教育機構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. 限制使用原則：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。

8. 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以遵守上述各項原則。

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。教育機構中常見之個人資料如教職員人事資料、學生基本資料、家長聯絡方式、家庭狀況、班級成績資料、健康檢查結果、心理輔導檔案等。

二、其餘用詞定義請參見「個人資料保護法」。

參、個人資料保護持續改善管理流程：

一、規劃

1. 機關學校應建立個人資料保護管理政策。
2. 機關學校應建立與維護個人資料檔案清冊並依個資法要求於網站上公布檔案大綱。
3. 個人資料檔案應指定管理者，管理者需評估資料處理流程上的風險，設定資料保護要求。
4. 機關學校應確認個人資料之蒐集與利用符合法令規定。包含：
   (a) 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。

(b) 蒐集個人資料時，應依法令規定告知當事人蒐集資料之目的、利用範圍等資訊。
(c) 除符合法令規定外，有關醫療、基因、性生活、健康檢查及犯罪前科之個人資料，不得蒐集、處理或利用。
(d) 當資料利用範圍超出蒐集的特定目的時，應依個資法規定取得當事人之書面同意。

二、執行

機關學校應依「教育體系資通安全管理規範」或「國中、小學資通安全管理系統實施原則」以及本工作事項之安全原則及參考注意事項實施個人資料相關資訊安全控管措施。

三、檢查

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。

四、改善行動

1. 機關學校應訂定個人資料資訊安全事件處理程序。
2. 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。

肆、個人資料保護及安全原則：

一、機關學校應指定單位副首長為機關召集人，統籌決策與執行單位內資訊安全與個資隱私業務之資源整合運用。

二、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」兼辦專責人員業務。

三、機關學校應設置並指定「個資保護聯絡窗口」，作為機關學校間個資業務協調聯繫之對口、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。另單位應將「個資保護聯絡窗口」之聯繫方式（如：電話、email）置於單位網站，以便利民眾提出申訴與救濟。

四、個人資料檔案應定期備份，並防止個人資料被竊取、竄改、毀損、滅失或洩露。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。個人資料檔案之處理行為應設置使用者代碼及通

行碼，不得與他人共用並定期更新。另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，並留存使用者身分、識別帳號與其行為紀錄以供事後稽查。

五、個人資料檔案儲存於個人電腦者，應於該電腦設置可辨識身份之登入通行碼，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，應即退出應用程式，不得留置於電腦終端機。

六、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。

七、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。

八、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。

九、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，應調閱原檔案查核。

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

十一、　學校應於法律允許之範圍內提供資料當事人下列權利：

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、處理或利用。
5. 請求刪除。

伍、參考注意事項：

一、處理個資之資訊設備使用參考注意事項：

1. 處理個人資料檔案之資訊設備，需設置使用者代碼及通行碼。
2. 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。

3. 禁止與他人共用電腦系統帳號。
4. 採取權限區隔，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。
5. 個人資料檔案應以安全的方式保護，例如：加密。
6. 至少每月備份資訊設備內個人資料檔案一次。
7. 個人資料檔案使用完畢後，應立即退出應用程式。
8. 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。
9. 交換個人資料檔案時，應對資料檔案加密，亦或是透過加密通道傳送。
10. 個人資料禁止存放於網路芳鄰分享目錄，並停用 Guest 帳號。
11. 存放個人資料之資訊設備應與外部網路隔絕（如：防火牆）。
12. 存放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瞄。
13. 存放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）。

二、設備管理參考注意事項：

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。
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），避免有心人士或非授權人員存取。
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。
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。
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、人員管理參考注意事項：

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。

2. 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。
3. 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。
4. 禁止人員使用 MSN 或其他即時通訊軟體傳輸個人資料檔案。
5. 禁止人員使用外部網頁式電子郵件(Webmail)傳輸個人資料檔案。
6. 禁止人員使用點對點(P2P)軟體及 Tunnel 相關工具下載或提供分享檔案。
7. 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。

四、系統開發及委外管理參考注意事項：

1. 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。
2. 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）。
3. 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。
4. 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。

