舒 聊　　S O O T H

你的談話，
我們是這樣保護的

一份寫給心理師與個案的資料安全說明。

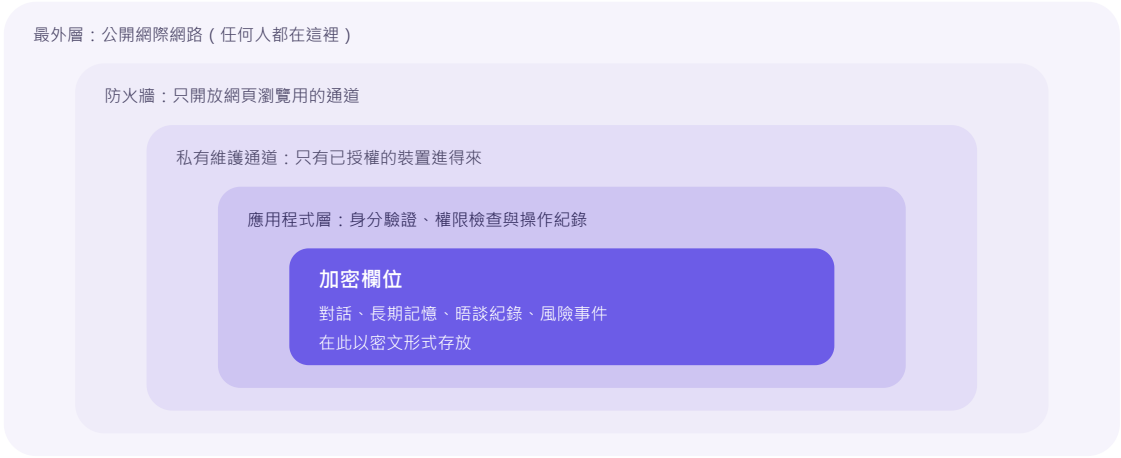
為什麼我們要寫這一份

願意說出口的話，往往是最不想被別人聽見的部分。我們認為，一個承接這些話的系統， 有義務把自己的保護方式攤開來講清楚——包括做得到的，以及**做不到的**。這份文件兩者都會寫。

1 一分鐘看懂：資料放在哪裡

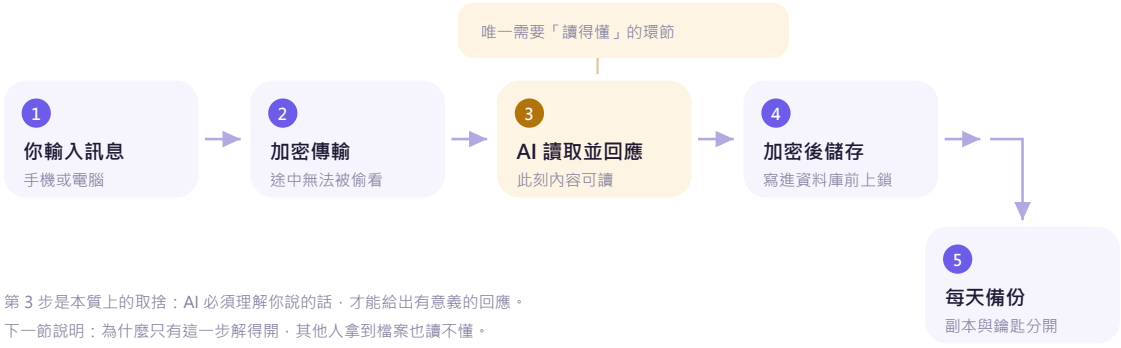
如果把舒聊的系統換成一個實體場景，最接近的其實是**銀行的保管庫**：

在銀行保管庫	在舒聊系統裡	意義
只留一個對外櫃檯，其他出入口封閉	對外只開放網頁通道	能被敲門的地方越少越好
行員走專用通道，要驗證本人與識別證	維護通道走私有網路，綁定身分與裝置	陌生人連門在哪都找不到
貴重物品逐件鎖進保管箱	敏感內容加密後才寫入資料庫	檔案被拿走也讀不懂
鑰匙不和保管箱放在同一個房間	金鑰與資料分開保管	拿到箱子不等於打得開
副本存放在另一個分行的金庫	異地加密備份、可回溯時間點	火災不會讓一切消失



