花蓮縣壽豐鄉豐山國民小學個人資料保護管理政策

一、花蓮縣壽豐鄉豐山國小(以下簡稱本校)為落實個人資料之保護及管理，特訂 定本要點。

二、本校各處組應指定專人辦理下列事項:

1. 當事人依個人資料保護法(以下簡稱本法)第十條及第十一條第一項至第四項
所定請求之考核。
2. 本法第十一條第五項及第十二條所定通知之考核。
3. 本法第十七條所定公開或供公眾查閱。
4. 本法第十八條所定個人資料檔案安全維護。
5. 依前款所為擬議之執行。
6. 個人資料保護事項之協調聯繫。
7. 處組內個人資料損害預防及危機處理應變之通報。
8. 本校個人資料保護方針及政策之執行、處組內個人資料保護之自行查核。
9. 其他單位內個人資料保護管理之規劃及執行。

三、本校應設置個人資料保護聯絡窗口，辦理下列事項:

1. 公務機關間個人資料保護業務之協調聯繫及緊急應變通報。
2. 非資訊面個人資料安全事件之通報。
3. 重大個人資料外洩事件之民眾聯繫單一窗口。
4. 本校個人資料專人名冊之製作及更新。
5. 本校個人資料專人與職員工教育訓練名單及紀錄之彙整。

四、本校蒐集、處理或利用個人資料之特定目的，以本校依適當方式公開者為限。有變更者，亦同。

五、各處組對於個人資料之蒐集、處理或利用，應確實依本法第五條規定為之。

六、各處組蒐集當事人個人資料時，應明確告知當事人下列事項。但符合本法第八條第二項規定情形之一者，不在此限:

1. 機關或單位名稱。
2. 蒐集之目的。
3. 個人資料之類別。
4. 個人資料利用之期間、地區、對象及方式。
5. 當事人依本法第三條規定得行使之權利及方式。
6. 當事人得自由選擇提供個人資料時，不提供對其權益之影響。

七、各處組蒐集非由當事人提供之個人資料，應於處理或利用前， 向當事人告知個人資料來源及前點第一款至第五款所列事項。但符合本法第九條第二項 規定情形之一者，不在此限。前項之告知，得於首次對當事人為利用時併同 為之。第一項非由當事人提供之個人資料，於本法修正施行前即已蒐

集者， 除有本法第九條第二項所定免為告知之情形外應自本法修正施行之日起一年內完成本法第九條第一項所列事項之告知。

八、各處組依本法第十五條第二款及第十六條但書第七款規定經當事人書面同意者，應取得當事人同意書。

九、各處組依本法第十五條或第十六條規定對個人資料之蒐集、處理、利用時，應詳為審核並簽奉核定後為之。 各處組依本法第十六條但書規定對個人資料為特定目的外之利用，應將個人資料之利用歷程做成紀錄。對於個人資料 之利用，不得為資料庫之恣意連結，且不得濫用。

十、本校保有之個人資料有誤或缺漏時，應由資料蒐集處組簽奉核定後，移由資 料保有處組更正或補充之，並留存相關紀錄。 因可歸責於本校之事由，未 為更正或補充之個人資料，應於更正或補充後，由資料蒐集處組以通知書通 知曾提供利用之對象。

十一、本校保有之個人資料正確性有爭議者，應由資料蒐集處組簽奉核定後，移 由資料保有處組停止處理或利用該個人資料。但符合本法第十一條第二項但 書情形者，不在此限。個人資料已停止處理或利用者，資料保有單位應確實 記錄。

十二、本校保有個人資料蒐集之特定目的消失或期限屆滿時，應資料蒐集單位簽 奉核定後，移由資料保有處組刪除、停止處理 或利用。但符合本法第十一條第三項但書情形者，不在此限。個人資料已刪除、停止處理或利用者，各 該處組應確實記錄。

十三、各處組依本法第十一條第四項規定應主動或依當事人之請求刪除、停止蒐 集、處理或利用個人資料者，應簽奉核定後移由資料保有處組為之。個人資 料已刪除、停止蒐集、處理或利用者，資料保有處組應確實記錄。

十四、本校遇有本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，經查明後，應由資料外洩處組以適當方式儘速通知當事人。

十五、當事人依本法第十條或第十一條第一項至第四項規定向本校為請求時，應 檢附相關證明文件向本校正式提出書面申請為之。 申請案件有下列情形之一者，應以書面駁回其申請:

1. 申請書件內容有遺漏或欠缺，經通知限期補正，逾期仍未補正。
2. 有本法第十條但書各款情形之一。
3. 有本法第十一條第二項但書或第三項但書所定情形之一。 4. 與法令規定不符。

十六、當事人依本法第十條規定提出之請求，應於十五日內為准駁之決定。前項 之准駁決定，必要時得予延長，延長期間不得逾十五日，並應將其原因以書 面通知請求人。 當事人閱覽其個人資料，應由承辦單位派員陪同為之。

十七、當事人請求查詢、閱覽或製給個人資料複製本者，準用彰化政府及所屬

機 關學校提供政府資訊收費標準收取費用。

十八、當事人依本法第十一條第一項至第四項規定提出之請求，應於三十日內為 准駁之決定。前項之准駁決定，必要時得予延長，延長期間不得逾三十日，並應將其原因以書面通知請求人。

十九、個人資料檔案，其性質特殊或法律另有規定不應公開其檔案名稱者，得依政府資訊公開法或其他法律規定，限制公開或不予提供。

二十、為防止個人資料被竊取、竄改、毀損、滅失或洩漏，本校指定之個人資料檔案安全維護專人，應依本要點及相關法令規定辦理個人資料檔案安全維護事項。

二十一、個人資料檔案應建立管理制度，分級分類管理，並針對接觸人員建立安全管理規範。

二十二、為強化個人資料檔案資訊系統之存取安全，防止非法授權存取，維護個人資料之隱私性，應建立個人資料檔案安全稽核制度。前項個人資料檔案資訊系統之帳號、密碼、權限管理及存取紀錄等相關管理事宜，依本府「網路安全管理規範」、「網路管理作業要點」及「存取控制管理規範」辦理之。第一項個人資料檔案安全稽核之運作組織、稽核頻率及稽核所應注意之相關事項，依本校資訊安全管理系統（ISMS）相關文件辦理之。

二十三、各處組遇有個人資料檔案發生遭人惡意破壞毀損、作業不慎等危安事件，或有駭客攻擊等非法入侵情事，如屬非資訊面之個資外洩事件，應進行緊急因應措施，並迅速簽報；如屬資訊面之個資外洩事件，應依「資訊安全事件通報級管理規範」及「資訊安全事件通報應變作業要點」迅速通報至本校資訊組，並由本校資安聯絡人通報至行政院國家資通安全會報緊急應變中心。

二十四、本校依本法第四條規定委託蒐集、處理或利用個人資料者，適用本要點。

二十五、本要點由 鈞長核可後實施，修正時亦同。