

教育部公告

中華民國 105 年 5 月 13 日

臺教授國部字第 1050042515A 號

主 旨：預告訂定「私立高級中等以下學校及幼兒園個人資料檔案安全維護實施辦法」。

依 據：行政程序法第 154 條第 1 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 27 條第 3 項。

三、「私立高級中等以下學校及幼兒園個人資料檔案安全維護實施辦法」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 14 日內陳述意見或洽詢：

(一) 承辦單位：教育部國民及學前教育署高中及高職教育組。

(二) 地址：臺中市霧峰區中正路 738 之 4 號。

(三) 電話：04-37061800。

(四) 傳真：04-23393247。

(五) 電子郵件：e-g210@mail.k12ea.gov。

部 長 吳思華

私立高級中等以下學校及幼兒園個人資料檔案安全維護實施辦法草案總說明

依個人資料保護法（以下簡稱本法）第二十七條規定：「（第一項）非公務機關保有個人資料檔案者，應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏。（第二項）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。（第三項）前項計畫及處理方法之標準等相關事項之辦法，由中央目的事業主管機關定之。」另依「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，教育部為私立高級中等以下學校及幼兒園（以下簡稱學校、幼兒園）之中央目的事業主管機關。考量學校、幼兒園就所保有個人資料檔案，有加強管理並確保個人資料檔案安全維護之必要，爰訂定私立高級中等以下學校及幼兒園個人資料檔案安全維護實施辦法（以下簡稱本辦法），共計十八條，其要點如下：

- 一、 本辦法之法源依據。（草案第一條）
- 二、 本辦法之主管機關。（草案第二條）
- 三、 本辦法用詞之定義。（草案第三條）
- 四、 明定本辦法之適用對象為學校、幼兒園，並規定其應訂定相關安全維護計畫。（草案第四條）
- 五、 明定學校、幼兒園指定之管理單位或人員之任務。（草案第五條）
- 六、 學校、幼兒園應界定所保有個人資料之類別及範圍，定期清查資料現況，並就非屬特定目的必要範圍或無保存必要之資料為適當之處置。（草案第六條）
- 七、 學校、幼兒園應分析評估可能產生之風險，訂定適當管控措施。（草案第七條）
- 八、 學校、幼兒園應建立個人資料侵害事故發生之應變機制。（草案第八條）
- 九、 學校、幼兒園委託他人蒐集、處理或利用個人資料時，應對受託者為適當之監督。（草案第九條）
- 十、 學校、幼兒園利用個人資料為宣傳、推廣或行銷時，應明確告

知當事人之事項；於首次利用個人資料時，應提供當事人表示拒絕之權利。(草案第十條)

十一、明定學校、幼兒園於當事人行使本法第三條規定之權利時，得採行辦理之方式。(草案第十一條)

十二、學校、幼兒園對所保有個人資料檔案應有之必要安全設備及防護措施。(草案第十二條)

十三、學校、幼兒園為確保個人資料安全，對其所屬人員應採取之人員管理措施。(草案第十三條)

十四、學校、幼兒園於業務終止後，對所保有個人資料之處理方式及留有紀錄。(草案第十四條)

十五、學校、幼兒園應對所屬人員施以教育訓練或認知宣導。(草案第十五條)

十六、學校、幼兒園應訂定個人資料檔案安全稽核機制及檢查安全維護計畫執行情形。(草案第十六條)

十七、學校、幼兒園應保存個人資料於蒐集、處理及利用過程之相關紀錄，及所需保存紀錄之類別。(草案第十七條)

十八、社區互助教保服務中心及部落互助教保服務中心，其個人資料檔案之安全維護準用本辦法之規定。(草案第十八條)

十九、本辦法之施行日期。(草案第十九條)

