附件一、

僑光科技大學

個人資料蒐集、處理、利用與安全管理程序書

目　　錄

一、 目的..... 1

二、 適用範圍..... 1

三、 定義..... 1

四、 作業內容..... 1

五、 相關文件..... 8

一、 目的

為落實辦理【個人資料保護法】(以下稱個資法）規定之個人資料蒐集、處理、利用與安全，特訂定本程序書。

二、 適用範圍

本校所有同仁及相關委外合作廠商,所產生或經手之書面、電子個人資料均適用之。

三、 定義

(一)個人資料 指自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。

(二)蒐集

係指以任何方式取得個人資料。

(三)處理

係指為建立或利用個人資料檔案所為資料之記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結或內部傳送。

(四)利用

係指將蒐集之個人資料為處理以外之使用。

(五)當事人

係指個人資料之本人。

(六)當事人行使個人資料之權利 指查詢或請求閱覽、請求給複製本、請求補充或更正、請求停止蒐集、處理或利用及 請求刪除其個人資料。

(七)儲存媒體

如磁片、磁碟、磁帶、IC卡、匣式磁帶、外接式硬碟、光碟、隨身碟、各式記憶卡、錄影帶、錄音帶等。

(八)國際傳輸 指將個人資料作跨國（境）之處理或利用。

四、 作業內容

(一)蒐集個人資料之控管原則：

1. 個資蒐集應秉持「適當、相當且不過度」」只蒐集必要的個資，以降低個資外洩風險。

2. 蒐集個資時，部份甚為敏感的欄位內容，譬如：密碼、身分證號等，應加上適宜之遮蔽措施。

3. 本校為行政目的使用資通系統或雲端資通服務(如 Google 表單、Microsoft Forms 等問卷調查服務）涉及蒐集個人資料者，應注意下列事項：

(1) 資料蒐集最小化：僅蒐集適當、相關且限於處理目的所必要之個人資料，處理及利用時，不得逾越特定目的之必要範圍，並應與蒐集之目的具有正當合理之關聯。

(2) 存取控制：應注意檔案存取權限設定，應採最小權限原則，僅允許使用者依目的，指派任務所需之最小授權存取。

(3) 使用雲端資通服務者，應詳閱設定內容，不宜使用者共同編輯個人資料檔案清冊，並應注意避免設定允許顯示其他使用者作答內容（如 Google 表單不應勾選「顯示摘要圖表和其他作答內容」），避免使用者能瀏覽其他 使用者資料，造成個人資料外洩。公佈前應確實做好相關設定檢查，並實際操作測試，確認無誤後再行發布。

(4) 應訂定個人資料保存期限,並於期限或業務終止後將蒐集之個人資料予以刪除或銷毀，避免個人資料外洩。

4. 各單位蒐集個人資料時，應明確告知當事人以下事項：

(1) 本校名稱、聯繫方式。

(2) 蒐集目的。

(3) 個人資料的類別。

(4) 向當事人說明資料使用期間、保存期限、使用範圍及使用方式。

(5) 當事人可以行使之權利及方式,例如當事人可請求查詢、閱覽、製給複製本、補充、更正、刪除、停止蒐集、處理或利用。

(6) 向當事人說明可自行判斷是否提供個人資料，若為本校提供服務時所必須之資訊，因而造成無法提供該服務情形時，讓當事人瞭解對其個人權益之影響。

(7) 本校如於網站上蒐集個人資料時，應說明採用之技術收集並儲存資訊之方式，如 cookies 等。

5. 各單位間接蒐集非由當事人提供之個人資料時，應於處理或利用前，確認是否已

取得當事人書面同意且已向當事人告知個人資料來源、本校名稱、蒐集之目的、個人資料之類別、個人資料利用之期間、地區、對象及方式、當事人依個資法第三條規定得行使之權利及方式。

(二)處理個人資料之控管原則

1. 與個資檔案有關之資訊系統(程式)使用完畢後，應立即登出應用系統(程式)。
2. 禁止在社群網站、部落格、公開論壇或其他利用網際網路形式公開業務上所知悉之個資。
3. 個資檔案禁止存放於網路共用目錄。
4. 網路傳送個資檔案時，應對資料檔案加密，確認傳送對象無誤後傳送，並請對方收到後回覆確認。
5. 使用可攜式儲存媒體時，遵循以下的使用規範：
   (1) 確定電腦安裝之防毒程式及病毒碼都有定時更新，足以偵測隱藏之病毒後，方可讀取可攜式儲存媒體內的檔案。
   (2) 可攜式儲存媒體只適宜儲存暫存的個資檔案,使用後應應儘快並確認已刪除。
6. 應定期備份含有個資電腦資料，及確認備份資料的可用性與安全性。
7. 報廢之個資文件須用碎紙機銷毀或依其他核可之方式進行銷毀；電子檔須確實刪除與清空資源回收桶。
8. 個資交付及傳輸：
   (1) 個資傳輸應使用 TLS 1.2 以上之版本。
   (2) 禁止使用點對點(P2P)軟體、LINE、FB、Skype、或其他即時通訊軟體傳輸或分享業務所知悉之個資。
   (3) 以 Email 方式為個資交付，交付人應保留相關紀錄。
   (4) 系統提供授權人連線下載方式為個資交付及傳輸，系統應有連線紀錄可供查閱。
   (5) 進行個資國際傳輸前,應檢視有無主管機關依個資法第 21 條規定為國際傳輸之限制，並且告知學生及教職員其個人資料所欲國際傳輸之區域，同時對資料接收方預定處理或利用個資之範圍、類別、特定目的、期間、地區、對象及方式進行監督。
9. 資訊系統設計上應提供個人查核本人的基本資料，並允許做適宜之資料更新，以維持個資正確性。
10. 個人資料正確性有爭議,個人資料權責單位應依當事人之請求停止處理或利用。但因

