

隱私權政策（Privacy Policy）—《【EcoWorld】》

最後更新日期：【0205-08-27】

資料控制者：個人開發者（以下稱「我們」）

聯絡信箱：FlameStickUnder@gmail.com

發行管理地區：台灣（僅於台灣提供服務）

本政策適用於我們提供的 ESG 養成建築手機遊戲《【EcoWorld】》（以下稱「本服務」）。使用本服務即表示你已閱讀、理解並同意本政策。為與 App Store／Google Play 的隱私揭露一致，若本政策更新，我們將於 App 內與本頁同步公告。

1. 我們蒐集哪些資料（What We Collect）

為讓你清楚了解，我們針對每一類資料，標示是否為使用服務所必須（必要/可選）、收集時機、資料來源。本節為**資料類型總表**；保存期間見第 5 節，資料分享見第 6 節。

1.1 帳戶識別

- **內容**：帳號（系統產生的玩家 ID）、玩家暱稱、（如需）電子郵件。
- **收集時機**：註冊或首次建立檔案、修改個人資料、帳號救援/驗證時。
- **來源**：你於 App 內輸入；部分欄位（玩家 ID）由系統產生。
- **用途提示**：登入、雲端同步、客服聯繫、違規處置通知。

1.2 認證資訊

- **內容**：密碼（僅保存不可逆雜湊+鹽值）、重設密碼用一次性權杖（短期）。
- **收集時機**：設定/變更密碼、申請重設時。
- **來源**：你於 App 內輸入。

- 安全提示：伺服器不保存明文密碼；一次性權杖到期即失效。

1.3 遊戲資料（遊戲進度與狀態）

- 內容：建築/關卡進度、資源與道具持有量、任務與成就紀錄、碳權與 ESG 指標、配對/對戰紀錄、世界/公會/好友關聯（如有）。
- 收集時機：遊戲過程自動同步、結算、登入/登出、重大事件（如交易、製作）發生時。
- 來源：裝置端遊戲客戶端自動上傳；由我們或受託處理者（PlayFab）代管。
- 用途提示：提供與維護服務、避免本地資料遺失、跨裝置續玩、爭議處理（例如道具回溯）。

1.4 操作與遙測（Telemetry）

- 內容：操作事件名稱與時間戳、App 版本、錯誤/崩潰日誌、啟動與載入耗時、網路狀態、（可選）畫面更新率/FPS。
- 收集時機：遊戲運行期間自動上報（頻率受限於最小化原則）。
- 來源：裝置端自動產生並上傳；伺服器端交叉比對。
- 用途提示：除錯與效能監控、提升穩定度；不做行為廣告或跨站追蹤。

1.5 社群與互動內容（UGC）

- 內容：遊戲內對話（公開/私訊）、留言、檢舉紀錄、你提交的回饋與附件（例如螢幕截圖）。
- 收集時機：你發送訊息、回饋或檢舉時即上傳；違規內容可能被自動過濾並標記。
- 來源：你主動提供；系統自動產生的審核標記與處置紀錄。
- 用途提示：社群治理、申訴與風險審查、依社群規範執行禁言/停權等措施。

1.6 必要技術資訊

- **內容**：IP 位址（可能推估粗略地理區域）、裝置型號、作業系統版本、語言與區域、連線狀態、裝置識別符（平台允許範圍內）。
- **收集時機**：啟動、登入、網路交換資料時。
- **來源**：裝置與伺服器連線過程自動產生。
- **用途提示**：網路連線診斷、資安防護、防止濫用與詐欺、法令遵循。
- **定位聲明**：我們**不收集精確 GPS 定位**；若未來特定功能需要，將另行告知並取得同意。

1.7 客服與問卷

- **內容**：你在客服單或問卷中提供的文字、聯絡方式、（如你主動上傳）截圖/紀錄檔。
- **收集時機**：你主動提交時。
- **來源**：你主動提供。
- **用途提示**：處理問題、追蹤回報、產品改進。

1.8 不蒐集的敏感資料與例外

- **預設不蒐集**：政府核發身分證號、財務或健康資料、**精確定位**、通訊錄、相簿內容等。
- **例外情境**：若未來特定功能（例如：活動實體兌換）**確實需要**其中任何一項，我們會在功能啟用前以清楚的**告知與明確同意**為前提，並僅於特定目的與期間內處理。

1.9 資料最小化與去識別化

- 我們採**資料最小化**原則：只收提供服務「必要」的欄位，保留時間不逾目的所需。
- 研究與統計原則上使用**去識別化/彙整**資料；若需處理可識別資料，將另行徵求**明確同意**並提供撤回。

2. 我們如何使用資料（Purposes & Legal Bases）

總則：我們僅於**特定、明確且合法**之目的下處理資料，並採**資料最小化**原則。若將資料用於原本未載明的新目的，我們會先公告並在法規要求時另行徵求你的**明確同意**。

2.1 提供與維護服務（註冊／登入／雲端同步／備份）

- **使用的資料類型**：帳戶識別、認證資訊、遊戲資料、必要技術資訊。
- **我們為什麼需要**：建立與維持你的帳號、跨裝置續玩、避免本機資料遺失、處理連線與版本相容。
- **你的選擇**：若你拒絕提供帳號／密碼或必要技術資訊，將無法建立帳號或正常使用雲端與多人功能。
- **法律依據**：契約必要（提供你要求的服務）／合法利益（確保服務可用與一致運作）。

2.2 安全與公平性（防外掛／反詐欺／風險控管）

- **使用的資料類型**：帳戶識別、遊戲資料、必要技術資訊、操作與遙測、（社群功能啟用時）社群互動。
- **我們為什麼需要**：偵測異常行為、保護帳號與資產、維持對戰公平與社群秩序、防止濫用退款。
- **你的選擇**：若你關閉部分遙測，可能降低偵測準確度並限制遊戲功能；對處置結果你可依第 11 節申請人工覆核。
- **法律依據**：合法利益（維護安全與公平）／法定義務（配合執法與合規要求）。

2.3 除錯與效能監控

- **使用的資料類型**：操作與遙測、必要技術資訊、（必要時）匿名化的裝置資訊與崩潰記錄。
- **我們為什麼需要**：縮短故障修復時間、提升 FPS 與載入速度、改善相容性。

- **你的選擇**：你可在設定中關閉非必要的擴充遙測；但**基礎穩定性資料**屬運作必要。
- **法律依據**：合法利益（改進與維持服務品質）。

2.4 客服與申訴

- **使用的資料類型**：帳戶識別、（你主動提供的）聯絡方式、社群互動（檢舉／申訴內容）、遊戲資料。
- **我們為什麼需要**：辨識身分、追蹤案件、查核爭議（如道具回溯、對戰爭議）。
- **你的選擇**：你可選擇不提供附加資訊，但可能影響處理進度與結果。
- **法律依據**：契約必要／合法利益。

