耕莘健康管理專校個人資料安全維護計畫

民國 103 年 10 月 13 日資訊安全推動小組會議通過

民國 105 年 9 月 30 日資訊安全推動小組會議通過

民國 111 年 5 月 6 日資訊安全推動小組會議通過

一、制定目的

為使本校個人資料管理與保護符合政府法令相關規範，並防止個人資料被竊取、竄改、毀損、滅失或洩漏，本校所屬人員應依本計畫及方法辦理個人資料檔案安全維護及業務終止後個人資料處理事項。

二、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。

三、依據

(一)個人資料保護法。

(二)個人資料保護法施行細則。

(三)教育體系資通安全管理規範。

(四)教育部提升校園資訊安全服務計畫。

(五)私立專科以上學校及私立學術研究機構個人資料檔案安全維護實施辦法。

(六)教育體系個人資料安全保護基本措施及作法。

四、權責單位及管理人員

(一)權責單位：本校「資訊安全推動小組」，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規範及配套措施。

2.本校個人資料隱私風險之評估及管理。

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.本校個人資料管理制度基礎設施之評估。

5.本校個人資料管理制度適法性與合宜性之檢視、審議及評估。

6.個人資料外洩事件通報暨危機處理。

7.其他本校個人資料保護、管理之規劃及執行事項。

(二)管理人員：

1.個資管理人(召集人)：副校長。

2.執行秘書：資訊暨圖書中心主任，負責綜理個資相關業務。

3.當然委員：教學及行政單位一級主管、資訊暨圖書中心二級主管及學生代表（由學生自治會推派一人參加)。

4.選任委員：各科推派教師代表1人，任期為1年，連選得連任之。

5.個資稽核人員：由資圖中心成立「個資保護稽核小組」，以進行個資內部稽核作業，負責評核個資安全維護計畫執行情形及成效。

6.聯絡窗口：資訊暨圖書中心圖書組長。

五、個人資料之範圍界定

(一)組織背景

1.本校為教育單位，主管機關為教育部技職司。

2.本校所蒐集、處理或利用之個人資料主要為履行法定義務。

(二)組織適用之特定目的

1.目前本校持有個人資料之特定目的分為以下幾類：

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

160　憑證業務管理

2.未來若有任何單位因非上述所列之特定目的或在上述特定目的外需蒐集、處理或利用個人資料，必須於「單位內部保有及管理個人資料之項目彙整表」，備註說明新蒐集、處理或利用之特定目的或特定目的外蒐集、處理或利用之原因。

3.本計畫之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。

(三)個資蒐集、處理與利用程序違反，可能導致行政處罰之行為

本校「資訊安全推動小組」與本校專責稽核個人資料管理執行成效之內控小組成員，需針對下列項目進行稽核，以確保本校對個人資料之管理符合「個人資料保護法」之規範。杜絕因違法而導致之各類罰責：

1. 未依規定蒐集個人資料(含告知個資當事人)
2. 未依規定處理個人資料
3. 未依規定利用個人資料
4. 未妥善保管個人資料
5. 未依規定提供當事人行使個資之權利
6. 未依規定對個資委外作業進行必要之監督

(四)界定個人資料範圍

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。
4. 完成個人資料盤點後，需產出下列文件，其維護權責單位為資訊暨圖書中心圖書組：
   (1)各單位管理個人資料之項目彙整表
   (2)本校個人資料檔案風險評鑑表
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。
6. 在完成個資盤點作業後，後續有任何新個人資料之蒐集、處理或利用之需求時，依本校「個資保護及管理作業程序」進行作業。

六、風險評估及管理機制

(一)個人資料之風險評估

1. 本校所有與個人資料相關之流程與檔案資料之管理皆必須進行衝擊與風險評鑑。

2.各類項目之衝擊評鑑項目與標準依「本校個人資料檔案衝擊評鑑標準表」進行評鑑。

3.所有評鑑結果需記錄於「本校個人資料檔案衝擊評鑑表」。

4.所有與個人資料相關之風險評鑑需依「流程」、「人員」與「技術」三類進行評鑑。

5.為確保本校與個人資料之管理機制符合「個人資料保護法」之規範，需依「本校個人資料檔案風險評鑑檢查項目表」進行個人資料作業程序之風險評鑑。評鑑結果紀錄於「本校個人資料檔案風險評鑑表」。

