健行科技大學個人資料檔案安全維護計畫

中華民國 104 年 7 月 20 日個人資料保護推動委員會議通過

壹、依據

依「個人資料保護法」及教育部 103 年 8 月 21 日臺教高通字第 1030117307B 號令訂定發布施行之「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」制(修)定之。

貳、目的

為落實本校個人資料檔案之安全維護及管理，以防止個人資料被竊取、竄改、毀損、滅失或洩漏，制定本計畫供本校各單位人員依循辦理。

參、實施內容

一、本計畫用詞，定義如下：

(一)個人資料(簡稱個資)：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)個人資料檔案:指依系統建立而得以自動化機器或其他非自動化方式檢索、整理之個人資料之集合。

(三)蒐集：指以任何方式取得個人資料。

(四)處理：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。

(五)利用：指將蒐集之個人資料為處理以外之使用。

(六)當事人：指個人資料之本人。

(七)個人資料管理代表：負責督導本計畫訂定與推動之人員(以下簡稱管理代表)

(八)個人資料保護稽核人員：負責評核本計畫執行情形及成效之人員(以下簡稱稽核人員)

(九)個人資料保護工作人員:各單位負責執行推動各項個人資料保護相關工作之人員。

(十)所屬人員：執行業務時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人員。

二、本校蒐集、處理或利用個人資料時，當履行下列義務：

(一)個人資料之蒐集、處理或利用，應尊重當事人之權益，依誠實及信用之方法為之，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。

