國立高雄師範大學個人資料保護管理辦法

107年9月19日107學年度第1次行政會議通過

第 一 章 總則

第　一　條 國立高雄師範大學（以下簡稱本校）為防止個人資料被竊取、竄改、毀損、滅失或洩漏，並落實個人資料之保護及管理，符合「個人資料保護法」（以下簡稱個資法)以及相關之管理規範,特訂定「國立高雄師範大學個人資料保護管理辦法」（以下簡稱本辦法）。

第　二　條 本辦法用詞，定義如下：

一、本辦法所稱個人資料、個人資料檔案、蒐集、處理、利用、傳輸等名詞定義，係指個資法第二條所述之內容。

二、當事人：指個人資料之本人。

三、各單位：指本校各行政單位及學術單位。

第　三　條 本辦法適用於本校之個人資料蒐集、處理、利用及傳輸等相關程序所產生之各種形式（含書面或電子）之個人資料檔案。

第　四　條 本校於「個人資料保護推動委員會」下設「個人資料保護執行小組」（以下簡稱執行小組），其任務如下：

一、個人資料保護政策之擬議、推展及管理。

二、推動個人資料之機密性、完整性及可用性，並符合相關法令、法規之要求。

三、確保個人資料管理保護制度所需各項過程之建立、實施與維持。

四、個人資料保護意識教育訓練之推動。

五、個人資料隱私風險之評估及管理。

六、個人資料管理制度適法性與合宜性之檢視、審議及評估。

七、其他個人資料保護、管理之規劃及執行事項。

第　五　條 執行小組以圖書資訊處為個人資料保護聯絡窗口，其辦理事項包含：

一、對其他機關個人資料保護業務之協調聯繫及緊急應變之通報。

二、以非自動化方式檢索、整理之個人資料安全事件之通報。

三、各單位個人資料管理人名冊之製作及更新。

四、教職員工教育訓練名單及紀錄之彙整。

第 二 章 個人資料範圍、蒐集、處理及利用

第　六　條 應以誠實信用方式進行個人資料之蒐集、處理、利用或傳輸，並以最小化且未逾越特定目的之必要範圍為限。

第　七　條 應確保個人資料之蒐集除個資法第六條第一項所規定資料外，應有特定目的，且應符合個資法第十九條第一項之規定，並明確告知當事人下列事項：

一、機關或單位名稱。

二、蒐集之目的。

三、個人資料之類別。

四、個人資料利用之期間、地區、對象及方式。

五、當事人依個資法第三條規定得行使之權利及方式。

六、於當事人得選擇是否提供其個人資料時，如不提供將影響其權益。

但符合個資法第八條第二項規定情形之一者，得免為前項之告知。

第　八　條　各單位蒐集非由當事人提供之個人資料，應於處理或利用前，向當事人告知個人資料來源及前條第一款至第五款所列事項。但符合個資法第九條第二項規定情形之一者，不在此限。

前項之告知，應於首次對當事人個人資料為處理或利用時為之。

第　九　條　各單位依個資法第十九條第一項第五款及第二十條但書第六款規定蒐集、處理或利用當事人個人資料時，應取得當事人同意。

第　十　條　各單位依個資法第十九條或第二十條蒐集、處理、利用個人資料時，應詳為審核，並經行政程序為之。

各單位應對於個人資料之處理、利用之歷程做成紀錄並保存之。

第 十一 條　各單位對於所保有之個人資料有錯誤或缺漏時，應由資料蒐集單位經行政程序更正後，通知資料保有單位更正或補充之，該單位應確實做成紀錄並保存之。

因可歸責各單位之事由而未為更正或補充個人資料時，其應於更正或補充後，由資料蒐集單位以書面通知曾利用該個人資料之單位。

第 十二 條　各單位保有之個人資料正確性有爭議者，應由資料蒐集單位經行政程序，通知資料保有單位停止之處理或利用，該單位應確實做成紀錄並保存之。但符合個資法第十一條第二項但書規定因執行職務或業務所須，或經當事人書面同意，並經註明其爭議者，不在此限。

