永年高級中學

個人資料檔案安全維護計畫

訂定日期：中華民國 115 年 07 月 20 日

核定機關：永年高級中學

（本計畫經個人資料保護委員會議通過並陳請校長核可後施行）

目　　次

壹、依　　據

本計畫依下列法規訂定之：

一. 《個人資料保護法》（中華民國 114 年 11 月 11 日修正公布）第 27 條第 2 項。

二. 《個人資料保護法施行細則》。

三. 教育部訂定之《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》第 4 條第 1 項。

四. 教育部主管目的事業之個人資料檔案自我檢查表（v20260505）相關規範。

貳、目　　的

本校為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，維護當事人權益，並促進個人資料之合理利用，特訂定本計畫。

參、適用範圍

本計畫適用於下列人員：

一. 本校專任、兼任、代課、鐘點之教職員工。

二. 本校國中部及高中部之學生。

三. 本校臨時約聘僱人員、工讀生、志工。

四. 接受本校委辦案派駐本校之人員及委外廠商人員。

五. 其他因執行本校業務須接觸個人資料之相關人員。

本計畫適用於本校持有、受委託蒐集處理利用、或委外辦理之所有個人資料檔案。

肆、權責單位及管理人員

一、權責單位

本校設「永年高級中學個人資料保護委員會」（以下簡稱本委員會），負責本校個人資料保護與管理相關事務，任務如下：

一. 審議本校個人資料檔案安全維護計畫及相關規章。

二. 督導個人資料盤點、風險評估及管控措施之執行。

三. 督導個人資料保護教育訓練之規劃與執行。

四. 監督個人資料事故通報與應變機制之運作。

五. 審議個人資料保護內部稽核結果並督導改善事項。

六. 其他有關個人資料保護管理事項。

二、組織成員及職掌

角色	擔任人員	主要職掌
管理人 （召集人）	校長	1. 綜理本校個人資料保護相關事務並督導本委員會運作。 2. 指定執行秘書及稽核人員。 3. 主持本委員會會議。 4. 聽取執行秘書及稽核人員之定期報告。 5. 遇個資事故時決定是否召開臨時會議。
執行秘書 （個資專責人員）	由校長指定 1 位主管	1. 統籌彙整全校個人資料檔案盤點資料。 2. 擔任個人資料保護對內對外聯絡窗口並填報系統。 3. 追蹤各處室個資保護業務辦理進度。 4. 負責個資事故通報之聯絡協調。 5. 每學年至少一次向管理人提出書面報告。 6. 執行本委員會決議事項。
當然委員 （個人資料管理人）	教務主任、學務主任、輔導主任、總務主任、人事主任、會計主任、圖書館主任	1. 督導所屬處室個人資料檔案之安全維護。 2. 執行本處室個人資料盤點及更新作業。 3. 落實本處室告知義務、委外監督、保密切結等事項。 4. 本處室發生個資事故時之第一線處理及通報。 5. 依稽核結果進行檢討改進並提出報告。 6. 出席本委員會會議並參與決議。

角色	擔任人員	主要職掌
稽核人員	由校長指定 1 位主管（不得為執行秘書）	1. 每學年至少一次執行個人資料保護內部稽核。 2. 依教育部檢查表相關項目辦理稽核。 3. 撰寫稽核報告陳報管理人及本委員會。 4. 追蹤前次稽核所提改善事項之落實情形。
所屬人員	執行業務接觸個人資料之全體教職員工	1. 遵守本校個人資料保護相關作業規範。 2. 執行本校個人資料保護之決策及交辦事項。 3. 在職及離退職後不得洩漏所知悉之個人資料。