(二)本校依個資法第十九條規定，向當事人蒐集個人資料時，應明確告知當事人下列事項：

1.本校名稱

2.蒐集之目的

3.蒐集個人資料之類別

4.個人資料利用之期間、地區、對象及方式

5.當事人依個資法第三條規定得行使之權利及方式

6.當事人得自由選擇提供資料時，如不提供將對其權益之影響

(三)非由當事人提供之個人資料，應於處理或利用前，或於對當事人首次利用時，向當事人告知個人資料來源及前條所列事項。

(四)本校應依當事人之請求，就其個人資料答覆查詢、提供閱覽或製給複製本。

(五)本校應維護個人資料之正確性，並應主動或依當事人之請求更正或補充之。

(六)本校若發生違反個資法規定，致個人資料被竊取、洩漏、竄改或其他侵害者，應查明後以適當方式通知當事人。

三、個人資料檔案盤點與風險評估

(一)個人資料盤點執行時機

1.本校每年定期執行一次個人資料盤點作業。

2.於下列情形發生時，需對影響範圍內之個人資料重新進行個人資料盤點：

(1)學校組織、業務權責變更時。

(2)作業流程變更時。

(3)個人資料項目新增或異動時。

(4)發生重大資訊安全事件時。

(二)個人資料盤點

1.分析業務作業流程

個人資料盤點應由分析業務作業流程開始,由單位所負責業務之相關程序與規範中（如：內部控制制度、ISO 標準作業程序、工作職掌、…等),了解資訊的流向。

2.識別不同作業流程之個資項目

(1)從業務或服務作業的流程中，分析各服務內容之作業流程與應用系統清單，以找出含個人資料之業務或服務作業流程，並找出與業務相關各種存在型式之個人資料檔案。

(2)不同型式的資料，如書面紙本、電子檔案或備份資料等皆應識別為不同的個資檔案。

3.識別個人資料檔案的相關屬性

識別出個人資料檔案的相關屬性,並填寫於「個人資料盤點表」中，相關屬性包含 ：

(1)個人資料項目基本資料：特定目的、個資類別、檔案型態、權責單位。

(2)個人資料項目生命週期活動：分析個資從蒐集、處理、利用、儲存、備份、傳輸、銷毀之活動及所需保存時間。

(3)個人資料項目相關人員：當事人、內部單位、委外單位、供應者。

(三)個人資料檔案風險評估

1.各單位應以「個人資料安全作業檢核表」確認單位對個人資料檔案保護是否落實。

2.針對「個人資料盤點表」中所有個資檔案進行風險評估，評估出應優先控管之個資檔案，並擬訂適當之管控措施進行管理。

四、個人資料蒐集處理利用作業

(一)個人資料蒐集

1.確認蒐集目的與範圍

進行資料蒐集前應有特定目的與範圍，並確認要蒐集個資欄位。

2.個資盤點表登記

(1)個資蒐集的內容應先進行評估蒐集的必要內容，確認每個欄位的必要性，不逾越蒐集的特定目的與必要範圍。

(2)訂定個資保留期限

A.所蒐集的個人資料應訂定保留期限，於個人資料蒐集之特定目的消失或期限屆滿後，進行個人資料的銷毀。

B.保留期限之訂定除有下列「因執行職務或業務所必須」者外，均應依本校文件分級分類管理相關規定辦理：

(a)有法令規定或契約約定之保存期限。

(b)有理由足認刪除將侵害當事人值得保護之利益。

(c)其他延長保留期限之正當事由。

(3)明確告知當事人事項

3.蒐集的個資依照「隱私權告知作業」履行告知義務，以尊重當事人隱私權。如有個資法第八條第二項情形，得免為告知：

A.依法律規定得免告知。

B.個人資料之蒐集係公務機關執行法定職務或非公務機關履行法定義務所必要。

C.告知將妨害公務機關執行法定職務。

D.告知將妨害第三人之重大利益。

E.當事人明知應告知之內容。

4.確認是否需書面同意

蒐集的個資如非屬下列情形之外，應取得當事人書面同意。

A.法律明文規定。

B.與當事人有契約或類似契約之關係。

C.當事人自行公開或其他已合法公開之個人資料。

D.學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或蒐集者依其揭露方式無從識別特定之當事人。

E.與公共利益有關。

F.個人資料取自於一般可得之來源。

5.依據個資的蒐集文件表單內容，於個人資料盤點表內登記，並經審查與單位主管同意後使用。

(二)個資處理

1.個人作業原則

(1)處理個人資料檔案之個人電腦，應設置使用者登入帳號及密碼，並啟動螢幕保護程式密碼功能。

(2)處理個人資料檔案時應有適當之安全措施，並依照「個人資料安全管理作業」程序辦理。

(3)機密個資檔案之處理，須經權責單位主管同意後進行，並須保留處理紀錄。

2.資訊系統作業原則

(1)資訊系統進行個資處理時，應進行權限控管，避免未經授權處理，權責單位應定期(至少每年)重新審核權限。

(2)新開發之資訊系統涉及個資處理者，應確保所處理的個資內容是相關且適法。

(3)處理個人資料之系統或業務，應每年定期檢視，確保個人資料處理之適當性及不過度使用。

3.資料正確維持原則

(1)於處理個人資料時，若發現資料不一致或不正確時，應主動追查，並進行資料的確認與更正，確保個人資料正確性

(2)因可歸責於本校之事由而未進行更正或補充的個資，應於更正或補充後，由權責單位通知當事人。

(3)當提供於第三方之個人資料有補充或更正時，應通知曾提供利用之對象。

(三)個資銷毀

1. 超過保存期限或不再需要使用之個人資料檔，經權責單位主管核准後，進行資料銷毀。但若有正當事由並經審核同意後得延長保留期限。
2. 個人資料檔案銷毀時，應依下列方式處理：
   (1)紙本若屬大量銷毀應由專責單位或專業廠商處理，並有相關安全控管措施（如：人員全程陪同或全程錄影監控)。
   (2)紙本若少量則應以碎紙機銷毀。
   (3)電子檔案應即刪除，並清除「資源回收筒」。
   (4)資料庫檔案，權責單位提出單位主管核准文件後，由資料庫管理人員進行刪除，並留下紀錄。
   (5)「限制使用」以上之機密等級的個資檔案，資料銷毀時應有相關人員陪同，並於銷毀後填寫「個資檔案銷毀紀錄表 」。
   (6)磁性媒介須報廢或不堪再使用時，依媒介性質則由個人或資訊單位人員以實體破壞或使用其他應用程式或工具清除資料或銷毀該媒介。