(二)事故之預防、通報及應變機制

1.為確保發生個資事故時能立即採取行動因應各種衝擊，由本校「資訊安全推動小組」負責整體個資事故之應變。

2.學校各單位應就衝擊與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。

3.針對不同層級之風險，校內各單位應制定不同層級之應變計畫，避免因所有風險一視同仁，造成資源之浪費。

4.整體應變機制的流程應為：

(1)啟動組織內部通報機制

(2)危害初步控管(終止或減緩個資事件持續擴大)

(3)評估事件影響與衝擊程度

(4)識別個資事件發生原因

(5)資料公開：擬定對外說明文件(如果影響範圍擴及組織外部人員)，並通報個資當事人以及必要之主管機關，內容需包括：

A.防止再發所採行之措施

B.誠信負責之態度

C.發生之原因

D.補償機制(確定學校疏失時才需要)

E.學校對外聯繫窗口與聯絡方式

(6)事件檢討：建立「事件處理分析報告(需包括避免類似事故再次發生之改善措施)」「個資安全事件報告單 3-310-006」，經決策主管核覆，以確保事件已完整結案

(7)文件歸檔：將事件所有處理經過以及文件完整歸檔。需歸檔之資料包括：

A 事故發生相關紀錄

B 事件處理經過

C 事故分析報告
D 通報紀錄

七、個人資料內容規範

(一)個人資料蒐集、處理、利用及傳輸：

1. 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。

2. 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。

3. 蒐集個人資料時，需經適當之授權與監督並僅就所需之必要欄位進行收集。經授權同意交換個人資料時，電子類文件需對資料檔案加密或透過加密通道傳送、紙本類文件以彌封或其他安全方式進行傳遞交換工作。傳遞接收個資之承辦人需將列印、轉交等行為登載於「個人資料簽收紀錄」(表單編號：3-310-002)。

4. 校內各單位因公務作業所需人事資料時，請填寫「人事資料需求表」(表單編號：3-310-003)，逕向相關單位提出申請，經授權同意後，依「個人資料保護法」規定辦理。

5. 當個人資料蒐集範圍逾法律、法規命令、行政規則及行政計畫(教育主管機關法令規範、學則等規定)，或係依作用法、組織法所定執行法定職務者之特定目的外，應依個資法規定取得當事人之同意。同意範本請參閱「個人資料蒐集、電腦處理、國際傳遞及利用同意書」(表單編號：3-310-004)，範本內容可依單位需求修改。

6. 個人資料依有關法令為特定目的外之利用時，應由該資料檔案承辦單位填具「個人資料調閱申請書」(表單編號：3-310-010)，簽奉核准後行之。

7. 個人資料若非經資料當事人之同意或經法令規定許可，不得任意揭露、販售或用於蒐集時的特定目的以外之用途。

8. 非由當事人提供之個人資料，得於處理或利用前向當事人補行告知義務，告知方式得以書面、電話、傳真、電子文件或其他適當方式為之。

9. 個人資料之處理行為需經單位主管核准，宜釐定使用範圍及調閱或存取權限。個資存取時應視需要考量採取權限區隔、資料加密機制，或相關

核准程序加以控管，並留存可識別之發送紀錄及個資使用者身分以供事後稽查。

10. 使用者經正式授權存取個人資料檔案時，其帳號必須為唯一，避免共用帳號。

11. 以電腦處理個人資料時，需核對個人資料之輸入、輸出、編輯或更正是否與原件相符。個人資料提供利用時，對資料相符與否如有疑義，應調閱原始檔案查核。

12. 禁止使用即時通訊軟體、外部信箱（如奇摩信箱、Gmail、Hotmail等）傳輸及存取個人資料檔案，利用校內信箱（webmail）傳輸個人資料時請加密保護與留存追查紀錄。

