# 高雄市私立中華藝術學校個人資料檔案安全維護計畫實施辦法

114 年 8 月 20 日

壹、依據

一、個人資料保護法第二十七條第三項規定訂定之。

二、「私立高級中等以下學校及幼兒園個人資料檔案安全維護計畫實施辦法」第四條規定辦理。

貳、主管機關

高中部屬教育部國前署；國小部屬高雄市政府。

參、計畫目的

落實個人資料檔案之安全維護及管理，防止個人資料被竊取、竄改、毀損、滅失或 洩漏。

肆、管理人員及個人資料保護管理政策

一、總管理人：由校長擔任，負責督導、考核本計畫各項工作。

二、個人資料管理人(以下簡稱管理人)：由各處室主任擔任，負責督導處室內個人資料檔案安全維護之執行，並將執行之相關作業程序、控制重點、納入各處室內部控制內容。

(一)發生個人資料被竊取、竄改、毀損、滅失或洩漏事件時，迅速處理，以保護當事人之權益。並將處理方式及結果，向總管理人提出書面報告。

(二)依據稽核人員就安全維護計畫執行之評核，於進行檢討改進後，向稽核人員及總管理人提出書面報告。

三、所屬人員：指本校執行業務之過程，必須接觸個人資料之人員，包括定 期或不定期契約人員及派遣員工。

伍、個人資料蒐集、處理及利用管理措施

一、直接向當事人蒐集個人資料時，應明確告知以下事項：

(一)本校名稱。

(二)蒐集目的。

(三)個人資料之類別。個人資料屬直接蒐集或間接蒐集。

(四)個人資料利用之期間、地區、對象及方式。

(五)當事人得請求閱覽、製給複製本、補充或更正、停止蒐集、處理、利用或刪除其個人資料。

(六)當事人得自由選擇提供個人資料時，不提供將對其權益之影響。

二、所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項應告知之事項。

三、利用個人資料為行銷時，當事人表示拒絕行銷後，應立即停止利用其個人資料行銷。

四、當事人表示拒絕行銷或請求閱覽、製給複製本、補充或更正、停止蒐集、 處理、利用或刪除其個人資料時， 視其屬性為學生相關、教師職員工相關、其他關係人，聯

絡窗口為對應之個資管理人。聯絡窗口及電話等資料，揭示於本校網頁。如認有拒絕當事人行使上述權利之事由，應附理由通知當事人。

五、負責保管及處理個人資料檔案之員工，其職務有異動時，應將所保管之儲存媒體及有關資料檔案移交，以利管理。

六、本校教職員工如因其工作執掌相關而須輸出、輸入個人資料時，均須鍵入其個人之使用者代碼及識別密碼，同時在使用範圍及使用權限內為之，其中識別密碼並應保密，不得洩漏或與他人共用。

七、本校教職員工對於非授權之校內系統，因業務需求之個資申請使用，需透過公文系統之電子申請表申請，經簽核會辦，雙方處室之個資管理人同意後，由系統管理人交付資料，申請人取得資料後仍需依本管理辦法管理使用取得之個資。

八、由稽核人員定期清查所保有之個人資料是否符合蒐集特定目的，若有非屬特定目的必要範圍之資料，或特定目的消失、期限屆滿而無保存必要者，即予刪除、銷毀或其他適當處置。

九、本校如有委託他人蒐集、處理或利用個人資料時，當對受託者為適當之監督並與其明確約定相關監督事項：

(一)所蒐集之個人資料如需作特定目的外利用，必須先行檢視是否符合規定。

(二)受託人應簽訂相關個資授權及保密義務約定文件。

(三)本校因故終止業務時，原保有之個人資料，即依規定不再使用，並採銷毀、移轉或其他妥適方式處理。

陸、事故之預防、通報及應變機制

一、預防：

(一)本校員工如因其工作職掌而須輸出、輸入個人資料時，均須鍵入其個人之使用者代碼及識別密碼，同時在使用範圍及使用權限內為之。

(二)本校對內或對外從事個人資料傳輸時，加強管控避免外洩。

(三)加強員工教育宣導，並嚴加管制。

二、通報及應變：

(一)發現個人資料遭竊取、竄改、毀損、滅失或洩漏即向管理人通報，並立即查明發生原因及責任歸屬，及依實際狀況採取必要措施。

(二)主管機關通報：上述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)，通報主管機關；國中及國小部通報之主管機關為縣(市)政府者，並應副知教育部；並自處理結束之日起一個月內，將處理方式及結果，報主管機關備查。

