

淡江大學
個人資料管理制度
個人資料管理制度政策

編號：PIMS-1-01

機密等級：內部使用

目 錄

壹、目的	3
貳、適用範圍	3
參、名詞定義	3
肆、權責	4
伍、內容	4
陸、參考文件	8
柒、相關表單	9

壹、 目的

淡江大學(以下簡稱本校)為落實個人資料保護及管理，並遵循【個人資料保護法】所述之相關要求及保障個人資料當事人之權利，降低任何個人資料檔案受侵害之事件所可能帶來的衝擊，特訂定本個人資料管理制度政策(以下簡稱本政策)。

本校亦導入 BS10012 之認證，藉由 BS10012:2017 PIMS 之規範，提高個人資料管理之有效性。有關 BS10012:2017 PIMS 之規範，將融入個人資料管理之各項規範與程序中。例如個人資料管理政策、內部稽核、管理審查。

貳、 適用範圍

- 一、本校所有人員均屬適用本政策之涵蓋對象。
- 二、個人資料管理制度之驗證範圍為本校個人資料流程之相關作業。

參、 名詞定義

一、個人資料管理制度

以營運風險導向為基礎，用以建立、實施、運作、監測、審查、維持及改進個人資料管理。

二、所有人員

涵蓋本校正式及約聘之教職員工、本校之委外廠商等。

三、有效性指標量測

界定如何衡量所選擇控制措施之有效性，以達成本校個人資料管理目標。

四、個人資料侵害事件

未經個人資料當事人授權使用或不當蒐集、存取及揭露個人資料而超乎預期使用狀況。

五、管理階層

本校個人資料管理之管理階層，包含校長、學術副校長、行政副校長、國際事務副校長、蘭陽校園主任、教學及行政單位一、二

級主管等。

肆、權責

本校所有人員，皆應瞭解並確實遵守本政策。

伍、內容

一、個人資料管理目標

本校個人資料管理目標如下：

- (一) 符合我國個人資料保護法及相關法規，以及本校簽訂合約或專業職責等要求。
- (二) 維護個人資料當事人之人格權，除法令與主管機關另有規範外，提供其個人資料之自主權。
- (三) 對個人資料之蒐集、處理及利用，將以誠實信用方法為之，不逾越特定目的之必要範圍，並與蒐集之目的具有正當合理之關聯。
- (四) 提供個人資料檔案適當之安全措施，以確保本校善盡良善管理之義務。
- (五) 訂定個人資料管理之可接受風險程度與因應措施。
- (六) 當個資事件發生導致利害關係人權益受損時，進行適當地回應與處理。

二、個人資料管理政策

(一) 本校個人資料管理政策如下：

1. 本校只會基於合法的特定目的，在確實必要的範圍內蒐集個人資料。
2. 基於合法的特定目的，蒐集最少的必要個人資料，且不會處理多餘的個人資料。
3. 本校會清楚告知當事人，其個人資料將如何被使用及被誰使用。
4. 已蒐集的個人資料只會作適當且相關的處理。

5. 公平合法地處理個人資料。
6. 維持本校處理的個人資料類別清單。
7. 確保個人資料的正確性，並於必要時進行更新。
8. 已蒐集的個人資料將會依法或在合法的特定目的及保存期限下保存。
9. 尊重當事人對其個人資料所能行使之權利，包含查詢或請求閱覽、請求製給複製本、請求補充或更正、請求停止蒐集、處理或利用及請求刪除等。
10. 確保所有個人資料的安全。
11. 在法令與主管機關允許或無禁止與限制下，經適當保護，本校才會將個人資料進行國際傳輸。
12. 當個人資料應用於《個人資料保護法》所允許之例外情形時，應確保其適當性與合法性。
13. 建立與實施個人資料管理制度，讓個人資料管理制度政策落實。
14. 鑑別內外部利害關係者及其參與個人資料管理制度治理與運作的程度。
15. 於個人資料管理制度運行中，明確界定相關人員之責任與義務。

有關個人資料管理政策，編列規範如下：

【PIMS-2-06 個人資料蒐集、處理與利用作業規範】。

【PIMS-2-07 管理監督規範】。

【PIMS-2-08 當事人權利行使作業規範】。

【PIMS-2-09 侵害事件管理規範】。

【PIMS-2-13 當事人申訴及諮詢作業規範】。

(二) 為宣達本校個人資料管理政策，亦以【PIMS-1-01-F01 個人資料管理政策聲明】進行公告。

三、個人資料管理組織

本校為落實個人資料之保護及管理，將明定個人資料管理制度內相關人員之權限及責任，以確實推行及監督個人資料管理制度。其權限與責任編列於【PIMS-2-01 權限與責任管理規範】。

四、個人資料管理制度

本校個人資料管理制度採用「Plan-Do-Check-Act (PDCA)」之循環運作模式，說明如下：

(一) 規劃與建立(Plan)