13. 各單位管理之網站或網頁內容，於確有必要公布個人資料時，需經單位主管核准，且依相關法律及規範處理，始得公布。

14.依個人資料保護法第 3 條規定，當事人可行使以下權利：

(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、處理及利用。

(5)請求刪除。

若當事人有上述需求，請與業務單位聯繫，並填妥本校「當事人個人資料權利行使申請書」(表單編號:3-310-011)後，業務單位將依法進行回覆。因業務單位執行職務或業務所必須者，業務單位得拒絕之。另依個人資料保護法第 14 條規定，查詢或請求閱覽個人資料或製給複製本者，業務單位得酌收必要成本費用。

(二)本校個人資料保護聯絡窗口

個資保護聯絡窗口:

資訊暨圖書中心圖書組

辦理事項如下：

1. 本校與機關間個人資料保護業務之協調聯繫及個資安全事件通報。

2. 本校發生重大個人資料外洩事件聯繫窗口。

3. 本校各單位之其他重大個人資料保護管理事項聯繫處理。

4. 公告本校保有個資項目於「個資法宣導執行專區」網頁供大眾閱覽。

(三)學術研究個資之處理方式：

1. 所需研究資料若涉及個人資料範圍時，請注意下列事項：

(1)資訊暨圖書中心並非個人資料的擁有者，僅是代管者，如未經適當合法程序，不宜擅自散布資料。

(2)未涉及個人資料者，請以專簽會資訊暨圖書中心辦理，資訊暨圖書中心將依「去識別化」之工作負荷提出會簽意見，待校長核可後，再依資訊安全管理制度之規定填具資料需求表（如提供研究使用，要另行加註明及需另填保密切結書）。

(3)涉及個人資料者，主管機關會依據個人資料保護法內容，針對學術研究資料進行詳細規範，供遵循辦理。

(四)個資處理人員管理：

1. 處理接觸機敏資料人員，應簽署「保密切結書」(表單編號：3-310-005)，克盡保密之責，並確認於離職時或合約終止時取消或停用其使用者識別帳號，且收繳其通行證及相關證件。

2. 禁止人員在社群網站、部落格、公開論壇或其他利用網際網路形式公開業務所知悉之個人資料。

(五)個人資料外洩(竊取、洩露、竄改或其他侵害事件)處理流程：

1. 立即通知本校個人資料保護聯絡窗口。

2. 個資外洩單位以最速件級別專簽會資訊暨圖書中心辦理。

3. 發生個資外洩事件，即時以書面、電話、傳真、電子文件或其他足以使當事人知悉或可得知悉的方式，通知個人資料受侵害項目、產生之影響及已採取之因應措施。

4.個資事件發生時，依通報順序逐級陳報，應於 36 小時內完成校內通報程序，並填報「個資安全事件報告單」(表單編號：3-310-006)

5.經校內程序釐清並確認為個資事件後，應依規定填具「個人資料侵害事故通報與紀錄表」，於事故發現時起 72 小時內通報主管機關。(表單編號：3-310-021)

(六)蒐集、利用及處理個人資料時，請務必遵守「個人資料保護法」，確實妥善保管所取得之個人敏感性資料。個人資料管理人若違反個人資料保護法規定者，將受法律制裁；其他未盡事宜，悉依個人資料保護法之規定辦理。