2.5 研究與學術用途（重要）

- **使用的資料類型**：去識別化／彙整後的遊戲資料、操作與遙測與社群互動統計。
- **我們為什麼需要**：分析 ESG 行為模式、效能與介面設計影響、撰寫論文與專題成果。
- **你的選擇**：預設僅用去識別化資料。若研究需要處理可識別資料或法律要求同意，我們會在 App 內清楚說明目的與範圍並另行徵求你的明確同意；你可隨時撤回而不影響遊戲使用。
- **法律依據**：合法利益（使用去識別化或彙整資料）／同意（僅限研究確需可識別資料的情形）。

2.6 法令遵循與權利保護

- **使用的資料類型**：與個案相關、**最小必要**之帳戶識別、遊戲資料、社群互動、必要技術資訊。
- **我們為什麼需要**：回應法院／主管機關之合法要求、執行防詐與權利保護、處理安全事件通報。
- **你的選擇**：在法定範圍內你可行使權利；若屬法定保存或執法要求，可能無法刪除或限制處理。

- 法律依據：法定義務／合法利益（主張或防禦法律權利）。
-

2.7 不做與將來變更的承諾

- **不販售或共享（sell/share）**你的個資用於跨情境行為廣告。
 - 不進行跨 App／網站的行為追蹤；若未來導入廣告或追蹤 SDK，將事前公告並依平台政策（如 iOS ATT）與地方法規徵求同意與提供退出機制。
 - 若目的或範圍有重大變更（例如新增不同於原目的的資料利用），我們將以醒目方式通知並（在需要時）再次取得同意。
-

2.8 精簡對照表（便於內外一致與審查）

目的	主要資料類型	你可否選擇	法律依據
提供與維護服務	帳戶識別、認證、遊戲資料、技術資訊	必要（拒絕則無法正常使用）	契約必要／合法利益
安全與公平性	帳戶識別、遊戲資料、技術資訊、遙測、（社群）	基礎偵測必要；可關閉 非必要遙測	合法利益／法定義務
除錯與效能	遙測、技術資訊、崩潰紀錄	基礎必要；擴充遙測可關閉	合法利益
客服與申訴	帳戶識別、你提供的聯絡資訊、遊戲與社群紀錄	可選（不提供可能影響處理）	契約必要／合法利益
研究與學術	去識別化統計（必要）；可識別資料（僅在同意時）	可撤回同意；撤回不影響使用	合法利益／同意
法令遵循	與個案相關之最小必要資料	法定範圍可能不得拒絕	法定義務／合法利益

3. 同意與你的選擇（Consent & Choices）

3.1 運作必要項目（無需另行同意）

為提供你要求的服務並維持系統安全、穩定與公平，以下處理屬提供服務或契約必要／合法利益，即使未額外同意也會進行：

- 帳號註冊與登入、雲端同步與備份（避免本機資料遺失）。
- 基礎安全措施與防外掛／反詐欺（含必要的裝置與網路資訊比對）。
- 基礎除錯與效能監控（崩潰記錄、啟動/載入耗時等**最小必要遙測**）。

若你拒絕提供上述**必要資料**，本服務可能無法正常運作或無法建立帳號。

3.2 需要你明確同意才會進行的情況

- 研究需要「可識別個資」的情境（一般情況採去識別化/彙整，不需個別同意）。
- 非必要的擴充遙測（如更細緻的使用流程事件）。
- 行銷通知（如日後新增電子報）；目前預設不發送。
- 平台要求的追蹤／廣告技術（若未來導入）——詳見 3.4。
我們會以清楚的彈窗或頁面說明目的、資料類型與用途，並提供同意／拒絕選項。

3.3 你可以如何管理或撤回

- App 內設定：你可在 【設定 ▶ 隱私與資料】（實際欄位名稱以 App 內為準）開/關
 - 擴充遙測、研究用可識別資料（如適用）、行銷訊息。
- 帳號/資料刪除：依第 8 節，你可在 **【設定 ▶ 帳號 ▶ 刪除帳號】**或來信請求刪除。
- 撤回同意：對以同意為基礎的處理（例如研究需可識別資料），你可隨時撤回；撤回不影響撤回前之合法處理，也不影響你繼續使用本服務的核心功能。

法律或權利主張所需的法定保存與安全稽核紀錄，於法定或必要期間內仍可能保留。

3.4 平台權限與追蹤 (iOS／Android)

- **系統權限**（如相機、麥克風、相簿、通知）：會在**首次使用前**由作業系統彈出授權視窗，你可於裝置**系統設定**隨時關閉；關閉後相關功能可能無法使用。
- iOS **追蹤**（App Tracking Transparency, ATT）：我們目前**不從事跨 App/網站之行為追蹤**。若未來導入第三方廣告或追蹤 SDK，將先以 ATT 彈窗徵詢同意；若你不同意，該追蹤將不會啟用。
- Android：若未來導入廣告/追蹤 SDK，將依 Google Play 政策提示並提供**退出**選項，且在 Data safety 表單與本政策同步揭露。

3.5 「不同意」對功能的影響（範例）

- 關閉**擴充遙測**：不影響基本遊玩，但可能降低問題診斷精準度。
- 不同意**研究用可識別資料**：仍可遊玩；研究僅使用去識別化/彙整資料。
- 關閉**通知**：你可能收不到活動或系統重要訊息（如恢復碼、處分通知），請改用 App 內信箱或客服。

3.6 對第三方與跨境的選擇

- 我們僅在**處理者**（service providers）**角色**下與第三方（如 Microsoft PlayFab）合作，並依第 6 節所述簽訂 DPA/SCC 等保障。
- 若未來引入會「自用資料」的第三方（例如廣告網路），我們會**另行取得同意**，並提供相關**退出與管理連結**。

3.7 日後變更與再同意

- 若我們**新增與原目的不相容的新目的**（例如導入定向廣告），會以**醒目方式事前通知**，並在需要時**再次徵求你的明確同意**；你可拒絕且仍可繼續使用不依賴該目的的核心功能。

3.8 記錄與證明

- 為符合法規與稽核需求，我們會保存你**同意／撤回同意**的版本與時間戳；你可來信查詢相關紀錄。

4. 我們如何保存與保護資料（Security）

我們採取「多層防護（defense-in-depth）」與「資料最小化」原則，從加密、身分與存取控制、應用與基礎設施安全、到備份與事件通報建置一系列措施。以下列出主要做法與你可預期的保障。

4.1 加密與金鑰管理

- **密碼安全**：密碼僅以 Argon2id／bcrypt／PBKDF2 等不可逆雜湊（含鹽）保存，**不儲存明文**；重設流程使用一次性短效權杖。
- **傳輸加密**：所有客戶端與伺服器間的連線均使用 TLS 1.2 以上（優先 1.3）；停用弱式密碼套件，並採 HSTS（如由 Web 端提供）。
- **靜態加密**：資料庫、儲存體與備份均採**靜態加密（at rest）**（例如 AES-256 等等級）；金鑰以受管機制保存並**定期輪替**；金鑰與資料分層管理，避免同域暴露。