第 十三 條　各單位保有個人資料蒐集之特定目的消失或期限屆滿時，應由資料蒐集單位經行政程序，通知資料保有單位刪除、停止之處理或利用，該單位應確實做成紀錄並保存之。但符合個資法第十一條第三項但書規定因執行職務或業務所須，或經當事人書面同意，並經註明其爭議者，不在此限。

第 十四 條　各單位違反個資法規定蒐集、處理或利用個人資料檔案者，經行政程序核定後通知資料保有單位刪除、停止之處理或利用，該單位應確實做成紀錄並保存之。

第 十五 條　針對病歷、醫療、基因、性生活、健康檢查、犯罪前科等個人資料，應建立符合下列要求之程序：

一、確保內部人員不得蒐集、處理及利用該資料。

二、確保例外得蒐集、處理或利用該資料時，符合個人資料保護相關法規之要求，並建立資料蒐集、處理或利用之控制與記錄機制。

第 三 章　當事人之相關權利

第 十六 條　原蒐集之特定目的範圍變更時，應進行下列程序：

一、確認原始蒐集之合法要件是否存續，其未存續者，應再取得當事人同意而為之。

二、建立特定目的範圍變更之控制與記錄機制。

第 十七 條　當事人依個資法第十條向個人資料保有單位請求查詢、閱覽個人資料或製給個人資料複製本，應填具申請書，並檢附相關證明文件。

前項書件內容，如有遺漏或欠缺，應通知限期補正。

申請案件有下列情形之一者，個人資料保有單位應以書面駁回其申請：

一、申請書件內容有遺漏或欠缺，經通知限期補正，逾期仍未補正者。

二、有個資法第十條但書各款情形之一者。

三、與法令規定不符者。

第 十八 條 當事人提出前條之請求時，個人資料保有單位應於十五日內為准駁之決定。必要時，得予延長，延長期間不得逾十五日，並應將其原因以書面通知當事人。

第 十九 條 當事人閱覽其個人資料時，承辦單位應派員陪同，並依相關程序辦理及繳納費用。

第 二十 條 當事人依個資法第十一條第一項至第四項規定向個人資料保有單位請求補充、更正、刪除、停止蒐集、處理或利用個人資料，應填具申請書，並檢附相關證明文件。

前項書件內容，如有遺漏或欠缺，應通知限期補正。

申請案件有下列情形之一者，個人資料保有單位應以書面駁回其申請：

一、申請書件內容有遺漏或欠缺，經通知限期補正，逾期仍未補正者。

二、有個資法第十一條第二項但書或第三項但書所定情形之一者。

三、與法令規定不符者。

第二十一條 當事人提出前條之請求時，個人資料保有單位應於三十日內為准駁之決定。必要時，得予延長，延長期間不得逾十五日，並應將其原因以書面通知當事人。

第 四 章 個人資料安全管理措施

第二十二條 個人資料保有單位於個資法第十二條所定個人資料有被竊取、洩漏、竄改或其他侵害情事者，應先行通報並進行緊急因應措施，其作業程序如下：

一、個人或單位接獲個人資料安全事件通知。

二、個人或單位主動先行上網通報。

三、執行小組釐清資料保有、處理等作業程序與責任所屬。

四、資料權責單位應即進行防禦或補救作業。

五、資料權責單位應即以適當方式通知當事人。

六、資料權責單位應將改善與預防措施納入工作準則，以降低事件再發生機率。

七、回報執行小組。

第二十三條 本校於「個人資料保護推動委員會」下設「個人資料保護稽核小組」，稽核小組得定期或不定期辦理個人資料保護管理稽核，稽核結果循行政程序陳核。

第二十四條 個人資料檔案安全維護工作，除本辦法外，並應符合法令、主管機關及本校相關作業安全與機密維護規範。

第 五 章 附則

第二十五條 本辦法經行政會議審議通過，陳請校長核定後實施，修正時亦同。

國立高雄師範大學個人資料保護管理辦法—附件

附件一：國立高雄師範大學資訊安全暨個人資料保護稽核重點參考項目

107 年 12 月 19 日 107-2 資訊安全及個資管審會議修正通過

本校資訊安全推動小組下設「資訊安全稽核小組」，辦理本校各單位資訊安全管理稽核作業。個人資料保護推動委員會下設「個人資料保護執行小組」，依本校個人資料保護管理辦法第二十三條辦理本校各單位個人資料保護管理稽核，檢核內容包括下列五大項，稽核結果將陳校長核備。