(七)每半年各單位資安與個資聯絡人請填寫「資安及個人資料保護檢核表」(表單編號：3-310-007)，確保單位內部個人資料受到保護，作業程序依規範辦理執行。

八、資料安全、設備安全及人員管理

(一)個人資料所在區域之實體環境保護

1.實體環境監控：

(1)需有安全之保存環境(溫度、濕度、火警)。

(2)對於資訊系統之實體存取需有監控機制，並在有實體安全事件發生時(例如：強行破壞管制設備)，可採取緊急應變措施。

(3)各單位需指派專人定期(每月)檢視與稽查實體環境之所有紀錄。

(4)在經費許可下，可在管制區域內設置環控設備，以自動檢測與保護管制區域。

2.實體環境進出管制：

(1)管制區域設有門禁。

(2)所有人員進出管制區域前需先獲得正式授權，並通過識別與認證。

(3)人員進出需留下作業紀錄，包括人員、進出時間、作業內容說明。

(4)管制區域需設有監控設備，例如：監視器。

(二)各類個人資料儲存媒體保護

1.媒體存取：

(1)非數位式媒體：例如：紙本。

A.需有限制存取之措施，例如：存放於上鎖之文件檯(櫃)。

B.儲存此類媒體之空間需有管控機制，例如：門禁管制、監視器。

C.可進出該管制空間之人員以及存取內存媒體者，需經過正式申請，獲得單位內權責主管同意，始可為之。同時，各單位需隨時維持管制人員之清單。

D.所有人員推出需填寫進出管制紀錄簿。

(2)數位式媒體：例如：硬碟

A.禁止人員進入私人之數位媒體-例如：隨身碟、行動式硬碟。

B.此類數位式媒體非經允許，不得攜出所在之管制區域外，除非經權責主管同意。

C.數位式媒體之存取需設有自動化之監控工具，記錄所有之存取活動。

D.儲存此類媒體之空間需有進出管控機制，例如：門禁管制、監視器。

E.所有人員推出需填寫進出管制紀錄簿。

F.對可攜式媒體之存取，需完整記錄其存取之行為與內容，並進行必要之稽核。

G.媒體所屬單位主管需定期稽核媒體保存空間之進出紀錄以及存取紀錄。

2.媒體儲存：

(1)所有數位與非數位之媒體，皆需儲存在有溫度、濕度控制之環境中。

(2)所有數位與非數位之媒體之儲存空間需要有防災設備，例如：滅火器。遇水有潮濕之虞之媒體，應使用適當包覆材料進行保護。

(3)儲存數位式之媒體，內存之機敏性資料(例如：個人資料)需以加密或其他足以保護其內容之方式進行儲存，以避免惡意人士能輕易取得機敏性資料。

(4)對於有儲存數位內容之媒體，需採取必要之保護措施，直至該媒體以合法授權之方式被銷毀為止。

(5)所有儲存媒體在報廢或另作他用時，必須徹底清除所含之數位或非數位資料，同時必須全程予以紀錄(例如：拍照或攝影)，以備後續之稽核。

(6)所有儲存媒體在報廢時，需經單位權責主管正式核可，且必須遵守組織設備報廢之程序進行如報廢作業委外進行，必須與承接廠商簽訂必要之保密協定，以確保組織之機敏性資料不外洩。

3.媒體淨化：

(1)媒體淨化是將媒體中原先儲存之資料進行消除，以避免內存之機密資料外洩，可進行之方式如下：

A.紙本：焚燒或是使用碎紙機粉碎。

B.硬碟：消磁、直接摔毀，USB隨身碟可破壞塑膠殼內部之記憶體顆粒。

C.光碟片：將光碟折斷、使用支援之碎紙機將碟片粉碎。

D.所有儲存機敏性資料之媒體，在報廢或要重複利用前，必須經過前項所述淨化措施。

E.整個淨化過程必須全程予以紀錄(例如：拍照或攝影)，以備後續之稽核。

(2)在將可攜式或可移動式之儲存媒體連接至組織之資訊系統時，必須徹底淨化這些媒體，一則確保不會保有先前儲存之資料，二則確保這些媒體不會隱藏惡意程式，進而威脅所連接之資訊系統。

(3)如果儲存機敏性資料之媒體無法進行淨化作業，則各單位必須採取破壞性且不可回復之處理方式，以確保媒體所儲存之資料不會被非法還原。

(三)媒體傳輸

1.避免在運輸過程中強調內容物。

2.在安全控管區域外傳輸運送儲存媒體時，必須採取防護措施保護儲存媒體：

(1)以保護材質覆蓋，避免遭受外力損傷。

(2)附加必要之封裝例如：傳送紙本之紙袋，其紙袋彌封處應有印記等標示，其紙袋彌封處應印記等標示，以確保在傳輸運輸過程中，未經非法之拆封。

(3)媒體傳送運送必須要有一專責之負責人，負起該傳輸運送作業之整體責任。

(4)負責媒體運輸之專人需為單位授權認可之人員。

(5)媒體傳輸運送過程需由執行之人員全程紀錄，包括過程中接觸之人員，傳輸運送工具、暫停地點與時間，最後由負責人員簽名以示負責。

(6)委由外部廠商進行媒體傳輸運送，需派員伴隨或由廠商提出可信賴之傳輸運送證據。

(7)如果所傳輸運送之媒體中所儲存之資料對組織至為重要且屬機敏性質，可將內存之資料進行必要之加密，並在傳輸運送到目的地後，確認資料之機密性、完整性，以及可使用性。