4.2 身分與存取控制（IAM）

- **最小權限與角色分離**：營運與管理操作僅授權最小必要權限；不使用共用帳號。
- **多因素驗證（MFA）**：所有管理介面與雲端主控台採 MFA。
- **存取審核**：對高權限存取進行**定期複核**與即時撤銷；敏感操作（如匯出、刪除）需二次確認或同儕覆核。
- **工作環境隔離**：開發／測試／正式環境相互隔離，避免資料洩漏或誤佈署。
- **工作階段安全**：存取權杖具**短期效期與閒置逾時**；密碼變更或風險事件會**全面撤銷舊權杖**。

4.3 應用程式安全

- **安全開發流程**：程式碼評審、靜態程式碼分析（SAST）、相依套件弱點掃描（SCA）；祕密值不寫入版本控制，使用密鑰庫或環境變數管理。
- **權限最小化**：行動端僅宣告必要系統權限；若未來導入追蹤或廣告 SDK，將先徵詢同意（詳見第 3 節）。

- **攻擊面防護**：使用預備語句與 ORM 防止 SQL 注入；輸出編碼與 CSP/同源策略降低 XSS/CSRF/點擊劫持/SSRF 風險。
- **濫用防護**：登入與敏感 API 設速率限制與異常偵測；必要時啟用 CAPTCHA／風險評分。

4.4 基礎設施與網路

- **網路分段與防火牆**：僅開放最小必要連接埠；管理介面限制來源。
- **WAF/DDoS 緩解**：依雲端供應商能力配置 Web 應用防火牆與 DDoS 緩解。
- **時間同步與設定管理**：所有節點採一致時間源；關鍵設定變更保留審計記錄並可回滾。

4.5 日誌、監控與稽核

- **稽核軌跡**：記錄登入/登出、權限變更、資料匯出/刪除與系統錯誤等事件。
- **去敏與保護**：日誌中不記錄密碼或完整標識；稽核日誌獨立保存並受權限保護。
- **保留與檢視**：營運與安全日誌保留合理期間（例如 180 天）以利調查與合規；異常觸發警報並有人值守處理。

4.6 備份與災難復原（BCP/DR）

- **滾動備份**：資料定期備份並加密保存，採多區或異地冗餘。
- **演練與目標**：定期進行還原演練；設定 RPO/RTO 目標（例如各 ≤24 小時；實際以公告為準）。
- **備份保留期**：備份一般保留 30 天（依第 5 節所定），期滿依程序清除不可復原。

4.7 刪除、匿名化與資料最小化

- **刪除流程**：你啟動刪帳後，我們會在作業系統中刪除或匿名化與帳號可識別連結的資料；
備份中的殘留將在**保留期屆滿**後隨循環覆寫而不可復原。

- **研究資料**：研究原則使用去識別化/彙整資料；需可識別資料時以同意為前提（見第3、2.5節）。

4.8 脆弱性管理與更新

- **修補流程**：持續關注安全公告與相依套件 CVE，依風險等級安排修補時程；關鍵弱點優先處理。
- **變更控管**：重要變更走審核與回滾機制，避免服務中斷或設定失誤。

4.9 事件應變與通報

- **SIRT 流程**：偵測 → 分級 → 隔離/抑制 → 根因分析 → 修復 → 事後檢討與預防改進。
- **通知原則**：如發生可能對你造成高風險之個資事件，我們將依法並於**合理期間**通知受影響玩家與主管機關，內容包含事件概述、可能影響、我們已採取與建議你採取的措施。

4.10 第三方服務供應商（PlayFab 等）

- **處理者角色**：如 Microsoft PlayFab 僅在我們指示下代管玩家帳號／雲端儲存／遙測等作業；我們與其簽有**資料處理協議（DPA）**並在跨境傳輸時採 SCCs 或等效機制。
- **安全對齊**：第三方需具備相當之安全控管與稽核能力；若更換或新增供應商，我們會更新本政策與商店揭露。

4.11 營運端點與裝置安全（單人開發者）

- **開發/營運裝置**啟用整碟加密、最新安全修補、螢幕自動鎖定與惡意程式防護；
存取機密資料需使用 MFA／硬體安全金鑰；
機密檔案與金鑰不以可攜式媒體傳遞；淘汰裝置採安全抹除。

4.12 弱點回報（Vulnerability Disclosure）

- 歡迎你將疑似安全問題回報至 FlameStickUnder@gmail.com（主旨請註明「Security」）。

請避免進行破壞性測試或存取他人資料；我們將於合理工作天內回覆並在驗證後儘速修補。

我們將持續審視並改進上述安全措施；若有重大調整，會在 App 內與本頁公告。

5. 資料保存期間 (Retention)

我們依「**目的限定**」與「**資料最小化**」原則設定保存期間；到期後會**刪除或不可逆匿名化**。不同資料類型的保存期間如下（與後台排程同步）：

5.1 分類保存期間（總表）

- **帳號與遊戲狀態**（帳號、暱稱、Email〔如有〕、進度/資源/ESG 指標、配對紀錄等）
→ 保存至**帳號存續期間**；你啟動刪帳或連續**【12】個月**未登入即排入刪除或匿名化流程。
- **操作／遙測**（事件與時間戳、版本、崩潰/錯誤、效能指標）
→ **【24】個月**後匿名化或刪除。
- **聊天／回饋／檢舉紀錄**（UGC 與處置紀錄）
→ **【24】個月**後匿名化或刪除（如涉及爭議，見 5.3 之例外）。
- **備份**（加密與異地／多區冗餘）
→ **滾動保留【30】天**；到期自動覆寫。你刪帳後，備份中的殘留會在此期間**完全覆寫**而不可復原。
- **研究資料集**
→ 以去識別化或彙整型式長期保存，用於統計與學術；**不可回溯個人**。
- **安全與稽核日誌**（登入/權限變更/匯出刪除等審計事件）
→ 一般保留 **【180】天**；若涉及安全事件或法定要求，依 5.3 之例外處理。

以上天期如因系統或營運調整需更動，將同步更新本政策並在 App 內公告。

5.2 刪除與匿名化的定義與方法

- **刪除（Delete）**：從**主資料庫與搜尋索引**移除紀錄；相關關聯（外鍵、快取）一併清理。

- **匿名化（Anonymize）**：移除或不可逆轉換可識別元素（如帳號/Email 以不可逆雜湊 + 分區鹽處理，去除 IP 的最後段，或聚合至群組層級），使其不再可與個人連結。
- **假名化（Pseudonymize）**：僅於除錯短期需要時使用；其「還原鍵」與生資料分開保存且限權限存取，達成目的即清除。

5.3 法律與安全例外（Legal Holds）

以下情況可能延長保存至處理結束或法定期間屆滿（以較長者為準）：

- 法令義務或主管機關合法要求（例如刑案調查、行政裁處）。
- 權利主張、防禦或爭議處理（例如對戰／道具爭議、檢舉申訴、濫用退款調查）。
- 資安事件鑑識：為釐清事件、強化防護，相關稽核與網路日誌得於合理期間內保存。

