教育部公告

中華民國 102 年 11 月 27 日
臺教高（一）字第 1020172751A 號

主　　旨：預告訂定「私立專科以上學校及學術研究機構個人資料安全維護實施辦法」草案。
依　　據：行政程序法第一百五十四條第一項。
公告事項：

一、訂定機關：教育部。
二、訂定依據：個人資料保護法第二十七條第三項規定。
三、「私立專科以上學校及學術研究機構個人資料安全維護實施辦法」草案如附件。本案另載於本部主管法規查詢系統網站（網址：http://edu.law.moe.gov.tw），「草案預告論壇」選項下。
四、對於本公告內容有任何意見或修正建議者，請於本公告刊登公報隔日起 7 日內陳述意見或洽詢：
(一) 承辦單位：教育部高等教育司。
(二) 地址：臺北市中山南路 5 號。
(三) 電話：(02)77365889。
(四) 傳真：(02)23976943。
(五) 電子信箱：yalan@mail.moe.gov.tw。

部　　長　蔣偉寧

私立專科以上學校及學術研究機構個人資料安全維護實施辦法草案總說明

個人資料保護法第二十七條第二項、第三項規定，中央目的事業主管機關得指定非公務機關訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法；其相關事項之辦法，亦由中央目的事業主管機關定之。

依據「個人資料保護法非公務機關之中央目的事業主管機關」列表，教育部爲大專院校及學術研究機構（以下簡稱學校及機構）之中央目的事業主管機關。考量學校及機構保有大量且重要之個人資料檔案，爰依上開規定之授權，擬具本辦法草案，以加強管理、確保個人資料之安全維護。

本辦法草案共分九章，計十九條，其訂定要點如下：

一、明定本辦法適用對象及用詞定義。（草案第二條）
二、學校及機構應訂定相關安全維護計畫。（草案第三條）
三、管理單位或人員之任務。（草案第四條）
四、明定學校及機構應訂定個人資料保護管理政策並說明政策重點事項應包含之內容。（草案第五條）
五、學校及機構應盤點個人資料並建立清冊。（草案第六條）

六、學校及機構應分析處理個人資料業務流程可能產生之風險，並訂定適當管控措施。（草案第七條）

七、學校及機構應建立預防、通報及應變機制。（草案第八條）

八、學校及機構委託他人蒐集、處理或利用個人資料時，應爲適當之監督。（草案第九條）

九、學校及機構利用個人資料爲宣傳、推廣或行銷時，應檢視事項。（草案第十條）

十、明定學校及機構對於當事人行使本法第三條規定之權利，應遵守事項。（草案第十一條）

十一、學校及機構應採取之資料安全管理措施。（草案第十二條）

十二、學校及機構應採取之人員管理措施。（草案第十三條）

十三、學校及機構宜採取之設備安全管理措施。（草案第十四條）

十四、明定學校及機構於業務終止後，其陳報個人資料處理方法之應記載事項。（草案第十五條）

十五、學校及機構應定期對所屬人員施以認知宣導及教育訓練。（草案第十六條）

十六、學校及機構應建立或採取個人資料安全稽核機制。（草案第十七條）

十七、學校及機構應保存個人資料於蒐集、處理及利用過程之相關紀錄以供查驗。（草案第十八條）

私立專科以上學校及學術研究機構個人資料安全維護實施辦法草案

條　　文	說　　明
第一章　總則	第一章章名
第一條　本辦法依個人資料保護法（以下簡稱本法）第二十七條第三項規定訂定之。	依個人資料保護法第二十七條第二項及第三項規定明定本辦法之法源依據。
第二條　本辦法用詞定義如下： 一、私立專科以上學校：指依私立學校法核准設立之私立專科以上學校（以下簡稱學校）。 二、學術研究機構：指依學術研究機構設立辦法核准設立之私立學術研究機構（以下簡稱機構）。 三、個人資料管理人（以下簡稱管理人）：由校長、機構負責人擔任或指定，負責督導個人資料檔案安全維護計畫（以下簡稱本計畫）規劃、訂定、執行、修訂及相關決策之人員。 四、個人資料稽核人員（以下簡稱稽核人	一、明定本辦法所稱專科以上私立學校，係指依私立學校法核准設立之專科以上私立學校。 二、明定本辦法所稱學術研究機構，係指依學術研究機構設立辦法核准設立之私立學術研究機構。 三、爲使個人資料檔案安全維護管理有效運作，爰明定由學校校長、機構負責人擔任或指定個人資料管理代表，以資明確。 四、學校、機構爲確保個人資料檔案安全維護管理，應指定稽核人員負責評核計畫執行情形及成效。 五、爲確保個人資料檔案之安全維護，凡執行