五、法規參考：

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：

個人資料保護法
http://law.moj.gov.tw/LawClass/LawContent.aspx?PCODE=I0050021

個人資料保護法施行細則
http://law.moj.gov.tw/LawClass/LawContent.aspx?PCODE=I0050022

私立學校及學術研究機構電腦處理個人資料管理辦法

http://law.moj.gov.tw/LawClass/LawAll.aspx?PCode=I0050024

教育體系資通安全管理規範
http://cissnet.edu.tw/rule_edu.aspx

國中、小學資通安全管理系統實施原則
http://cissnet.edu.tw/rule_network.aspx

教育機構個人資料保護檢核表

查檢單位：_____ 填表日期：___年___月___日

查核項目 (紅色為進階選項)	自我評審			稽核評量結果			
				完整性			
	是	否	不適用	非常	尚屬	不盡	不適用
1 個人資料保護持續改善管理流程							
1.1 是否建立個人資料保護管理政策？	☐	☐	☐	☐	☐	☐	☐
1.2 是否建立「個人資料檔案清冊」，並依個資法要求於網站公布個人資料檔案大綱？	☐	☐	☐	☐	☐	☐	☐
1.3 個人資料檔案是否指定管理者？	☐	☐	☐	☐	☐	☐	☐
1.4 管理者是否評估資料處理流程上的風險，設定資料保護要求？	☐	☐	☐	☐	☐	☐	☐
1.5 是否確認個人資料之蒐集與利用符合法令規定？包含： ● 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。 ● 蒐集個人資料時，應依法令規定告知當事人蒐集資料之目的、利用範圍等資訊。 ● 除符合法令規定外，有關醫療、基因、性生活、健康檢查及犯罪前科之個人資料，不得蒐集、處理或利用。 ● 當資料利用範圍超出蒐集的特定目的時，應依個資法規定取得當事人之書面同意。	☐	☐	☐	☐	☐	☐	☐
1.6 是否依下列相關規定執行個人資料保護作業 ● 教育體系資通安全管理規範 ● 國中、小學資通安全管理系統實施原則	☐	☐	☐	☐	☐	☐	☐
1.7 是否定期執行稽核作業，以確保相關個人資料保護管理措施之有效性？	☐	☐	☐	☐	☐	☐	☐
1.8 是否訂定個人資料資訊安全事件處理程序？	☐	☐	☐	☐	☐	☐	☐
1.9 針對資訊安全事件及稽核缺失是否訂定改善行動或預防措施，以減低事件再次發生機會？	☐	☐	☐	☐	☐	☐	☐

註：藍色與紅色字體為100年新增或調整項目。

查核項目	自我評審			稽核評量結果			
				完整性			
	是	否	不適用	非常	尚屬	不盡	不適用
2 個人資料保護與安全							
2.1 是否指定機關副首長為個資隱私業務之機關召集人？	☐	☐	☐	☐	☐	☐	☐
2.2 是否指定專人依法令規定辦理安全維護及保管事項？	☐	☐	☐	☐	☐	☐	☐
2.3 是否設置「個資保護聯絡窗口」，協調聯繫個資事宜，並將聯繫方式（如：電話、email）置於單位網站，以便利民眾提出申訴與救濟？	☐	☐	☐	☐	☐	☐	☐
2.4 個人資料之處理行為是否經權責單位核准，釐定使用範圍及調閱、存取權限？	☐	☐	☐	☐	☐	☐	☐
2.5 個人資料之處理行為是否留存使用者身分與其行為紀錄以供事後稽查？	☐	☐	☐	☐	☐	☐	☐
2.6 含有個人資料之紙本報表，其處理及利用行為是否有適當之授權、監督，及記錄列印、轉交等行為？	☐	☐	☐	☐	☐	☐	☐
2.7 交換紙本個人資料時，是否採取彌封或其他具備保密機制之傳遞方式？	☐	☐	☐	☐	☐	☐	☐
2.8 交換個人資料時，是否記錄轉交或傳輸行為之流向？	☐	☐	☐	☐	☐	☐	☐
2.9 對於個人資料之調閱，是否有申請及核准程序？	☐	☐	☐	☐	☐	☐	☐
2.10 對於個人資料之調閱，是否記錄並保存調閱者身分及行為？	☐	☐	☐	☐	☐	☐	☐
2.11 若需於單位管理之網站或網頁公布個人資料時，是否經所屬單位主管核准，並依相關法律及規範處理？	☐	☐	☐	☐	☐	☐	☐
2.12 是否於法律允許之範圍內提供資料當事人下列權益： ● 查詢或請求閱覽 ● 請求製給複製本 ● 請求補充或更正 ● 請求停止蒐集、處理或利用 ● 請求刪除	☐	☐	☐	☐	☐	☐	☐
2.13 處理個人資料檔案之個人電腦，是否設置使用者代碼及通行碼？	☐	☐	☐	☐	☐	☐	☐
2.14 通行碼是否至少每六個月更換一次，長度應至少8碼，且包含文數字？	☐	☐	☐	☐	☐	☐	☐
2.15 是否未與他人共用電腦系統帳號？	☐	☐	☐	☐	☐	☐	☐
2.16 處理個人資料是否採取權限區隔，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？	☐	☐	☐	☐	☐	☐	☐
2.17 個人資料檔案是否以安全的方式保護，例如：加密？	☐	☐	☐	☐	☐	☐	☐
2.18 是否至少每月備份電腦內個人資料檔案？	☐	☐	☐	☐	☐	☐	☐
2.19 個人資料檔案使用完畢後，是否立即退出應用程式？	☐	☐	☐	☐	☐	☐	☐
2.20 電腦是否使用螢幕保護程式並設定密碼，並將螢幕保護啟動時間設定為15分鐘以內？	☐	☐	☐	☐	☐	☐	☐
2.21 交換個人資料檔案時，是否對資料檔案加密，或是透過加密通道傳送？	☐	☐	☐	☐	☐	☐	☐
2.22 是否禁止開啟網路芳鄰分享目錄與檔案？	☐	☐	☐	☐	☐	☐	☐
2.23 是否停用作業系統Guest帳號？	☐	☐	☐	☐	☐	☐	☐
2.24 是否將存放敏感性個人檔案資料的電腦與外部網路隔絕（如：防火牆）？	☐	☐	☐	☐	☐	☐	☐
2.25 存放個人資料之資訊設備是否安裝防毒軟體，並至少每日更新病毒碼，且每週執行排程掃瞄？	☐	☐	☐	☐	☐	☐	☐
2.26 存放個人資料之資訊設備是否定期檢視、更新作業系統及應用程式漏洞？	☐	☐	☐	☐	☐	☐	☐