我們會遵循**最小必要原則**，只保留與個案直接相關的資料，並於事由消滅後立即刪除或匿名化。

5.4 使用者觸發的刪除：作業時序（範例）

當你在 **【設定 ▶ 帳號 ▶ 刪除帳號】**提出刪除要求時，系統會按下列時序處理（若你於寬限期內取消刪除，流程即終止）：

- T+0：標記帳號為「待刪除」、立即停用登入與同步；從主要查詢路徑下架資料；寄送確認通知。
- T+7 日內：**自主資料庫**刪除或匿名化與帳號關聯之資料（遊戲進度、UGC 除涉及申訴/違規者外）。
- T+14 日內：清理快取／搜尋索引／內部分析表的對應切片。
- T+30 日內：備份輪替覆寫完成（見 5.1）；此後資料不可復原。

若帳號因連續**【12】**個月未登入觸發「不活躍刪除」，會在 T - 7 先發到期提醒；逾期未登入即依上列流程處理。

5.5 同意、條款與申訴紀錄

- 為符合法規與查核需要，我們保留**同意／撤回同意**、條款接受、申訴流程之**時間戳與版本**，保存期為：**帳號存續期間 + 最長【3年】**（或至爭議終結／法定期間屆滿）。
- 這些紀錄**不包含**你的密碼或完整可識別內容，主要用於合規證明與爭議處理。

5.6 你的其他選擇

- 你可隨時依第8節行使**查閱、更正、刪除、限制處理**等權利；我們會在**【30】天**內回覆（依法得延長並說明理由）。
- 若你只希望**停用帳號**而保留進度資料（例如短期休息），可來信提出；停用**不啟動刪除流程**，到期前我們會再提醒你是否轉為刪除。

6. 資料分享與第三方（Sharing & Third Parties）

我們不出售或共享（sell/share）你的個資用於跨情境行為廣告，亦不允許第三方將你的資料用於其自有行銷目的。除以下情形外，我們不會向第三方揭露個資：

6.1 服務供應商（處理者 / Service Providers）

我們為提供與維運本服務，委託合格的第三方供應商在我們**書面指示**下代為處理資料。這些供應商僅在**達成本政策載明之目的**所需的範圍內處理資料，並與我們簽署**資料處理協議（DPA）**與（如涉及跨境）**標準合約條款（SCCs）**或其他等效機制。我們仍為資料控制者並負最終責任。

- Microsoft PlayFab
角色：處理者（代管）
用途：玩家帳號、雲端儲存、遙測/防濫用、配對與遊戲狀態維護
處理資料：帳戶識別、密碼雜湊與重設權杖、遊戲資料、操作/遙測、必要技術資訊
安全：依其平台安全與合規標準運作；與我們簽有DPA，跨境傳輸採SCCs或等效機制
保留：依我們設定之保存期間與刪除指示執行

*若日後新增 Crash/分析/CDN/郵件等供應商（如 Crashlytics、Application Insights、CloudFront 等），我們會更新下方「**第三方清單表**」與本節說明。

6.2 學術研究合作

為達成第2節所述之研究目的，我們可能與研究機構合作。原則上僅提供去識別化或統計化資料；如研究確需處理可識別資料且法律要求，我們會**事前明確告知並徵得你的同意**，並簽立資料使用/保密協議以確保安全。

6.3 法律需求與權利保護

在以下情形，我們可能於**最小必要範圍**內揭露資料：

- 遵循法院、檢調或主管機關之合法請求或法律義務；
- 針對詐欺、濫用、資安事件或侵害權利之行為，為主張、行使或防禦法律上權利所必須。

6.4 公司交易

若發生合併、投資或資產移轉，我們將要求受讓方依本政策持續保護你的資料，並在交易完成前以**醒目方式**告知；如受讓方所採政策有重大差異，將另行徵詢你的選擇或同意。

6.5 不出售、不共享廣告用途

我們不出售（sell）你的個資；也不共享（share）你的個資供第三方用於跨情境行為廣告。若未來政策變更（例如導入廣告網路），我們將事前通知並提供退出/同意選項（詳見第3節）。

6.6 第三方 SDK 原則

- 僅納入運作必要之 SDK，並進行**隱私與安全評估**；
- 於 App 內、App Store 「App Privacy」與 Google Play 「Data safety」一致揭露；
- 若 SDK 涉及追蹤或需要額外權限，將**事先徵求同意**並提供**退出機制**。

6.7 跨境傳輸與保護

如資料需傳輸至你所在法域以外，我們將採 SCCs 或其他合法機制，並評估接收方的保護水準（詳見第7節）。所有處理者須符合與我們**等同**的安全要求。

6.8 你的選擇與查詢

你可依第8節行使權利，並來信要求我們提供目前使用中的**第三方處理者清單**與其所在地、用途與資料類型摘要。我們將於法定時限內回覆。

6.9 第三方清單表（維護用／對外可公開）

供應商名稱	角色	主要用途	取得之資料	主要地區/雲區*	合法基礎	保存/刪除
Microsoft PlayFab	處理者	帳號、雲端存檔、遙測/防濫用	帳戶識別、密碼 雜湊、遊戲資料、遙測、技術資訊	【例如：美國/亞太（供參考，依實際專案標註）】	契約必要/合法利益	依我們指示（見第 5 節）

* 實際雲區與資料中心位置，請依你的部署填寫（例如「亞洲東北 1／美國東部」）。

我們會隨服務變更**更新本表**。如新增會影響你權益的第三方或用途，我們將以醒目方式告知，必要時再次徵求同意。

7. 國際資料傳輸 (Cross-Border Transfer)

為確保可用性與備援，我們使用雲端與受託處理者（例如第 6 節所列 Microsoft PlayFab）提供本服務。據此，你的資料可能於不同雲區/資料中心處理或備援（例如：東亞、東南亞、美國等；實際地點視部署與服務供應商而定）。

7.1 轉移情境與必要性

- 為了註冊/登入、雲端存檔、配對、除錯與安全等核心功能，我們可能將資料傳輸至你所在法域以外的雲區進行處理。
- 這些跨境傳輸僅限於提供與維運本服務所必須的範圍與次數，不以行為廣告或第三方自行用途為目的。

7.2 法源與契約保障

- 我們與受託處理者簽訂**資料處理協議（DPA）**，要求其僅依我們指示處理，並落實等同之安全標準與刪除機制。
- 如涉及 **EEA/UK → 第三國**的資料轉移（若未來服務擴及該地區），我們將採用：
 - **歐盟標準合約條款（SCCs）**，以及必要時的**補充措施**；
 - 或 **英國 IDTA／SCCs 英國附加條款**（視情況適用）。
- 對於其他法域，我們將依當地法令選用等效的**契約或合規機制**，並確保受方受相當之保護義務拘束。