員）：由校長、機構負責人指定，負責評核本計畫執行情形及成效之人員。 五、所屬人員：執行業務之過程必須接觸個人資料之人員，包括學校、機構之定期或不定期契約人員及派遣員工。 前項第三款管理人與第四款稽核人員不得爲同一人。	業務之過程必須接觸個人資料之人員，包括學校、機構之定期或不定期契約人員及派遣員工，均應依本計畫之相關程序，執行本計畫。
第三條　學校、機構應訂定本計畫，以落實個人資料檔案之安全維護與管理，防止個人資料被竊取、竄改、毀損、滅失或洩漏。 前項計畫應包括業務終止後個人資料處理方法等相關個人資料管理事項。	一、本辦法適用對象爲專科以上私立學校、學術研究機構，並明定其應訂定相關安全維護計畫，以建立並執行相關管理程序或機制。 二、爲加強業務終止後之資料管理，業務終止後個人資料處理方法等相關個人資料管理事項應納入計畫。
第四條　學校、機構得設置或指定管理單位或指定專人，並配置相當資源，負責個人資料檔案安全維護。其任務如下： 一、規劃、訂定、執行與修訂安全維護計畫，包括業務終止後個人資料處理方法。 二、定期就個人資料檔案安全維護管理情形向管理人提出書面報告。 三、依據稽核人員就計畫執行之評核，於進行檢討改進後，向管理人及稽核人員提出書面報告。	依本法施行細則第十二條規定學校、機構得設置管理單位或指定專責人員，並配置相當資源，負責個人資料檔案安全維護，爰明定管理單位（人員）之任務。
第二章　個人資料保護規劃	第二章章名
第五條　學校、機構應訂定個人資料保護管理政策，公告周知，使所屬人員均明確瞭解及遵循。 前項管理政策至少應包括下列事項之說明： 一、遵守我國個人資料保護相關法令規定。 二、其所蒐集、處理及利用個人資料之依據、特定目的及其他相關保護事項。 三、以合理安全之方式，於特定目的範圍	一、爲使學校、機構所屬人員對於個人資料之保護能有所體認，進而能落實本計畫，故學校、機構應訂定個人資料保護管理政策，將本計畫相關重點事項於政策內闡明。爲達上述目的，該等政策應加以公開周知，以明示保護個人資料之旨。 二、政策相關重點事項包括：遵守我國個人資料保護相關法令規定、合法正當蒐集、處理及利用個人資料；應以適當之技術保護