(四)技術管理措施

1.合法使用者與設備之識別與認證

(1)所有可能接觸學校相關資訊系統、管制區域，或其他存有機敏性資料控制點之人員或設備，皆必須配有唯一且可被本校識別之識別碼或通行證件，持有人有義務保管，並嚴禁借於他人使用。

(2)各單位內盡可能避免有適用公用識別碼或公用通行證件之情況，以確保能連到「可歸責性」。

(3)被存取之設備或受管制之通行區域、紀錄存取者/進出者之識別碼、時

間、地點、存取之標的物等，必須確保這些紀錄不被變更或刪除。

2.設備之識別與認證：

(1)校內所有之設備都必須有一個唯一之識別碼，資訊系統在與設備連線時，需使用此識別碼進行連線。

(2)資訊組必須備有一設備清冊，此清冊記錄所有之設備名稱、所有位置、唯一之識別碼、保管人、保管單位、可存取之授權清單，並隨時保持更新。

(3)資訊系統在與設備完成連線之前，必須完成與設備間之雙向認證，且須以安全技術。例如加密技術確保雙方連線之安全。

(4)如果從外部攜入之私人或非本校可控管之設備，需經本校之資訊權責單位確認無任何危害後，給予一組唯一之識別碼後可在內部使用。該設備所有使用情況應被確實完整記錄。

3.識別碼管理：

(1)資訊系統必須為能存取其內容或服務之使用者以及設備(例如：MAC，Internet，IP)建立唯一之識別碼。

(2)本校由資訊組建立一套授權程序，以便能為使用者或是設備建立唯一之識別碼。

(3)儘量避免重覆使用曾經建立之識別碼名稱，即便該識別碼名稱已不再使用。

(4)本校應依其組織政策、資訊安全政策、設備管理政策制定識別碼可以使用之期限，當人員異動、設備汰換，或其他特別情況，應將已不再允許使用之識別碼進行失效。

(5)在必要情況下，應避免以使用者之帳號作為對外之電子郵件地址，以避免被惡意程式破解，進而以使用者之帳號作為進行非法行為之代罪羔羊。

(6)每一個資訊系統之管理者識別碼以及密碼應妥善保管，嚴禁給予其他非管理人員，必要時，需進行更換，所有管理者識別碼之使用過程應在技術可行下，儘量紀錄使用過程。

(7)如無合理且必要之理由，嚴禁使用公用之識別碼。

4.帳密安全性及病毒碼更新

(1)各單位必須在電腦、相關設備或系統上設定認證機制，帳號及密碼必須具備一定安全之複雜度，並定期更換密碼。

(2)各單位必須於處理個人資料之電腦系統中安裝防毒軟體，並定期更新病毒碼。

(3)對於電腦作業系統及相關應用程式之漏洞，定期安裝修補之程式。

(4)具備存取權限之終端機不得安裝檔案分享軟體。

(5)定期檢查處理個人資料之資訊系統之使用狀況及個人資料存取之情形。

(五)存取控制

1.帳號管理：

(1)使用者或設備需透過帳號始能與資訊系統進行互動。設備與設備間也應套用相同運作模式。

(2)當不使用資訊系統或資訊資源時，帳號應被登出系統。

(3)資訊系統之管理者帳號應被妥善管理，且盡可能限制少數人使用。

(4)定期(每月)於每一資訊系統分析所有帳號之登錄與使用情況，尤其是系統管理者帳號。

(5)所有帳號登錄系統之紀錄不允許修改及刪除。

2.職務區域：

(1)在各單位人力許可下，應避免一項資訊系統管理業務僅授權給一位同仁，以避免該員工掌握所有單位核心安全，而增加資訊安全管理之風險。

