和春技術學院人員管理措施要點

一、人員管理措施

（一）依據作業之必要，設定本校所屬人員關於個人資料蒐集、處 理或利用，以及保有個人資料媒體之相關權限，且定期確認 權限內容設定之適當與必要性。

（二） 本校所屬人員應落實本程序書中各項安全管理措施之執行。（三） 本校所屬人員調離職務時，應將所保管之個人資料，返還本 校或刪除、銷毀。並移除或停止其所擁有之個資相關權限。

（四） 應與本校所屬人員約定保密義務，至少應包括下列內容：

1. 個資蒐集、處理及利用之注意義務。
2. 蒐集、處理及利用之個資之範圍。
3. 保密義務期間，應及於人員調離職務之後。
4. 人員調離職務時，其所保管之個人資料，應返還本校或加 以刪除、銷毀。

二、個人資料之傳輸

（一） 個人資料之傳輸應有妥善的安全措施。

（二）在本校內之傳輸，屬於高風險個資（本校依第肆章個資風險 評估作業後，所評定屬於較高風險之個資，本校可依自身業 務特質自行決定高風險個資之範圍）者，由承辦人員親送。

（三）在本校外之傳輸，屬於高風險個資者，應由承辦人員親送。 屬於非高風險個資者，得由承辦人員所指定人員傳輸，或以 掛號函件傳輸。

（四）個人資料非由承辦人員親送者，應密封交遞。以電子通信工 具傳輸高風險個資者，應以適當加密機制傳輸。

三、 個人資料之複製 個人資料如於作業過程中有複製之必要，其複製品應視同原 件妥善保管，無繼續使用之必要時，應即銷燬。

四、 個人資料之保管

（一） 依據作業內容之不同，實施適宜之進出管制方式。

（二） 妥善保管個人資料之儲存媒介物。

（三） 針對不同媒介物存在之環境，審酌建置適度之保護設備或技 術。

（四） 針對所保有之個人資料內容，如有加密之需要，於蒐集、處理或利用時，宜採取適當之加密機制。

（五） 高風險個資檔案應保管於辦公處所；其有攜離必要者，須經單位主管或其授權之具管理職責之人員核准。

(六)高風險個資檔案之存放場所，對於人員及物品之進出，應予 以管制，並造冊列管，載明進出人員、時間及目的。