東莞台商子弟學校資訊安全暨

個人資料檔案安全維護管理辦法

第一條　本辦法依據「個人資料保護法」(簡稱本法）及「海外臺灣學校及大陸地區臺商學校個人資料檔案安全維護計畫實施辦法」第 6 條訂立。

第二條　東莞台商子弟學校(簡稱本校)為維護整體資訊安全與個人資料保護(簡稱資安暨個資保護)，強化各項資訊資產及個人資料保護之安全管理，確保其具機密性、完整性、可用性、鑑別性與不可否認性，以因應業務運作需要，支援教職員工生各應用系統之使用及妥善保護其相關個人資料，特訂定本辦法。

第三條　本辦法相關名詞定義如下：

一、資訊安全：指保護資訊資產，避免遭受各種不當使用、洩漏、竄改、竊取、破壞等事故威脅，並降低可能影響及危害本校業務運作之損害程度。

二、資訊資產：指本校所蒐集、產生、運用之資料與檔案，以及為完成以上工作所需使用之相關設備。其中個人資料相關定義如下：

（一）個人資料：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）個人資料檔案：依系統建立而得以自動化機器，或其他非自動化方式檢索、整理之個人資料之集合。

（三）個人資料管理人：人事主任負責個人資料檔案安全維護及執行，其任務如下：

1. 訂定及執行安全維護計畫，包括業務終止後的個人資料處理方法。

2. 定期就個人資料檔案安全維護管理情形，提出書面報告。

3. 依據稽核人員就安全維護計畫執行之評核，檢討改進後，提出書面報告。

4. 個人資料稽核人員：教務主任為評核安全維護計畫執行及成效之人員（簡稱稽核人員）。

5. 所屬人員：指執行業務之過程，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，均須遵守本辦法；各處室應依業務權責，適時增修與個資保護相關之作業要點及程序。

第四條　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。

第五條　為保護本校資訊資產安全，各處室應建立資訊資產清冊，分類分級，並訂定管制措施。如需利用個人資料為宣傳、推廣或行銷時，應明確告知當事人本校名稱及個人資料來源，並於首次利用個人資料為宣傳、推廣或行銷時，應提供當事人表示拒絕接受宣傳、推廣或行銷之方式；當事人表示拒絕宣傳、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。

第六條　為降低內部人為因素，對本校資安及個資保護之影響，各處室應考量人力與工作職掌，實行分工及輪調措施。本校應視需要實施資安及個資保護教育培訓及宣導，以提高人員對資安暨個資保護之認識。

第七條　避免資訊資產因未授權之存取，而使機密性或敏感性資料遭不當使用，應考量人員職務授予相關權限，必要時得採行加解密及身分鑑別機制，以加強資料安全。

第八條　定期實施各處室標準作業程序，結合個資清查作業，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、銷毀或為其他停止蒐集、處理或利用等適當之處置，以確認保有之個人資料，符合蒐集、處理、利用及銷毀作業之要求。

第九條　各處室之公務資料，應使用本校網路儲存系統、校務行政系統，進行檔案共用存取及保存時，加解密碼，確保個人資料檔案皆經合法授權存取。

第十條　確保網路服務及使用之安全及主機作業平臺及資料庫之安全，應訂定管理安全技術規範。

第十一條　避免資訊資產遭受災害而影響業務運作，應訂定應變及復原計畫，落

實資安暨個資保護管理制度，資安暨個資保護稽核人員，應訂定稽核實施作業要點，並定期測試演練。

第十二條　對個人資料檔案之保存，應針對下列事項，依處室權責設置必要之安全設備及採取防護措施：

一、訂定「資訊安全管理制度」並落實各項作業。

二、訂定紙本資料保存方式、年限及銷毀之標準作業程序。

三、訂定電腦或儲存媒介等廢棄物處理之標準作業流程。

四、訂定電腦安全自我檢查表。

第十三條　為確實保護個人資料之存取安全，應針對下列事項，依處室權責採取防護措施：

一、教職員工到本校任職時，應簽訂保密切結，確保服務期間因職務對所接觸之個人資料應遵守保密義務，離職時亦同，以落實個人資料保護。

二、每年對各處室所屬人員，實施資訊安全及個人資料保護教育培訓，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。

第十四條　各處室執行本辦法各項程序及措施，應保存下列紀錄備查：

一、個人資料之交付及傳輸。

二、個人資料之維護、修正、刪除、銷毀及轉移。

三、提供當事人行使之權利。

四、存取個人資料系統之紀錄。

五、備份及還原之測試。

六、所屬人員權限之異動。

七、所屬人員違反權限之行為。

八、因應事故發生所採取之措施。

九、定期檢查處理個人資料之資訊系統。

十、教育訓練。

十一、安全維護計畫稽核及改善措施之執行。

十二、業務終止後處理紀錄。

第十五條　本校於當事人行使本法第 3 條規定之權利時，得採取下列方式辦理：

一、提供聯絡窗口及聯絡方式。

二、確認是否為資料當事人之本人或經其委託。有本法第 10 條但書、第 11 條第 2 項但書或第 3 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。

第十六條　應訂定應變機制，發生個人資料被竊取、洩露、竄改或其他侵害事故時，迅速處理 以保護當事人之權益。

前項應變機制，應包括下列事項：

一、採取適當之措施，控制事故對當事人造成之損害。

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。

三、研議改進措施，避免事故再度發生。學校應自第一項事故發現之日起三日內，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。

第十七條　本校委託他人蒐集、處理或利用個人資料之全部或部分時，依本法施行細則第 8 條規定，對受託者做適當之監督，並明確約定相關監督事項及方式。

第十八條　本辦法適用於本校各項資訊資產及其個人資料使用者，個人資料及資訊使用者應確實遵守，如有違反者，依相關法令辦理。

第十九條　本辦法經主管會議通過，報教育部核備後實施，修正亦同。