三、資訊組

本校資訊組非本委員會之當然委員，惟負責全校資訊系統技術層面之個人資料保護工作，包括：

一. 全校資訊系統帳號權限管理。

二. 系統設備、網路設備、儲存媒介之防護。

三. 系統登入、存取、異動軌跡紀錄。

四. 資通訊系統安全防護（身分確認、傳輸加密、防外部入侵、異常監控等）。

五. 資通安全檢測（弱點掃描、資安健診等）。

六. 機房環境之核心管理。

本委員會開會時，遇議題涉及資訊系統、資安防護等技術性事項，得邀請資訊組列席說明。

伍、個人資料檔案之安全維護管理措施

一、蒐集、處理及利用個人資料之範圍及特定目的

（一）個人資料範圍

本校對於個人資料之定義依《個人資料保護法》第 2 條第 1 款規定，係指自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。

（二）特種個人資料

依《個人資料保護法》第 6 條規定，有關病歷、醫療、基因、性生活、健康檢查及犯罪前科之個人資料，屬「特種個人資料」，原則上不得蒐集、處理或利用。本校依《學校衛生法》規定建立學生健康管理制度，其健康檢查及疾病檢查結果之個人資料屬特種個人資料，適用第 6 條第 1 項第 2 款（非公務機關履行法定義務必要範圍內）之例外規定，並採取本計畫所定之適當安全維護措施。

（三）個人資料盤點

本校依《個人資料保護法》立法精神進行全面性個人資料盤點，範圍包括：

1. 本校目前持有之個人資料。
2. 本校受委託蒐集、處理或利用之個人資料。
3. 本校委託外部機關蒐集、處理或利用之個人資料。

個資盤點作業由各處室依業務職掌辦理，由執行秘書統籌彙整全校個人資料檔案清冊，並每年至少更新一次。

（四）本校個人資料之特定目的

本校持有個人資料之特定目的，依法務部公告之「個人資料保護法之特定目的及個人資料之類別」，包括但不限於下列項次：

代號	特定目的名稱	主要對應處室
002	人事管理	人事室
063	非公務機關依法定義務所進行個人資料之蒐集處理及利用	全校性
069	契約、類似契約或其他法律關係事務	總務處、會計室
109	教育或訓練行政	教務處、學務處、人事室、輔導室

代號	特定目的名稱	主要對應處室
136	資（通）訊與資料庫管理	資訊組
146	圖書館管理	圖書館
157	調查、統計與研究分析	全校性
158	學生（員）資料管理（含畢、結業生）	教務處、學務處

（五）依資料屬性訂定管理程序

本校依個人資料之屬性，分別訂定管理程序：

1. 一般個人資料：依本計畫第伍章第五節、第六節之管理措施辦理。
2. 特種個人資料（本校主要為學生健康檢查資料）：除依前款措施外，並採取下列額外保護：
   (1) 存取權限限制於健康中心校護、學務主任及經校長核可之特定人員。
   (2) 紙本資料存放於健康中心專用檔案櫃並上鎖。
   (3) 電子檔案（含教育部學生健康資訊系統 SSHIS/shiscloud）之操作應符合平台方之安全規範。
   (4) 調閱應留存紀錄，含調閱人、時間、目的、範圍。

（六）定期檢視

管理人員應定期檢視本校保有之個人資料，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，並留存相關紀錄。

二、個人資料之風險評估及管理機制

（一）風險評估

本校每學年由執行秘書統籌，各處室協助，針對本校蒐集、處理、儲存及傳輸之所有個人資料進行風險評估，識別潛在之內部、外部及人為風險，並分析資料敏感度與處理過程中之風險點（如資料外洩、未授權存取、系統故障等）。

（二）風險評估方法

風險值之計算依下列公式辦理：

風險值 ＝ 衝擊程度 × 發生可能性

前開二項因子分別評估如下：

1. 衝擊程度：評估個人資料事故發生後對當事人及本校造成之傷害程度，考量因素包括受影響資料筆數規模、資料敏感度（一般個資／特種個資）、法律責任、當事人權益損害及社會觀感等，區分為 1 至 5 級（1 級最低、5 級最高）。
2. 發生可能性：評估該風險情境實際發生之機率，考量因素包括歷史事件紀錄、既有控制措施完善程度、資料暴露頻率及外部威脅環境等，區分為 1 至 5 級（1 級最低、5 級最高）。