(四)個資利用

1. 應明確界定本校執行相關業務或為行銷研究調查目的之使用的必要範圍，包括業務承辦單位與受委託單位。
2. 對於個人資料的利用應確認利用目的是否與原蒐集的特定目的相符。如逾越原特定目的，則須再取得當事人書面同意方可利用。
3. 利用個人資料對當事人進行第一次行銷或研究時，應提供當事人拒絕行銷或研究的機制，並支付所需費用。當事人拒絕接受行銷時，應即停止利用其個人資料行銷。
4. 個人資訊的公開(布)，應符合學校特定目的，並考量資訊公開的範圍，應進行適當遮罩或僅公告必要的資訊，並經權責單位主管核定後為之。
5. 含有個人資料之報廢紙張不得回收及再利用。

6. 個人資訊如由第三方提供蒐集，應於首次對當事人為利用時一併告知資料來源與其他蒐集時應告知事項。

(五)第三方資料分享

1. 個人資料需在特定目的且必要的情形下，方可進行第三方資料分享，資料的分享需做成文件記錄。
2. 資料分享於第三方前，雙方應有書面合約或協議，載明能被使用的特定目的與對個資之責任，並應提出承諾或證明不牴觸法令的方式處理資訊。
3. 對於資料的傳輸方式應符合「個人資料安全管理作業」程序，以保護傳輸期間的資訊安全。
4. 進行傳輸或移轉個人資料時，亦應特別注意確認收受資料者是否為有權收受之本人或代理人。

(六)國際傳輸

1. 因業務需求需將個人資訊移轉到非本國之處，傳輸雙方的合約或協議中應載明個資保護與符合目的處理與利用的條件，確保個資的處理與利用符合法令規範並受到保護。
2. 在移轉到外國前，應先確認個資將被移轉的單位是否已提出符合該國個資相關法令要求的證明。
3. 確認目的地國家或地區是否已被評估為能夠提供充足的保護。
4. 對於資料的傳輸方式應符合「個人資料安全管理作業」程序，以保護傳輸期間的資訊安全。
5. 建立對該資料傳輸目的地組織進行監督與評估，以確保個資處理及利用的安全。

五、個人資料權利行使作業

(一)本校師生欲行使當事人權利時,可向各業務權責單位提出申請及申訴；校外人士可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。

(二)若單位已有訂定對應之申請流程，可依單位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。

(三)當事人權利行使之流程

當事人填寫本校「個人資料權利行使申請表」，並附上必要之佐證資料，可親送或寄至本校個資保護聯絡窗口。如為代理人申請則須附委託同意書。

(四)個人資料權責單位之處理流程

1.資料查詢或閱覽

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。

2.請求製給複製本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：

(1)親自領取並核對證件如下：

A.本人申請：身分證正本。

B.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。

C.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)。

(2)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。

(3)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。

3.請求補充或更正

(1)應查明其資料是否正確，如為正確資料，應於經業務權責單位主管同意後進行補充或更正作業，並將作業結果通知當事人。

(2)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。

4.請求停止蒐集、處理或利用，應查明是否為依法規或執行職務或

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。

5. 請求刪除，應查明是否為依法規或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。

(五)業務單位駁回之處理方式

1. 所有請求如依據規定或因執行職務或業務所必需，而無法同意其請求，均應以正式書面函覆，並以掛號方式寄出。

2. 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。

(六)當事人申訴抱怨之作業方式

1. 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抱怨；各業務承辦單位若接獲個資相關申訴抱怨後，需記錄相關事件內容及當事人聯絡方式後，將訴怨事件移交個資保護聯絡窗口進行處理。

2. 個資保護聯絡窗口需填寫「個人資料申訴事件紀錄單」記錄申訴抱怨案件。

3. 如投訴抱怨案件如屬本校業務時，應由本校「個人資料保護工作小組」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，由本校個資權責單位向當事人說明回覆。

4. 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。

(七)各項申請之處理原則

1. 查詢或請求閱覽個人資料或製給複製本者，如須繳交費用，則依本校繳費方式繳費。

2. 個人資料權責單位應就當事人之請求，提供查詢、閱覽個人資料或請求製給複本。但若有下列情形之一者，不在此限：

(1)妨害國家安全、外交及軍事機密、整體經濟利益或其他國家重大利益。

(2)妨害公務機關執行法定職務。

(3)妨害該蒐集機關或第三人之重大利益。

3. 當事人就其個人資料提出查詢、提供閱覽或製給複製本之要求，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。