圖一：一層一層往內包的保護。要碰到最裡面的內容，必須依序穿過每一層。

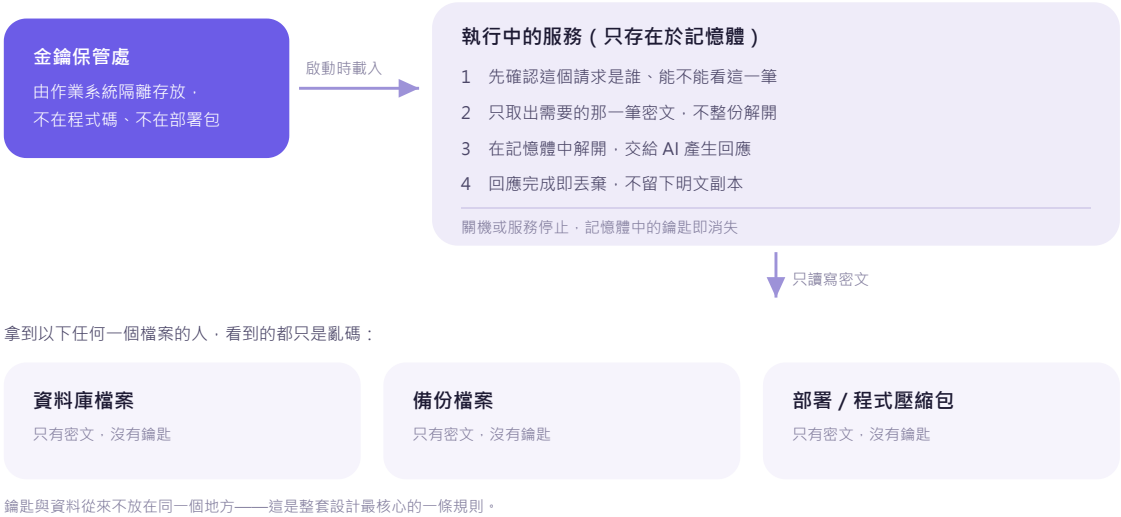
2 訊息路徑



圖二：訊息的完整路徑。除了 AI 處理的瞬間，內容在傳輸與儲存時都是上鎖狀態。

3 鑰匙在哪裡：為什麼只有第 3 步解得開

「加密」如果鑰匙就放在旁邊，等於沒鎖。真正的關鍵是**鑰匙的保管方式**與**解密的時機**。



圖三：金鑰的流向。資料可以被複製，但複製資料的人不會同時得到鑰匙。

四個具體的保障

其一　鑰匙不寫在任何檔案裡

加密金鑰不寫進程式碼、不進版本控制、不放進部署壓縮檔，也不出現在一般的環境變數列表中。 它只在服務啟動時由作業系統的隔離機制交給程式，存在於執行中的記憶體。金鑰、程式與資料三者分開管理。

其二　解密是逐筆、即時、用完即丟

系統不會「整份資料庫解開來備用」。只有當一個通過身分驗證的請求要讀取某一筆資料時， 程式才解開**那一筆**，用完就從記憶體釋放。也就是說，解密永遠伴隨一次可被記錄的存取行為。

其三　每段密文都綁定「屬於誰、哪一筆」

加密時會把資料表、資料編號與個案識別一起算進驗證碼。 若有人把甲的密文複製到乙的欄位企圖冒充，解密會直接失敗，而不是回傳一段看似正常的內容。

其四　刪掉的帳號，不會從舊備份爬回來

帳號資料會從線上系統確實刪除，同時把刪除回執、時間，以及一段反推不回身分的內部識別雜湊， 寫進一本獨立的刪除帳本。日後若要還原某份舊備份，系統會先把這本帳重播一遍，資料庫才准上線。 這樣「已經刪掉的帳號，被舊備份帶回來」這件事就不會發生。

以上機制能有效防止「檔案被複製」「備份外流」「開發環境誤用正式資料」這類最常發生的狀況。 但它**無法**防止已經取得執行中主機最高權限的人——因為鑰匙就在那台機器的記憶體裡。 這條界線我們在第 6 節第二點正面說明。