依評估結果將風險等級分為「高、中、低」三級，並訂定對應之控制措施：

（1）低度風險（風險值 1－5 分）：維持現有控制措施，並納入下年度風險評估追蹤。

（2）中度風險（風險值 6－14 分）：由執行秘書列管改善，定期追蹤處理進度。

（3）高度風險（風險值 15－25 分）：優先處理並訂定改善期限，由本委員會列管，改善後再次評估。

（三）管理機制

1. 強化技術防護措施：包括資料加密、身分驗證、系統防火牆等，確保資料存取權限與處理流程符合最小存取原則。
2. 訂定各類風險（如駭客攻擊、內部濫用、資料外洩等）之具體防範措施。
3. 定期檢視資料安全性與合規性。
4. 完成風險評鑑後，產出「個人資料檔案風險評鑑彙整表」，由執行秘書維護。

三、告知義務

本校向當事人蒐集個人資料時，依《個人資料保護法》第 8 條規定，明確告知下列事項：

一. 本校名稱。

二. 蒐集之目的。

三. 個人資料之類別。

四. 個人資料利用之期間、地區、對象及方式。

五. 當事人依《個人資料保護法》第 3 條規定得行使之權利及方式（查詢閱覽、請求製給複製本、請求補充或更正、請求停止蒐集處理或利用、請求刪除）。

六. 當事人得自由選擇提供個人資料時，不提供將對其權益之影響。

非由當事人提供之個人資料，本校應於處理或首次利用前，向當事人告知個人資料來源及前項所列事項；如屬首次利用個資進行行銷者（如招生宣傳、校友活動邀請等），應併同告知當事人得表示拒絕接受行銷之方式，並支付所需費用。

告知作業由各處室依業務辦理，並留存告知紀錄。

四、事故之預防、通報及應變機制

（一）預防機制

1. 本校保有之個人資料檔案，限承辦人員於執行業務所必要範圍內使用或存取，且存取電子檔案時須輸入個人使用者帳號及識別密碼。非承辦人員參閱、使用或存取相關個人資料檔案或書件時，應經權責主管同意並留存紀錄。
2. 存有個人資料之儲存媒體（含可攜式媒體）視必要性採取適當之加密機制；存有個人資料之紙本文件於不使用或下班時，遵守桌面淨空，置於抽屜或儲櫃並上鎖。
3. 存有個人資料之紙本及儲存媒介物於報廢汰換或轉作其他用途前，確實刪除資料或格式化，或採物理方式破壞、銷毀。
4. 電腦安裝防毒軟體並定期更新病毒碼，避免惡意程式與系統漏洞對作業系統之威脅。
5. 對內或對外傳輸個人資料時，加強管控避免外洩。
6. 加強所屬人員教育宣導，並嚴加管制。
7. 本校各處室應就風險評鑑中所可能發生之各種情境進行必要之演練，詳細記錄演練過程，建立標準之個資事故處理標準作業程序。

（二）72 小時內通報流程

依《個人資料保護法》第 12 條規定，本校知悉所保有之個人資料被竊取、竄改、毀損、滅失或洩漏時，通報流程如下：

1. 所屬人員發現或知悉個人資料事故，應立即向所屬處室主任及執行秘書通報。
2. 執行秘書應立即會同相關處室評估事故性質及影響範圍，並向管理人（校長）報告。
3. 自本校知悉個人資料事故發生之時起 72 小時內，由執行秘書代表本校依主管機關規定之方式向主管機關通報，並填寫「個人資料侵害事故通報與紀錄表」。
4. 通報事項應包含：事件發生時間、事件種類、影響之個資筆數（區分一般個資與特種個資）、發生原因、損害狀況、擬採取之因應措施等。