4. 當事人就其個人資料提出請求補充或更正、停止蒐集、處理、利用及刪除之要求，個人資料權責單位應於三十日內，為准駁之決定；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。

5. 個人資料蒐集之特定目的消失或期限屆滿時，應就當事人之請求，刪除、停止處理或利用該個人資料。但因執行職務或業務所必須或經當事人書面同意者，不在此限。

6. 個人資料正確性有爭議時，個人資料權責單位應就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。

7. 當事人的資訊不正確，但應實際需求須保留相關歷史紀錄時，應須能指出該資訊為不正確，並在適當之處提供正確的個人資料。

六、隱私權告知作業

(一)隱私權告知時機與方式

1. 個資蒐集告知聲明書

對於本校之教職員工與學(員)生，基於特定之目的，必須蒐集各項個人資料時，權責單位得提供告知聲明書方式，於蒐集個資前明確對當事人陳述應告知事項。

(1)教職員工應於新進人員報到時告知。

(2)學(員)生應於帳號啟用前告知。

(3)蒐集個人資料超出原特定目的外之新的目的時。

2. 一般網站瀏覽

因網站瀏覽的行為，可能留存相關涉及個人行為紀錄於伺服器，應於網站明顯處提供隱私權聲明，讓當事人了解會如何處理網站服務時蒐集到的個人識別資料。

(1)網站隱私權聲明內容應放置於本校首頁明顯處。

(2)網站隱私權聲明聲適用於本校各網站，各網站亦應加入該隱私權聲明連結。

3. 電子表單個資蒐集

於利用資訊系統線上表單蒐集個人資料時，若所需蒐集個人資料非原「個資蒐集告知聲明書」告知對象或已超出告知的特定目的時，應讓當事人於開始填寫資料前，閱讀應告知事項，同意後繼續填寫。

4. 書面表單個資蒐集

於利用填寫書面表單蒐集個人資料時，若所需蒐集個人資料非原「個資蒐集告知聲明書」告知對象或已超出告知的特定目的時，應於表單適當且明顯地方，列出應告知事項，讓當事者於填寫資料時，便於閱讀該告知事項。

(二)隱私權告知聲明內容修(新)訂

1. 個資蒐集告知聲明書經權責單位修(新)訂後，簽請校長同意後使用。

2. 網站隱私權聲明由網站負責單位修(新)訂後，簽請校長同意後使用。

3. 電子或書面表單個資蒐集告知，由個資蒐集單位擬訂，單位個資保護代表審定內容，經單位個資保護工作負責人同意後使用。

(三)隱私權公告、個資蒐集告知聲明書或表單告知聲明等，應進行版本控制並保留紀錄,紀錄保留時間至少與相關的個人資訊保留時間相同。

七、個人資料安全管理作業

(一)本校同仁於處理個人資料時，均有負責保護個人資料安全之責任，應遵循個資保護相關法規進行個資資料之處理及利用。

(二)個人資料檔案之機密分級及標示：

1. 所有個人資料檔案在其被產生或收受時，即應確認個資檔案中所包含之個資類別，並依「個人資料類別清單」所列之資料分級，評鑑此個資檔案之機密等級。
2. 個人資料檔案機密等級分為：「公開」、「限制使用」與「機密」三級。
3. 個資檔案中若含多種不同機密等級之個人資料時，應以最高之等級為判定個資檔案機密等級之依據。
4. 個人資料分級如下表所示：

普	1. 指個人資料單獨存在，且無法由此資料加以識別個人，例：僅有姓名。 2. 具有個人資料兩項，具去識別性，且不足以直接或間接識別方式識別該個人之資料(例：王Ｏ行，H123456XXX)。 3. 公務使用之電子郵件、電話、職稱及學經歷資料
中	1. 具個人資料三項（含）以上，未經去識別性，足以直接或間接方式識別個人資料。 2. 個人資料內含下列任兩項資料皆屬之： 國民身分證統一編號、護照號碼、特徵、婚姻、家庭、教育、職業等資料。
高	個人資料內含病歷、醫療、基因、性生活、健康檢查、犯罪前科、私人之聯絡方式、財務情況、社會活動等資料皆屬之。