內，蒐集、處理及利用個人資料。 四、採用安全技術保護其所蒐集、處理、利用之個人資料檔案。 五、設置聯絡窗口，供個人資料當事人行使其個人資料相關權利或提出相關申訴與諮詢。 六、規劃緊急應變程序，以處理個人資料被竊取、竄改、毀損、滅失或洩漏等事故。 七、委託蒐集、處理及利用個人資料者，應妥善監督受託機關。 八、持續維運本計畫之義務，以確保個人資料檔案之安全。	個人資料；應提供當事人行使權利之方式；規劃緊急應變程序以處理事故；監督受託機關之責任；持續維運本計畫之義務。
第六條　學校、機構應依個人資料保護法令，盤點所保有之個人資料檔案，界定其範圍，納入本計畫並建立清冊，並定期確認其變動情形。	依本法施行細則第十二條第二項第二款之規定，安全維護計畫中得就界定個人資料範圍相關事項加以規定，爰明定學校、機構應盤點個人資料並建立清冊，方能有效對其所保有之個人資料加以保護。
第七條　學校、機構應依前條界定之個人資料範圍與個人資料蒐集、處理、利用及其相關業務流程，分析可能產生之風險，並依據風險分析結果，訂定適當管控措施。	依本法施行細則第十二條第二項第三款之規定，安全維護計畫得就個人資料之風險評估及風險管理加以規定，爰明定學校、機構應依據其相關業務流程，判斷於蒐集、處理及利用之過程中，個人資料安全可能發生之風險，以及其風險性之高低，方能進一步以適當之方式保護個人資料並降低其風險。
第八條　學校、機構為因應所保有之個人資料被竊取、竄改、毀損、滅失或洩漏等事故，應建立預防、通報及應變機制，並就下列事項建立相關程序： 一、採取適當之應變措施，以降低或控制事故對當事人之損害。 二、查明事故之狀況並適時通知當事人。 三、研議預防機制，避免類似事故再次發生。	一、發生個人資料被竊取、竄改、毀損、滅失或洩漏等事故時，常造成資料當事人財產及非財產上之損害，學校、機構應訂定相關之因應機制，以降低或控制損害。 二、事故應變之首要目標即根據事故之類型，採取應變措施以降低或控制損害。其次，應讓當事人瞭解相關狀況，使當事人亦能採取相關措施防止損害發生或擴大。最後，避免類似事故再次發生亦為應變措施之重點。

第三章　個人資料之管理程序	第三章章名
第九條　學校、機構委託他人蒐集、處理或利用個人資料之全部或一部時，應對受託人依本法施行細則第八條規定爲適當之監督，並明確約定相關監督事項與方式。	學校、機構如將個人資料之蒐集、處理或利用委託他人爲之，應對受託人爲適當之監督，以使資料之蒐集、處理或利用仍符合法令之要求，爰爲本規定。
第十條　學校、機構利用個人資料爲宣傳、推廣或行銷時，應檢視下列事項： 一、當事人表示拒絕宣傳、推廣或行銷後，應立即停止利用其個人資料宣傳、推廣或行銷，並周知所屬人員。 二、至少於首次宣傳、推廣或行銷時，提供當事人免費表示拒絕接受宣傳、推廣或行銷之方式。	爲查知利用個人資料行銷行爲，有無符合本法第二十條第二項及第三項規定，爰爲本規定。
第十一條　當事人行使本法第三條所規定之權利時，學校、機構應依下列規定辦理： 一、確認是否爲個人資料之本人。 二、提供當事人行使權利之方式，並遵守本法第十三條有關處理期限之規定。 三、如認有本法第十條及第十一條得拒絕當事人行使權利之事由，一併附理由通知當事人。 四、告知所酌收必要成本費用之基準。	明定學校、機構對於當事人行使本法第三條規定之權利，應遵守本法第三條、第十條及第十一條規定，以保障其權利。
第四章　個人資料安全管理措施	第四章章名
第十二條　學校、機構應採取下列資料安全管理措施： 一、運用電腦或自動化機器相關設備蒐集、處理或利用個人資料時，宜訂定使用可攜式設備或儲存媒體之規範。 二、針對所保有之個人資料內容，如有加密之需要，於蒐集、處理或利用時，宜採取適當之加密機制。 三、作業過程有備份個人資料之需要時，應比照原件，依本法規定予以保護之。 四、個人資料存在於紙本、磁碟、磁帶、光碟片、微縮片、積體電路晶片等媒介	一、使用可攜式儲存媒體，可能提高處理個人資料之電腦及相關設備遭受惡意程式攻擊及個人資料外洩之風險，因此若有使用可攜式儲存媒體之情況，應訂定相關使用規範。 二、針對個人資料處理之不同態樣，包括儲存、傳輸及備份之狀況，如資料有加密之必要，即應採取適當之加密機制。 三、針對有備份必要之個人資料，除有必要時採取加密機制，儲存備份資料之媒體亦應以適當方式保管，且定期進行備份資料之還原測試，以確保備份之有效性。