7.3 補充技術與組織措施

為降低跨境傳輸風險，我們採取下列**補充措施**：

- 傳輸加密（TLS 1.2+）與靜態加密（*at rest*），金鑰採分層管理並定期輪替；
- 存取最小化、角色分離與多因素驗證（MFA）；
- 視需求對分析/研究資料施行去識別化或假名化；
- 日誌與稽核：對跨區存取、匯出與刪除行為留存稽核軌跡並定期檢視。

7.4 你的查詢與取得資訊的權利

你可來信 FlameStickUnder@gmail.com 要求了解：

- 目前使用的主要雲區/資料中心所在地；
- 適用的**傳輸機制**（例如 SCCs/IDTA）與**主要保護措施**的概要；
- 在符合法令與保密義務前提下，**相關契約保障**的摘要或可提供之副本。

7.5 變更通知

若我們新增實質不同的接收方、改變主要雲區或變更傳輸機制，且可能重大影響你的權益，我們將以醒目方式事前通知；必要時會再次徵求你的同意（見第 3 節）。

提醒：基於服務運作必要之跨境處理，若你要求完全禁止則可能導致**無法建立帳號**或**使用雲端存檔/多人功能**；你仍可依第 8 節行使存取、刪除、限制處理等權利。

8. 你的權利與行使方式 (Your Rights)

依台灣《個人資料保護法》及適用法規，你得就你的個人資料行使下列權利。我們將以清楚透明的方式處理你的申請。

8.1 你可以行使的權利

- **查詢或請求閱覽／製給複本**：取得我們是否持有你的資料及其內容（在技術可行範圍內提供可攜格式）。
- **請求補充或更正**：若資料不完整或不正確，你可以要求更正。
- **請求停止蒐集／處理／利用**：於特定情況下可限制或反對處理（如非必要之擴充遙測、行銷訊息等）。
- **請求刪除**：於法定與合約許可範圍內，要求刪除與你可識別連結的資料。
- **撤回同意**：對以同意為基礎的處理（例如研究若需可識別資料），你可隨時撤回，且不影響撤回前之合法處理。

若你位於適用提供**資料可攜權**的法域（如部分海外法令），我們亦會善盡協助。

8.2 如何申請

- App 內：**【設定 ▶ 帳號 ▶ 刪除帳號】** 可直接啟動刪帳流程。
- Email：寫信至 FlameStickUnder@gmail.com，標題建議為「個資申請 - (查閱／更正／限制／刪除／可攜)」。
請附：
 1. 你的遊戲帳號／暱稱、
 2. 申請的項目與範圍、
 3. 能證明你身份的資訊（例如從註冊用信箱寄出、或提供客服指定的驗證碼）。

我們可能為確認申請人身份而請你補充資訊；若你委託他人代為申請，需提供**書面授權與可驗證之身分資料**（遮蔽非必要欄位即可）。

8.3 回覆時程與方式

- 我們將於**【30天】內回覆你的申請；如因技術或案件複雜度需要依法得延長**，會先告知延長理由與預計時程。
- 原則上提供電子方式回覆（如可攜格式檔案）；對於重複、過度或顯不相當的請求，法令允許時我們得收取合理成本費用或婉拒並說明理由。

8.4 刪帳後會發生什麼

- 你在 **【設定 ▶ 帳號 ▶ 刪除帳號】**提出刪帳後，系統會依第 5 節規範進行：
 - 立即停用登入與同步，並排入刪除／匿名化作業；
 - 主資料庫於 T+7 日內刪除或匿名化與帳號可識別連結的資料；
 - 快取／索引／內部分析表於 T+14 日內清理；
 - 備份在 【30】天滾動覆寫完成後不可復原；
 - 公開社群內容（如在頻道張貼之訊息）原則上以匿名化方式保留社群脈絡（例如顯示「已刪除使用者」）。
- 刪帳為不可逆動作；所有進度與虛擬資產將一併移除且無法復原。

8.5 法律與安全之例外

在以下情形，我們可能依法延後或拒絕刪除／限制請求，並提供說明：

- 依法須保存或配合法院／主管機關合法要求；
- 為主張、行使或防禦法律上權利所必要（例如對戰／道具爭議、資安事件鑑識）；
- 為保護你或他人之生命、身體、自由或財產所必須；
- 為維護服務安全與公平性所必要且無較小侵害之替代方式。

我們會遵循**最小必要**原則，只保留個案直接需要的資料，事由消滅後立即刪除或匿名化。

8.6 申訴與救濟

- 若你對我們的回覆不滿意，你可再次來信或依你所在地法令向**主管機關**提出申訴。
- 我們將善盡協助並提供必要的處理紀錄摘要（於法律允許範圍內）。

8.7 (如上架 Android) Google Play 之刪帳網頁要求

- 未安裝 App 的使用者亦可透過以下網頁提出刪帳請求：**【<https://你的網域/delete>】**（請建立此頁）。
- 我們會在此頁驗證你的身份並啟動與 App 內相同的刪除流程與時程。

9. 兒童與青少年 (Children & Teens)

本服務面向 13 歲以上之使用者，不以 13 歲以下兒童為對象，也不主動蒐集其個人資料。若你認為 13 歲以下兒童在未經同意下提供了資料，請立即來信 FlameStickUnder@gmail.com (主旨：Underage Report)，我們將依下列程序處理。

9.1 年齡原則與家長同意

- 13 歲以下：我們**不主動提供帳號註冊**；如確有必要且法律允許的特定方案，將以**「可驗證之法定代理人同意」（下稱**家長同意**）為前提，並僅處理提供該特定功能所必須**之最小資料。
- 13 - 17 歲（青少年）：可於一般條款下使用本服務；我們採**預設保護**（見 9.2）。若某些功能/研究需要額外權限或敏感資料，會**另行徵求同意**；如屬需家長同意之情形，將同時徵詢家長。

（國際適用說明）若未來服務面向 EU/UK 等地區，將依當地「兒少同意年齡」規範（約 13 - 16 歲間，依國別不同）調整同意與驗證機制。

9.2 對未成年使用者的預設保護

為降低風險，我們對 13 - 17 歲使用者採下列**預設更嚴格**的做法（除非法律允許且經當事人／家長明示同意變更）：

- **資料最小化**：僅收集運作所需資料，不要求提供不必要的聯絡或身分資訊。
- **公開度預設較低**：聊天/社群功能預設為較保守的可見性與互動權限；可使用**封鎖、檢舉與靜音**機制。

- 不作定向行為廣告：不以未成年者資料進行跨情境行為廣告或相似的追蹤用途。
- 研究用途：原則上僅使用去識別化／彙整資料；若研究需要處理可識別資料，會事前清楚說明並徵求本人與（必要時）家長同意，且可隨時撤回。