私立高級中等以下學校及幼兒園個人資料檔案安全維護實施辦法草案

條 文	說 明
第一條 本辦法依個人資料保護(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規定：「(第一項)非公務機關保有個人資料檔案者，應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏。(第二項)中央目的事業主管機關得指令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。(第三項)前項計畫及處理方法之標準等相關事項之辦法，由中央目的事業主管機關定之。」爰明定本辦法之法源依據。
第二條 本辦法所稱主管機關：在中央為教育部；在直轄市為直轄市政府；在縣(市)為縣(市)政府。	明定本辦法之主管機關。
第三條 本辦法用詞，定義如下： 一、個人資料管理人(以下簡稱管理人)：指由校長、園長擔任或指定，負責督導安全維護計畫訂定及執行之人員。 二、個人資料稽核人員(以下簡稱稽核人員)：指由校長、園長指定，負責評核安全維護計畫執行情形及成效之人員。 三、所屬人員：指學校、幼兒園執行業務之過程，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員工。 前項第一款管理人與第二款稽核人員不得為同一人。	一、第一項明定個人資料安全維護相關人員，包括個人資料管理人、個人資料稽核人員及所屬人員，並規定所屬人員之定義。 二、第二項明定個人資料管理人與個人資料稽核人員不得為同一人，以區別上開人員之權責。
第四條 私立高級中等以下學校(以下簡稱學校)及幼兒園應訂定個人資料檔案安全維護計畫(以下簡稱安全維護計畫)，落實個人資料檔案之	一、第一項明定本辦法適用對象為依私立學校法核准設立之私立高級中等以下學校及幼兒園；又為落實個人資料檔案之安全維護與管理，學

<p>安全維護及管理，防止個人資料被竊取、竄改、毀損、滅失或洩漏。</p> <p>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。</p>	<p>校、幼兒園應訂定相關安全維護計畫。</p> <p>二、第二項明定安全維護計畫，應包括業務終止後之資料管理事項。</p>
<p>第五條 學校、幼兒園得指定或設管理單位，或指定專人，負責個人資料檔案安全維護；其任務如下：</p> <p>一、訂定及執行安全維護計畫，包括業務終止後個人資料處理方法。</p> <p>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。</p> <p>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。</p>	<p>依本法施行細則第十二條第二項第一款規定，學校、幼兒園得配置管理之人員及相當資源，以負責個人資料檔案安全維護，爰明定管理單位或人員之任務。</p>
<p>第六條 學校、幼兒園應確認蒐集個人資料之特定目的，依特定目的之必要性，界定所蒐集、處理及利用個人資料之類別或範圍，並定期清查所保有之個人資料現況。</p> <p>學校、幼兒園經定期檢視，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。</p>	<p>一、依本法施行細則第十二條第二項第二款規定，個人資料安全維護措施中包括界定個人資料範圍，爰第一項明定學校、幼兒園應界定所保有個人資料之類別或範圍，並定期清查其現況。</p> <p>二、第二項明定學校、幼兒園就非屬特定目的必要範圍或無保有必要個人資料之處置方式。</p>
<p>第七條 學校、幼兒園應已界定個人資料之範圍與蒐集、處理及利用流程，分析評估可能產生之風險，訂定適當之管控措施。</p>	<p>依本法施行細則第十二條第二項第三款規定，個人資料安全維護措施中包含個人資料之風險評估及風險管理機制，爰明定學校、幼兒園應依其業務流程，分析評估於蒐集、處理及利用之過程中，個人資料安全可能發生之風險及其風險性之高低，訂定適當之管理措施以保護個人資料，並降低其風險。</p>