（三）應變措施（控制損害）

1. 採取即時有效之應變措施，防止事故擴大：包括立即中斷相關系統存取、暫停相關作業程序、隔離受影響之資料等。
2. 對事件的影響與衝擊程度進行全面評估，確定洩漏資料的範圍、性質以及對當事人和機構的潛在風險。
3. 記載相關事實、影響、已採取之因應措施，並保存相關紀錄以備主管機關查驗。

（四）通知當事人程序

經查明個人資料事故後，本校應儘速以適當方式通知當事人下列事項：

1. 個人資料事故發生之事實。
2. 本校已採取之處理措施。
3. 本校提供當事人之聯絡窗口電話及其他聯絡資訊。

通知方式包括：

(1) 透過電話、電子郵件、書面等方式直接通知當事人。

(2) 若事故較為嚴重或當事人眾多而難以直接通知者，得於本校網站公告，並提供具體之聯絡管道。

（五）預防機制之研議

事故處理完畢後，應對事故原因進行深入分析，並研擬矯正預防措施，避免類似事件再次發生。事故自發生起至結束，應產出下列文件：

1. 個人資料侵害事故通報與紀錄表。
2. 事件處理經過紀錄。
3. 事故原因分析報告。
4. 改善措施及改善追蹤紀錄。
5. 本委員會審查會議紀錄。

五、個人資料蒐集、處理及利用之內部管理措施

一. 向當事人蒐集個人資料時，除《個人資料保護法》第 8 條第 2 項所列免告知情形外，需經當事人同意並明確告知蒐集目的、個人資料類別、利用期間、地區、對象及方式。

二. 蒐集個人資料應符合特定目的，並確保資料之正確性、完整性及時效性。

三. 當事人得依《個人資料保護法》第 3 條規定，向本校請求閱覽、製給複製本、補充或更正、停止蒐集處理利用或刪除其個人資料。當事人權利行使之聯絡窗口為執行秘書，公告於本校網站首頁及行政大樓公告欄。如拒絕當事人行使上述權利，應附理由通知當事人。

四. 所蒐集之個人資料非由當事人提供者，應於處理或首次利用前，向當事人告知其個人資料來源及應告知事項。若當事人表示拒絕接受行銷，本校應立即停止利用其個人資料進行行銷。

五. 本校保有之個人資料利用期限屆滿時，除因法令規定、執行業務所必須或經當事人書面同意者外，將主動刪除或銷毀其個人資料，並留存相關紀錄。

六. 負責保管及處理個人資料檔案之人員，其職務有異動時，應將所保管之儲存媒體及有關資料檔案完整移交，並留存交接紀錄。

七. 本校所屬人員輸出、輸入個人資料時，須輸入個人使用者帳號及識別密碼，並在使用範圍及使用權限內為之。識別密碼應保密，不得洩漏或與他人共用。

八. 本校所屬人員離職時，即時取消其登錄電腦之使用者帳號及識別密碼，其在職期間所持有之個人資料應確實移交，不得私自複製或留存。

九. 各處室主任應每學年檢視本處室所保有之個人資料是否符合特定目的，若有非屬特定目的必要範圍之資料，或特定目的消失、期限屆滿而無保存必要者，即予刪除、銷毀或其他適當處置，並留存相關紀錄。

十. 本校保有之個人資料如需作特定目的外利用，應先行檢視是否符合《個人資料保護法》第 20 條第 1 項但書之規定，並經執行秘書簽報管理人核可。

十一. 本校委託他人蒐集、處理或利用個人資料時，應對受託者為適當之監督，並依《個人資料保護法施行細則》第 8 條規定於契約中明確約定監督事項。委外業務由各業務權責處室辦理監督。