若文件涉及上表「中」級者，則該文件檔案機密等級應設為「限制使用」或「機密」；若涉及「高」級者，則應設為「機密」。

(三)個人資料檔案應於明顯處標示其機密等級，藉以讓保管人及使用者能清楚的知道該如何處理及防護。

1. 書面文件於表頭或封面右上角標示「機密等級：○○○」。

2. 電子檔案於電子頁面右上角或明顯處標示機密等級。

3. 儲存媒體於外殼、外盒或光碟上標示機密等級。

4. 空白表單均視為公開，待填寫資料後機密等級即開始生效。

(四)本校各「限制使用」及「機密」等級之個資檔案，不論其屬書面文件、電子檔案及儲存媒體等型式，於進行儲存、傳送及銷毀時均應依下列規定作業方式進行。

1.「限制使用」及「機密」等級個資檔案之儲存

(1)僅開放給被授權人員存取，不可在公開場合使用。

(2)書面文件及儲存媒體必須存放於可上鎖的抽屜、文件櫃或檔案室，且必須上鎖保護。

(3)電子檔案須加密或以適當的權限管控方式進行保護，避免遭人任意檢視或拿取。

(4)未加密之電子檔案禁止存放於第三方提供之雲端服務（如Google Drive、Microsoft SkyDrive 等）。

(5)使用書面文件及儲存媒體時，於離座或下班時須妥善收藏，不可遺留於桌面。

(6)「限制使用」等級個資檔案除業務單位同仁取用外，非單位同仁取用時須將個資檔案之取用時間及取用人，記錄於機密資料取用紀錄表，或保存電子檔案之存取軌跡記錄。

(7)「機密」等級之個資檔案除業務承辦人取用外，非承辦人取用須將所有個資檔案之取用時間及取用人，記錄於機密資料取用紀錄表，或保存電子檔案之存取軌跡記錄。

2.「限制使用」及「機密」等級個資檔案之傳輸

(1)校園內部人工傳遞時，須親自傳遞，或加貼密件封條，由公務傳送人員遞送。

(2)書面文件及儲存媒體以郵寄方式傳送到校外時，須加貼密件封條且確實密封，並以掛號或其它適當方式寄出。

(3)傳真、掃瞄、列印或影印時，須有人看守，不可任由文件遺留於機器上。

(4)電子檔案透過網路進行線上傳輸（譬如電子郵件、網頁或 FTP 上傳等），須將個資檔案加密後始得傳輸。

(5) 前項之解密密碼，必須與經加密之個資電子檔案分開傳送。

3.「限制使用」及「機密」等級個資檔案之銷毀

(1)書面文件無繼續保管必要時，不可再生利用，應利用碎紙機進行銷毀，使文件無法再復原資訊。

(2)磁帶、錄影帶、錄音帶等以磁帶方式紀錄之裝置，銷毀時須破壞外殼，切割數段後收集成袋集中回收。

(3)硬碟或 USB 儲存媒體若將被汰換且不再被繼續使用，須將內部資料清除及實體破壞，使其無法再利用。

(4)硬碟或 USB 儲存媒體送修、移轉他人或移作其他用途，因“清理資源回收桶”、“磁碟格式化” 或“重新設置分割區”等動作均無法將檔案內容完全銷毀，須先進行磁碟抹除，避免機敏資料被恢復造成資料外洩。

