

私立高級中等以下學校及幼兒園個人資料 檔案安全維護計畫實施辦法總說明

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（以下簡稱學校及幼兒園）之中央目的事業主管機關。考量學校及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計畫實施辦法（以下簡稱本辦法），其要點如下：

- 一、本辦法之法源依據。（第一條）
- 二、本辦法之主管機關。（第二條）
- 三、本辦法之用詞定義。（第三條）
- 四、學校及幼兒園應訂定相關安全維護計畫。（第四條）
- 五、學校及幼兒園指定專責人員負責個人資料檔案安全維護之任務。
（第五條）
- 六、學校及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，並為適當之處置。（第六條）
- 七、學校及幼兒園蒐集及傳輸個人資料時應符合相關規定，並採取必要保護措施。（第七條）
- 八、學校及幼兒園應分析評估可能產生之風險，訂定適當管控措施。
（第八條）
- 九、學校及幼兒園蒐集個人資料應遵守本法規定之告知義務。（
第九條）
- 十、學校及幼兒園利用個人資料為宣傳、推廣或行銷時，應符合本法之規定，並提供當事人或法定代理人拒絕行銷之機制。（第十條）
- 十一、學校及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。（第十一條）

十二、學校及幼兒園於當事人或其法定代理人行使本法第三條規定之權利時，得採取之辦理方式。（第十二條）

十三、學校及幼兒園應建立個人資料侵害事件發生之應變機制與通報當事人及主管機關之義務。（第十三條）

十四、學校及幼兒園對所保有個人資料檔案應設置必要安全設備及防護措施。（第十四條）

十五、學校及幼兒園為確保個人資料安全，對其所屬人員應採取之管理措施。（第十五條）

十六、學校及幼兒園應訂定個人資料檔案安全稽核機制，並應定期檢視稽核結果與執行改善及預防措施。（第十六條）

十七、學校及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其類別。（第十七條）

十八、學校及幼兒園應對所屬人員施以教育訓練或認知宣導。（第十八條）

十九、學校及幼兒園於業務終止後，對所保有個人資料之處理方式、留存紀錄及留存年限。（第十九條）

二十、學校及幼兒園應參酌相關因素，檢視所定安全維護計畫之合宜性，並持續改進個人資料保護機制。（第二十條）

二十一、本辦法之施行日期。（第二十一條）

私立高級中等以下學校及幼兒園個人資料 檔案安全維護計畫實施辦法

條 文	說 明
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(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。」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。	一、參酌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、短期補習班個人資料檔案安全維護計畫實施辦法及運動彩券業個人資料檔案安全維護計畫實施辦法第二條訂定。 二、明定本辦法之主管機關。
<p>第三條 本辦法用詞，定義如下：</p> <p>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，負責督導個人資料檔案安全維護計畫(以下簡稱安全維護計畫)訂定及執行之人員。</p> <p>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。</p> <p>三、所屬人員：指私立高級中等以下學校(以下簡稱學校)及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。</p> <p>前項第三款所定幼兒園，包括依幼兒教育及照顧法對幼兒提供教育及照顧服務之幼兒園、社區互助教保服務中心及部落互助教保服務中心。</p> <p>第一項第一款管理人與第二款稽核人員不得為同一人。</p>	<p>一、參酌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第四條訂定。</p> <p>二、為使個人資料檔案安全維護計畫(以下簡稱安全維護計畫)有效運作，爰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。</p> <p>三、依幼兒教育及照顧法第十條及其授權訂定之社區互助式及部落互助式教保服務實施辦法之規定，社區互助教保服務中心或部落互助教保服務中心(以下簡稱互助教保服務中心)對二歲以上至入國民小學前幼兒提供教育及照顧服務，考量互助教保服務中心提供之服務與幼兒園並無二致，個人資料之保護責任亦不應為差異規範，爰增訂第二項，使互助教保服務中心與幼兒園一體適用本辦法。故互助教保服務中心亦應對所屬人員施以認知宣</p>