檢核項目	建議方式
一、個人資料保護持續改善管理流程	
(一)個人資料檔案需指定管理者	由一級或二級主管擔任，並將個資指定管理者併入分層負責表，納入內控管理
(二)個人資料之蒐集與利用應符合法令規定，包含： 1. 個人資料之蒐集、處理或利用，應尊重當事人之權益，依誠實及信用方法為之，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. 蒐集個人資料時，應依法令規定告知當事人蒐集資料之目的、利用範圍等資訊。 3. 除符合法令規定外，有關醫療、基因、性生活、健康檢查及犯罪前科之個人資料，不得蒐集、處理或利用。 4. 當資料利用範圍超出蒐集的特定目的時，應依個資法規定取得當事人之書面同意。	個資法所保護的個人資料，是指自然人的姓名、出生年月日、身分證號、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識別該個人的資料。 二、圖資處提供各單位公版--個人資料蒐集告知暨同意書(範例)
二、個人資料保護與安全	
(一) 含有個人資料之紙本報表，其處理及利用行為應有適當之授權、監督，及記錄列印、轉交等行為。	含有個人資料之紙本報表需有負責人員蓋章
(二) 交換紙本個人資料時，應採取彌封或其他具備保密機制之傳遞方式。	以校內文件公文袋遞送時，寫明收件者
(三) 於單位管理之網站或網頁公布個人資料時，應經所屬單位主管核准，並依相關法律及規範處理。	各單位於網頁公布個人資料時應依符合個資法保護個人資料
(四) 是否於法律允許之範圍內提供資料當事人下列權益： 1. 查詢或請求閱覽 2. 請求製給複製本 3. 請求補充或更正 4. 請求停止蒐集、處理或利用 5. 請求刪除	各單位讓提供資料當事人透過本校資安暨個資事件通報平台請求權益
(五) 處理個人資料檔案之個人電腦，應設置使用者帳號及密碼。	公務使用之個人電腦均應設置使用者帳號與密碼

(六) 密碼每六個月需更換一次，長度應至少 8 碼且包含文數字。	系統需每六個月提醒更換密碼
(七) 禁止與他人共用電腦系統帳號。	每位人員均需建立專屬帳號與密碼，並妥善保管勿讓他人知悉。
(八) 處理個人資料需採取權限區隔，非專責處理特定個人資料者不得具有存取或查閱個人資料之權限。	每位人員須依據專責事項給予相關權限，非承辦人員不得任意取得權限並存取查閱
(九) 個人資料檔案應以安全的方式保護，例如：加密、鎖在鐵櫃中。數位形式的個人資料檔案，建議透過壓縮軟體加上密碼方式存放。	紙本形式的個人資料檔案，建議統一集中鎖在鐵櫃中，鑰匙交由單位個資管理者。
(十)每月應備份電腦內個人資料檔案。	可備份至隨身碟、光碟或是校內 GSuit 雲端空間。備份資料應以安全方式：如加密、鎖在鐵櫃中等，妥善管理存放。
(十一)使用個人資料檔案時，完畢後應立即退出應用程式，非作業時間時需手動啟動螢幕保護程式。	例如寄信完成後，應將寄件軟體(如：Outlook)關閉，若是寫信寫到一半有事暫離，則須手動登出系統。
(十二)電腦應使用螢幕保護程式並設定密碼，並將螢幕保護啟動時間設定為 5 分鐘以內。	電腦需啟用螢幕保護程式(含密碼)，並將時間設在上限 5 分鐘。站在資安保護的立場，建議離開電腦時手動登出作業系統。
(十三)交換個人資料檔案時，若為數位形式，應對資料檔案加密或是透過加密通道傳送。	數位形式的個人資料檔案，在傳輸過程中若未加密，易被監聽封包後知悉，因此要求傳輸前至少透過壓縮軟體加上密碼後再傳送，或是透過加密協定(如：HTTPS)進行傳送。
(十四)禁止開啟網路芳鄰分享目錄與檔案。	近年流行的勒索病毒便是透過作業系統網路芳鄰的漏洞擴散的，校內強烈禁止開啟網路芳鄰。
(十五)應停用作業系統 Guest 帳號。	Guest 帳號預設為啟用，應手洞關閉，避免透過該 Guest 瀏覽到個資相關檔案。
(十六)電腦應安裝防毒軟體，並至少每週更新病毒碼並執行排程掃瞄。	公務電腦均應安裝防毒軟體(如：校內採購之趨勢科技)並定期更新與掃描，若是安裝校內趨勢防毒，已由中控台控制推送更新病毒碼與預約掃描，可以省掉人工定期的工作。

