限制。您最清楚應用程式的運作方式，為確保 Google Play 上的應用程式適合全家使用，我們需要您協力配合。

請前往「[家庭版自主認證廣告 SDK 計畫](#)」頁面，進一步瞭解計畫規定。

違規處置

對於可能違反政策的情況，防患未然總好於事後管理。不過，當應用程式出現違規行為時，我們會致力確保開發人員瞭解如何改正違規事項，讓應用程式符合規定。如果您[發現任何違規行為](#) 或是對[管理違規情事](#) 有任何疑問，請與我們聯絡。

政策適用範圍

我們的政策適用於您的應用程式所顯示或連結的任何內容，包含應用程式向使用者顯示的任何廣告，以及應用程式所管理或連結的任何使用者自製內容。同時，這些政策也適用於您的開發人員帳戶在 Google Play 上公開顯示的任何內容，包括您的開發人員名稱，以及您所列出的開發人員網站的到達網頁。

我們禁止應用程式讓使用者在裝置上安裝其他應用程式。如要讓使用者以免安裝方式存取其他應用程式、遊戲或軟體 (包括第三方提供的功能和體驗)，這些內容均須符合所有 [Google Play 政策](#) 規範，且可能須另外接受政策審查。

相關政策所定義之詞彙與《[開發人員發布協議](#)》(DDA) 的用語相同。除了遵循這些政策與 DDA 之外，您的應用程式內容還須依據《[內容分級規範](#)》進行分級。

我們禁止會在 Google Play 生態系統中損害使用者信任的應用程式或應用程式內容。在評估要讓應用程式在 Google Play 上架還是下架時，我們會考慮諸多因素，包括但不限於有害行為模式或高濫用風險；判定濫用風險時會考量多項因素，包括但不限於對特定應用程式和開發人員提出的申訴、新聞報導、先前的違規記錄、使用者意見回饋、是否使用熱門的品牌、角色和其他資源。

Google Play 安全防護的運作方式

Google Play 安全防護會在您安裝應用程式時執行檢查，也會定期掃描您的裝置。如果偵測到可能有害的應用程式，這項服務可能會採取以下措施：

- 傳送通知給您。如要移除該應用程式，請依序輕觸通知和 [解除安裝]。
- 停用應用程式，直到您解除安裝為止。
- 自動移除應用程式。在大多數情況下，如果 Google Play 安全防護偵測到有害的應用程式，您會收到系統已將應用程式移除的通知。

惡意軟體防護的運作方式

為了防範第三方惡意軟體、網址和其他安全性問題的侵擾，Google 可能會收集下列資訊：

- 您裝置的網路連線
- 可能有害的網址
- 作業系統，以及透過 Google Play 或其他來源安裝在裝置上的應用程式

假使 Google 認定應用程式或網址有安全疑慮，將向您發出警告。如果 Google 發現應用程式或網址會危害裝置、資料或使用者，將移除或封鎖該應用程式或網址，不進行安裝程序。

您可以在裝置設定中停用部分防護措施，但 Google 可繼續針對透過 Google Play 安裝的應用程式收集相關資訊，而系統也會繼續檢查透過其他來源安裝到裝置上的應用程式，看看是否有任何安全性問題，只是不會傳送任何資訊給 Google。

隱私權警訊的運作方式

如果 Google Play 商店以應用程式可能存取您的個人資訊為由，將您安裝的應用程式下架，這時 Google Play 安全防護服務就會向您傳送通知，並提供解除安裝應用程式的選項。

違規處置流程

我們在審視內容或帳戶是否違反法律/政策時，會考量各種資訊來做出決定，包括應用程式中繼資料 (例如應用程式名稱、說明)、應用程式內體驗、帳戶資訊 (例如之前違反政策的記錄)、應用程式中的第三方程式碼，以及透過檢舉機制 (如有) 和 Google 內部審查取得的其他資訊。請注意，您必須負責確保應用程式中所用的任何第三方程式碼 (例如 SDK)，以及該第三方對應用程式的處理方式，完全符合《Google Play 開發人員計畫政策》。