	<p>導及教育訓練，使其明瞭個人資料保護之相關法令規定、責任範圍、作業程序及應遵守相關措施。</p> <p>四、為確保稽核制度獨立性及確實執行，爰於第三項明定個人資料管理人與稽核人員不得為同一人。</p>
<p>第四條 學校及幼兒園應依本辦法規定訂定安全維護計畫，落實個人資料檔案之安全維護及管理，防止個人資料被竊取、竄改、毀損、滅失或洩漏。</p> <p>學校及幼兒園訂定安全維護計畫時，應視其經營型態、規模、保有個人資料之性質及數量等事項，訂定適當之安全維護措施。</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>一、參酌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、運動彩券業個人資料檔案安全維護計畫實施辦法第三條訂定。</p> <p>二、第一項明定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，應訂定相關安全維護計畫，以建立並執行相關個人資料檔案管理程序或機制。</p> <p>三、考量學校、幼兒園規模不一，經營型態未盡相同，且參照本法施行細則第十二條第二項規定意旨，所採行之安全措施與所欲達成之個人資料保護目的間，具有適當比例為原則，爰第二項明定學校、幼兒園訂定安全維護計畫時，應視其經營型態、規模、保有個人資料之性質及數量等事項，訂定適宜並符合比例原則之安全維護措施。</p> <p>四、第三項明定前項安全維護計畫，應包括業務終止後之資料管理事項。</p>
<p>第五條 學校及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。</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、依據稽核人員就安全維護計畫執行之評核，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>一、參酌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第五條、運動彩券業個人資料檔案安全維護計畫實施辦法第六條訂定。</p> <p>二、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（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，爰明定管理單位或人員之任務。</p>
<p>第六條 學校及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>學校及幼兒園經定期檢視，發現有</p>	<p>一、參酌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第六條、運動彩券業個人資料檔案安全維護計畫實施辦法第七條訂定。</p> <p>二、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</p>

<p>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>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>三、為維護當事人權益，爰於第二項明定學校、幼兒園對個人資料應定期檢視及清查，並為適當處置。</p>
<p>第七條 學校及幼兒園於蒐集個人資料時，應檢視是否符合前條第一項所定之類別及範圍。</p> <p>學校及幼兒園於傳輸個人資料時，應採取必要保護措施，避免洩漏。</p>	<p>一、參酌短期補習班個人資料檔案安全維護計畫實施辦法及運動彩券業個人資料檔案安全維護計畫實施辦法第八條訂定。</p> <p>二、第一項明定學校、幼兒園蒐集個人資料時，應符合第七條第一項所定之類別及範圍。</p> <p>三、第二項明定學校、幼兒園如有傳輸個人資料之情事，應採取必要保護措施，避免洩漏。</p>
<p>第八條 學校及幼兒園應依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>一、參酌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第七條、短期補習班個人資料檔案安全維護計畫實施辦法及運動彩券業個人資料檔案安全維護計畫實施辦法第九條訂定。</p> <p>二、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得包括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，並予以管控。</p>
<p>第九條 學校及幼兒園於蒐集個人資料時，應遵守本法第八條及第九條有關告知義務之規定，並區分個人資料屬直接蒐集或間接蒐集，分別訂定告知方式、內容及注意事項，要求所屬人員確實辦理。</p>	<p>一、參酌短期補習班個人資料檔案安全維護計畫實施辦法及運動彩券業個人資料檔案安全維護計畫實施辦法第十條訂定。</p> <p>二、明定學校、幼兒園依本法第八條及第九條規定，除有例外免告知事由，應採取適當告知方式以履行告知義務。</p>
<p>第十條 學校及幼兒園依本法第二十條第一項規定利用個人資料為宣傳、推廣或行銷時，應明確告知當事人學校及幼兒園立案名稱及個人資料來源。</p> <p>學校及幼兒園於首次利用個人資料為宣傳、推廣或行銷時，應提供當事人或其法定代理人表示拒絕接受宣</p>	<p>一、參酌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第十條、短期補習班個人資料檔案安全維護計畫實施辦法及運動彩券業個人資料檔案安全維護計畫實施辦法第十一條訂定。</p> <p>二、依本法第八條第一項規定，非公務機</p>