執行職務或業務所必須並註明其爭議或經當事人書面同意者，不在此限。

11. 若當事人的資料不正確，但應實際需求需保留相關歷史紀錄時，應須能指出該資料為不正確，並在適當之處提供正確的個人資料。

12. 當事人行使個人資料之權利：

(1)當事人行使權利之申請

A. 本校師生同仁行使權利時應填寫本校「個人資料權利行使申請表」，並附上必要之佐證資料，可向各業務權責單位提出申請，如為代理人申請則 須附委託同意書。

B. 校外人士行使權利時應填寫本校「個人資料權利行使申請表」，並附上必要之佐證資料，向本校個資保護聯絡窗口提出，再由個資保護聯絡窗口轉達業務權責單位，如為代理人申請則須附委託同意書。

C. 前兩項之業務權責單位已有訂定對應之申請流程，可依原有之申請流程 及表單進行，但仍應保留當事人之各項申請記錄。

(2) 業務權責單位之處理程序

A. 資料查詢或請求閱覽：

a. 個人資料查詢或請求閱覽,如須繳交費用,則依本校繳費方式進行繳費。

b. 個人資料權責單位應於十五日內，為准駁之決定；必要時，得予延長，延長之期間不得逾十五日，並應將其原因以書面通知請求人。

c. 資料查詢或請求閱覽由業務承辦人員與當事人聯繫，確認當事人身分後提供查詢結果,或請當事人至業務單位進行資料閱覽,亦可在安全控制下提供線上查詢或閱覽。

B. 請求給付複製本

a. 個人資料請求給付複製本,如須繳交費用,則依本校繳費方式進行繳費。

b. 個人資料權責單位應於十五日內，為准駁之決定；必要時，得予延長，延長之期間不得逾十五日，並應將其原因以書面通知請求人。

c. 由業務承辦人員於申請單陳核後依據申請人選擇方式交付文件,取件方 式如下：

(a) 親自領取並核對證件如下：

i. 本人申請：身分證正本。

ii. 由代理人(配偶、父母、成年子女)申請：當事人身分證正本、代理人身分證正本及當事人之委託書。

iii. 未成年人由法定代理人申請：法定代理人身分證正本、法定代理人與當事人關係證明文件(戶口名簿或當事人身分證正本)。

(b) 郵寄方式：與當事人連絡確認為當事人所提之申請後，郵寄至申請人指定之地點，須繳納掛號郵資。

(c) 傳真：與當事人連絡確認為當事人所提之申請後，請對方接收傳真。

(d) 前三項取件方式如須繳交費用，則依本校繳費方式進行繳費。

C. 請求補充或更正

a. 當事人就其個人資料提出請求補充或更正、停止蒐集、處理、決定；必要時，得予延長，延長之期間不得逾三十日，並應將其原因以書面通知請求人。

b. 業務權責單位應查明其資料是否正確，若需補充或更正，應經業務權責 單位主管同意後行之，補充或更正之結果應留存記錄，並將補充或更正之結果通知當事人。

c. 個人資料經補充或更正後，應避免舊資料再被誤用，並應通知相關或委外單位資料已被更新。

D. 請求停止蒐集、處理或利用應查明是否為依法規、執行職務或業務所必須之資料，若為必須之資料而無法停止，則應以書面函覆當事人說明原由，以取得瞭解。非必須之資料，則經業務權責單位主管同意後進行停用作業，並書面函覆當事人。

E. 請求刪除應查明是否為依法規、執行職務或業務所必須之資料，若為必須之資料而無法刪除，則應以書面函覆當事人說明原由，以取得瞭解。非必須之資料，則經業務權責單位主管同意後進行刪除作業，並書面函覆當事人。

F. A 至 E 之所有請求如為依法規、因執行職務或業務所必需，惟業務權責單 位無法同意其請求，應以正式書面函覆，並以掛號方式寄出，函覆內容應包含申請項目、駁回原因、申訴管道及相關連絡資訊。

(3) 當事人申訴

A. 若當事人發現本校於個人資料處理有不當之處，可向本校個資保護聯絡窗口或各業務承辦單位提出申訴；各業務承辦單位若接獲個資相關申訴後，需記錄相關事件內容及當事人聯絡方式後，將申訴事件移交個資保 護聯絡窗口進行處理，並

由個資保護聯絡窗口需填寫「個人資料申訴事 件紀錄單」記錄申訴案件。

