

中華民國 103 年 2 月 27 日
教育部公告 臺教社（一）字第 1030024369A 號

主 旨：預告訂定「短期補習班個人資料檔案安全維護計畫實施辦法」。

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。
- 三、「短期補習班個人資料檔案安全維護計畫實施辦法」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：教育部終身教育司。
 - （二）地址：臺北市中山南路 5 號。
 - （三）電話：02-7736-5676。
 - （四）傳真：02-2397-6926。
 - （五）電子郵件：kpchang@mail.moe.gov.tw。

部 長 蔣偉寧

短期補習班個人資料檔案安全維護計畫實施辦法草案總說明

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。」考量短期補習班保有大量教職員工、學生及相關人員之個人資料檔案，為有效保護該等檔案，避免遭到竊取、竄改、毀損、滅失或洩漏，短期補習班就該檔案應訂定安全維護計畫，包括於業務終止後對該檔案之適當處理方法。本部為使短期補習班於訂定個人資料檔案安全維護計畫時有所依循，爰擬訂短期補習班個人資料檔案安全維護計畫實施辦法（以下簡稱本辦法）草案，共計二十二條，其要點如下：

- 一、法源依據。（草案第一條）
- 二、本辦法之主管機關。（草案第二條）
- 三、補習班應訂定個人資料檔案安全維護計畫之規定及本辦法適用範圍。（草案第三條）
- 四、補習班訂定個人資料檔案安全維護計畫得參酌之規定。（草案第四條）
- 五、補習班應訂定個人資料檔案安全維護計畫之期程規範及主管教育行政機關檢查之規定。（草案第五條）

- 六、補習班應指定專責人員負責個人資料檔案安全維護之相關任務。（草案第六條）
- 七、補習班為維護其所保有個人資料之特定目的消失或期限屆滿時應辦理方式。（草案第七條）
- 八、補習班所屬人員蒐集個人資料時之監督規範。（草案第八條）
- 九、補習班依個人資料範圍訂定適當管控措施。（草案第九條）
- 十、補習班蒐集個人資料應遵守之義務。（草案第十條）
- 十一、補習班利用個人資料行銷時應提供當事人拒絕機制及應遵守事項。（草案第十一條）
- 十二、規範補習班對於當事人行使本法第三條規定之權利，得採行之方式。（草案第十二條）
- 十三、補習班與消費者簽訂契約書之刪除或銷毀規範。（草案第十三條）
- 十四、補習班應於個人資料檔案安全維護計畫訂定應變機制。（草案第十四條）
- 十五、補習班應採取必要適當之安全設備或防護措施。（草案第十五條）
- 十六、補習班應對其所屬人員採取之措施。（草案第十六條）
- 十七、補習班應訂定個人資料檔案安全維護查核機制。（草案第十七條）
- 十八、補習班應留存個人資料使用紀錄、自動化機器設備之軌跡資料。（草案第十八條）
- 十九、補習班應定期對所屬人員施以宣導或訓練講習。（草案第十九條）
- 二十、補習班業務終止後對個人資料處理方法。（草案第二十條）
- 二十一、補習班應檢視或修訂個人資料檔案安全維護計畫，以持續改善個人資料保護等機制。（草案第二十一條）

短期補習班個人資料檔案安全維護計畫實施辦法草案

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。	個人資料保護法第二十七條規定：「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。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。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。	明定本辦法之各級主管機關。
第三條 短期補習班（以下簡稱補習班）應訂定個人資料檔案安全維護計畫（以下簡稱計畫），落實個人資料檔案之安全維護及管	一、第一項明定短期補習班應訂定個人資料檔案安全維護計畫，以建立相關管理機制並落實執行。