(十七)存放個人資料之資訊設備應定期檢查作業系統更新及應用程式修補釋出。	存放的資訊設備，如：Windows7 的公務電腦。需定期檢查有無作業系統更新與存取資料的應用程式更新。
三、設備管理	
(一)應指定專人負責管理儲存個人資料檔案之資訊設備與其他相關設施，並檢視、處理其錯誤或異常事件等訊息。	由一級或二級主管擔任，並將專責人員併入分層負責表，納入內控管理
(二)儲存個人資料之資訊設備須置放於實體安全區域（如：門禁控管之辦公區域、機房）。	例如以紙本、光碟、隨身碟儲存個資檔案，須將該設備放置於受控管之空間，如：上鎖的鐵櫃。
(三)儲存個人資料檔案之磁碟、磁帶，及紙本等相關儲存媒體，須指定專人管理，並置於實體保護(例如上鎖的鐵櫃)之環境。	同上
(四)儲存個人資料檔案之儲存媒體，須建立備援機制。	例如隨身碟存放時，應同時複製另一份當作備援
(五)儲存個人資料檔案之媒體須有攜出、拷貝或複製的管控機制，並留存紀錄。	個資管理人員遇到有外單位之攜出、拷貝或複製的業務要求時，至少需有書面管控紀錄做佐證。
(六)外部廠商或個人更新或維修儲存個人資料檔案之電腦設備時，單位須指派專人在場確保資料安全。	至少需單位個資管理人員需在場，若是個資管理人進行更新或維修的話，則須另外指派單位同仁陪同。
(七)儲存個人資料檔案之電腦或相關設備如需報廢或移轉他用，須刪除其所儲存之個人資料檔案。	因資料救援軟體可以救出刪除的檔案，為避免有心人士，對於儲存的媒介(通常為硬碟)，硬碟資料銷毀處理的方式主要分為三種: 硬體破壞，資料抹除以及磁盤消磁等。
四、人員管理	
(一)機關學校對處理個人資料檔案之人員施予資訊安全與個資隱私保護之教育訓練，並於單位內宣導個資隱私保護之重要性。	由圖資處進行教育訓練，惟各單位需於內部宣導個資保護重要性
(二)處理個人資料檔案之人員職務異動時，應列冊移交相關儲存媒體及資料。	職務異動應有移交清冊
(三)處理個人資料檔案之人員職務異動時，接替人員須於相關系統重置通行碼，並視需要更換使用者識別帳號。	為避免前手人員進入相關系統做操作，應將前手人員帳號吊銷，並替接替人員開通新帳號。
(四)處理個人資料檔案之人員，須簽訂保密切結書。	任一人員須處理個人資料相關業務時，均須簽署保密切