B. 如申訴案件如屬本校業務時，應由本校權責人員會同個資權責單位進行調查，並依據調查結果建議處理方式。若經確認非屬本校業務時，由本校權責人員向當事人說明回覆。

C. 調查結果與建議處理方式經由本校個資權責單位主管同意後，以書面函覆結果，並進一步與申訴人取得聯繫與同意。

(4) 本校「個人資料保護網頁專區」網站中「提供當事人行使權利」應清楚說明個人資料保護法第三條，當事人得行使之相關權利，如：請求閱覽等，並提供本校各單位個資窗口之詳細連絡資訊。

13. 接觸個資檔案之人員應依照本校個人資料保護管理政策要求，執行相關規定之程序，負擔個資保密及保護之義務，並於離職、職務調動或合約終止時，重要資訊系統負責人應即對權限異動人員之系統使用權限重新設定，異動人員亦應繳回通行 證及相關證件，並保留相關紀錄。

14. 委外廠商人員於專案服務期間所知悉之業務資訊，應遵守個資法及本校個人資訊管理 制度相關規定，且不得對外洩露。

15. 個資保管人應對已超過保留期限之個資或相關紀錄，應依規定銷毀(如碎紙與刪除 電子檔），並記錄之。

(三)利用個人資料之控管原則

1. 影印、列印、傳真使用後須確認設備內並未遺留個資資料及原稿。

2. 含有個人資料之報廢紙張不得回收及再利用。

(四)其它控管原則

1. 委託他人蒐集、處理或利用個人資料時，委託機關應對受託者為適當之監督，並明確約定相關事項、方式、義務及責任。

2. 非電腦教室個人電腦報廢時：

(1) 硬碟繼續使用，應對硬碟執行低階格式化或其他可確保資料不會被恢復之方法。

(2) 硬碟不繼續使用，應對硬碟執行低階格式化或其他可確保資料不會被恢復之方法，或將其實體破壞。

(3) 硬碟無法使用，應將其實體破壞。

3. 資訊中心主機房（確認是否已在其他程序書中有提到以下相關訊息的部分。）：

(1) 非權責單位指定之人員不得擅自進入或使用相關資訊設備。

(2) 外部人員或未具進出權限之人員，因執行業務需求進入時，必須指派人員隨行並填寫「機房進出登記表」後方可進出，並遵守相關資訊安全管理之規定。

4. 重要資訊系統主機應做防火牆設定。

5. 重要資訊系統應適宜的限制存取 IP。

6. 電腦作業系統及相關應用程式之漏洞，應進行修補。

7. 資訊系統主機，必要時需進行弱點掃描，並應適當進行弱點處理。

8. 公務個人電腦應安裝防毒程式並設定自動更新病毒碼及做系統更新。

9. 存有個資的電腦及伺服器，應設定登入密碼，且其密碼要符合安全之複雜度，至少 8 碼以上，且至少每 180 天須更換密碼一次。

10. 個人電腦應設定螢幕保護密碼，且螢幕保護啟動時間定在 10 分鐘以內。

11. 維持個資存取權限的正確性,且原則上不得共用存取權限,並留意個資被存取的情形。

12. 本校各單位每年應執行個資盤點，檢查個資之使用狀況及存取情形。

(五)保護個人資料之認知宣導與教育訓練

1. 應鼓勵教職員工生參與校內外資訊安全與個資保護之教育訓練,並定期宣導個資保護之重要性。

2. 本校教職員工每年至少參與 2 個小時(含)以上之校內、外所舉辦個資保護相關宣導及教育訓練。

3. 校內所舉辦個資保護相關宣導及教育訓練，應保留舉辦紀錄。

4. 本校負責個資窗口應將取得授權之研習課程講義或簡報檔公告於「個人資料保護網頁專區」網站。

5. 本校負責個資窗口應時常注意個資保護相關知識與訊息，並摘要彙整於本校「個人資料保護網頁專區」網站，以作為教職員工生獲取個資保護資訊的重要管道。

(六)個資事故通報處理及應變

1. 依私立專科以上學校及私人學術研究機構個人資料檔案安全維護實施辦法規定，在發生個資被竊取、洩漏、竄改或其他侵害事故發現時起七十二小時內,填具「個人資料侵害事故通報與紀錄表」(如附件)，迅速處理以保護當事人之權益。

五、 相關文件

(一)個人資料保護法

(二)個人資料權利行使申請表

(三)個人資料侵害事故通報與紀錄表