慈濟大學個人資料安全維護辦法

104 年 6 月 26 日第 134 次行政會議審議通過

111 年 3 月 11 日第 187 次行政會議審議通過

第一章 總則

第一條　慈濟大學（以下簡稱本校）為依循「個人資料保護法」（以下簡稱個資法）「私立專科以上學校及私立學術研究機構個人資料檔案安全維護計畫實施辦法」（以下簡稱安全維護實施辦法）之要求，落實個人資料保護及管理，特訂定「慈濟大學個人資料安全維護辦法」（以下簡稱本辦法）。

第二條　本辦法所稱之個人資料、個人資料檔案、蒐集、處理、利用、國際傳輸、當事人，其定義同個資法第二條之規定。

第三條　本校為確實執行個人資料保護及管理，設置「慈濟大學個人資料保護推動委員會」，其設置要點另定之。

第四條　本校對外重大個人資料安全事件之聯繫窗口，由秘書室擔任之。

第五條　本校各權責單位應由單位主管指定單位個人資料保護業務聯絡人（以下簡稱個資業務聯絡人）。個資業務聯絡人負責校內個資相關業務之聯絡窗，並負責督導其單位內同仁辦理下列事項：

一、單位內個人資料保護相關業務（含個人資料盤點及風險評鑑）之執行與檢核。

二、依個資法規定之當事人個人資料蒐集作業程序。

三、依個資法規定之當事人個人資料處理、利用或國際傳輸作業程序。

四、依個資法規定之當事人請求個人資料查詢、閱覽或製給複製本之作業程序。

五、依個資法規定維護個人資料之正確、刪除、停止蒐集、處理或利用個人資料之作業程序。

六、單位內個人資料遭竊取、竄改、毀損、滅失、洩漏之預防、危機處理、應變及通報等作業程序。

七、本校個人資料保護相關業務之協調、聯繫。

第二章 個人資料範圍、蒐集、處理及利用

第六條　本校對個人資料之蒐集、處理及利用，應尊重當事人之權益，依誠實及信用方法為之，不得逾越特定目的之必要範圍，並應與蒐集之目的具有正當合理之關聯。

第七條　對個人資料之蒐集或處理，除個資法第六條第一項所規定資料外，應有特定目的，並符合個資法第十九條第一項之規定，且明確告知當事人下列事項：

一、機關或單位名稱。

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、當事人依個資法第三條規定得行使之權利及方式。
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。
符合個資法第八條第二項各款規定情形之一者，得免為前項之告知。

第八條　各單位蒐集非由當事人提供之個人資料，應於處理或利用前，向當事人知個人資料來源及前條第一項第一款至第五款所列事項。但符合個資法第九條第二項各款規定情形之一者，不在此限。前項之告知，得於首次對當事人之個人資料為利用時併同為之。

第九條　各單位依個資法第十九條第一項第五款及第二十條第一項但書第六款規定蒐集、處理或利用當事人個人資料時，應取得當事人書面授權同意書。當事人為限制行為能力人，其授權同意應得法定代理人之允許。當事人為無行為能力人，應由法定代理人代為授權同意。

第十條　各單位對個人資料之利用，應符合個資法第二十條之規定。

第十一條　各單位負責保管及處理個人資料檔案之人員，其職務有異動時，應將所保管之相關個人資料檔案移交，以利控管。

第十二條　各單位須定期清查所保有之個人資料是否符合蒐集之特定目的，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、銷毀或為其他適當處置，並保存相關紀錄以供查驗。但符合個資法第十一條第三項但書情形者，不在此限。

第十三條　本校遇有個資法第十二條所定個人資料被竊取、洩漏、竄改或其他侵害情事者，應進行緊急因應措施，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。
並自第一項事故發現時起七十二小時內，填具個人資料侵害事故通報與紀錄表（如附件），通報教育部，未依時限內通報者，應附理由說明；並自處理結束之日教育部備查。

第十四條　本校依個資法第二十條第一項規定利用個人資料為宣傳、推廣或行銷時，應明確告知當事人學校單位名稱及個人資料來源。
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，並支付所需費用；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，並周知本校相關人員。

第十五條　本校於當事人行使個資法第三條規定之權利時，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。

三、有個資法第十條但書、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。

四、告知是否酌收必要成本費用及其收費基準，並遵守個資法第十三條處理期限規定。

第十六條　本校業務終止後，其保有之個人資料之處理方式及留存紀錄如下：

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、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。

第十七條　本校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。包括下列事項：

一、紙本資料檔案之安全保護設施及管理程序。

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。

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。

第三章 個人資料安全管理措施

第十八條　本校提供電子商務服務系統或個資法第六條所定個人資料種類之資通系統時，應採取下列資訊安全措施：

一、使用者身分確認及保護機制。

二、個人資料顯示之隱碼機制。

三、網際網路傳輸之安全加密機制。

四、應用系統於開發、上線、維護等各階段軟體驗證及確認程序。

五、個人資料檔案與資料庫之存取控制及保護監控措施。

六、防止外部網路入侵對策。

七、非法或異常使用行為之監控及因應機制。

第十九條　本校進行個人資料國際傳輸前，應檢視有無教育部依個資法第二十一條規定為國際傳輸之限制，並且告知學生及教職員其個人資料所欲國際傳輸之區域，同時對資料接收方為下列事項之監督：

一、預定處理或利用個人資料之範圍、類別、特定目的、期間、地區、對象及方式。

二、當事人行使個資法第三條所定權利之相關事項。

第二十條　本校對個人資料之蒐集、處理及利用，除應符合個資法之規定，並視需要定期或不定期對教職員工及學生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。

第二十一條　為提高委外作業之資訊安全，本校應要求受託者簽署保密協議或契約書，訂定相關委外專案人員各項資訊安全之責任及違反之罰則，並明確約定資料存取權限、保存期限及銷毀方式。

第二十二條　為避免本校蒐集、產生、運用之個人資料或檔案因未授權存取而使機密性或敏感性資料遭不當使用，應考量人員職務而授予相關權限，必要時得採行加解密及身分鑑別機制，以加強資料之安全。

第二十三條　個人資料檔案安全維護工作，除本辦法外，並應符合法令、主管機關及本校訂定之相關個人資料保護、資訊作業安全與機密維護規範。

第四章　附則

第二十四條　為強化本校個人資料保護管理制度之有效性，應定期或不定期辦理個人資料保護管理稽核，稽核成員得由本校內部控制稽核人員或具個資稽核相關證照之專家組成之，本校各單位對稽核人員之稽核應予以配合。稽核結果應提報校長。

第二十五條　本辦法如有未盡事宜，依相關規定辦理或由本校個人資料保護推動委員會檢討修正之。

第二十六條　本辦法經行政會議審議通過，陳請校長核定後公布實施，修正時亦同。