

# 台灣職業健康護理學會

## 個人資料與資訊安全內部行政管理標準流程

### 壹、目的

為避免個人資料外洩、文件誤寄、權限失控及資訊安全事件，建立本會及各計畫案之文件管理、資料處理、資訊設備與行政作業標準程序，作為全體工作人員執行業務之依據。

### 貳、適用範圍

凡涉及會員資料、健康資料、計畫文件、雲端系統、Email 寄送及資訊設備使用者均須遵守。適用對象包含：

- 一、理監事
- 二、計畫主持人
- 三、行政與秘書人員
- 四、專兼任助理
- 五、財務人員
- 六、外部委員與合作人員
- 七、臨時或工讀實習人員

### 參、管理原則

#### 一、資料最小化原則

- (一) 非必要不得調閱、下載或寄送完整會員資料
- (二) 行政作業應優先去識別化、遮罩化、分批處理、限縮欄位
- (三) 避免單一文件含完整敏感資料

#### 二、權限分級原則

依業務需求設定權限，不得共用帳號、私下轉交權限、或使用他人帳號，權限設定如下表：

| 身分      | 權限       |
|---------|----------|
| 理事長／主持人 | 督導與核定    |
| 專案主管    | 管理與審核    |
| 承辦人員    | 限必要資料    |
| 外部委員    | 不提供完整名冊  |
| 工讀與臨時人員 | 禁止接觸完整資料 |

#### 三、留痕管理原則

所有資料之調閱、下載、列印、寄送、分享、刪除均須建立追溯紀錄。

## 肆、文件管理程序

### 一、文件建立程序

含個資文件應加密並：

- (一) 標示「限內部使用」
- (二) 標示版本編號
- (三) 記錄建立者
- (四) 避免含非必要欄位

並禁止：

- (一) 建立完整未分級資料庫供多人使用
- (二) 將敏感資料集中於單一公開檔案

### 二、文件分類管理

| 等級   | 說明           | 處理原則         |
|------|--------------|--------------|
| 高敏感  | 身分證、健康、住址、證照 | 加密、限權、留存調閱紀錄 |
| 敏感   | 聯絡資訊、學經歷     |              |
| 一般內部 | 行政文件         |              |
| 公開   | 對外公告         |              |

### 三、文件存放管理

文件應存放於指定雲端或內部加密管理資料夾，禁止存放於：私人 Google Drive、個人桌面長期保存、或未授權隨身碟。

## 伍、Email 與附件寄送程序

### 一、寄送前四階段檢核

| 階段要旨 | 檢核重點                                                                                                                    |
|------|-------------------------------------------------------------------------------------------------------------------------|
| 內容確認 | <ol style="list-style-type: none"> <li>1. 附件是否正確</li> <li>2. 是否含隱藏欄位</li> <li>3. 是否含修訂紀錄</li> <li>4. 是否含完整個資</li> </ol> |
| 權限確認 | <ol style="list-style-type: none"> <li>1. 收件者是否有必要取得</li> <li>2. 是否應分批寄送</li> <li>3. 是否需去識別化</li> </ol>                 |
| 安全確認 | <ol style="list-style-type: none"> <li>1. 是否加密</li> <li>2. 是否需密碼保護</li> <li>3. 是否應限制下載</li> </ol>                       |
| 寄送確認 | <ol style="list-style-type: none"> <li>1. 是否使用 BCC</li> <li>2. 收件名單是否正確</li> <li>3. 是否由第二人複核</li> </ol>                 |

## 二、雙人複核制度

以下資料寄送前須第二人確認，並應保留複核人姓名及時間紀錄：

- (一) 完整會員名冊
- (二) 身分證資料
- (三) 健康資料
- (四) 財務資料
- (五) 超過 20 人以上大量 Email
- (六) 含附件之群發通知