物，嗣該媒介物於報廢或轉作其他用途時，宜採適當防範措施，以免由該媒介物洩漏個人資料。 五、委託他人執行前款行爲時，對受託人依本法施行細則第八條規定爲適當之監督，並明確約定相關監督事項、方式、義務及責任。	四、儲存個人資料之媒體於廢棄或移轉與他人前，應確實刪除媒體中所儲存之資料，或以物理方式破壞之，以避免資料不當外洩。 五、說明委託他人執行前款行爲時，對受託人依本法施行細則第八條規定爲適當之監督，並明確約定相關監督事項、方式、義務及責任。
第十三條　學校、機構應採取下列人員管理措施： 一、依據作業之需要，適度設定所屬人員不同之權限並控管其接觸個人資料之情形。 二、檢視各相關業務流程涉及蒐集、處理及利用個人資料之負責人員。 三、與所屬人員約定保密義務。	針對個人資料蒐集、處理及利用之不同態樣，如個人資料內容有加密之需要，即應採取適當之加密機制，爰爲本規定。
第十四條　學校、機構就個人資料存在於紙本、磁碟、磁帶、光碟片、微縮片、積體電路晶片、電腦或自動化機器設備等媒介物之環境，宜採取下列設備安全管理措施： 一、依據作業內容之不同，實施適宜之進出管制方式。 二、所屬人員妥善保管個人資料之儲存媒介物。 三、針對不同媒介物存在之環境，審酌建置適度之保護設備或技術。	在實體環境管理方面，學校、機構亦應針對不同之作業內容、作業環境及個人資料之種類與數量，實施必要之門禁管理，以適當方式或場所保管個人資料之儲存媒體，並建置必要之防災設備。
第五章　業務終止後個人資料處理方法	第五章章名
第十五條　學校、機構業務終止後個人資料處理方法得參酌下列方式爲之，並留存下列紀錄： 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。	明定學校、機構於業務終止後，其陳報個人資料處理方法之應記載事項。

三、其他刪除、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。	
第六章　認知宣導及教育訓練	第六章章名
第十六條　學校、機構應定期對所屬人員施以認知宣導及教育訓練，使其明瞭個人資料保護相關法令之要求、所屬人員之責任範圍及各種個人資料保護事項之作業程序、方法或管理措施。	爲落實執行本計畫相關管理程序，學校、機構應透過認知宣導及教育訓練使所屬人員均能明瞭個人資料保護相關法令之要求、所屬人員之責任範圍及各種作業程序。
第七章　計畫稽核及改善程序	第七章章名
第十七條　學校、機構應建立（採取）個人資料安全稽核機制，定期檢查本計畫所定相關事項是否落實執行。 學校、機構就個人資料安全稽核結果有不符合法令之虞者，應規劃、執行改善及預防措施及程序。	本計畫及依據本計畫所訂定之相關程序，學校、機構所屬人員是否皆已落實執行，必須通過一定之檢查機制方能確定。
第八章　紀錄機制	第八章章名
第十八條　學校、機構就本計畫各項程序之執行，至少應保存下列紀錄： 一、個人資料交付、傳輸之紀錄。 二、確認個人資料正確性及更正之紀錄。 三、提供當事人行使權利之紀錄。 四、個人資料刪除、廢棄之紀錄。 五、存取個人資料系統之紀錄。 六、備份及還原測試之紀錄。 七、所屬人員權限新增、變動及刪除之紀錄。 八、所屬人員違反權限行爲之紀錄。 九、因應事故發生所採取行爲之紀錄。 十、定期檢查處理個人資料之資訊系統之紀錄。 十一、教育訓練之紀錄。 十二、本計畫稽核及改善程序執行之紀錄。 前項紀錄得以採取個人資料使用紀錄、留存自動化機器設備之軌跡資料或其他相關	爲確認本計畫及依據本計畫所訂定之相關程序是否落實執行，以及釐清個人資料於蒐集、處理及利用過程之相關權責，學校、機構應保存相關紀錄以供查驗。

證據保存機制爲之。	
第九章　施行日期	第九章章名
第十九條　本辦法自發布日施行。	本辦法施行日期。