<p>理，防止個人資料被竊取、竄改、毀損、滅失或洩漏。</p> <p>所稱補習班，指辦理補習及進修教育法第三條所定短期補習教育之機構，並經直轄市、縣（市）主管教育行政機關核准立案者。</p>	<p>二、第二項明定本辦法適用對象係指辦理短期補習教育之機構，並經直轄市、縣（市）主管教育行政機關核准立案之補習班。</p>
<p>第四條 補習班訂定計畫時，得視其規模、特性、保有個人資料之性質及數量等事項，參酌第六條至第二十四條規定，訂定適當之安全維護管理措施。</p>	<p>考量補習班規模不一，經營主體與型態未盡相同，尚難作統一規範，爰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。因此規定補習班得參酌其規模、特性、保有個人資料之性質、方法及數量等事項，參考本辦法第六條至第二十四條規定之內容標準，訂定適宜並符合比例原則之安全維護管理措施。</p>
<p>第五條 補習班應將訂定之計畫留班備查，由直轄市、縣（市）主管教育行政機關派員檢查。</p> <p>補習班應於本辦法發布施行後，六個月內完成前項計畫之訂定。</p>	<p>明定短期補習班個人資料檔案安全維護計畫應於本辦法發布施行後，六個月內完成訂定，並將計畫留班備查，由直轄市、縣（市）主管教育行政機關派員檢查。</p>
<p>第六條 補習班應指定專責人員，負責規劃、訂定、修正與執行計畫或業務終止後個人資料處理方法等相關事項，並定期向負責人提出報告。</p>	<p>依本法施行細則第十二條規定，本法第二十七條第一項所稱適當之安全措施，指為防止個人資料被竊取、竄改、毀損、滅失或洩漏，採取技術上及組織上之措施，得包括配置管理之人員及相當資源，為有效訂定與執行本計畫，補習班應指定專人並投入相當資源辦理有關事項。爰明定補習班應配置適當人員及相當資源，並指定專責人員，負責個人資料檔案安全維護，並明定專責人員之任務。</p>
<p>第七條 補習班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>補習班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</p>	<p>補習班應依據本法施行細則第十二條第二項第二款之規定，於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，爰明定補習班應定期清查個人資料之種類與數量並建立檔案，方能有效對其所保有之個人資料加以保護。</p>

<p>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>第八條 補習班所屬人員為執行業務所蒐集之個人資料應視為該補習班所蒐集持有，於蒐集時應檢視是否符合蒐集要件及特定目的之必要範圍，並接受監督。</p> <p>前項個人資料有傳送必要時，應採取必要保護措施，以防範發生個人資料洩漏事故。</p>	<p>一、明定補習班所屬人員與業者間不論是基於何種法律關係，其所蒐集之個人資料均應視為所屬補習班所蒐集持有，須納入所訂定計畫之規範，接受監督。</p> <p>二、補習班如以加盟方式經營，而有傳輸個人資料之情事。在傳輸個人資料之過程中，應採取必要保護措施。如：必須事先告知當事人，於取得當事人之同意後，始得將其個人資料傳輸，並應避免在傳輸過程中發生洩漏事故。</p> <p>三、參照本法施行細則第十二條第二項第五款規定。</p>
<p>第九條 補習班應依已界定個人資料之範圍與蒐集、處理及利用流程，分析評估可能發生之風險，訂定適當之管控措施。</p>	<p>一、補習班應參酌整體業務運作狀況，就已界定之個人資料之範圍與蒐集、處理及利用流程，分析評估可能發生之風險，並針對該可能發生之風險，採取必要之防範與管控措施，避免個人資料被竊取、竄改、洩漏、毀損、滅失或濫用。</p> <p>二、參照本法施行細則第十二條第二項第三款規定。</p>
<p>第十條 補習班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>本條明定依本法第八條及第九條規定，短期補習班原則上應適時履行告知義務，除經檢視有例外無須告知之事由外，依據資料蒐集之情形，採取適當之告知方式，以確實履行告知義務。</p>
<p>第十一條 補習班利用個人資料行銷時，應明確告知當事人其所屬補習班立案名稱。</p> <p>補習班首次利用個人資料行銷時，應提供當事人免費表示拒絕接受行銷之方式。</p> <p>補習班利用個人資料進行行銷，當事人表示拒絕接受行銷時，應立即停止利用其個人資料繼續行銷，並周知所屬人員。</p>	<p>一、第一項明定補習班利用個人資料行銷時，應明確告知當事人補習班核准立案名稱。</p> <p>二、第二項及第三項，為查知短期補習班利用個人資料行銷有無符合本法第二十條第二項及第三項規定，爰於第一項規定其應提供當事人表示拒絕接受行銷之方式及拒絕效果。</p>