9.3 家長同意與驗證方式

當法律或功能需要家長同意時，我們會以**清楚可理解**的方式說明資料類型、用途、保存期間與風險，並透過合適方式完成**可驗證**之家長同意（例如：

經註冊信箱驗證+附加核對流程、可驗證之數位簽章／電子同意、或其他法律允許的方法）。

我們會採**最少資料**驗證原則，不會要求不必要的證件影本；驗證資料只在必要期間內保存。

9.4 發現未成年誤用的處理

若我們發現或合理懷疑有**未經家長同意**的 13 歲以下註冊／使用，將採下列措施：

1. 立即凍結帳號與資料新蒐集；
2. 聯繫帳號持有人與（如可行）家長，進行年齡與同意確認；
3. 若確認未符合要求，**刪除或不可逆匿名化**與帳號可識別連結的資料（依第 5 節之時序），並以匿名化方式處理其公開社群脈絡；
4. 將處理結果回覆通報人與/或家長（在法律許可範圍內）。

9.5 家長與監護人的權利

法定代理人可代表未成年使用者行使第 8 節所載之權利（如查閱、刪除、限制處理、撤回同意等）。

請以監護人身分寫信至 FlameStickUnder@gmail.com（主旨：**Guardian Request**），並按照我們的身分確認指引提供必要資訊（可遮蔽非必要欄位）。

9.6 社群與互動的安全補充

針對未成年人，我們會優先執行：

- 自動化濾字與異常偵測（例如暴力、仇恨或色情關鍵字）；

- 容易存取的檢舉入口與人工覆核；
- 對於屢犯或嚴重違規者，採取禁言、停權等處置，並在必要範圍內保留稽核紀錄以供申訴與安全目的（依第 5 節保存期間）。

10. 社群與互動內容（Community & UGC）

本節適用於你在本服務中產生或傳送的使用者產生內容（UGC），例如：公開頻道與任務登陸訊息、私訊、留言、回饋、檢舉與其附件（如截圖、文字記錄），以及與這些內容相關的處置與稽核紀錄。

10.1 可見性與公開範圍

- **公開頻道**：你在公開頻道張貼的內容，任何有權進入該頻道的玩家都可見，並可能被他人轉傳或截圖。我們無法控制他人後續使用行為。
- **半公開/群組**（如公會、隊伍）：內容對該群組可見。群組管理員可能擁有額外管理權限。
- **私訊**：僅限收/發雙方可見；但為處理檢舉、法令或安全需求（見 10.3、10.5、10.6），在**最小必要範圍**內得由授權人員調閱。

請避免在任何頻道分享能辨識你或他人的敏感資訊（例如真實姓名、住址、聯絡方式、財務與健康資料等）。

10.2 我們如何處理你的社群內容

- **目的**：提供交流功能、維護秩序與安全、處理檢舉/申訴、改進服務（詳見第 2 節）。
- **資料最小化**：僅處理與上述目的相關之最小必要資料。
- **研究用途**：原則上僅以去識別化/彙整後的社群互動資料進行統計分析；若研究確需可識別資料，將另行徵求同意（見第 2、3 節）。
- **不作行為廣告**：不以你的社群內容從事跨情境行為廣告或出售/共享個資。

10.3 社群治理機制（自動與人工）

- **自動化過濾**：為阻擋垃圾訊息與顯著違規內容（如惡意連結、嚴重辱罵），我們可能使用關鍵字/規則或機器學習模型先行標記或**暫時隱藏**內容。

- **人工審查**：遭檢舉或系統標記的內容，由受訓且受保密義務拘束的授權人員，在**最小必要範圍**內審查。
- **風險控制**：對異常互動（洗頻、詐騙）適用速率限制、冷卻時間或暫時性限制功能。
- **工具**：提供**靜音/封鎖/檢舉**等使用者控管工具，降低你暴露於不當內容的風險。

10.4 違規處置

若內容或行為違反社群規範/服務條款或法律，我們得視情節採下列一種或多種處置：

- 內容下架/隱藏/標記；
- 警告、禁言、短期或長期停權；
- 重置或回溯遊戲資源/戰績（如因外掛或濫用取得）；
- 必要之通知（涉違法者得通報主管機關）。

你可依 10.6 節啟動**申訴流程**；我們將在合理時間內完成複核。

10.5 保存與刪除（與第 5 節銜接）

- **一般保存**：社群內容與處置紀錄通常保留 **【12 - 24】個月**（見第 5 節實際期間）後刪除或匿名化。
- **法定/爭議例外**：涉及爭議、檢舉或法令需求者，依第 5.3 節得延長保存至結案或法定期間屆滿。
- **刪帳時**：你刪除帳號後，我們將依第 5 節時序刪除或匿名化與你可識別連結的內容；為維持討論脈絡，公開貼文通常以「**已刪除使用者**」等匿名化方式保留。

10.6 檢舉與申訴流程

- **檢舉**：你可於訊息選單或玩家頁面使用「**檢舉**」；請提供必要資訊（時間、頻道、說明）。
- **申訴**：對於禁言/停權或內容處置結果，你可透過 App 內客服或寄信 **FlameStickUnder@gmail.com** 提出申訴（建議主旨：**Appeal + 你的帳號/暱稱**）。

- 時程：我們將於**合理時間內**（通常 【X】個工作天）回覆並完成人工覆核；必要時可要求你補充資料。

10.7 你的責任與安全提醒

- 你應確保上傳或張貼的內容**不侵犯他人權利**（著作權、人格權、隱私），且不含違法或具高度風險的資訊（詐騙、色情、仇恨、個資公開等）。
- 請妥善使用**封鎖/靜音**功能並避免點擊可疑連結；若發現安全問題，請立即檢舉並通知我們。

10.8 第三方與跨境

- 若社群或儲存由第三方處理者（如 PlayFab）代管，將受第 6、7 節之DPA/SCCs 等保障與跨境措施拘束。
- 若你透過第三方連結或外部平台互動，其資料處理受該第三方政策約束。

我們會隨服務演進持續改進治理工具與政策；若社群治理方式有重大變更（例如導入新型自動化過濾），將於 App 內與本頁**醒目公告**，必要時再次徵求你的同意。

11. 自動化決策與申訴（Automated Decisions）

我們不以純自動化方式做出對你產生法律效果或其他**重大影響**（例如永久停權、刪除帳號、不可逆資產處置）的最終決策。

本服務的自動化系統（例如**反作弊**、**濫用與垃圾訊息偵測**、**風險評分**）主要用於**即時風險控管與預警**，其輸出為**分數/標記**，供人員複核或觸發**短期、可逆的保護性措施**（例如暫時限速、暫時隱藏訊息）。

11.1 自動化系統會使用哪些訊號

- **遊戲與操作遙測**：異常操作節奏、非人類輸入軌跡、版本/裝置不一致。
- **帳號與裝置/網路訊息**：多帳共用、異常登入地區、可疑代理樣態（僅限**必要技術資訊**）。
- **社群互動**：被多次檢舉、典型垃圾訊息樣式（見 §10）。

