三信家商個人資料檔案安全維護計畫

訂定(或修訂)日期：中華民國115年11月10日討論通過

壹、依據：

個人資料保護法第27條第2項及「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4條第1項。

貳、目的：

落實個人資料檔案之安全維護及管理，防止被竊取、竄改、毀損、滅失或洩漏。

參、適用範圍

本校師、生、員工、臨時約聘/雇人員及接受本校委辦案派駐本校之人員。

肆、權責單位及管理人員

(一)權責單位

本校「校長室」，負責有關個人資料保護與管理相關工作，推動下列業務：

1. 擬訂本校個人資料保護管理計劃的制定與實施。
2. 本校個人資料隱私風險評估與管理。
3. 本校教職員工之個人資料保護意識提升、教育訓練計畫之擬議及宣導作業。
4. 本校個人資料管理基礎設施的評估與強化。
5. 本校個人資料安全保護措施與技術加強。
6. 本校個人資料洩漏與事故應對機制。
7. 本校個人資料保護監控與改善。
8. 其他資料保護管理的規劃與執行事項。

（二）管理人員：

1. 管理人(召集人)： 校長擔任

2. 執行秘書：人事主任

3. 個資專職人員：人事組長、註冊組長

4. 個資保護聯絡窗口：圖資處資訊組長

伍、個人資料檔案之安全維護管理措施

一、蒐集、處理及利用個人資料之範圍及特定目的

（一）個人資料範圍：

1. 本校對於個人資料之定義：「個人資料保護法」第2條所規範之19項個人資料以及「個人資料保護法之特定目的及個人資料之類別」所規範之個人資料類別。

2. 「特種個人資料」之蒐集、處理與利用：本校依照「學校衛生法」規定，學校應建立學生健康管理制度；健康檢查及疾病檢查結果，應載入學籍資料。依「勞工安全衛生法」規定：可蒐集、處理與利用「員工」之「健康檢查」及「醫療」相關資訊。特種個人資料得經當事人書面同意蒐集、處理或利用。

3. 依「個人資料保護法」立法精神，本校需進行全面性之個人資料盤點，範圍包括本校目前持有之個人資料、本校受委託蒐集、處理或利用之個人資料以及本校委託外部機關蒐集、處理或利用之個人資料皆屬之。個資盤點項目依本校「個人資料盤點表」進行。蒐集、處理及利用個人資料之特定目的。

(1) 目前本校持有個人資料之特定目的

002 人事管理

063 非公務機關依法定義務所進行個人資料之蒐集處理及利用

069 契約、類似契約或其他法律關係事務

109 教育或訓練行政

110 產學合作

136 資（通）訊與資料庫管理

146 圖書館管理

157 調查、統計與研究分析

158 學生(員)資料管理(含畢、結業生)

159 學術研究

(2) 管理人員須定期檢視，發現有非屬特定目的必要範圍內之個人資料或特定目的消失、期限屆滿而無保存必要者，應予刪除、銷毀或其他停止蒐集、處理或利用等適當之處置。

4. 完成個人資料盤點後，需產出下列文件，其維護權責單位為人事室：

(1) 個人資料盤點清冊

5. 完成個資盤點後，如果所蒐集、處理或利用之個人資料類別不屬本校個人資料檔案清冊中所列之清單，即需對相關個資之當事人進行告知。並將所有告知行為與內容需有紀錄留存備查。

二、個人資料之風險評估及管理機制

（一）風險評估

針對學校收集、處理、儲存及傳輸的所有個人資料進行風險評估，識別潛在的內部、外部及人為風險，並分析資料敏感度與處理過程中的風險點（如資料外洩、未授權存取等）

（二）管理機制

1、 強化技術防護措施（如資料加密、身份驗證、系統防火牆），確保資料存取權限與處理流程符合最小存取原則，並定期檢視資料的安全性與合規性。

2、 針對各類風險（如駭客攻擊、內部濫用、資料外洩等），設定具體的防範措施並加強資料處理流程的監控。

3、 完成風險評鑑後，需產出下列文件，其維護權責單位為人

事室：

(1)個人資料檔案風險評鑑彙整表

四、事故之預防、通報及應變機制

（一）預防：

1、指定專人或小組辦理安全維護事項，防止本校保有之個人資料被竊取、竄改、毀損、滅失或洩漏。

2、本校保有之個人資料檔案，限承辦人員使用或存取，使用或存取範圍限與其本身業務相關，且存取檔案時須鍵入其個人之使用者代碼及識別密碼。非承辦人員參閱、使用或存取相關個人資料檔案或書件時，應經負責人或經授權之管理人員同意。