查　　核　　項　　目	自我評審			稽核評量結果			
				完整性			
	是	否	不適用	非常	尚屬	不盡	不適用
3 設備管理							
3.1 是否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，並檢視、處理其錯誤或異常事件等訊息？	☐	☐	☐	☐	☐	☐	☐
3.2 儲存個人資料之資訊設備是否置放於實體安全區域（如：門禁控管之辦公區域、機房）？	☐	☐	☐	☐	☐	☐	☐
3.3 儲存個人資料檔案之磁碟、磁帶，及紙本等相關儲存媒體，是否指定專人管理，並置於實體保護之環境？	☐	☐	☐	☐	☐	☐	☐
3.4 儲存個人資料檔案之儲存媒體，是否建立備援機制？	☐	☐	☐	☐	☐	☐	☐
3.5 儲存個人資料檔案之媒體是否有攜出、拷貝或複製的管控機制，並留存紀錄？	☐	☐	☐	☐	☐	☐	☐
3.6 外部團體或個人更新或維修儲存個人資料檔案之電腦設備時，是否指派專人在場確保資料安全？	☐	☐	☐	☐	☐	☐	☐
3.7 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，是否刪除其所儲存之個人資料檔案？	☐	☐	☐	☐	☐	☐	☐
4 人員管理							
4.1 機關學校是否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，並定期於單位內宣導個資隱私保護之重要性？	☐	☐	☐	☐	☐	☐	☐
4.2 處理個人資料檔案之人員職務異動時，是否依規定列冊移交相關儲存媒體及資料？	☐	☐	☐	☐	☐	☐	☐
4.3 處理個人資料檔案之人員職務異動時，接替人員是否於相關系統重置通行碼，並視需要更換使用者識別帳號？	☐	☐	☐	☐	☐	☐	☐
4.4 處理個人資料檔案之人員，是否簽訂保密切結書？	☐	☐	☐	☐	☐	☐	☐
4.5 處理個人資料檔案之人員離職或合約終止時，是否依規定取消或停用其使用者識別帳號並收繳通行證件？	☐	☐	☐	☐	☐	☐	☐
4.6 是否禁止使用MSN或其他即時通訊軟體傳輸個人資料檔案？	☐	☐	☐	☐	☐	☐	☐
4.7 是否禁止使用外部網頁式電子郵件(Webmail)傳輸個人資料檔案？	☐	☐	☐	☐	☐	☐	☐
4.8 是否禁止使用點對點(P2P)軟體及Tunnel相關工具下載或提供分享檔案？	☐	☐	☐	☐	☐	☐	☐
4.9 是否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 系統開發及委外管理							
5.1 處理個人資料檔案之資訊系統，是否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系統開發考量（如：邏輯測試）？	☐	☐	☐	☐	☐	☐	☐
5.2 處理個人資料檔案的資訊系統之維護、更新、上線、及版本異動等作業，是否有安全管控措施？	☐	☐	☐	☐	☐	☐	☐
5.3 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時，是否透過加密通道進行（如：HTTPS、SSH等）？	☐	☐	☐	☐	☐	☐	☐
5.4 自行開發或委外處理個人資料檔案之資訊系統，是否將個人資料(包含測試用個人資料)施予妥善之保護與控管？	☐	☐	☐	☐	☐	☐	☐
5.5 委外建檔的個人資料檔案，是否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？	☐	☐	☐	☐	☐	☐	☐