<p>傳、推廣或行銷之方式，並支付所需費用；當事人或其法定代理人表示拒絕宣傳、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>關向當事人蒐集個人資料時，應明確告知當事人非公務機關之名稱，以利當事人知悉，向其為宣導、推廣或行銷之主體。爰第一項明定學校、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、為利當事人或其法定代理人查知利用個人資料行銷，是否符合本法第二十條第二項及第三項規定，爰第二項明定學校、幼兒園應提供當事人或其法定代理人表示拒絕接受行銷之方式及拒絕效果。</p>
<p>第十一條 學校及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>一、參酌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第九條訂定。</p> <p>二、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、處理或利用符合法令之要求。</p>
<p>第十二條 學校及幼兒園於當事人或其法定代理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其法定代理人，或經其委託。</p> <p>三、有本法第十條但書、第十一條第二項但書或第三項但書得拒絕當事人或其法定代理人行使權利之事由，一併附理由通知當事人或其法定代理人。</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>一、參酌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第十一條、短期補習班個人資料檔案安全維護計畫實施辦法及運動彩券業個人資料檔案安全維護計畫實施辦法第十二條訂定。</p> <p>二、明定學校、幼兒園於當事人或其法定代理人行使本法第三條規定之權利時，應遵守本法第三條、第十條、第十一條及第十三條規定，採取相關方式辦理，以保障當事人權利。</p>
<p>第十三條 學校及幼兒園應訂定應變機制，在發生個人資料被竊取、洩漏、竄改或其他侵害事件時，迅速處理，以保護當事人之權益。</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，控制事件對當事人造成之損害。</p> <p>二、查明事件發生原因及損害狀況，並以適當方式通知當事人或其法</p>	<p>一、參酌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第八條、短期補習班個人資料檔案安全維護計畫實施辦法及運動彩券業個人資料檔案安全維護計畫實施辦法第十三條訂定。</p> <p>二、依本法施行細則第十二條第二項第四款規定，事故之預防、通報及應變機制為本法第二十七條第一項所稱適當之安全措施之一，爰於第一項及第二</p>

<p>定代理人。</p> <p>三、研議改進措施，避免事故再度發生。</p> <p>學校及幼兒園應自第一項事件發生之日起三日內，通報主管機關；並自處理結束之日起一個月內，將處理方式及結果，報主管機關備查。</p>	<p>項明定個人資料被竊取、洩漏、竄改或其他侵害事件發生時，應採取適當應變措施降低對當事人之損害，並通知當事人或其法定代理人。</p> <p>三、第三項明定學校、幼兒園應於事件發生之日起三日內通報主管機關，嗣後亦需研議預防機制及報主管機關備查，以避免事故再次發生。</p>
<p>第十四條 學校及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、參酌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第十二條、短期補習班個人資料檔案安全維護計畫實施辦法及運動彩券業個人資料檔案安全維護計畫實施辦法第十四條訂定。</p> <p>二、明定學校及幼兒園為確保其所保有之個人資料檔案不被竊取、竄改、毀損、滅失或洩漏，應建立個人資料檔案(包括紙本及電子資料)儲存之防護措施及銷毀程序，必要時採取加密機制，以維護資料安全。</p>
<p>第十五條 學校及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>一、參酌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第十三條、短期補習班個人資料檔案安全維護計畫實施辦法及運動彩券業個人資料檔案安全維護計畫實施辦法第十五條訂定。</p> <p>二、第一款明定境外臺校應設定接觸個人資料之分級權限，並應定期檢視擁有權限之人員，減少個人資料外洩之可能。</p> <p>三、第二款及第三款明定對個人資料採取適當之資料安全管理措施，例如加密、個人資料報廢或移轉作其他用途時，應採取適當防範措施並訂定相關使用規範。</p> <p>四、第四款明定個人資料應避免不當移轉，以降低資料外洩之情形發生。</p>

