102 年度教育機構 C、D 級學校資安稽核之個人資料保護工作事項

壹、 文件目的：

一、 本指引係依據「個人資料保護法」、「個人資料保護法施行細則」及「教育體系資通安全管理規範」等相關規定為基礎引申訂定之。

二、 除遵循上述法令及規範外，教育機構教、職、員、生、約聘人員及相關委外合作廠商等，應參考本工作事項之管理措施，或配合各校所修改或引用適當之規範，保護機關學校相關程序所產生或經手的各種形式（含書面或電子）之個人資料。

三、 學校機關個人資料的基本應用原則如下：

1. 限制蒐集原則：經當事人同意或於具有其他法律所允許之事由時，以合法、公正手段於適當場所蒐集。

2. 資料內容原則：符合蒐集個人資料特定目的，並確保資料之正確性、完整性和時效性。

3. 目的明確化原則：應於蒐集個人資料之當時即向當事人明確闡述蒐集的目的，或依法令另為告知；爾後亦須於當初蒐集的目的範圍內使用，不得他用。

4. 限制利用原則：若非經資料當事人之書面同意或經法令規定許可，個人資料不得任意揭露、販售或用於蒐集時的特定目的以外之用途。

5. 安全保護原則：資料必須採取合理適當安全保護措施，以免資料遭遺失、盜用、毀損、竄改或揭露的風險。

6. 公開原則：對個人資料之開發、蒐集、利用、以及有關之政策等，應於法律允許之範圍內，採取一般的公開政策。

7. 個人參與原則：

   當事人權益：

   (a) 向資料管理人確認是否保有當事人個人資料及其內容；

   (b) 資料管理人在合理時間內、以合理價格、可接受的態度及可理解的形式，向當事人聯絡溝通協調其資料之保有與使用；

(c)若當事人提出以上(a).(b).兩樣請求被資料管理人拒絕時，應允許當事人有權就此提出質疑，並有權要求資料管理人提出合理解釋；

(d)當事人除有上述(c)權利之外，若質詢不滿意，應有權要求資料之增刪、校正、或修改。

四、 責任義務原則：學校機關以及資料管理者應確保學校政策之落實與執行已遵守上述各項原則。

貳、 本指引用詞定義：

一、 個人資料：指自然人之姓名、出生年月日、國民身分證統一編號、特徵、家庭、教育、職業、病歷、醫療、健康檢查、聯絡方式、財務情況及其他得以直接或間接方式識別該個人之資料。

二、 其餘用詞定義請參見「個人資料保護法」。

參、 個人資料保護安全維護措施建議事項

一、 規劃

1. 配置管理之人員及相當資源

1.1 機關學校應建立個人資料保護管理政策。

1.2 機關學校應成立個人資料保護管理小組，由單位副首長擔任召集人，統籌決策與單位內資訊安全與個人資料業務之資源整合運用。

1.3 機關學校應指定專人依相關法令辦理安全維護及保管事項，作為機關內部之個人資料管理代表。機關組織編制較小者，則統一由該機關「個資保護聯絡窗口」兼辦上述專人業務。

1.4 機關學校應決定並提供有關單位規劃與施行個人資料保護工作所需的資源，包含人力、物資或外部諮詢顧問等。

2. 界定個人資料之範圍

2.1 機關學校應定期執行個人資料檔案鑑別作業，建立與維護個人資料檔案清冊，公務機關並依個資法要求於網站上公開相關資訊。

3. 個人資料保護之風險評估及管理機制。

3.1 機關學校應針對「個人資料檔案清冊」內容，訂定個資衝擊影響程度評估準則，並進行個資資產之衝擊影響程度分析。

3.2 個人資料檔案風險評鑑應定期執行，以瞭解處理各種個人資料的可

能風險，並針對這些風險訂定處理計畫。

4. 事故之預防、通報及應變機制

4.1 學校機關的人員應瞭解個人資料保護法之要求，克盡職責保護及管理相關業務所接觸之個人資料。

4.2 當發生個人資料資訊安全事件時，應通報主管機關；若事件發生導致個人資料被竊取、洩漏、竄改或其他侵害者，應依個資法第 12 條查明後以適當方式通知當事人。

4.3 機關學校應訂定個人資料資訊安全事件處理程序。

4.4 機關學校所設置的「個資保護聯絡窗口」除作為機關學校間個資業務協調聯繫之對口外，也擔任機關學校本身個資安全事件通報之對口，以及重大個資外洩事件之民眾聯繫單一窗口。機關學校應將「個資保護聯絡窗口」之聯繫方式（如：電話、email）置於機關學校網站，以便利民眾提出申訴與救濟。