	結書
(五)處理個人資料檔案之人員離職或合約終止時，須依規定取消或停用其使用者識別帳號並收繳通行證件。	任一人員離職時，須停用相關功能權限，並繳回通行證件，例如：職員證
(六)禁止使用點對點(P2P)軟體及 Tunnel 相關工具下載或提供分享檔案。	禁止使用未加密通道進行資料傳輸，如 P2P 軟體本身的漏洞導致駭客入侵
五、系統開發及委外管理	
(一)處理個人資料檔案之資訊系統，於系統開發生命週期之初始階段，須將個人資料檔案的安全需求納入系統開發考量。	系統於規劃時，須將個人資料保護的需求納入考量，避免系統使用發生個資洩漏事件
(二)處理個人資料檔案的資訊系統之維護、更新、上線、及版本異動等作業，須有安全管控措施。	系統每次的異動、上線均須詳細紀錄，並於上線前完成完善的測試，達到安全管控目標
(三)維護人員或系統服務廠商以遠端登入方式進行牽涉個人資料的資訊系統維護或其他有關之運作時，須透過加密通道進行（如：SSH 等），並搭配防火牆限制通行的時間。	外包廠商開發之系統需要遠端協助處理 Bug 的時候，為避免遠端時的資料外洩，透過加密通道與防火牆的限制，降低外洩的風險。
(四)自行開發或委外處理個人資料檔案之資訊系統，須將個人資料(包含測試用個人資料)施予妥善之保護與控管。	系統中的個人資料(包含測試資料)，須妥善保管，禁止帶離至非工作場所，並將每次的複製、傳輸等操作詳細紀錄進行有效控管
(五)委外建檔的個人資料檔案，須於委外合約中載明所處理之個人資料保密義務、資訊安全相關責任及違反罰則。	委外廠商開發系統時須於合約中載明個資保護及資安相關責任說明及違反時的罰則。

附件二：國立高雄師範大學個人資料蒐集

107 年 9 月 19 日 107 學年度第 1 次行政會議通過

國立高雄師範大學(以下簡稱本校)為校務所需蒐集、處理及利用您的個人資料，依據個人資料保護法規定，向 您告知下列事項，請詳閱：

一、蒐集之目的：辦理本校人事管理、學生(含畢、結業生)資料管理、教育或訓練行政、產學合作、資通安全與管理、學術研究、調查、統計與研究分析、圖書館與出版品管理、稅務行政、存款與匯款、契約、類似契約、保險、保健醫療服務、衛生行政、國內外交流業務及其他校務相關業務之需要。

二、蒐集之個人資料類別:識別類(例如:姓名、身分證統一編號、護照號碼、電話號碼、行動電話、通訊及戶籍地址、電子郵遞地址、工作單位、職稱與緊急聯絡人姓名電話地址)、特徵類(例如:出生年月日、國籍、性別)、家庭情形、教育、技術或其他專業(例如:學校紀錄、資格或技術、職業專長、著作、應考人紀錄）、受僱情形、健康紀錄及符合蒐集目的之各項個人資料類別等。

三、個人資料利用之期間、地區、對象及方式:

（一）期間：個人資料蒐集之特定目的存續期間、依相關法令規定、契約約定或本校因執行業務所必須之保存年限。

（二）地區：本國與境外學術研究交流地區。

（三）對象：本校及其他與本校有業務往來之公務及非公務機關。

（四）方式：以自動化機器或其他非自動化之利用方式。

四、您可依個人資料保護法，就您的個人資料行使以下權利：

（一）查詢或請求閱覽。

（二）請求製給複製本。

（三）請求補充或更正。

（四）請求停止蒐集、處理或利用。

（五）請求刪除。

惟依相關法令規定、契約約定或本校因執行業務所必須者，得不依您請求為之。

五、個人資料之提供：

（一）您若拒絕提供個人資料，本校將無法提供相關服務，亦可能無法維護您的權益。

（二）請依各項服務需求提供您正確、最新及完整的個人資料，若您的個人資料有任何異動，請主動向本校各單位申請更正。

（三）若您提供錯誤、過時、不完整或具誤導性的資料，而損及您的相關權益，本校將不負相關賠償責任。

六、個人資料之保密：本校將善盡個人資料保護之責。如因天災、事變或其他不可抗力致使您的個人資料被竊取、洩漏、竄改、遭其他侵害者，將於查明後以電話、電子郵件或網站公告等方法，擇適當方式通知您。

七、個人資料保護申訴窗口 電話：07-7172930 轉 1689

＝＝

簽章欄　　（本告知暨同意書由本校承辦單位收存）

本人瞭解上述告知事項，並同意在符合上述告知事項範圍內，蒐集、處理及利用本人所提供之各項個人資料。

立同意書人: _____　　（簽名）

中華民國　　年　　月　　日

附件三：

資安暨個資事件通報及處理流程