4　五道防線

第一道　只留一個對外窗口

就像：一棟大樓封掉所有側門與地下通道，只留一個有人看著的正門。想進來的人沒得選路。

伺服器對外只保留提供網頁服務所必需的網路通道；管理用的遠端登入不再暴露在公開網路上，也不接受密碼登入。

第二道　員工通道要驗證身分

就像：機場的工作人員通道，不在旅客動線上，外人根本走不到門口；要進去得驗本人身分加上指定識別證，證件遺失可以立刻註銷。

系統維護只能從已授權的裝置，經私有且需身分驗證的管理通道進入。授權以「人員身分＋特定裝置」為單位發放，可隨時撤銷其中任何一個。

第三道 內容鎖進保管箱

就像：貴重物品逐件鎖進保管箱，而不是放在櫃檯後面。整個櫃子被搬走，打開也只有亂碼；而且每個箱子上都刻著「屬於誰、哪一筆」。

對話原文、長期記憶、晤談紀錄、風險事件等高敏感欄位，都先加密再寫入資料庫，採用業界標準的驗證式加密——解密的同時會一併驗證內容有沒有被竄改。

第四道 鑰匙不和箱子放在一起

就像：鑰匙收在另一個房間，只有真的要開箱那一刻才拿出來，用完立刻收回；另有一把備份鑰匙，放在完全不同的地點。

詳見第 3 節。金鑰只在服務執行期載入記憶體，並帶有版本編號可定期輪替。

第五道 副本放在另一座城市

就像：每天把一份副本收進金庫，而且每份都附一組校驗碼。取出來要用之前先對一次，確認這份副本中途沒有壞掉、也沒有被換過。

每天建立一份 SQLite 一致性備份，執行完整性檢查並留下 SHA-256 校驗值。啟用異地副本時，採用獨立的儲存空間與保留週期。還原能力不是看排程有沒有亮綠燈，而是實際演練過才算數。

一句話總結

我們使用業界成熟、可靠、不容易出錯的防守與維運方案，優先處理現實中**最可能真的發生**的風險： 伺服器被亂試密碼、資料庫檔案外流、備份丟失等等。

5 誰看得到什麼

身分	看得到	看不到
個案	自己的全部對話與紀錄，可查閱、匯出	其他任何人的資料
個案之心理師	個案同意分享的範圍（例如摘要與風險提示）	未經個案同意分享的部分
其他心理師	無	個案的全部資料
系統管理者	技術上具備最高權限（見第 6 節第二點）	——

我們刻意「不記錄」的東西

系統日誌只保留「誰在什麼時候登入、做了什麼管理動作」，**不會**把對話原文、長期記憶、完整電子郵件、密碼、權杖或金流秘密寫進一般日誌裡。 許多資料外洩事故其實不是資料庫被攻破，而是日誌檔裡留了不該留的東西。

6 三個誠實告知

以下是我們**做不到**、或必須說清楚的部分。我們寧可先講明白，也不想讓你在錯誤的期待下使用。

一、這不是「連我們自己都看不到」的加密

真正的端對端加密（像某些通訊軟體）之所以能做到誰都看不到，是因為系統本身完全不需要理解訊息內容。 但舒聊的核心是 AI 陪伴與整理，AI 必須讀懂你說的話才能回應。因此在處理的那一刻，內容是可讀的。 任何宣稱「AI 對話服務且連業者都看不到內容」的說法，通常需要持保留態度。