(5)CD、DVD 等碟片類型紀錄產品，銷毀時以尖銳工具切刮碟片兩面，使其無法再讀取資料，並折半集中回收。

(6)銷毀不限於以上之方式，但須確保資料不可被解讀或恢復。

(五)處理個人資料檔案使用之相關資訊系統,其處理作業程序應遵守本校「資訊存取控制程序」(ISO 文件編號:CC-P-704)要求進行之。

八、個人資料事件管理

(一)個資事件類別

個資事件依發生原因分為 3 大類：

1. 系統類

發生在網路環境、主機系統、個人電腦的事件，軟體、硬體與資訊紀錄相關者均屬之。例如系統故障、網路斷線、硬碟損毀、程式錯誤、機密檔案外洩等。

2. 實體環境類

發生於實體環境內之事件，與實體文件及環境相關者均屬之。例

如門禁故障、門窗未關、過載跳電、闖空門、重要紙本資料外流、火災等。

3. 人員類

與人員相關之事件，例如人員作業疏失、意外事故、商業間諜混入偷竊等。

(二)個資事件通報作業說明

1. 由本校個資保護聯絡窗口受理校內自行發現或校外單位告知本校之個人資料事件：

各單位於發現個資事件時，應通知本校個資保護連絡窗口，判斷是否發生個資事故。

2. 個資保護連絡窗口接獲個資事件通報後，須依所通報之內容進行瞭解，判斷是否為個資事故，將結果回覆個資事件通報單位，並填寫本校「個人資料事件處理單」。

(1)若確定為個資事故且涉及資訊安全問題，應即通知相關權責單位進行處理，權責單位處理完成後，須將處理結果回覆個資保護連絡窗口，並由電算中心資安工作小組，於教育機構資安通報平台進行通報。

(2)當發生個資事故違反個資法，導致個人資料被竊取、洩漏、竄改或其它侵害者，應查明後以適當方式通知當事人並留下通報紀錄。此處理之適當方式，依據個資法施行細則第二十二條，以言詞、書面、電話、簡訊、電子郵件、傳真、電子文件或其他足以使當事人知悉或可得知悉之方式為之。但需費過鉅者，得斟酌技術之可行性及當事人隱私之保護，以網際網路、新聞媒體或其他適當公開方式為之。

3. 權責單位視事件種類及嚴重性，須聯絡相關業務負責人及相關系統管理員，並視情況聯絡技術專家協助。

4. 個人資料事件若涉及資訊安全問題，須通知本校電算中心協助處理。

5. 若為校外單位告知本校之事件或屬校外通報事件，應於事件處理

完成後回報進行結案。

(三)個資事件處理作業原則

1.於非工作時間(例假日)發現個資事件,仍應依循程序通報處理。

2.識別事件所影響之資源與系統,供復原作業時參考。

3.處理作業時間應於指定時間內完成,作業內容應記錄於「個人資料事件處理單」,並經由權責人員審視確認。

4.個資事件處理應確實做好證據保存工作。

5.應鑑別個資事件發生根本原因,以利事件處理作業。

6.個資若遭到人為竄改或失竊等涉及民、刑事案件時,應即時通知校安中心協助通報警政或檢調單位請求處理。

7.個資事件若屬系統漏洞、弱點或非法入侵所致,應依本校「資訊安全通報處理程序」(ISO 文件編號:CC-P-705)處理。

9.為防止問題再度發生,個資事件須依「矯正預防作業」進行處理。

九、內部稽核作業

(一)稽核計畫及稽核員

1.定期稽核:本校「個人資料保護工作小組」於每次內稽前,需擬定「年度稽核計畫」,陳校長或管理代表核准;稽核月份依計畫所排訂為主;稽核計畫經校長或管理代表核准後,以公告或 email 通知各單位。

2.不定期稽核:當校長或管理代表臨時決定需執行內部個資稽核時,則由「個人資料保護工作小組」以公告或 email 通知相關被稽核單位及稽核日期。

3.定期稽核之稽核範圍,可視稽核員之人數及人力負荷,分開數次執行部份之稽核;不定期稽核則依校長或管理代表指示範圍或單位執行稽核。

4.合格稽核人員,需同時符合下列條件:

(1)曾受相關訓練 3 小時以上,且有相關訓練紀錄者。

(2)經校長或管理代表核准,並登錄於「內部稽核人員名冊」內。

5. 每次稽核前，由「個人資料保護稽核小組」負責安排內部稽核人員；被稽核單位內，若有合格之稽核員，不得參與對自己負責業務執行內部稽核。

(二)稽核準備

1. 個資內部稽核組長召集相關稽核員，說明本次稽核之目的，並協調分配稽核範圍；稽核對象及範圍分配，可依各單位執行狀況、重要性及以前稽核結果做為參考。
2. 「個人資料保護工作小組」在稽核前以電子郵件通知被稽核單位有關稽核項目及稽核日期等資訊，以便被稽核單位做好相關之準備工作。
3. 通知接受稽核單位之單位個資保護代表，在稽核時間內需親自或指派適當人員陪同稽核。