二、 執行

5. 個人資料蒐集、處理及利用之內部管理程序

5.1 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。

5.2 蒐集個人資料時，應依個人資料保護法第 8 條明確告知當事人相關資訊：

(a) 機關名稱。
(b) 蒐集目的。
(c) 個人資料的類別。
(d) 個人資料利用期間、地區、對象及方式。
(e) 當事人行使之權利事項及方式等。
(f) 當事人不提供個人資料對其權益之影響。

5.3 機關學校應於法律允許之範圍內提供資料當事人下列權利：

(a) 查詢或請求閱覽。
(b) 請求製給複製本。
(c) 請求補充或更正。
(d) 請求停止蒐集、處理或利用。
(e) 請求刪除。

5.4 蒐集非由當事人提供之個人資料時，應於處理或利用前，依個人資料保護法第 9 條，向當事人告知個人資料來源及應告知資訊，如本文件 5.2 所列之 (a) ~ (e) 項目。

5.5 學校機關應維護個人資料的正確性，並主動依當事人的請求更正或補充之。

5.6 當資料利用範圍超出蒐集的特定目的時，應依個人資料保護法第 16 條與第 20 條有關特定目的以外之利用規範。

6. 資料安全管理及人員管理

資料安全管理

6.1 機關學校管理之網站或網頁內容，於確有必要公布個人資料時，需經所屬主管核准，且依相關法律及規範處理，始得公布。

6.2 對於個人資料之調閱宜經申請並核准，並加以記錄其調閱身分及行為。調閱紀錄可視機關實際需求存檔，以利後續人員查詢及追蹤。

6.3 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，應調閱原檔案查核。

6.4 個人資料檔案應定期備份（例如每個月），並防止備份檔案被竊取、竄改、毀損、滅失或洩露。

6.5 個人資料輸入、輸出、存取、更新、更正或註銷等處理行為，宜釐定使用範圍及調閱或存取權限。

6.6 含有個人資料之紙本報表的申請、讀取、列印、使用、存檔、轉交及銷毀等處理及利用行為，宜建立相關之授權、監督及行為記錄機制。

6.7 個人資料檔案之處理行為應設置使用者代碼及通行碼，使用者代碼不得與他人共用且通行碼須定期更新，並視業務及資料重要性，考量其他輔助安全措施。個人資料檔案使用完畢後，應立即退出應用程式。

6.8 學校機關應訂定處理個人資料檔案資訊設備或系統登入通行碼之更換與設定規則，例如通行碼至少每六個月更換一次，通行碼長度應至少 8 碼，且包含文數字等。

6.9 針對個人資料檔案之處理，可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，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，並留存使用者身分、識別帳號與其行為紀錄以供事後稽查。

6.10 個人資料檔案禁止存放於網路芳鄰分享目錄。

6.11 儲存個人資料的資訊設備應使用螢幕保護程式，設定螢幕保護密碼，並將螢幕保護啟動時間設定為 15 分鐘以內。

6.12 儲存個人資料之資訊設備應安裝防毒軟體，除至少每日更新病毒碼外，並應每週執行排程掃描。

6.13 儲存個人資料之資訊設備應定期檢視、更新作業系統、應用程式漏洞（如：Windows 作業系統、Windows Office、Adobe Acrobat 等）。

6.14 內部傳遞或與其他機關交換個人資料時，應選擇可靠且具備保密機制之傳遞方式，如於實體文件封袋加上彌封、或對資料檔案壓縮加密，並對轉交或傳輸行為加以記錄流向備查。