(2)對於系統管理人員必須依其職務進行區域，以防止人員共謀進行惡意之資訊竊取行為。

(3)系統管理帳號之密碼應限制要求定期變更，並符合組織密碼強度之要求（至少 6 碼，包含英數字或特殊符號，中等安全等級以上)。

3.最小使用權限：

(1)各單位應依據業務需求，採用「最小使用權限」原則，僅提供必要之權限予使用者。

(2)所有可以接觸資訊系統或機敏性資料之人員或角色皆需有明確之授權定義，嚴禁任何模糊空間。

(3)對於管理資訊系統以及稽核資訊系統使用情況等功能，需明確授權給專人負責，並需針對權限使用情況進行定期之稽核。

4.企圖登入資訊系統之失敗管理：

(1)針對所有需要登入進行身分識別之資訊系統，需設定在一定時間內允許登入之次數(3 次)為上限。

(2)身份識別作業若失敗次數超過一定次數後需鎖定該帳號並通知系統管理員。

5.遠端存取：

(1)需針對遠端存取行為制定政策，以規範所有遠端存取行為。

(2)對於遠端存取之方式需制定明確之程序以及相關限制。

(3)應隨時更新與允許進行遠端存取之人員與設備清單。

(4)在進行遠端存取連線前，需進行身分認證以及授權程序。

(5)每一個可進行遠端存取之個體(人員或設備)必須可被唯一識別，亦即需具有可歸責性。

(6)在成本以及技術能力許可下，應建立必要之機制來執行遠端存取之監控

與紀錄，以稽核使用者行為，並確保遠端存取符合本校資訊安全相關之政策。

(7)所有遠端存取之連線運作需限制在組織可控制之安全環境內；對於外部因業務需求，需遠端連線至組織內之資訊損壞，需另行建置相關受保護與監控之遠端存取機制，且需記錄所有此類之遠端存取行為。

(8)對於以遠端存取方式進行之安全功能與安全相關資訊需建立嚴謹之保護措施，且所有行為皆需被記錄以供後續稽核使用。

(9)所有遠端連線所存取之資料皆需以或合法授權並被詳細記錄存取內容與情況。

(10)提供予外部廠商使用之帳號，應全程記錄其遠端存取之行為，並在完成每一次之遠端存取需求後，確認其遠端行為遵守本校資訊安全之規定，並立即取消該帳號之有效性。

(六)資料之備份

1.備份之場所：

(1)各單位無法對所有非預期中之天災人禍進行全面性之預防，因此對於各類個人資料，需有另一安全備份。

(2)各單位應建立一異地備份之機制，以儲存備份之個人資料。

(3)此一異地儲存空間之環境條件不得低於主要儲存空間。

(4)儲存於異地備份之資料將用於主要資料損毀之復原使用。

(5)為確保備份資料在還原時能有最少之損失，各單位應依資料之重要性設定異地備份之頻率與時間間隔。

(6)對於進出該異地備援/備份機房之人員需進行嚴格管制，且進出人員需留下必要之紀錄。

(7)若無必要，不應揭露這些場所所存放之機敏性資料。

(8)存放備份資料之地點需有適當之安全防護，包括門禁管制、環境控制機制。

(9)組織需指派專人管理備份資料以及儲存地點。

(10)備份過程需完整記錄，包括：

A.負責人員。

B.執行之設備。

C.備份標的物。

D.備份後儲存地點。

E.備份作業是否成功。

F.為確保備份資料之可用性，組織需指派專人定期進行資料之還原測試，並記錄所有之還原作業。

G.備份資料之存取需由權責單位主管核可後始可進行。

H.對於備份資料之存取，需留下相關紀錄。

(七)作業管理措施(資料安全管理)