(三)對於個人資料遭竊取之當事人，應以適當方式通知使其知悉及本校個人資料外洩事實、已採取之處理措施、聯絡電話窗口等資訊。

(四)針對事故發生原因研議改進措施。

柒、資料安全管理、員工管理及設備安全管理

一、資料安全管理：

(一)電腦存取個人資料之管控：

1. 本校所屬員工應妥善保管個人電腦存取資料之硬體，並設定登入及螢幕保護程式密碼。個人資料使用完畢，應即退出電腦使用檔案，不得留置於電腦上。下班前應關閉電腦電源，並將所保有其他個人資料之媒介物置於專用抽屜內上鎖保管。
2. 本校員工如因其工作職掌相關而須輸出、輸入個人資料時，均須鍵入其個人之使用者代碼及識別密碼，同時在使用範圍及使用權限內為之，其中識別密碼並應保密，不得洩漏或與他人共用。
3. 個人資料檔案使用完畢應即退出，不得任其停留於公用電腦上。
4. 電腦系統防毒、掃毒應時時開啟保持最新安全狀態。
5. 建置個人資料之個人電腦，不得直接作為公眾查詢之前端工具。
6. 儲存個人資料之電腦主機系統應設置防火牆，降低外部入侵風險。
7. 主機置放之機房應設置門禁、監視錄影及防滅火設備。
8. 可攜式儲存媒體如為機關內共同使用，使用者切記在使用完畢後將所有資料文件移除，以免資料遭他人誤用。

(二)紙本資料之保管：

1. 本校保有個人資料存在於紙本者，應儲存於上鎖之保管箱或檔案室內，僅業務主管有開啟調閱權限， 其他所屬人員因業務需要而須調閱或使用個人資料者， 應提出申請，經業務主管人員同意後調閱或使用。員工非經學校校長或營業處所主管同意不得任意複製或影印。
2. 儲存個人資料紙本之保管箱或檔案室內，應設置適當之防竊措施。
3. 對於記載個人資料之紙本丟棄時，應先以碎紙設備進行處理。

(三)使用電子商務服務系統或個人資料種類之資通系統時之資訊安全措施：

1. 使用者身分確認及保護機制。
2. 個人資料顯示之隱碼機制。
3. 網際網路傳輸之安全加密機制。
4. 應用系統於開發、上線、維護等各階段軟體驗證及確認程序。
5. 個人資料檔案與資料庫之存取控制及保護監控措施。
6. 防止外部網路入侵對策。
7. 非法或異常使用行為之監控及因應機制。
8. 前述第 6 及第 7 所定措施，應定期演練及檢討改善。

前項所稱電子商務，指透過網際網路進行有關商品或服務之廣告、行銷、供應或訂購等各項商業交易活動；資通系統，指用以蒐集、控制、傳輸、儲存、流通、刪除資訊或對資訊為其他處理、使用或分享之系統。

二、人員管理：

(一)依業務職掌授予所屬人員不同權限的帳號密碼登入電腦系統，以進行個人資料的蒐集、處理、利用。

(二)因業務需要而須利用非權限範圍之特定個人資料者，應事前提出申請，經業務主管人員同意後由業務單位依申請範圍提供資料。

(三)所屬人員就於本校任職期間因業務所接觸個人資料均負保密義務與責任。

三、設備安全管理：

(一)所保有個人資料存在於紙本者，應儲存於上鎖之保管箱或檔案室內，僅業務主管及業務相關授權人員有開啟調閱權限。所保有個人資料庫之應設置權限，僅僅業務主管及業務相關授權人員有開啟權限。

(二)所屬員工應妥善保管個人電腦存取資料之硬體，並設定登入密碼。所屬員工於下班前應關閉電腦電源，並將所保有其他個人資料之媒介物置於個人抽屜內上鎖保管。

(三)個人資料紙本之保管箱或檔案室內，應設置防火裝置及防竊措施。儲存個人資料之電腦主機系統應設置防火牆，降低外部入侵風險。置放之機房應設置門禁、監視錄影及防火設備。

捌、業務終止後之個人資料處理方法

一、本校停止辦學後，所保有之個人資料不得繼續使用，並留存相關處理紀錄至少五年。

二、因業務終止後個人資料特定目的消失、契約或法令規定期限屆滿等，所保有之紙本個人資料應以碎紙、委外焚化等方式銷毀紙本，個人資料儲存於磁碟、磁帶、光碟片、微縮片、積體電路晶片等媒介物者，應以消磁、剪斷、敲擊等破壞措施銷毀。

三、進行前項個人資料銷毀處理前應報請主任管理人核准後始得為之，應記載處理之時間、地點，並以照相或錄影方式留存紀錄。

玖、本辦法經行政會議通過，陳請校長核准後實施，修正時亦同。