

短期補習班個人資料檔案安全維護計畫實施辦法

總說明

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。」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個人資料檔案安全維護計畫（以下簡稱計畫），包括於業務終止後對該檔案之適當處理方法。教育部為使短期補習班於訂定計畫時有所依循，爰訂定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），其要點如次：

一、法源依據。（第一條）

二、本辦法之主管機關。（第二條）

三、補習班應訂定計畫。（第三條）

四、補習班訂定計畫時，應視規模、特性等訂定適當之安全維護措施。
（第四條）

五、補習班應完成計畫訂定之期程及主管機關得派員檢查該計畫。（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。
（第六條）

七、補習班所其保有之個人資料，經定期檢視，應予刪除、銷毀或停止蒐集、處理及利用之情形。（第七條）

- 八、補習班蒐集及傳輸個人資料時應符合之規定。(第八條)
- 九、補習班應依已界定之個人資料範圍與蒐集、處理及利用流程，訂定適當管控措施。(第九條)
- 十、補習班蒐集個人資料應遵守之告知義務。(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。(第十一條)
- 十二、補習班對於當事人行使本法第三條規定之權利，得採行之辦理方式。(第十二條)
- 十三、補習班應訂定應變機制。(第十三條)
- 十四、補習班應設置必要之安全設備及採取必要之防護措施。(第十四條)
- 十五、補習班應對其所屬人員採取之措施。(第十五條)
- 十六、補習班應訂定個人資料檔案安全維護查核機制。(第十六條)
- 十七、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。(第十七條)
- 十八、補習班應定期或不定期對其所屬人員施以個人資料保護相關法令規定之教育訓練或宣導。(第十八條)
- 十九、補習班業務終止後，對其保有之個人資料之處理方法及留存紀錄。(第十九條)
- 二十、補習班應檢視所定計畫之合宜性，以持續改進個人資料保護機制。(第二十條)

短期補習班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。	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。	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理，防止個人資料被竊取、竄改、毀損、滅失或洩漏。 前項所稱補習班，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）主管機關核准立案者。	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（以下簡稱計畫），以建立相關管理機制並落實執行。 二、第二項明定本辦法適用對象係辦理短期補習教育，並經直轄市、縣（市）主管機關核准立案之短期補習班（以下簡稱補習班）。
第四條 補習班訂定計畫時，應視其規模、特性、保有個人資料之性質及數量等事項，訂定適當之	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，且依本法施行細則第十二條第二項規

<p>安全維護措施。</p>	<p>定，所採行之安全措施與所欲達成之個人資料保護目的間，以具有適當比例為原則，爰明定補習班訂定計畫時，應參酌其規模、特性、保有個人資料之性質、方法及數量等事項，訂定適宜並符合比例原則之安全維護措施。</p>
<p>第五條 補習班應於本辦法發布施行後六個月內，完成計畫之訂定。</p> <p>補習班應將訂定之計畫留班備查；直轄市、縣（市）主管機關得派員檢查。</p>	<p>一、第一項明定補習班之計畫應於本辦法發布施行後，六個月內完成訂定。</p> <p>二、第二項明定前項計畫應留班備查，直轄市、縣（市）主管教育行政機關得派員檢查。</p>
<p>第六條 補習班應指定專責人員，負責規劃、訂定、修正、執行計畫及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，補習班應指定專人辦理有關事項，爰明定補習班應指定專責人員，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、補習班應依本法施行細則第十二條第二項第二款之規定，於安全維護計畫中就界定個人資料範圍相關事項加以規定，爰於第一項明定補習班應依蒐集之特定目的，界定所蒐集、處理及利用個人資料之類別或範圍，並定期清查個人資料現況。</p> <p>二、第二項明定補習班就其保有之個人資料，經定期檢視，應予刪除、銷毀或停止蒐集、處理及利用之</p>

	情形。
<p>第八條 補習班於蒐集個人資料時，應檢視是否符合前條第一項所定之類別及範圍。</p> <p>補習班於傳輸個人資料時，應採取必要保護措施，避免洩漏。</p>	<p>一、明定補習班蒐集個人資料，應符合前條第一項所定之類別及範圍。</p> <p>二、第二項明定補習班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>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、毀損或滅失。</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>明定補習班除有例外免告知之事由外，應踐行告知規定。</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及個人資料來源。</p> <p>補習班於首次利用個人資料行銷時，應提供當事人表示拒絕接受行銷之方式，並支付所需費用；當事人表示拒絕接受行銷者，應立即停止利用其個人資料，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及個人資料來源。</p> <p>二、為查知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，爰於第二項規定補習班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>明定補習班對於當事人行使本法第三條規定之權利，得採行之辦理方式。</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>第十三條 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，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、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，爰於第一項明定補習班在計畫中應訂定應變機制。</p> <p>二、第二項明定前項應變機制應包括事項，俾利發生個人資料外洩時，得迅速遵循處理，以保護當事人權益。</p>
<p>第十四條 補習班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>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、資料儲存媒介物及其數量等，爰於第一項明定，補習班對所保有之個人資料，應設置必要之安全設備及採取必要之防護措施。</p> <p>二、第二項明定安全設備或防護措施之內涵。</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>第十五條 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>補習班與所屬人員，不論是何種法律關係，補習班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，導致侵害當事人權益情事，爰明定應採取必要且適當之管理措施。</p>
<p>第十六條 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，並將檢查結果向負責人提出報告。</p> <p>前項查核人員與第六條指定之專責人員不得為同一人。</p>	<p>一、補習班為確保個人資料維護安全措施發生效能，第一項明定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。依本法第五十條規定，對非公務機關之代表人，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</p>

	<p>緩處罰時，除能證明已盡防止義務者外，應受同一額度罰鍰，爰規定向負責人提出檢查結果報告，促使負責人得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>二、第二項明定查核人員與負責規劃、訂定、修正及執行計畫之專責人員不得為同一人。</p>
<p>第十七條 補習班應採行適當措施，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>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，應視其規模及業務性質採行適當措施，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>第十八條 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。</p>	<p>補習班應定期對所屬人員施以教育訓練或認知宣導，使所屬人員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。</p>
<p>第十九條 補習班業務終止後，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>一、補習班業務因停辦、廢止設立、撤銷立案或其他原因終止後，自不得再繼續使用其所保有之個人資料檔案，並應作妥善處置。爰終止業務之補習班，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。</p> <p>二、第一項明定補習班銷毀、刪除、移轉或刪除、停止處理或利用個人資料過程中，應保存處理方式、地點、時間、執行人員、接</p>

<p>前項紀錄應至少留存五年。</p>	<p>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。</p> <p>三、第二項明定銷毀、刪除、移轉或刪除、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 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。</p>	<p>明定補習班應參酌相關因素，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>