1.電子個人資料管理

(1)儲存於電子媒體之個人資料應適當進行編碼或加密，避免以明確儲存而造成不必要之資料外洩。

(2)儲存個人資料或其他機敏性資料之電子媒體，應設置必要之稽核工具，確保任何之存取行為皆可被記錄並禁止非法之存取與變更。

(3)若使用加密技術保護個人或機敏性資料，應指派專人保管加密工具所使用之金鑰，並對金鑰之使用情況建立管理與稽核機制。

(4)存取過程之電子通道應予以加密。

(5)存取過程之行為應予以紀錄。

(6)存有個人資料檔案之資訊系統應顯示警語，提醒使用者遵守必要之保密責任。

2.紙本個人資料管理

(1)包含個人資料之紙本檔案，非特定目的之業務需要，業務職掌人員不得逕自呈現及公開討論。

(2)紙本資料之管理重點應從源頭開始控管：

A.內部自行列印部分：應該嚴格管制所有可以列印之資料，不應被列印輸出或需管制輸出之個人資料，應從列印權限開始管制，以降低輸出紙本所衍生之後續管理問題。

B.列印輸出至紙本行為設定權限控管。

C.列印輸出時需留下相關紀錄。

D.列印輸出時，在可能情況下，在紙本上列印浮水印警語(例如，會議資料內含個資，請勿攜出會場..)。

(3)外部蒐集而來部分：

A.造冊管制蒐集之紙本，蒐集者需於紙本上註記何人於何時向何對象蒐集。

B.非必要留存之紙本個資：於蒐集時確認其內容後即返還當事人。

C.於蒐集後，將該紙本進行掃描，轉換成電子型式或將紙本之內容輸入單位內部資訊系統後銷毀該紙本。

(4)個人資料之紙本需置於受管制區域。

(5)進出以及存取紙本個人資料之人員需獲得授權始可存取。

(6)進出以及存取紙本個人資料之人員需留下紀錄。

(7)如無必要，相同之個人資料應管制列印份數(例如：履歷表)，必要時再向保管人借閱。借閱亦需留下相關借還記錄。

(8)紙本傳遞需採行保護措施(例如：使用公文信封袋進行傳遞)，且需有傳遞送收紀錄。

(9)銷毀時需造冊並留下銷毀紀錄。

(10)學校內部稽核單位應定期稽核列印輸出紙本之去向。

(11)各單位列印輸出之紙本包含個人資料，該紙本在不需使用時，必須強制進行銷毀，嚴禁作為回收再利用之用途。

3.資料呈現

(1)若非必要，呈現個人資料內容時，應盡量使用去識別化方式，對個人資料進行個資保護，例如：以「李○明」取代「李小明」。以避免揭露過多之個人資料，但若因業務必要或其他符合完整呈現之標準，仍應以完整之內容呈現。