<p>第八條 學校、幼兒園應訂定應變機制，在發生個人資料被竊取、洩漏、竄改或其他侵害事故時，迅速處理以保護當事人之權利。</p> <p>前項應變機制，應包括下列事項：</p> <p>一、採取適當之措施，控制事故對當事人造成之損害。</p> <p>二、查明事故發生原因及損害狀況，並以適當方式通知當事人。</p> <p>三、研議改進措施，避免事故再度發生。</p>	<p>一、以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，爰第一項明定學校、幼兒園應訂定相關之應變機制，以降低或控制損害。</p> <p>二、又事故應變之首要處理原則，即根據事故之類型，採取應變措施以降低或控制損害；其次，應讓當事人了解相關狀況，使當事人亦能採取相關措施防止損害發生或擴大；最後，研議改進措施避免類似事故再次發生亦為應變措施之重點。爰依上開原則，於第二項明定應變機制應備之措施。</p>
<p>第九條 學校、幼兒園委託他人蒐集、處理或利用個人資料之全部或一部時，應依本法施行細則第八條規定對受託者為適當之監督，並明確約定相關監督事項及方式。</p>	<p>明定學校、幼兒園如將個人資料之蒐集、處理或利用委託他人為之，應對受託者為適當之監督，以使資料之蒐集、處理或利用符合本法施行細則之要求。</p>
<p>第十條 學校、幼兒園利用個人資料為宣傳、推廣或行銷時，應明確告知當事人其所屬學校、幼兒園立案名稱及個人資料來源。</p> <p>學校、幼兒園於首次利用個人資料為宣傳、推廣或行銷時，應提供當事人表示拒絕接受宣傳、推廣或行銷之方式，並支付所有費用；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。</p>	<p>一、為確認利用個人資料行銷行為，有無符合本法第二十條第二項及第三項規定，爰為本規定。</p> <p>二、第一項明定學校、幼兒園利用個人資料為宣傳、推廣或行銷時，應明確告知當事人之事項。</p> <p>三、第二項明定學校、幼兒園如為首次利用時，應提供當事人表示拒絕之權利，及於當事人拒絕後之相關處理方式。</p>
<p>第十一條 學校、幼兒園於當事人行使本法第三條規定之權利時，得採取下列方式辦理：</p> <p>一、提供聯絡窗口及聯絡方式。</p> <p>二、確認是否為資料當事人之本人，或經其委託。</p> <p>三、有本法第十條但書、第十一條</p>	<p>明定學校、幼兒園於當事人行使本法第三條規定之權利時，得採行之辦理方式。</p>

<p>第二項但書或第三項但書得拒絕當事人行使權利之事由，一併附理由通知當事人。</p> <p>四、告知是否酌收必要成本費用及其收費基準，並遵守本法第十三條處理期限規定。</p>	
<p>第十二條 學校、幼兒園對所保有之個人資料檔案，應設置必要之安全設備及採取必要之防護措施。</p> <p>前項安全設備或防護措施，應包括下列事項：</p> <p>一、紙本資料檔案之安全保護設施及管理程序。</p> <p>二、電子資料檔案存放之電腦或自動化機器相關設備，配置安全防護系統或加密機制。</p> <p>三、訂定紙本資料之銷毀程序；電腦、自動化機器或其他儲存媒介物需報廢汰換或轉作其他用途時，應採取適當防範措施，避免洩漏個人資料。</p>	<p>一、儲存個人資料之媒體於廢棄或移轉與他人，應訂有適當安全管理措施，例如刪除媒體中所儲存之資料，或以物理方式破壞等，以避免資料不當外洩，爰第一項明定學校、幼兒園所保有之個人資料檔案，應有必要安全設備及防護措施。</p> <p>二、第二項明定安全設備及防護措施應具備事項，包括針對個人資料處理之不同態樣，包括儲存、內部傳送及備份之狀況，如資料有加密之必要，即應採取適當之加密機制。又針對有備份必要之個人資料，除必要時採取加密機制，儲存備份資料之媒體應以適當方式保管，且定期進行備份資料之還原測試，以確保備份之有效性。</p>
<p>第十三條 學校、幼兒園為確實保護個人資料之安全，應對其所屬人員採取下列措施：</p> <p>一、依據業務作業需要，建立管理機制，設定所屬人員不同之權限，以控管其接觸個人資料之情形，並定期確認權限內容之適當性及必要性。</p> <p>二、檢視各相關業務之性質，規範個人資料蒐集、處理及利用等流程之負責人員。</p> <p>三、要求所屬人員妥善保管個人資料之儲存媒介物，並約定保管及保密義務。</p> <p>四、所屬人員離職時，取消其識別</p>	<p>學校、幼兒園與其所屬人員，不論是何種法律關係，都應避免其保管或蒐集、處理及利用個人資料時，違反個人資料保護相關法令規定，導致處理上發生弊端，侵害當事人權益情事，爰明定學校、幼兒園對其所屬人員應採取必要且適當之管理措施。</p>