六、實體環境安全管理、資料安全管理及人員管理措施

（一）實體環境及設備安全管理

1. 本校機房為個人資料保護之核心區域，由資訊組主要管理；總務處持有機房備用鑰匙，任何人進出機房仍需向資訊組登記，並由資訊組人員陪同才可進入。
2. 指派專人管理儲存個人資料之電腦及其他儲存媒介物，定期清點、保養維護、資料備份，並注意設備防竊、未經授權攜出等安全措施。
3. 重要個人資料備份應異地存放，並建置防止個人資料遭竊取、竄改、損毀、滅失或洩漏等事故之機制。
4. 建置個人資料之個人電腦，不得直接作為公眾查詢之前端工具。
5. 電腦、資訊設備、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，由資訊組確認個人資料已確實刪除，並留存清除紀錄。
6. 各處室辦公室應加裝門禁或於非上班時間鎖門；辦公室內存有個人資料之檔案櫃應上鎖，鑰匙由各處室主任指定人員保管。
7. 各棟大樓網路、光纖等機櫃需上鎖，並由資訊組保管鑰匙，非經同意，任何人皆不得自行開啟使用。

（二）資(通)訊系統資料安全管理

本校自建及維運之校內資訊系統（包括校務行政系統、Google Workspace 教育版、校內電腦、伺服器主機及網路設備等），對其所保有及處理之個人資料採取下列資訊安全管理措施：

1. 使用者身分確認：於儲存個人資料之電腦及系統設置識別密碼、保護程式密碼及相關安全措施。
2. 個人資料顯示之隱碼機制：對系統輸出畫面及紙本輸出資料，將身分證字號、電話等敏感欄位進行部分遮罩處理。
3. 網際網路傳輸之安全加密機制：對外連線採 SSL/TLS 加密，遠端連線使用 VPN。
4. 個人資料檔案與資料庫之存取控制及保護監控措施：資料庫存取權限限最小必要範圍，並定期審查存取紀錄。
5. 防止外部網路入侵對策：部署防火牆、防毒軟體、入侵偵測系統，並區隔內外網路。
6. 非法或異常使用行為之監控及因應機制：監控系統日誌，設定異常告警機制。
7. 個人資料檔案使用完畢應即關閉檔案，不得任其停留於螢幕上。

8. 所屬人員非經權責主管核可，不得任意複製本校保有之個人資料檔案。

至於本校保有之特種個人資料（學生健康檢查資料），係使用教育部委託南華大學建置之「學生健康資訊系統」（SSHIS/shiscloud）辦理，本校為該系統之使用者，由健康中心校護執行資料登打作業。該系統之伺服器主機、傳輸加密、防火牆、內外網區隔、系統日誌監控、入侵偵測等資通訊安全管理措施，屬平台方（教育部委辦團隊）之管理權責範圍；本校之配合面在於使用者帳號權限管理及系統輸出資料之隱碼處理（詳前開第 1、2 項），其餘平台層之資安事項依平台方規範辦理。

（三）紙本資料之保管

1. 記載有個人資料之紙本文件，在未使用時存放於公文櫃內並上鎖。所屬人員非經權責主管核可，不得任意複製、拍攝或影印。
2. 丟棄記載有個人資料之紙本文件時，應先以碎紙設備進行處理或委外銷毀，並留存銷毀紀錄。
3. 各處室應建立紙本個人資料之調閱申請單或存取登記簿，記錄調閱人、時間、目的及範圍。

（四）人員管理

1. 依業務需求適度設定所屬人員（主管、非主管人員）對個人資料蒐集、處理及利用之不同權限。
2. 所屬人員登錄電腦之識別密碼，應定期變更（至少每 3 個月一次）。
3. 所屬人員應妥善保管個人資料之儲存媒介物，執行業務時依《個人資料保護法》規定蒐集、處理及利用個人資料。
4. 本校與所屬人員之勞務、承攬及委任契約均列入保密條款及違約罰則，以促使其遵守個人資料保密義務（含契約終止後）。
5. 所屬人員（含新進、離職、異動）應簽署個人資料保密切結書，由人事室彙整保存。
6. 所屬人員離職時，應即取消其電腦使用者帳號及識別密碼，其在職期間所持有之個人資料應確實移交，不得私自複製、留存並在外繼續利用。