我們不使用**敏感類別**（如種族、宗教、健康等）作為判定依據，也不進行跨 App/網站的行為追蹤。

11.2 可能採取的自動措施（預防性、可逆）

- 即時限速／冷卻、暫時隱藏內容、暫時禁言、強制重新驗證。
- 這些措施皆以**最小必要與最短時間**為原則，並保留人工覆核與還原機制。

11.3 何時需要人工覆核與「人做最後決定」

- 永久性處置或具有重大影響的處置（如永久停權、不可逆資產回收/回溯、刪除帳號）在執行前必須由授權人員審查並做出最終決定。
- 對於反作弊高風險個案，我們會檢視**關鍵證據**與**偵測脈絡**（在不危及安全與規避風險的前提下）再決定。

11.4 你如何申請人工覆核／申訴

- 來信：FlameStickUnder@gmail.com（建議主旨：Appeal + 你的帳號/暱稱）。
- 請提供：事件時間、你看到的系統訊息/畫面截圖、相關頻道或對戰編號、你認為的正當說明。
- 回覆時程：我們將於**【30】個工作天內回覆並完成人工覆核**；複雜個案得延長並先行告知。
- 結果內容：我們會說明處置是否維持/調整/撤銷與主要考量因素；為防止規避，可能不公開可導致規避的偵測細節或模型參數。

11.5 若判定有誤，我們會怎麼補救

- 立即撤銷或調整處置、還原受影響的虛擬資產/進度（可行範圍內）、清除不當標記。
- 同步校正模型/規則或門檻，並記錄於事後檢討以避免重發。

11.6 日誌、保存與權利

- 與自動化判定相關的稽核與事件日誌會依 §5.1、§5.5 的期間保存（一般 【180】天；涉爭議/法令例外依 §5.3）。
- 你可依 §8 行使查詢、更正、刪除或限制處理等權利；但如涉及法定保存或安全鑑識，我們可能在必要範圍內延後或拒絕並說明理由。

11.7 選擇與影響

- 你可在 §3 所述關閉非必要的擴充遙測；但基礎安全與穩定性訊號屬運作必要，否則可能無法提供核心功能或將提高誤判風險。
- 任何重大改動（例如導入新型自動化審核或用途轉變）將醒目公告並（如需）再次徵求同意。

總結：人負責最後決定。自動化只作輔助與短期保護；你永遠可以申請人工覆核，我們也承諾在有誤時更正並補救。

12. 第三方服務與 SDK

為提供本服務之登入、雲端儲存、穩定性與社群功能，我們可能於 App 內或伺服器端使用第三方服務與 SDK。

原則：只納入「運作必要」的服務，並以資料最小化、安全等級不低於本服務為前提。與我們合作之第三方多屬資料處理者（service provider / processor），僅依我們指示處理資料並簽有 DPA；如涉及跨境傳輸，依 §7 採 SCCs 或等效機制。

若你「直接使用第三方帳號／平台」登入或互動（例：某社群平台、語音服務），該第三方就其收集/使用之資料可能為獨立資料控制者，其處理受該第三方的隱私政策約束。

12.1 我們可能使用的第三方類型（依實際導入為準）

- 身分與雲端存檔：玩家帳號、雲端儲存、配對、遙測/防濫用（例：Microsoft PlayFab）。
- 崩潰回報／效能分析：收集錯誤與效能指標（僅最小必要）。
- 內容傳遞（CDN）與檔案儲存：加速下載、聊天附件（如有）。
- 客服/郵件：回覆工單、寄送重要通知（不做廣告郵件）。

- 語音/社群（如未來導入）：即時通話、群組社群功能。

目前已使用之供應商與用途，詳見 §6「資料分享與第三方」及其**第三方清單表**；後續新增將同步更新兩節內容。

12.2 資料類型與用途

依 §1/§2 所述，我們可能透過第三方處理帳戶識別、密碼雜湊、遊戲資料、必要技術資訊、最小必要遙測與（啟用時）社群內容等，用途限於：提供與維護服務、除錯與安全、客服與申訴，以及（在去識別化原則下）研究統計。

我們**不出售或共享（sell/share）**你的個資供跨情境行為廣告，也不允許第三方自用你的資料作行銷。

12.3 權限、追蹤與同意

- 系統權限（相機/麥克風/相簿/通知等）僅在功能需要且你操作觸發時，由系統彈出授權；你可於裝置設定隨時關閉，相應功能可能不可用。
- 目前不導入跨 App/網站的追蹤。若未來新增可能涉及追蹤的 SDK（例如廣告網路），我們將事前公告，於 iOS 以 ATT 彈窗徵詢同意，並在 Google Play Data Safety 與本政策同步揭露與提供退出選項（詳見 §3）。

12.4 第三方清單（節錄）

完整清單與更新以 §6.9 為準。下列為目前已使用或規劃項目之格式示例：

服務/SDK	供應商	角色	主要用途	資料類型	跨境機制	退出/同意
PlayFab	Microsoft	處理者	帳號、雲端存檔、配對、遙測/防濫用	帳戶識別、密碼雜湊、遊戲資料、遙測、技術資訊	SCCs/等效	不適用（運作必要）

12.5 外部連結與第三方網站

若你自 App 連往第三方網站或服務（例如官方社群、說明文件），其資料處理由該第三方負責；請閱讀其隱私政策與服務條款。我們不對第三方之內容與作法負責。

12.6 管理你的偏好

- 你可在 【設定 ▶ 隱私與資料】（實際名稱以 App 內為準）關閉非必要的擴充遙測；核心功能所需之處理則屬運作必要。
- 權限可於裝置系統設定管理；若關閉，相關功能可能不可用。
- 若要查詢第三方清單、地區與用途摘要，或請求刪除由處理者代管的你的資料，可依 § 8 聯絡我們。

12.7 變更與通知

新增或更換可能實質影響你權益的第三方（例如新增類型為廣告/追蹤的 SDK）時，我們會以醒目方式事前通知並在需要時再次徵求同意；同時更新本節與 §6/§7、App Store 「App Privacy」與 Google Play 「Data Safety」填報內容。

13. 平台揭露一致性（App Store / Google Play）

我們在 App Store 「App Privacy」與 Google Play 「Data safety」所填資訊，與本政策內容一致。如有重大變更（見 13.2），我們會同步更新兩平台與本政策，並以醒目方式通知；如屬以「同意」為基礎的處理或對你權益有重大影響者，將再次取得同意。

13.1 一致性原則

- **單一資料清冊**（source of truth）：以本政策與內部資料清冊為準，平台表單為其摘要。
- **最小必要與真實揭露**：只收集與目的相符之最小資料，據實勾選「收集/分享/用途」。
- **同步更新**：任何對資料類型、用途、分享對象、保存期、權利行使流程之調整，均同步更新政策與平台表單。

13.2 需要更新與通知的「重大變更」示例

- 新增/更換 **第三方 SDK** 或服務供應商，導致**資料類型/用途/分享**改變。
- 新增 **追蹤/廣告**相關處理（需 iOS ATT 與 Play 表單更新）。
- 新增蒐集**敏感類型**（例如精確定位、生物特徵等）。
- **研究**從僅用去識別化改為需處理可識別資料（需再次同意）。
- **保存期間、刪帳機制、或跨境機制**（SCCs 等）改變。
- **兒少政策或社群治理**有實質調整。