<p>碼，並要求將執行業務所持有之個人資料(包括紙本及儲存媒介物)辦理交接，不得攜離使用，並應簽訂保密切結書。</p>	
<p>第十四條 學校、幼兒園業務終止後，其保有之個人資料之處理方式及留存紀錄如下：</p> <p>一、銷毀：銷毀之方法、時間、地點及證明銷毀之方式。</p> <p>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。</p> <p>三、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。</p>	<p>明定學校、幼兒園於業務終止後，其個人資料處理之方式及留存紀錄。</p>
<p>第十五條 學校、幼兒園對於個人資料之蒐集、處理及利用，應符合本法第十九條及第二十條規定，並應定期或不定期對其所屬人員施以教育訓練或認知宣導，使其明瞭個人資料保護相關法令規定、責任範圍、作業程序及應遵守之相關措施。</p>	<p>為落實執行本計畫相關管理程序，明定學校、幼兒園應透過教育訓練或認知宣導，使所屬人員均能明瞭個人資料保護相關法令規定、責任範圍、作業程序及應遵守之相關措施。</p>
<p>第十六條 學校、幼兒園應訂定個人資料檔案安全稽核機制，定期或不定期檢查安全維護計畫所定相關事項是否落實執行。</p>	<p>為使學校、幼兒園所屬人員落實安全維護計畫，明定學校、幼兒園應訂定個人資料檔案安全稽核機制，並檢視安全維護計畫執行情形。</p>
<p>第十七條 學校、幼兒園執行安全維護計畫各項程序及措施，應保存下列紀錄：</p> <p>一、 個人資料之交付及傳輸。</p> <p>二、 個人資料之維護、修正、刪除、銷毀及轉移。</p> <p>三、 提供當事人行使之權利。</p> <p>四、 存取個人資料系統之紀錄。</p> <p>五、 備份及還原之測試。</p> <p>六、 所屬人員權限之異動。</p> <p>七、 所屬人員違反權限之行為。</p> <p>八、 因應事故發生所採取之措施。</p>	<p>為確保學校、幼兒園於蒐集、處理及利用個人資料過程，能依權責辦理及落實安全維護計畫之執行，爰明定學校、幼兒園應保存之相關紀錄。</p>

<p>九、定期檢查處理個人資料之資訊系統。</p> <p>十、教育訓練。</p> <p>十一、安全維護計畫稽核及改善措施之執行。</p> <p>十二、業務終止後處理紀錄。</p>	
<p>第十八條 社區互助教保服務中心及部落互助教保服務中心，其個人資料檔案之安全維護準用本辦法之規定。</p>	<p>一、依幼兒教育及照顧法第十條規定，離島、偏鄉於幼兒園普及前，及原住民族幼兒基於學習其族語、歷史及文化機會與發揮部落照顧精神，得採社區互助式或部落互助式方式對幼兒提供教保服務，並依該條訂定「社區互助式及部落互助式教保服務實施辦法」。現行全國計有五家社區互助教保服務中心，與幼兒園同樣招收二歲以上至入國民小學前之幼兒，爰應將是類中心列為適用本辦法，以為周全規範對象。</p> <p>二、社區互助教保服務中心及部落互助教保服務中心應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規定、責任範圍、作業程序及應遵守之相關措施。</p>
<p>第十九條 本辦法自發布日施行。</p>	<p>明定本辦法之施行日期。</p>