如果您的應用程式或開發人員帳戶違反任一政策，我們會採取下列適當處置，並透過電子郵件提供有關處置的資訊。若您認為我們的處置有誤，可以透過郵件隨附的操作說明提出申訴。

請注意，下架處置或管理通知可能不會逐一指出帳戶或特定/所有應用程式的每件政策違規事項。開發人員應負責修正任何政策違規問題，並致力確保應用程式或帳戶的其餘內容完全符合政策規範。如未修正帳戶和所有應用程式的政策違規問題，可能會受到進一步違規處置。

如果屢次違反這些政策或《[開發人員發行協議](#)》(DDA)，或是違規情節重大 (例如涉及詐欺行為、發布惡意軟體以及可能傷害使用者或裝置的應用程式)，我們會終止個人或相關的 Google Play 開發人員帳戶。

違規處置

不同的違規處置可對應用程式帶來不同影響。我們結合人工與自動化評估機制來審查應用程式和其內容，偵測及評估哪些內容不僅違反政策，還對使用者和整體 Google Play 生態系統造成傷害。採用自動化模型有助於偵測更多違規事項及加速評估潛在問題，可確保 Google Play 為所有人提供安全的服務體驗。自動化模型會移除違反政策的內容，但如果判定需要更縝密的審查 (例如需要通盤瞭解特定內容的情境脈絡)，模型會為內容加上標記，交由經過專業培訓的專員和分析人員評估。我們會利用這類人工審查結果建立訓練資料，進一步改善機器學習模型。

以下說明 Google Play 可能採取的各項處置，以及您的應用程式和/或 Google Play 開發人員帳戶受到的影響。

除非違規處置通知中另有註明，否則這類處置的影響範圍會涵蓋所有地區。舉例來說，如果應用程式遭到停權，就無法提供給所有地區的使用者。此外，除非另有說明，否則這類處置將持續有效，直到您對處置提出申訴並獲得核准為止。

拒絕

- 送審的新應用程式或應用程式更新不會在 Google Play 中上架。
- 如果現有應用程式的更新版本遭拒，更新之前所發布的版本仍會保留在 Google Play 商店中。
- 即使遭拒，您仍可查看遭拒應用程式的現有使用者安裝次數、統計資料和評分。
- 拒絕處置不會影響您的 Google Play 開發人員帳戶記錄。

注意：在修正所有政策違規事項之前，請勿嘗試重新提交遭拒的應用程式。

下架

- 應用程式及其先前的任何版本都將從 Google Play 下架，無法再供使用者下載。
- 應用程式下架後，使用者將無法查看應用程式的商店資訊。一旦您為遭下架的應用程式提交符合政策規範的更新版本，系統就會還原這些資訊。
- 在 Google Play 核准符合政策規範的版本之前，使用者可能無法進行任何應用程式內購交易，或使用任何應用程式內結帳功能。
- 下架處置不會立即影響您的 Google Play 開發人員帳戶記錄，但如果累積多次下架記錄，我們可能會採取停權處分。

注意：在修正所有政策違規問題前，請勿嘗試重新發布遭下架的應用程式。

停權

- 應用程式及其先前的任何版本都將從 Google Play 下架，無法再供使用者下載。
- 如果應用程式違規情節重大、屢次違反政策，或是多次遭到拒絕/下架，我們就可能採取停權處分。
- 應用程式遭停權後，使用者將無法查看應用程式的商店資訊。
- 您無法再使用停權應用程式的 APK 或應用程式套件。
- 使用者將無法購買應用程式內商品，也無法使用任何應用程式內結帳功能。
- 停權視同系統對 Google Play 開發人員帳戶發出警告，您的良好記錄可能因此受到影響。如果累積多次警告，可能導致個人和相關的 Google Play 開發人員帳戶遭到終止。