## 陸、文件加密與傳輸管理程序

### 一、加密原則

含敏感資料文件如使用 Email 寄送、雲端分享、或外部傳輸時，應優先採取加密保護。

### 二、附件加密程序

高敏感文件應：

- (一) ZIP 加密
- (二) PDF 密碼保護
- (三) Office 文件加密

且密碼不得同信寄送，應採 LINE 另傳、電話通知、或第二封信通知。

### 三、密碼設定原則

密碼不得使用：連續數字、生日、電話號碼，而建議使用：英文大小寫與數字混合並至少 8 碼以上。

### 四、最小資料原則

非必要不得提供完整名單，應優先：

- (一) 去識別化
- (二) 部分遮罩
- (三) 僅提供必要欄位

## 柒、雲端與共享管理

### 一、共享權限管理

權限管理禁止設定：知道連結即可觀看、公開下載、及任意轉寄共享連結，而應設置：指定帳號存取、設定期限、並應定期清查共享名單。

### 二、下載管理

高敏感文件之下載，原則禁止自由下載，若為必要時則須經主管同意。

## 捌、LINE 與通訊軟體管理

### 一、禁止事項

不得於 LINE 或通訊軟體傳送：

- (一) 完整會員名冊
- (二) 身分證資料
- (三) 健康資料
- (四) 財務文件
- (五) 未加密附件

### 二、群組管理

群組之管理應指定管理員並定期清查成員，一旦有成員離職須立即移除，並於計畫結束時關閉群組。

## 玖、內部行政作業電腦與設備加密管理程序

### 一、公務專用原則

行政資料應以公務設備處理，禁止使用私人電腦長期存放會員資料、私人雲端同步公務文件、或家用設備永久保存敏感資料。

### 二、登入密碼管理

所有公務設備應：設定開機密碼、設定螢幕鎖定、及閒置 5-10 分鐘自動鎖定。開機密碼之設定應：至少 8 碼以上、含英文大小寫與數字、不得使用生日或電話，並禁止將密碼貼於電腦或多人共用帳號。

### 三、硬碟加密

存有敏感資料之設備應啟用：Windows BitLocker、Mac FileVault 或其他硬碟加密功能。

### 四、檔案加密

高敏感文件不得以未加密檔案存放完整個資。

### 五、外接設備管理

外接設備非必要不得用來儲存會員資料。如需使用則應加密、使用後立即刪除，並不得長期保存。另外禁止使用來路不明之外接設備、將個人外接設備混用公務資料、或未加密攜出敏感資料。

### 六、防護與更新管理

所有公務設備應安裝防毒軟體、定期更新系統並啟用防火牆，不得停止更新系統、或使用未授權軟體

### 七、設備遺失或異常處理

如發生電腦遺失、外接設備遺失、帳號異常登入、疑似中毒、檔案遭異常存取等狀況，應於 30 分鐘內通報主管。並立即：

- (一) 停用帳號
- (二) 變更密碼

- (三) 關閉權限
- (四) 保留紀錄
- (五) 啟動事件處理程序

## 壹拾、個資事件處理程序

### 一、事件定義

- (一) Email 誤寄
- (二) 附件誤傳
- (三) 群組外流
- (四) 雲端公開
- (五) 帳號遭盜
- (六) 非授權下載
- (七) 資料遺失

### 二、即時通報原則

發現後 30 分鐘內通報，並禁止私下刪除紀錄、自行對外回覆、隱匿不報。

### 三、事件處理流程

發現人員立即呈報專案主管、理事長或主持人，作資訊與行政處理，進行風險評估，並紀錄與改善。

### 四、緊急應變措施

事件發生後應立即：

- (一) 停止文件流通
- (二) 關閉共享權限
- (三) 回收或要求刪除文件
- (四) 保留系統紀錄
- (五) 建立事件時序表
- (六) 盤點影響範圍

## 壹拾壹、教育與管理制度

### 一、教育訓練

針對資料安全，每年至少進行 1 次個資保護教育、1 次資訊安全宣導，新進人員須完成教育簽屬保密協定後始得接觸資料。

### 二、保密切結

所有工作人員須簽署(1)保密切結書、(2)個資使用聲明。

### 三、定期稽核

定期檢查：

- (一) 雲端權限
- (二) 群組成員
- (三) 共享文件

- (四) 大量 Email 紀錄
- (五) 敏感資料下載紀錄

## 壹拾貳、離職與計畫結束程序

當員工離職或計畫執行結束後，應完成：帳號停用、權限回收、群組移除、文件繳回、本機刪除、及交接確認之事項。

## 壹拾參、違規處理原則

以上程序如有私存資料、任意轉傳、未授權下載、規避通報、違反加密規範等情事發生，得依情節作書面警告、停止權限、終止合作、移送法律程序。

## 壹拾肆、核心管理原則

### 一、三不原則

- (一) 不私存
- (二) 不亂傳
- (三) 不公開

### 二、三要原則

- (一) 要加密
- (二) 要複核
- (三) 要留痕

### 三、即時通報原則

任何異常均須立即通報處理，不得延遲或隱匿。

TAOHN