宏國學校財團法人宏國德霖科技大學
個人資料保護政策

民國106年1月19日105學年度第1學期第1次資訊安全暨個人資料保護委員會議通過
民國106年7月25日105學年度第2學期第3次校務會議修正通過
民國115年7月1日114學年度第2學期第1次資訊安全暨個人資料保護委員會議修正通過

1 總則

1.1 為保護宏國學校財團法人宏國德霖科技大學（以下簡稱「本校」）於各項業務作中秉持落實個人資料保護及管理措施，免於個人資料因內部或外部、蓄意或意外之各種威脅與破壞，致使資料外洩、資料不正確、資料無法正常使用或資訊遭受竄改、揭露、破壞或遺失等風險，落實個人資料之保護及管理並符合「個人資料保護法」、「個人資料保護法施行細則」及國際標準之要求，特制訂本政策。

1.2 本政策適用之範圍係含全校各單位之個人資料管理與處理相關業務。

1.3 本校教職員、委外廠商及相關接觸個人資料相關業務之第三方人員均應遵守本政策。

2 目標

2.1 本校之個人資料保護政策包含下列目標：

2.1.1 已成立個人資料保護組織，明確定義相關人員之責任與義務。

2.1.2 已建立與實施隱私資訊管理系統（Privacy Information Management System，以下簡稱 PIMS），以確認本政策之實行；全體員工及委外廠商應遵循隱私資訊管理系統（PIMS）之規範與要求。

2.1.3 基於合法的組織目的，在必要範圍內蒐集最少的必要個人資訊，且採行適當安全措施，確保個人資訊被公平合法的處理及利用。

2.1.4 建立本校個人資料盤點清單，並維持所經手個人資訊的正確性，並於必要時進行更新。

2.1.5 建立當事人對其個人資料所能行使之權利，包含查詢或請求閱覽、請求製給複製本、請求補充或更正、請求停止蒐集、處理或利用與請求刪除等。

3 個人資料保護安全準則

3.1 維持個人資料的正確性，並透過實施適當技術面與組織面的安全機制與控制措施，確保個人資料檔案的安全。

3.2 蒐集的個人資料將會依法進行保存，並定期檢視資料保存的必要性，以確保資料保存的適法性與合理性。

3.3 建立與實施個人資料管理制度並持續維運改進，讓個人資料保護政策落實。

3.4 規劃緊急應變程序要點以處理個人資料被竊取、竄改、毀損、滅失或洩漏等事故。

3.5 揭露個人資料予第三方之相關作業應遵循相關法令規章之要求，如有委託蒐集、處理及利用個人資料時，應對受託者為適當之監督。

3.6 個人資料之蒐集、處理及利用過程應適當留存軌跡紀錄。

3.7 辨識內外部利害關係者及其參與個人資料管理制度治理與運作的程度，並將以適當方式向相關利害團體提供個人資料保護政策，以增進其對政策內容及要求的了解。

3.7.1 內部全景議題，可分為組織管理層面(安全政策、管理者支持、安全組織與措施、風險管理、文件控管程序、事故應變程序、存取權限控管等)、人事層面(安全意識建立、持續教育訓練、保密、安全通報等)、技術層面(安全的資訊環境、安全的應用軟體開發、軟體與硬體維護、安全通訊、網路環境安全、防範惡意軟體、存錄等)、實體安全層面(進出管理、場域安全、設備安置及保護等) 、個人資料流程賦予角色(PII 控制者、PII 處理者、PII 聯合控制者)及氣候變遷相關議題。

3.7.2 外部全景議題，考量現行作業之各項外部環境議題，包括自然環境災害、法令要求、客戶要求、公共資源提供、外包服務及氣候變遷議題等。

3.7.3 各關注方(內外部關注方)，如主管單位(之法令法規)、客戶(之合約內容需求)、外包商(之合約及管理需求)、高階主管、本校董事會(穩定永續經營)等。

4 責任

4.1 為能有效確保本校之個人資料保護安全，應針對各個人資料保護安全領域訂定管理規範。

4.2 應每年至少召開 1 次管理審查會議，審核個人資料保護安全業務執行狀況，建立管理指標量測方式與評估管理指標量測結果。

4.3 高階主管應積極參與個人資料保護安全管理活動，提供對個人資料保護安全之支持及承諾。

4.4 所有相關同仁皆應遵循本校個人資料保護安全事件通報機制，並每年演練 1 次通報程序演練作業。若發生個人資料外洩事件，應依主管機關規定之時效與程序進行通報。

4.5 應建立個人資料盤點作業及隱私風險評鑑機制，每年至少進行 1 次隱私風險評鑑，並訂定可接受風險值。

4.6 每年應規劃並提供本校人員資訊安全與個人資料保護通識課程，以提昇人員資訊安全與個人資料保護安全認知。

4.7 與本校簽署合約之委外廠商應簽署保密協議書，並遵循本政策以及相關程序之規定，不得未經授權使用或濫用各類有關個人資料內容。

4.8 組織全景於管理審查會議，將與隱私資訊管理系統相關之關注方需求和期望的變更、關注方的回饋等進行報告，並評估氣候變遷是否為相關議題、內外部利害相關團體對氣候變遷可提出要求等。

4.9 本校規劃、實作及控制要求事項所需過程之相關準則，並實作控管措施，以「個人資料保護適用性聲明書」作為文件化資訊紀錄，對控制所規劃之變更，需審查非預期變更之後果，必要時採取行動以減輕任何負面效果，藉此確保與隱私資訊管理系統相關的外部提供的過程、

產品或服務受到控制。當學校確定需要對隱私資訊管理系統變更時，應以規劃的方式執行變更。

4.10 於規劃隱私資訊管理系統時，應了解關注方的需要及期望，並依據國際標準之要求事項來建立、實作、維持即持續改善，包括所需過程及其互動，以決定因應之風險及機會，達成隱私資訊管理系統之預期成果、預防或減少非預期的影響、確保持續改善。

4.11 透過所訂定風險接受準則及具備有效、可比較與重複評鑑產生一致結果之原則執行隱私風險評鑑，適切選擇風險處理方法。

4.12 當決定對隱私資訊管理系統進行重大變更時，採事先規畫提請管理審查會議審議後執行變更。

4.13 對於隱私資訊管理系統執行成效，除依擬定適於比較即可重製的監督、量測、分析及評估方法外，應規劃、建立、實作及維持稽核作業，並具備文件化資訊作為稽核活動及結果之佐證。

4.14 當發現不符合事項，應採取行動以控制並矯正，對消除不符合事項之原因及矯正措施進行有效性審查。

5 審查與實施

5.1 本政策應每年定期審議，或因組織、業務、法令或環境等因素之變迭時，予以適當修訂。

5.2 本政策應由資訊安全暨個人資料保護委員會審議通過，呈請校長核定後公布施，修正時亦同。