<p>第十六條 學校及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，並將檢查結果向管理人提出報告。</p> <p>執行前項稽核之人員與第五條指定之專責人員，不得為同一人。</p> <p>學校應將第一項稽核機制，納入其內部控制制度訂定作業程序、內部控制點及稽核作業規範（內部管理及稽核作業規章）規定辦理。</p>	<p>一、參酌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、短期補習班個人資料檔案安全維護計畫實施辦法第十六條及運動彩券業個人資料檔案安全維護計畫實施辦法第十七條訂定。</p> <p>二、為確保個人資料維護安全措施發生效能，爰於第一項明定學校、幼兒園應訂定個人資料檔案安全維護稽核機制，定期或不定期檢查計畫之執行情形；又依本法第五十條規定，對非公務機關之代表人、管理人或其他有代表權人，因該非公務機關依本法第四十七條至第四十九條規定受罰鍰處罰時，除能證明其已盡防止義務者外，應受同一額度罰鍰處罰，並於同項明定學校、幼兒園稽核人員應向管理人提出檢查結果報告，俾利管理人得據以監督計畫之執行事項，落實對個人資料之保護。</p> <p>三、第二項明定稽核人員與負責規劃、訂定、修正及執行計畫之專責人員不得為同一人。</p> <p>四、因個人資料檔案安全維護屬內部控制及稽核制度之重要一環，爰依據學校財團法人及所設私立學校內部控制制度實施辦法，於第三項明定學校將稽核機制納入其內部控制制度訂定作業程序、內部控制點及稽核作業規範（內部管理及稽核作業規章）規定辦理，避免因本辦法施行加重行政負擔。至私立幼兒園部分，因幼兒教育及照顧法並未規範幼兒園應建立內部控制制度，爰依第一項規定訂定個人資料檔案安全稽核機制，毋須比照各私立學校另行建立內部控制制度，避免私立幼兒園為落實本辦法產生額外之行政負擔。</p>
<p>第十七條 學校及幼兒園執行安全維護計畫各項程序及措施，至少應保存下列紀錄：</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>一、參酌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第十七條訂定。</p> <p>二、為確認本辦法及依本辦法所訂定之相關程序是否落實執行，及釐清個人資料於蒐集、處理與利用過程之相關權</p>

<p>三、提供當事人或其法定代理人行使之權利。</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>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>責，並證明學校、幼兒園確實執行本安全維護計畫，且已盡防止個人資料遭侵害之義務，爰明定學校、幼兒園應保存相關紀錄，以供日後發生問題時提供說明及查驗。</p>
<p>第十八條 學校及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>一、參酌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第十五條、短期補習班個人資料檔案安全維護計畫實施辦法第十八條及運動彩券業個人資料檔案安全維護計畫實施辦法第十九條訂定。</p> <p>二、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，以落實本辦法之執行。</p>
<p>第十九條 學校及幼兒園業務終止後，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、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。</p> <p>前項紀錄應至少留存五年。</p>	<p>一、參酌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第十四條、短期補習班個人資料檔案安全維護計畫實施辦法第十九條及運動彩券業個人資料檔案安全維護計畫實施辦法第二十條訂定。</p> <p>二、第一項明定學校、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>三、依本法第三十條規定「損害賠償請求權，自請求權人知有損害及賠償義務人時起，因二年間不行使而消滅；自損害發生時起，逾五年者，亦同。」爰第二項明定銷毀、移轉、刪除、停止處理或利用個人資料之紀錄至少應留存五年。</p>

<p>第二十條 學校及幼兒園應參酌安全維護計畫執行狀況、技術發展、法令依據修正等因素，檢視所定安全維護計畫是否合宜，必要時應予以修正。</p>	<p>一、參酌短期補習班個人資料檔案安全維護計畫實施辦法第二十條及運動彩券業個人資料檔案安全維護計畫實施辦法第二十一條訂定。</p> <p>二、明定學校及幼兒園應參酌相關因素，依據實務運作及法令變化等情形，檢視或修正計畫。</p>
<p>第二十一條 本辦法自發布日施行。</p>	<p>明定本辦法之施行日期。</p>