6.15 自行開發或委外處理個人資料檔案之資訊系統，應在系統開發生命週期之初始階段，將個人資料檔案的安全需求納入考量（如：邏輯測試）；系統之維護、更新、上線、及版本異動等作業，應予安全管制，避免危害個人資料安全。

6.16 宜避免允許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；若需使用遠端登入方式進行維護，則應透過加密通道進行（如：HTTPS、SSH 等）。

6.17 自行開發或委外處理個人資料檔案之資訊系統，應將個人資料（包含測試用個人資料）施予妥善之保護與控管。

<u>人員安全管理</u>

6.18 處理個人資料檔案之人員，其職務如有異動，應將所保管之儲存媒體及有關資料列冊移交，接辦人員除應於相關系統重置通行碼外，應視需要更換使用者識別帳號。

6.19 處理個人資料檔案之人員，應簽訂保密切結書，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。

6.20 針對個人資料檔案處理人員訂定電腦使用規範，例如禁止以下操作行為：

(a) 禁止使用即時通訊軟體傳輸個人資料檔案。
(b) 禁止使用外部網頁式電子郵件(Webmail)傳輸個人資料檔案。
(c) 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。
(d) 禁止在社群網站、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。

6.21 個人資料檔案若委外建檔，應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之罰則。

6.22 與委外廠商所簽訂正式書面協議或契約中，應明確陳述契約終止時，相關個人資料的銷毀或交還程序。

7. 認知宣導及教育訓練

7.1 機關學校應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（內、外訓皆可），並定期於單位內宣導個資隱私保護之重要性。

7.2 機關學校全體教職員生及相關經手個人資料之第三人應對以下法令及規範有基礎認知：

(a) 個人資料保護法
(b) 個人資料保護法施行細則
(c) 教育體系資通安全管理規範
(d) 國中、小學資通安全管理系統實施原則

7.3 機關學校辦理個人資料保護認知宣導活動完畢後，應留存相關紀錄備查。

8. 設備安全管理

8.1 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等，並檢視、處理其錯誤或異常事件等訊息。

8.2 儲存個人資料之資訊設備應置放於實體安全區域（如：門禁控管之辦公區域、機房），或與外部網路隔絕（如：防火牆），避免有心人士或非授權人員存取。

8.3 儲存個人資料檔案之磁碟、磁帶，及紙本等相關儲存媒體，應指定專人管理，並置於實體保護之環境（如：上鎖之防潮箱、書櫃），必要時應建立備援機制，以防止資料損壞、遺失或遭竊取。相關儲存媒體非經權責單位同意並留存紀錄，不得任意攜出或拷貝複製。

8.4 外部團體或個人更新或維修電腦設備時，應指派專人在場，確保個人資料之安全及防止個人資料外洩。

8.5 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時，應確實刪除該設備所儲存之個人資料檔案。

三、檢查

9. 資料安全稽核機制

9.1 機關學校應定期執行稽核作業，以確保相關管理措施之有效性。

9.2 機關學校若業務變更，應立即執行稽核作業，以確保作業變更後的風險。

10. 使用紀錄、軌跡資料及證據保存

10.1 機關學校可依實際業務狀況及需求與業務評估，針對以下個人資料處理相關活動，進行紀錄的保存，以為未來舉證等用途。

(a) 因應事故發生所採取行為之紀錄。
(b) 確認受託人執行委託人要求事項之紀錄。
(c) 提供當事人行使權利之紀錄。
(d) 確認資料正確性及更正之紀錄。
(e) 權限新增、變動及刪除之紀錄。
(f) 備份及還原測試之紀錄。
(g) 個人資料交付、傳輸之紀錄。
(h) 個人資料刪除、廢棄之紀錄。
(i) 存取個人資料系統之紀錄。
(j) 定期檢查處理個人資料之資訊系統之紀錄。
(k) 教育訓練之紀錄。
(l) 計畫稽核及改善程序執行之紀錄。

四、改善行動

11. 個人資料安全維護之整體持續改善

11.1 針對資訊安全事件及稽核缺失應訂定改善行動或預防措施，以減低事件再次發生機會。

11.2 稽核發現缺失改善情形、風險評估結果及個人資料資訊安全事件等，必須每年定期呈報個人資料保護管理小組。