(三)執行稽核

1. 稽核員應就所分配之稽核範圍，於稽核前充份瞭解各相關程序及辦法，並制作「內部稽核查檢表」；若委由外部合格稽核員執行，則免製作「內部稽核查檢表」，可直接展開稽核作業。
2. 稽核員以「內部稽核查檢表」做為稽核指引，請被稽核單位提供相關文件及表單紀錄做為稽核佐證，例如：作業程序書、相關紀錄文件等進行內部品質稽核作業。
3. 稽核員應秉持公正及客觀的態度，對被稽核單位執行稽核，受稽核單位應全力配合稽核員進行查核。

(四)稽核報告

1. 稽核員應將稽核過程中所發現之缺失，依據事實紀錄於「不符合報告」，並交被稽核單位主管簽認。
2. 被稽核單位依「不符合報告」所列缺失逐項討論，並依規定期限提出改善對策，交給稽核小組進行追蹤和確認。
3. 稽核員依被稽核單位提出之改善對策進行追蹤確認，並將追蹤狀況紀錄於「不符合報告」中。
4. 「個人資料保護稽核小組」應彙整稽核員之「不符合報告」，交由

校長或管理代表審核後，於管理審查會議中提出報告和說明；若「不符合報告」中提及之改善對策，需檢討相關程序並修訂該程序者或必須長時間處理者，另立「矯正與預防處理單」並將該單號做成紀錄以利追蹤。

5. 稽核相關紀錄依規定期限加以保存。

(五)績效衡量

內部稽核所發現之缺失，應於規定期限內確實改善完成，並做到類似缺失之再發防止；若其他單位有類似問題時，應提出預防措施並於「個人資料保護推動委員會」中宣導。

十、矯正預防作業

(一)矯正措施

1. 各相關單位於執行相關業務時，發現呈異常情況時須進行改善，「個人資料保護工作小組」應開立「矯正與預防處理單」並敍明異常情形，送權責處理單位處理。
2. 「矯正與預防處理單」開立後，權責單位應即針對異常狀況會同權責人員進行資料搜集與原因分析，擬定改善對策並確實執行對策。
3. 各權責單位於收到「矯正與預防處理單」後，應於規定期限內擬妥改善對策及完成期限，並徹底執行改善對策；各相關單位亦需協助責任單位擬定改善對策及執行。
4. 由「個人資料保護工作小組」對責任單位所擬定改善對策及完成期限之「矯正與預防處理單」執行狀況進行追蹤，於確認改善對策執行成效無異議後，填寫確認結果，陳校長或管理代表核示是否結案；若改善無效則需重新檢討改善對策並確認有效至結案為止。

(二)預防措施

1. 採取預防措施時，發生單位應蒐集適切的資料來源作為品質改善之依據，如內部稽核、矯正措施、品質記錄、服務作業表報、抱

怨申訴資料…等相關的品質記錄，以做為發掘、分析不合格潛在原因的基礎，同時期能避免相同異常事件的再發生。

2. 依據發掘之潛在問題，填寫「矯正與預防處理單」後，再依(一)2至4之流程執行處理。

3.「個人資料保護工作小組」需將矯正及預防措施之作業狀況，於「個人資料保護推動委員會」會議中提出報告及審查。

(三)標準化

各權責單位針對品質異常狀況提出之矯正及預防有效措施，若有必要修改相關文件予以標準化，則依規定提出文件制訂、修訂、廢止申請，修訂相關文件之作業內容，以符合品質要求。

(四)績效衡量

矯正及預防措施之執行績效，以異常事項於規定期間內處理完畢、並就異常狀況之再發防止為主；若異常狀況經矯正後再次發生，則應由權責單位重新分析原因、擬定對策，並持續追蹤確認其矯正效果。

肆、其他

(一)為落實本校個人資料檔案之安全維護及管理,請本校所屬單位及人員確實依本計畫實施內容辦理。

(二)本計畫未盡事宜，得視需要修正或補充之。

(三)本計畫經個人資料保護推動委員會議通過,陳請校長核定後施行;修正時亦同。