二、系統管理者在技術上握有最高權限

這是所有自架系統的共同事實。我們不會假裝這個權限不存在，而是用三個方式讓它**更難被濫用、也更難被冒用**：

- **權限最小化**——日常維護不使用系統最高權限帳號，而是專用的維護帳號；每個程式只拿到完成自己工作所需的最小範圍，例如備份程式的憑證只能寫入指定的備份路徑，不能讀取其他資料。產品穩定後，維護權限會進一步收斂為幾個固定的部署指令，而不是開放任意操作。這樣一來，就算某一組憑證外流，能造成的破壞範圍也是有限的。
- **操作留痕**——登入、管理操作、資料分享、刪除、匯出、金鑰輪替都會留下時間與身分紀錄，而日誌本身不記錄對話原文。留痕的意義有兩層：不尋常的操作事後查得到、有人要負責；以及異常存取（例如短時間大量讀取）能被發現，而不是悄悄發生。
- **金鑰隔離**——鑰匙不在資料庫、不在備份、不在程式碼與部署包中，只在服務執行期載入記憶體（見第 3 節）。 這樣做的理由是：如果鑰匙跟資料放在一起，複製走檔案的人會連鑰匙一起拿到，加密就等於白做。 分開之後，攻擊者必須分別完成兩件事——先取得資料檔，再另外攻進正在運行的主機、挖出記憶體中的鑰匙——只做到前者，手上就只有一堆亂碼。 而現實中最常發生的事故（備份儲存空間權限設錯、舊硬碟快照外流、工程師為了除錯把正式資料庫下載到自己電腦）幾乎都停在前者。

這些措施能大幅縮小風險，但無法完全排除「已取得執行中主機最高權限的人」。 因此我們同時採取：離職或裝置遺失即撤銷授權、恢復碼離線保存、定期檢視誰握有哪些權限。 最終你信任的是兩件事：技術上的保護，以及營運者的專業倫理。

三、舒聊不是危機處理系統

它可以陪你梳理，也會在偵測到風險訊號時提醒，但它**不能**取代真人的即時介入。 如果你正處於立即的危險中，請不要只依賴這裡的對話。

如果現在就需要有人陪你

1925 安心專線（24 小時免付費） ｜ **1995** 生命線協談專線 ｜ **1980** 張老師專線

110 ／ 119 遇到立即危險時，請直接撥打。

7 系統備援方案

這一節談的是伺服器故障、連線中斷或主機損毀時的備援安排——重點是「系統出狀況時，你的資料還在不在、多久能回來」。我們刻意保留三條互不依賴的路線。

圖四：三層恢復路徑。備份與解密金鑰刻意分開保存在不同供應商、不同帳號。

我們的定期功課

- 每天建立一份 SQLite 一致性備份，跑完整性檢查並留下 SHA-256 校驗值。
- 定期拿備份真的還原一次，驗證資料確實可讀；只看排程亮綠燈不算數。
- 還原之前先重播刪除帳本，避免已刪的帳號從舊備份回來。
- 緊急恢復手冊以書面保存；恢復碼離線存放於實體安全位置。
- 定期檢視誰擁有哪些權限，離職或不再需要時立即撤銷。

8 你的權利

你可以	說明
查閱	要求我們提供你在系統中被保存的資料範圍。
匯出	下載自己的資料副本，格式以機器可讀的 JSON 為主。
修正	自行編輯 AI 的長期記憶與可管理的帳號內容；其他更正可寫信給我們。
刪除	依你選擇的範圍確實刪除，並取得一份刪除回執。帳號刪除會另外寫進獨立帳本，備份還原前重播，確保已刪的帳號不會活回來。
知情	若發生可能影響你資料的資安事件，我們會主動通知你，說明發生了什麼、影響範圍，以及我們採取的處置。

「刪除」和「依法留存」不是同一件事

登入憑證、個人檔案、對話、AI 記憶，以及可以立刻清掉的衍生資料，會照你選的範圍確實刪除。 但有兩類刪不掉，我們寧可先說：一是**已經在你同意下送到心理師手上的摘要**，那份屬於心理師端的專業紀錄，我們沒有權限也不應該去刪； 二是**付款、退款、爭議與稅務**依法必須留存的資料，不過其中能直接識別你的欄位會移除或分開存放。 刪除回執上這兩類會分開列出，你看得到哪些走了、哪些還在。

有任何疑問，都可以直接問

這份文件不會是最後一版。技術會更新，我們也會持續補強。 如果你對其中任何一段有疑慮，或希望我們補充說明某個部分，歡迎直接聯繫我們：**cs@sooth.tw**——對安全提出質疑，本來就是使用者應有的權利。

舒聊 Sooth ｜ 資料安全說明（公開版） 文件版本 v3.0 發布日期：2026 年 8 月
本文件為面向使用者的白話說明。合作機構如需完整技術規格與稽核資料，可另行索取機構版。