13.3 變更時的標準作業程序（SOP）

1. **影響評估**：盤點資料→用途→合法依據→分享對象→保存期。
2. **更新文件**：修訂本政策（與版本/日期）、內部資料清冊與刪除/匿名化排程。
3. **更新平台表單**：
 - App Store Connect：App Privacy（必要時更新Privacy Manifest／Required-Reason AP Is 說明）。
 - Play Console：Data safety（含「是否分享給 service providers」與**刪帳網頁 URL**）。
4. **App 內提示**：以橫幅、彈窗或版本更新說明顯示；如需要，**再次取得同意**。
5. **紀錄保存**：保存舊版政策與變更紀錄、同意/撤回同意時間戳（見 §5.5）。

13.4 iOS 專項

- **App Privacy**：據實勾選資料類型（如 Contact Info/Identifiers/User Content/Usage Data/Diagnostics）與用途（App 功能、分析、安全、客服等）。
- **Privacy Manifest／Required-Reason APIs**：若使用被列為需說明之 API，於清單中敘明理由並與政策一致。
- **帳號刪除**：App 內提供刪帳入口（見 §8），與政策一致。

13.5 Google Play 專項

- **Data safety**：
 - 「是否收集」：就各資料類別據實填答；
 - 「是否分享」：如由**service provider（處理者）**代處理（如 PlayFab），勾選並註明屬服務供應商；
 - **安全作法與資料刪除**：對應 §4、§5；
 - **刪帳網頁 URL**：提供未安裝 App 之用戶的刪帳入口（見 §8）。

13.6 迷你對照表（供填報參考）

我們的資料類別 (§1)	App Store 類別	Play Data safety 類別/用途
帳戶識別（帳號/暱稱/E-mail）	Contact Info / Identifiers	Personal info (收集)；用途：App 功能、客服
密碼雜湊	不公開（屬認證內部）	不單獨揭露（安全實作）；於安全說明呈現
遊戲資料（進度/資源/ESG 指標）	Usage Data / User Content (依呈現)	App activity / App info & performance；用途：App 功能、分析

操作與遙測、崩潰	Usage Data / Diagnostics	App info & performance；用途：分析、除錯
社群內容（聊天/檢舉）	User Content	App activity；用途：社群治理、客服
技術資訊（IP/裝置/OSS）	Identifiers / Diagnostics	Device or other IDs / App info & performance；用途：安全、防詐

上表為歸類範例；最終以平台選單與實作為準。

13.7 查詢與反饋

若你發現**平台揭露與實際行為/本政策不一致**，或有疑問，請來信 FlameStickUnder@gmail.com；我們會儘速查核與更正，並在必要時**重新通知與取得同意**。

14. 政策變更（Changes）

我們可能因服務調整、法規更新或安全需要而更新本政策。除法律另有要求外，我們會依下述原則辦理：

14.1 何謂「重大變更」

以下情形屬**重大變更**，將以醒目方式通知，並在需要時**再次徵詢同意**（見 §14.3）：

- 新增或變更**資料類型**（例如開始收集精確定位、聲音、影像、生物特徵）。
- 新增或變更**處理目的**（例如導入行為廣告/追蹤、將研究從去識別化改為需可識別資料）。
- 新增或更換**第三方服務/SDK**，導致資料的**收集、分享對象或用途改變**（見 §6、§12）。
- **保存期間、刪帳機制、跨境傳輸機制**（例如 SCCs）等影響你權益的調整（見 §5、§7）。
- 兒少/未成年人相關政策的實質改動（見 §9）。

14.2 通知方式與時程

- **一般更新**：於 App 內與本頁**標示最新日期**並提供更新摘要。
- **重大變更**：以 App 內彈窗/橫幅、版本更新說明或（如你提供聯絡方式）Email通知；原則上將於**生效日前【7】天**提前公告。
- **緊急安全或法遵更新**：可能即刻生效，並在合理期間內補行通知。

14.3 同意機制

- **以同意為基礎的新處理**（例如可識別資料用於研究、廣告追蹤）：將以**明確同意（opt-in）**為前提；不同意者不會啟用該處理，且不影響核心功能（若可行）。
- **非同意基礎的調整**（例如文字澄清、流程優化、提升安全）：屬一般更新，公告後持續使用即表示你理解並同意更新內容。
- 若你不同意重大變更且該變更非提供服務所必須，你可依 §8 行使**限制處理或刪除/刪帳權利**。

14.4 版本標示與存檔

- 我們會在本頁顯示「**最後更新日期**」與**版本編號**，並提供**更新摘要/變更記錄**。
- 舊版政策將**存檔至少【24】個月**以供查閱；如你需要更久的歷史版本，可來信索取（在法令與保密義務允許範圍內）。

14.5 生效日與解釋

- 除另行說明，**生效日**為本頁所示之最新日期。
- 如多語版本內容有歧異，以**中文版本**為準。
- 對更新內容有疑問或需協助，請聯絡：FlameStickUnder@gmail.com。

提醒：若未來導入會影響你權益的新用途（例如廣告/追蹤或改變第三方分享），我們將依本節與 §3、§13 的流程事前通知並（如需）再次取得同意。

15. 聯絡方式（Contact）

- 資料控制者：個人開發者【林耿賢】（單人／無註冊團隊）
- 聯絡信箱：FlameStickUnder@gmail.com
- 通訊地址：高雄市楠梓區裕昌里藍昌路119巷38號

若未來服務涉及 EU/UK 使用者，將依規定補充 **歐盟/英國代表** 之聯絡資訊；若面向 **加州** 使用者，將另行提供 CCPA/CPRA 專區與行使權利的網頁表單。

附錄：資料 × 目的 × 合法依據 × 保存期

本表為快速對照，細節以 §1（資料類型）、§2（處理目的與法源）、§5（保存期間）為準；遇爭議或法定需要時，適用 §5.3 的**法律／安全例外**與留存規則。

資料類別	目的	合法依據	保存期
帳戶識別（帳號／暱稱／Email）	註冊、登入、雲端同步、客服通知	契約必要／合法利益	帳號存續；你刪除帳號或連續【12】月未登入後刪除或匿名化
密碼雜湊	身分驗證（不保存明文）	契約必要	與帳號同
遊戲資料（進度／資源／ESG 指標 等）	提供與維護服務、備份、爭議處理	契約必要／合法利益	與帳號同；備份滾動保留 30 天
操作與遙測（事件／崩潰／效能）	除錯、效能監控、相容性改善	合法利益	24 個月
社群互動（聊天／檢舉／回饋）	社群治理、申訴處理、客服	合法利益／法定義務	24 個月（依 §5 實際設定）

技術資訊 (IP／裝置 ／OS 等)	安全、防詐、連 線診斷	合法利益／法定 義務	24 個月
研究資料 (去識別 化)	行為研究與論文	合法利益／(需 識別時：同意)	去識別化後 長期 保存，不可 回溯個人