七、認知宣導及教育訓練

一. 本校每學年至少辦理一次全校教職員個人資料保護法規宣導或教育訓練，由執行秘書規劃辦理。

二. 教育訓練應留存相關紀錄或佐證資料（例如：簽到表、教材、時數認證等）。

三. 對於新進人員，於報到時給予個人資料保護特別指導，確保其明瞭個人資料保護相關法令規定及責任範圍。

四. 各處室應派員參加教育訓練，並將本處室業務相關之個資保護要點納入處室內部業務講習。

八、個人資料安全維護內部稽核機制

一. 本校每學年至少辦理一次本計畫及處理方法執行情形之內部稽核，由稽核人員依教育部主管目的事業之個人資料檔案自我檢查表相關項目辦理。

二. 稽核人員由校長指定，依《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》第 3 條第 3 項規定，稽核人員不得為執行秘書。

三. 稽核結果應以書面報告陳報管理人及本委員會，相關文件至少保存 5 年。

四. 若稽核結果發現不符合法令或有不符合之虞，依下列事項規劃改善措施：

（1）確認不符合法令之內容及發生原因。

（2）提出改善及預防措施方案，指定改善責任單位及期限。

（3）紀錄稽核情形、改善進度及改善結果。

五. 稽核人員應追蹤前次稽核所提改善事項之落實情形。

九、使用紀錄、軌跡資料及證據保存

一. 本校建置個人資料之電腦及系統，其個人資料使用查詢紀錄（含 LOG 紀錄），應定期備份並設定密碼保存。

二. 個人資料使用紀錄以紙本登記者（如各處室之調閱申請單、存取登記簿），應存放於公文櫃內並上鎖，非經權責主管核可不得任意取出。

三. 以上使用紀錄、軌跡資料及相關證據至少留存 5 年，作為稽核及事故調查之依據。

四. 軌跡紀錄之管理由資訊組負責電子系統面，紙本部分由各業務權責處室負責。

十、個人資料安全維護之整體持續改善

本校將隨時參酌業務執行狀況、技術發展、法規變動及主管機關檢查結果等因素，檢討本計畫是否合宜，必要時由本委員會提出修正建議，經委員會議通過並陳請校長核可後修正發布，並於修正後保存備查。

陸、業務終止後之個人資料處理方法

本校業務終止（含全校性業務停辦、部分業務停辦、單一契約終止等）後，所保有之個人資料依下列方式處理，不再繼續使用，並將相關紀錄陳報主管機關：

（一）銷毀

1. 銷毀方法：紙本資料以碎紙機絞碎或送焚化處理；電腦磁碟及其他媒介物之資料，以消磁、折斷光碟片、擊毀硬碟等物理方式破壞。
2. 銷毀時間及地點：由執行秘書會同相關處室確定執行時間及地點。
3. 銷毀證明：留存銷毀作業紀錄，包含執行銷毀之照片或影片（標註日期、地點），並由執行人員簽章。

（二）移轉

1. 移轉原因：如業務合併、由他校辦理等。
2. 移轉對象：符合法定要件之接收機關或機構。
3. 移轉方法：紙本移交，或以電腦磁碟、磁帶、光碟片、微縮片、積體電路晶片等儲存媒介物傳遞。
4. 移轉時間及地點：由執行秘書會同相關處室確定。
5. 受移轉對象保有該項個人資料之合法依據：依《個人資料保護法》相關規定辦理。

（三）其他處置

採用其他刪除、停止處理或利用個人資料之方法者，應留存書面紀錄，說明方法、時間、地點及理由。

（四）業務終止之留存紀錄

本校業務終止之個人資料檔案清冊、處置紀錄應由執行秘書統籌保存，並依本計畫第伍章第九節之保存年限規定辦理。

柒、附　　則

一. 本計畫經個人資料保護委員會議通過，並陳請校長核可後施行；修正時亦同。

二. 本計畫未盡事宜，依《個人資料保護法》、《個人資料保護法施行細則》、《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》及其他相關法規辦理。

三. 本計畫相關表單、清冊、紀錄格式，由執行秘書另行訂定並公告使用。