(2)無法立即銷毀之非數位類型媒體中，應以加蓋隱私保護章，將非必要呈現之機敏性資料予以處理，避免揭露過多之資料。

(3)記錄個人或機敏性資料之媒體，例如：紙本、電子檔案，在不影響作業之合法性之情況下，應適當加註「浮水印」，以警告接觸該資料之人員必須小心謹慎。

(八)人員管理措施

1.所有教職員工生(包括新進以及現有)皆應簽屬「個人資料蒐集、電腦處理、國際傳遞及利用同意書」。

2.教職員工(包含校內工讀生及委外廠商)報到時皆應簽屬「保密切結書」，以確保所接觸個人資料相關資訊系統及紙本之個人資料內容相關保密協定。

3.各類個資相關之宣導與教育訓練(應視職務內容而有所區別)：

(1)定期對校內教職員工生進行個人資料保護之宣導與教育訓練。

(2)禁止校內教職員工在公開媒體洩漏本校教職員工生之個人資料。

(3)同仁離開位置需將桌面上之機敏性紙本資料上鎖；需將電腦關機或登出。

4.權限管制：

(1)對所有保管個人資料，管理個人資料儲存媒體，以及可以存取個人資料之人員進行必要之權限管理。

(2)針對這些相關之人原設定權限控管，依照其職務的角色、內容等，設定系統存取權限，並且簽屬保密協定，以確實擔負保密義務。

(3)對於個人資料之存取活動需有紀錄，以提供人員進行稽核。

(4)所有人可接觸機敏性個人資料之人員，外寄電子郵寄須經過部級以上主管簽核。

(5)資訊單位建立電子郵件關鍵字過濾機制，以攔截可能之資料外洩。

(6)人員接觸個人資料時需有門禁管制並確實留下進出紀錄。

(7)對於管理資訊系統且有機會接觸到個人資料者，需建置監控工具，記錄所有存取個人資料之活動軌跡，包括直接存取資料庫。

(8)對於保存個人資料之實體環境應設置監視系統，紀錄所有人員之進出以及活動情況。

(9)員工需確實保管校內所提供之資訊系統帳號與密碼，各類通行證件，嚴禁借用予他人。

(10)各類權限之授予以最小且滿足業務所需為限。

(11)禁止開放公用帳號以及公用通行證件。

(12)人員進出管制區域之控管機制：以職務所需之最小權限為原則。

(13)對於高風險值之個資檔案，所屬單位主管需加強管制業務內，可以接觸機敏性個人資料人員。

(14)存有機敏性個人資料之資訊系統需啟用存取記錄功能，對各類管理帳號之存取尤須紀錄，並禁止任何之修改與刪除舉動。

5.各類可透過人員使用而外洩之資訊管理員工具之管制(IM 即時通訊軟體、E-Mail，...)：

(1)在校內禁止 IM(即時通訊軟體)工具傳遞個資檔案。

(2)在校內禁用外部 E-Mail 傳遞個資檔案。

(3)在校內禁用網際網路所提供之網路硬碟傳遞個資檔案。

(4)禁止人員在社群網站、部落格、公開論壇或其他利用網際網路形式公開業務所知悉之個人資料。

(5)不隨意開啟或執行來路不明之網站或電腦程式。

6.解除聘僱關係或服務異動後之人員安全管理

(1)人員職務異動時，關閉原先所有該人員使用之各類權限以及通行證件。

(2)人員離職時，需關閉其所有資訊系統或接觸個人資料媒體之權限。

(3)處理個人資料檔案之人員職務異動或離職時，需依規定列冊移交相關儲存媒體及資料。

(4)處理個人資料檔案之人員職務異動或離職時，交接人員需於相關系統重置通行碼，並視需要更換使用者識別帳號。

(5)負責個資檔案員工離職時，單位主管確認其是否有異常之個資接觸紀錄（資料安全稽核機制、稽核紀錄設備、資料庫、防火牆）。

九、認知宣導及教育訓練

(一)對象：包括校內教職員工及合作廠商

(二)訓練內容說明：宣導及教育訓練需依其業務與需要有不同之訓練內容。

1.個資法要求個人資料需有「專人辦理安全維護事項」，需具備：

(1)個人資料保護法之專業知識或維護。

(2)熟悉本校所持有個人資料檔案之蒐集，處理或利用之流程。

(3)熟悉各種資訊安全知識或工具，用以強化安全維護之層級。

2.個人資料保護機制負責人：個資、資訊安全、隱私保護等之控制措施。

3.個人資料保管人：隱私保護(校內利用個資之教職員工生)。

4. 資訊基礎環境負責人：資訊安全、媒體淨化技術、資料庫管理。
5. 資訊應用系統負責人：資訊應用系統安全設計、密碼技術。
6. 個人資料保護窗口：風險管控與危機處理。
7. 一般員工：個人資料保護之觀念，宣導個資相關案例。

(三)辦理時間與方式

1. 每學年開始 8 月初，定期辦理全校性個資宣導。
2. 每學期定期辦理校內教職員工個資教育訓練課程。
3. 數位學習網之個資保護教育訓練。

十、業務終止後個資處理與紀錄機制

(一)定期檢視：學校各單位須於每學期期末，檢核所屬個資檔案，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，並填具「個人資料銷毀申請表」(表單編號：3-310-008)。

(二)處理方式及留存紀錄如下：

1. 銷毀：銷毀之方法、時間、地點及證明銷毀之方式，並填具「個人資料銷毀申請表」(表單編號：3-310-008)。
2. 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。
3. 刪除、停止處理或利用個人資料：刪除、停止處理或利用之方法、時間或地點。

(三)各單位須留存之必要紀錄及種類

1. 個資交付、傳輸的紀錄。
2. 個人資料新增及修改之相關紀錄。
3. 提供當事人行使權利之紀錄。
4. 所屬人員權限新增、變動及刪除之紀錄。
5. 個人資料刪除、銷毀之紀錄。
6. 辦理個資教育訓練之紀錄(資訊暨圖書中心統整)。