3、存有個人資料之儲存媒體(含可攜式媒體)，視必要性採取適當之加密機制；存有個人資料之紙本文件於不使用或下班時，遵守桌面淨空，置於抽屜或儲櫃並上鎖。

4、存有個人資料之紙本及存放媒介物於報廢汰換或轉作其他用途前，確實刪除資料或格式化，或採物理方式破壞、銷毀。

5、電腦安裝防毒軟體並定期更新病毒碼，避免惡意程式與系統漏洞對作業系統之威脅。

6、對內或對外從事個人資料傳輸時，加強管控避免外洩。

7、加強所屬人員教育宣導，並嚴加管制。

8、學校各單位應就風險評鑑中所可能適逢之各種情境進行必要之演練，詳細記錄演練之過程，建立標準之個資事故處理標準作業程序。

（二）通報及應變：

1、本校所屬人員發現個人資料遭竊取、竄改、毀損、滅失或洩漏等安全事故時，應立即向負責人或管理組織人事室、教務處或圖資處通報，可由圖資處依教育機構資安通報平台，進行通報。

2、自事故發現起72小時內，依內政部要求向事業主管機關通

報，並填寫「個人資料事故通報及紀錄表」。

3、進行危害初步控管，通過終止或減緩事件擴大，防止資料進一步洩漏或被濫用。

4、對事件的影響與衝擊程度進行全面評估，確定洩漏資料的範圍、性質以及對當事人和機構的潛在風險，進而制定相應的應對策略。

5、發生個人資料安全事故後，應儘速以適當方式通知當事人事故發生的事實、已採取的處理措施，以及本校窗口電話等聯絡資訊。

通知方式可以包括：

(1)透過電話、電子郵件、短信等方式直接通知當事人。

(2)若事故較為嚴重，應視情況進行公開說明，並提供具體的聯絡管道。

6、對事故原因進行深入分析，並研擬改進措施，以避免類似事件的再次發生。

7、事故自發生起至結束需產出下列文件，：

(1) 通報紀錄

(2) 事件處理經過

(3) 事故分析報告

(4) 改善措施及改善紀錄

(5) 審查會議記錄

五、個人資料蒐集、處理及利用之內部管理措施

（一） 向當事人蒐集個人資料時，除法律明文規定外，需經當事人同意並明確告知蒐集目的、個人資料之類別、利用期間、地區、對象及方式。

（二） 蒐集個人資料應符合特定之目的，並確保資料之正確性、完整性和時效性。

（三） 當事人得向本校請求閱覽、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。

（四） 所蒐集之個人資料非由當事人提供者，應於處理或首次利用

前，向當事人告知其個人資料來源及前項應告知之事項，若當事人表示拒絕提供，應立即停止處理、利用其個人資料。

（五） 另本校保有之個人資料利用期限屆滿時，除因法令規定、執行業務所必須或經當事人書面同意者外，將主動刪除或銷毀其個人資料，並留存相關紀錄。

（六） 當事人得向本校表示拒絕提供，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之聯絡窗口為圖資處；聯絡電話：學校總機，分機號碼:1300。以上聯絡資料公告於本校處所(有網站或其他適當處所者，請增列網站首頁及其他適當地點，如分支機構名稱)。如拒絕當事人行使上述權利，應附理由通知當事人。

（七） 負責保管及處理個人資料檔案之人員，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。

（八） 本校所屬人員輸出、輸入個人資料時，須鍵入其個人之使用者代碼及識別密碼，並須在使用範圍及使用權限內為之。識別密碼應保密，不得洩漏或與他人共用。

（九） 本校所屬人員離職時，主動刪除或銷毀其個人資料，並留存相關紀錄。

（十） 指定管理人員定期(週、月、年)清查本校所保有之個人資料是否符合特定目的，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，並留存相關紀錄。