曝光度受限

- 應用程式在 Google Play 的曝光度會受限。使用者仍可透過應用程式的商店資訊直接連結，在 Google Play 存取該應用程式。
- 應用程式處於「曝光度受限」狀態不會影響您的 Google Play 開發人員帳戶記錄。
- 即使應用程式處於「曝光度受限」狀態，使用者仍可查看應用程式的現有商店資訊。

限定地區

- 只有特定地區的使用者可以透過 Google Play 下載您的應用程式。
- 其他地區的使用者無法在 Play 商店找到該應用程式。

- 先前已安裝應用程式的使用者可以繼續在個人裝置上使用應用程式，但不會再收到更新。
- 限定地區不會影響您的 Google Play 開發人員帳戶記錄。

帳戶受限狀態

- 如果您的開發人員帳戶處於受限狀態，自身目錄中的所有應用程式都將從 Google Play 下架，而且您無法再發布新的應用程式或重新發布現有應用程式，但仍可使用 Play 管理中心。
- 所有應用程式都下架後，使用者將無法查看開發人員設定檔和應用程式的商店資訊。
- 現有使用者將無法進行任何應用程式內購交易，或使用任何應用程式內結帳功能。
- 您依然可以使用 Play 管理中心，向 Google Play 提供更多資訊，以及修改帳戶資訊。
- 修正所有政策違規問題後，即可重新發布應用程式。

帳戶終止

- 如果您的開發人員帳戶遭到終止，自身目錄中的所有應用程式都將從 Google Play 下架，而且您無法再發布新的應用程式。此外，任何相關的 Google Play 開發人員帳戶也會受到永久停權。
- 屢次遭受停權或因嚴重違反政策而受到停權，同樣可能導致 Play 管理中心帳戶遭到終止。
- 遭終止帳戶的應用程式下架後，使用者將無法查看開發人員設定檔和應用程式的商店資訊。
- 現有使用者將無法進行任何應用程式內購交易，或使用任何應用程式內結帳功能。

注意：您試圖建立的所有新帳戶也會遭到終止 (而且開發人員註冊費不會退還)，因此如果有任何遭終止的帳戶，請勿嘗試註冊新的 Play 管理中心帳戶。

停滯帳戶

停滯帳戶指的是處於閒置或棄用狀態的開發人員帳戶，不符合《[開發人員發行協議](#)》規定的記錄良好條件。

Google Play 開發人員帳戶是供發布並積極維護應用程式的開發人員使用。為防止濫用情形，我們會定期關閉停滯、未使用或沒有明顯活動 (例如發布及更新應用程式、存取統計資料或管理商店資訊) 的帳戶。

[長期未使用](#)會導致您的帳戶遭到關閉，除非您恢復帳戶權限，否則將無法再存取 Play 管理中心的任何報表、統計資料、深入分析或其他資訊。您的註冊費將不予退還並直接沒收。在關閉停滯帳戶前，我們會使用該帳戶的聯絡資訊通知您。

即使停滯帳戶遭到關閉，往後您決定在 Google Play 發布內容時，仍可以建立新帳戶。

管理及檢舉違反政策規定的行為

針對違規處置提出申訴

如果處置有誤，而且我們查明您的應用程式並未違反《Google Play 計畫政策》和《開發人員發行協議》，就會讓您的應用程式恢復上架。詳閱政策說明後，如果您認為我們的處置有誤，請查看您收到的違規處置電子郵件通知或[按這裡](#)，按照當中的指示提出申訴。

其他資源

如需有關違規處置或特定使用者評分/評論的更多資訊，請參考以下資源，或是透過 [Google Play 說明中心](#) 與我們聯絡。不過，我們無法為您提供任何法律方面的建議，如需法律意見，請洽詢您的法律顧問。

- [應用程式驗證](#)
- [檢舉違反政策規定的內容](#)
- [與 Google Play 團隊聯絡，洽詢帳戶終止或應用程式下架的相關資訊](#)
- [一般警告](#)
- [檢舉內容不當的應用程式與評論](#)
- [我的應用程式已經從 Google Play 下架](#)

- [瞭解終止 Google Play 開發人員帳戶的相關資訊](#)

