新竹縣十興國民小學個人資料保護管理要點

一、新竹縣十興國民小學（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、本校應指定專人辦理單位內之下列事項：

(一)辦理當事人依個人資料保護法（以下簡稱個資法）第十條及第十一條第一項至第四項所定請求事項之考核。

(二)辦理個資法第十一條第五項及第十二條所定通知事項之考核。

(三)個資法第十七條所定公開或供公眾查閱。

(四)個資法第十八條所定個人資料檔案安全維護。

(五)個人資料保護法令之諮詢。

(六)個人資料保護事項之協調聯繫。

(七)各處室個人資料損害預防及危機處理應變之通報。

(八)個人資料保護之自行查核及本校個人資料保護政策之執行。

(九)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：

(一)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。

(二)非資訊面個人資料安全事件之通報。

(三)重大個人資料外洩事件之民眾聯繫單一窗口。

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

五、各處室對於個人資料之蒐集、處理或利用，應確實依個資法第五條規定為之。

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

(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。

(六)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、各處室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。但符合個資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。

八、各處室依個資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，應符合個資法第七條、個資法施行細則第十四條及第十五條所定之方式。

九、各處室依個資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，應詳為審核並將其審核結果於個人資料檔案中記明後為之。

各單位依個資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，應由資料蒐集單位簽奉核定後，移由資料保有單位更正或補充之，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，由資料蒐集處室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，應由資料蒐集單位簽奉核定後，移由資料保有單位停止處理或利用該個人資料。但符合個資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，應由資料蒐集單位簽奉核定後，移由資料保有單位刪除、停止處理或利用。但符合個資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，資料保有單位應予以確實記錄。

十三、 各處室依個資法第十一條第四項規定刪除、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室為之。

個人資料已刪除、停止蒐集、處理或利用者，資料保有處室應予以確實記錄。

十四、 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，經查明後，應由資料外洩單位以適當方式儘速通知當事人。

十五、 當事人依個資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，應填具申請書，並檢附相關證明文件。

前項書件內容，如有遺漏或欠缺，應通知限期補正。

申請案件有下列情形之一者，應以書面駁回其申請：

(一)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。

(二)有個資法第十條但書各款情形之一。

(三)有個資法第十一條第二項但書或第三項但書所定情形。

(四)與法令規定不符。

十六、 當事人依個資法第十條規定提出之請求，本校應於十五日內為准駁之決定。

前項准駁決定期間，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「新竹縣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、 當事人依個資法第十一條第一項至第四項規定提出之請求，本校應於三十日內為准駁之決定。

前項准駁決定期間，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，依縣府「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「資訊安全事件通報程序」迅速通報至本校資安聯絡人，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、個人資料檔案安全維護工作，除本要點外，並應符合行政院及本校訂定之相關資訊作業安全及機密維護規範。

二十五、本校依個資法第四條規定委託蒐集、處理或利用個人資料之受託者，於適用個資法範圍內，應適用本要點。

二十六、本要點由校長核可後實施，修正時亦同。