(十一)本校保有之個人資料如需作特定目的外利用，應先行檢視是否符合個人資料保護法第20條第1項但書之規定。

(十二)本校委託他人或其他第三方蒐集、處理或利用個人資料時，對受託者為適當之監督並與其明確約定相關監督事項。

六、實體環境安全管理、資料安全管理及人員管理措施

（一）設備安全管理

1、指派專人管理儲存個人資料之電腦及其他儲存媒介物，定期清點、保養維護、資料備份，並注意設備防竊、未經授權攜出等

安全措施。

2、重要個人資料備份應異地存放，並建置防止個人資料遭竊取、竄改、損毀、滅失或洩漏等事故之機制。

3、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。

4、電腦、自動化機器或其他儲存媒介物需報廢汰換或轉作其他用途時，檢視個人資料是否確實刪除。

（二）資料安全管理

1、資通訊系統存取個人資料之管控：

（1）於儲存個人資料之電腦設置識別密碼、保護程式密碼及相關安全措施。

（2）個人資料檔案使用完畢應即關閉檔案，不得任其停留於螢幕上。

（3）定期進行防毒、掃毒等必要之安全措施。

（4）重要個人資料檔案應另加設密碼，非經陳報核可不得存取。

（5）所屬人員非經本校校長核可，不得任意複製本校保有之個人資料檔案。

（6）本校蒐集、處理或利用個人資料達1百筆以上時，設置使用者身分確認及保護機制、個人資料顯示之隱碼機制(註：如將身分證字號末4碼以****標示，或將姓名其中1個字以〇標示)、網際網路傳輸之安全加密機制、個人資料檔案與資料庫之存取控制及保護監控措施，防止外部網路入侵對策及非法或異常使用行為之監控及因應機制。

2、紙本資料之保管：

（1）記載有個人資料之紙本文件，在未使用時存放於公文櫃內並上鎖。所屬人員非經各科室主管、承辦人員核可，不得任意複製、拍攝或影印。

（2）丟棄記載有個人資料之紙本文件時，應先以碎紙設備進行處理。

（三）人員管理

1、依業務需求適度設定所屬人員(註：例如主管、非主管人員)對

個人資料蒐集、處理及利用之不同權限。

2、所屬人員登錄電腦之識別密碼，應定期變更。

3、所屬人員應妥善保管個人資料之儲存媒介物，執行業務時依個人資料保護法規定蒐集、處理及利用個人資料。

4、本校與所屬人員間之勞務、承攬及委任契約均列入保密條款及違約罰則，以促使其遵守個人資料保密義務（含契約終止後）。

5、所屬人員離職時，應即取消其登錄電腦之使用者代碼（帳號）及識別密碼。其在職期間所持有之個人資料應確實移交，不得私自複製、留存並在外繼續利用。

6、承辦相關業務之所屬成員應定期變更識別密碼，並於變更識別密碼後始可繼續使用電腦。

七、 認知宣導及教育訓練

（一）每年派遣所屬人員參與相關單位辦理之個人資料保護法宣導或數位學習教育訓練至少3小時(或每學年自行辦理個人資料保護法基礎認知宣導及教育訓練2次，上、下學期至少各1次)。參加或自辦教育訓練應留存相關紀錄或佐證資料（例如：簽到表或教育訓練教材等佐證資料)。

（二）對於新進人員給予特別指導，確保其明瞭個人資料保護相關法令規定及責任範圍。

八、 個人資料安全維護內部稽核機制

（一）本校每半年進行1次本計畫及處理方法執行情形之檢查，檢查結果向負責人(或管理組織)提出報告，相關文件至少保存5年。

（二）若檢查結果不符合法令或有不符合法令之虞，依下項事項規劃改善措施：

1、確認不符合法令之內容及發生原因。

2、提出改善及預防措施方案。

3、紀錄檢查情形及結果。

九、 使用紀錄、軌跡資料及證據保存

（一）本校建置個人資料之電腦，其個人資料使用查詢紀錄，需每年備

份並設定密碼，儲存該紀錄之儲存媒介物保存於適當處所以供備查。

（二）個人資料使用紀錄以紙本登記者，應存放於公文櫃內並上鎖，非經各科室主管、承辦人員核可，不得任意取出。

（三）以上使用紀錄、軌跡資料及相關證據至少留存5年。

十、個人資料安全維護之整體持續改善

本校將隨時參酌業務及執行本計畫狀況、技術發展及相關法規定修等因素，檢討本計畫是否合宜，必要時予以修正，並於修正後保存備查。

十一、業務終止後之個人資料處理方法

本校業務終止後，所保有之個人資料依下列方式處理，不再繼續使用，並將相關紀錄報送上級主管機關。

（一）銷毀：銷毀之方法、時間、地點及證明銷毀之方式。

（二）移轉：移轉之原因、對象、方法、時間、地點及受移轉對象得保有該項個人資料之合法依據。

十二、本辦法核可後公佈實行，修正時亦同。