Play 管理中心規定

為了維護我們生機蓬勃的應用程式生態系統，帶給所有人安全的體驗，Google Play 規定所有開發人員必須完成 Play 管理中心要求的事項，包括確認與 Play 管理中心開發人員帳戶連結的資料。驗證完成的資訊將顯示在 Google Play，協助開發人員贏得使用者的信任與信心。進一步瞭解 [Google Play 顯示的資訊](#)。

Google Play 提供兩種類型的開發人員帳戶，分別是「個人」和「機構」帳戶。為順利開始使用帳戶，請務必選擇正確的開發人員帳戶類型，並完成必要驗證。瞭解如何[選擇開發人員帳戶類型](#)。

建立 Play 管理中心帳戶時，提供下列服務的開發人員必須以「機構」身分註冊：

- 金融商品和服務，包括但不限於銀行業務、貸款、股票交易、投資基金、加密貨幣軟體錢包和加密貨幣交易。進一步瞭解[金融服務政策](#)。
- 健康應用程式，例如醫療應用程式和人體研究應用程式。進一步瞭解[健康應用程式類別](#)。
- 獲准使用 [VpnService](#) 類別的應用程式。進一步瞭解 [VPN 服務政策](#)。
- 政府應用程式，包括政府機關開發或委託開發的應用程式。

選取帳戶類型後，必須完成下列事項：

- 提供正確的開發人員帳戶資訊，包括以下資料：
 - 法定姓名和地址
 - [鄧白氏環球編碼](#)（如果註冊身為機構的話）
 - 聯絡電子郵件地址和電話號碼
 - Google Play 上顯示的開發人員電子郵件地址和電話號碼 (如適用)
 - 付款方式 (如適用)
 - 連結至開發人員帳戶的 Google 付款資料
- 如果註冊身為機構，請確保您的開發人員帳戶資訊符合現況，且與鄧白氏資料檔案所記錄的資訊相符。

提交應用程式前，請完成下列事項：

- 據實提供所有應用程式資訊和中繼資料
- 上傳應用程式的隱私權政策，並填寫「資料安全性」專區需要揭露的各項資訊
- 提供 Google Play 審查應用程式時所需的有效試用帳戶、登入資訊和其他必要資源 (特別是[登入憑證](#)、QR code 等等)

一如既往，您應確保應用程式提供穩定可靠、引人入勝、操作順暢的使用者體驗，並仔細確認所有應用程式內容都符合《[Google Play 開發人員計畫政策](#)》，包括廣告聯播網、數據分析服務和第三方 SDK 在內；此外，如果應用程式的目標對象包含兒童，請務必遵守[家庭政策](#)規定。

請注意，您有責任詳閱《[開發人員發行協議](#)》和《[開發人員計畫政策](#)》的所有規定，並確保您的應用程式完全符合規範。

帳戶轉移

為提供安全可靠的生態系統，讓開發人員和使用者可以安心使用，Google Play 要求開發人員對於帳戶擁有權必須保持公開透明，並承擔相應的責任。我們瞭解，基於正當商業理由 (例如收購、組織重組、人事異動和其他業務需求)，開發人員帳戶可能需要轉移擁有權。為滿足這些需求，同時維護生態系統完整性，Google Play 規定必須使用正式的帳戶轉移程序。

帳戶擁有權轉移規定

如要變更 Google Play 開發人員帳戶的擁有權，開發人員必須使用[官方的帳戶擁有權轉移程序](#)。帳戶轉移雙方都必須對轉移過程中 (包括過渡期間) 採取的所有行動負責。

轉移帳戶擁有權時不得採用非官方方式，包括但不限於：

- 在第三方市集上買賣或租借透過非法手段取得的帳戶

如要轉移應用程式擁有權，而非整個 Google Play 開發人員帳戶，請參考[應用程式擁有權轉移程序](#)。

[Developer Distribution Agreement](#)

還有其他問題嗎？

嘗試以下步驟：



與我們聯絡

進一步說明相關資訊，我們會盡力協助您