依據本校整體目標與策略，藉由成立個人資料管理組織，控制潛在之威脅及弱點，規劃風險評估與安全控管機制，以建立個人資料管理制度。

(二) 實施與運作(Do)

依據評估規劃之結果，建立或修正應有之個人資料管控機制。

(三) 監督與查核(Check)

監督個人資料管理制度各項作業之執行，並查核其有效性。本政策將與本校現行稽核制度並行，定期實施個人資料管理制度內部稽核，以確保個人資料管理之落實。有關內部稽核，編列於【PIMS-2-14 內部稽核作業規範】。

(四) 維護與改進(Act)

根據監督查核之結果與建議，執行矯正與預防措施，改善並執行應有之控管機制，以持續維護個人資料管理制度之運作。有關矯正預防，編列於【PIMS-2-11 矯正及預防措施管理規範】。

五、有效性指標量測

(一) 為確保個人資料管理目標之達成度，本校將制訂有效性量測指標，編列於【PIMS-2-02 有效性指標管理規範】。

(二) 有效性量測指標應衡量所選擇控制措施之有效性，並依評估控制措施及衡量時機，以產生可比較與可再製的結果。

六、管理階層責任

對於本校個人資料管理制度之規劃、建立、實施、運作、監督、查核、維護與改進各項作業，管理階層應訂定並遵循下列事項：

(一) 管理階層承諾

管理階層應確保完成下列工作，表示對個人資料管理發展及增進的充分支持：

1. 核准個人資料管理目標與政策。
2. 確認有效性指標之建立。
3. 訂定個人資料管理之角色與職責。
4. 提供個人資料管理制度各項作業所需之資源。
5. 決定風險可接受水準。
6. 執行個人資料管理制度之管理審查作業。
7. 依本政策要求建立、實施及督導個人資料管理制度。

(二) 組織文化的深植

1. 確認所有人員均具備工作所需相關職能。
2. 評估職能訓練與相關措施之有效性。
3. 建立並維護教育訓練、技能、經驗與資格之相關紀錄。
4. 宣導遵守本政策與法令規章、達成有效性指標及持續改善之重要性。

有關風險管理，編列於【PIMS-2-03 風險評鑑管理規範】。

有關教育訓練，編列於【PIMS-2-04 教育訓練規範】。

七、個人資料管理制度之查核

管理階層應確保定期或不定期進行個人資料管理制度的評估或查核作業，以檢討目標、控制措施與程序是否合乎相關標準、法令規章或個人資料管理需求，並依預期規劃有效執行與維持，以持續增進個人資料管理制度的有效性。

上述查核包括稽核，也包括文件及相關紀錄之查核。有關文件管理，編列於【PIMS-2-12 文件管理規範】。

八、個人資料管理制度之管理審查

管理階層應定期或在發生重大變化時執行管理審查，確保個人資料管理制度運作之適切性、充足性及有效性。

有關管理審查，編列於【PIMS-2-10 管理審查作業規範】。

九、個人資料管理制度之持續改進

本校應藉由查核和稽核結果、矯正及預防措施及管理審查，以持續改進個人資料管理制度之有效性。

十、政策指導與覆核

本政策每年應至少評估一次，並於管理審查會議中討論，以反映政府法令、資訊技術及本校業務等最新發展狀況，確保個人資料管理制度之有效性。

十一、政策與法令之遵循

本校所有人員均應遵循本政策，違反者得依本校相關規定予以處分。如涉有相關民事賠償、刑事責任、行政裁罰者，本校得衡酌情節追訴其法律責任。所有人員對於本校之個人資料保護義務於雙方終止聘僱關係後仍繼續有效。

有關遵循政策與法令，編列於【PIMS-2-05 法令遵循規範】。

有關懲處，編列於【PIMS-2-15 違反個資管理之懲處規範】。

陸、參考文件

一、【PIMS-2-01 權限與責任管理規範】

二、【PIMS-2-02 有效性指標管理規範】

三、【PIMS-2-03 風險評鑑管理規範】

四、【PIMS-2-04 教育訓練規範】

五、【PIMS-2-05 法令遵循規範】

六、【PIMS-2-06 個人資料蒐集、處理與利用作業規範】

七、【PIMS-2-07 管理監督規範】

八、【PIMS-2-08 當事人權利行使作業規範】

- 九、【PIMS-2-09 侵害事件管理規範】
- 十、【PIMS-2-10 管理審查作業規範】
- 十一、【PIMS-2-11 矯正及預防措施管理規範】
- 十二、【PIMS-2-12 文件管理規範】
- 十三、【PIMS-2-13 當事人申訴及諮詢作業規範】
- 十四、【PIMS-2-14 內部稽核作業規範】
- 十五、【PIMS-2-15 違反個資管理之懲處規範】
- 十六、【個人資料保護法】(外來文件)

柒、相關表單

- 一、【PIMS-1-01-F01 個人資料管理政策聲明】