<p>第十二條 補習班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、如認有本法第十條但書各款、第十一條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>明定短期補習班對於當事人行使本法第三條規定之權利，得採行之方式。</p>
<p>第十三條 補習班與當事人簽訂之契約書，應於契約期限屆滿時主動刪除或銷毀。但因執行業務所必須或經當事人書面同意者，不在此限。</p>	<p>一、補習班所蒐集、持有、保管之最重要個人資料文件為契約書。如該契約書有約定保存年限，且同意業者得繼續為利用者，當然得依其約定辦理。</p> <p>二、參照本法施行細則第十二條第二項第五款規定。</p>
<p>第十四條 補習班應訂定應變機制，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、採取適當之措施以控制事故對當事人造成損害。</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，避免類似事故再度發生。</p>	<p>一、本法第十二條規定，非公務機關所持有之個人資料發生被竊取、洩漏、竄改或其他侵害事故者，應查明後以適當方式通知當事人。爰本條規定補習班在計畫中應訂定應變機制及其必要作為之相關事項，在發生資料外洩等意外事故時，得迅速遵循處理，以保護當事人之權益。</p> <p>二、參照本法施行細則第十二條第二項第四款規定。</p>
<p>第十五條 補習班對所保有之個人資料檔案，應採取必要適當之安全設備或防護措施。</p> <p>前項安全設備或防護措施應包含下列事項：</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</p>	<p>一、為確保補習班所保管之個人資料檔案不被竊取、竄改、毀損、滅失或洩漏，業者得視其規模、業務性質、資料儲存之媒介物及其數量等，在安全維護計畫中採取必要且適當之安全設備或防護措施。例如：對紙本及電子資料之安全保護、制定紙本資料之銷毀程序、電腦或其相關設備需報廢</p>

<p>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、自動化機器或其他存放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>汰換或轉作其他用途時，應確實刪除所存放之個人資料檔案等。</p> <p>二、參照本法施行細則第十二條第二項第八款規定。</p>
<p>第十六條 補習班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，並應要求將執行業務所持有之個人資料（包括紙本及載體）辦理交接，不得攜離在外繼續使用，並應簽訂保密切結書。</p>	<p>一、補習班與所屬人員，不論是何種法律關係，補習班都必須避免在個人資料之保管與處理上發生弊端，導致侵害當事人權益情事，爰應於安全維護計畫中，採取必要且適當之管理措施。補習班應根據業務性質，檢視容易發生問題之處，預先予以防範。例如：與業務無關人員不得任意接觸資料、利用個人資料人員不同等級之權限、規範嚴密保管個人資料檔案及所屬人員離職時，對所保有之個人資料的交接與保密切結等事項。</p> <p>二、參照本法施行細則第十二條第二項第五款及第六款規定。</p>
<p>第十七條 補習班應訂定個人資料檔案安全維護查核機制，定期或不定期檢查計畫之執行情形，檢查結果並應向負責人提出報告。</p>	<p>補習班為確保個人資料維護安全措施發生效能，應訂定個人資料檔案安全維護查核機制，定期或不定期檢查計畫之執行情形，檢查結果並應向負責人提出報告。另參照本法第五十條規定，對非公務機關之代表人得併同處罰，爰規定檢查結果須向負責人提出報告，促使負責人能據以監督計畫之執行事項，落實對個人資料保護之工作。</p>
<p>第十八條 補習班得採行適當措施，留存個人資料使用紀錄、自動化機器設備之軌跡資料或其他相關之證據資料，以供必要時說明其所定計畫之執行情況。</p>	<p>一、補習班為證明確實執行計畫，已盡防止個人資料遭侵害之義務，得視其規模及業務性質採行適當的措施，留存相關證據，以供日後發生問題時提供說明佐證，以免除或減輕其法律責任。</p> <p>二、參照本法施行細則第十二條第二項第十款規定。</p>

第十九條 補習班對於個人資料蒐集、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。	一、補習班應定期對所屬人員施以宣導或訓練講習，以使所屬人員能充分認知個人資料保護相關法令及責任範圍，避免發生違法情事。 二、參照本法施行細則第十二條第二項第七款規定。
第二十條 補習班業務終止後，其保有之個人資料不得繼續使用，保存期限屆滿後，應依下列方式處理，並留存相關紀錄： 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。 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。	一、補習班因停辦、廢止設立、撤銷立案或其他原因終止業務後，自不得再繼續持有使用個人資料檔案，應作妥善處置。因此終止業務之補習班，應視其終止業務之原因，將所保有之個人資料予以銷毀、刪除、移轉或其他停止處理或利用等方式處理。 二、補習班在銷毀、刪除、移轉或其他停止處理或利用個人資料過程中，宜保存執行方式、地點、時間、執行人員、接受移轉資料之對象及合法移轉依據等資料，以便日後得以提出舉證。 三、參照本法施行細則第十二條第二項第六款規定。
第二十一條 補習班應參酌計畫執行狀況、技術發展、法令依據修正等因素，檢視所定計畫是否合宜，必要時應予以修正。	明定補習班參酌相關因素，檢視或修訂個人資料檔案安全維護計畫。
第二十二條 本辦法自發布日施行。	明定本辦法之施行日期。