**天主教崇光學校財團法人新北市崇光高級中學
個人資料保護與安全管理計畫**

中華民國114年 8 月 8 日 行政會議通過

**一、依據**

本計畫是依照「私立高中以下學校及幼兒園個人資料安全維護辦法」來制定的。

**二、目的**

為了防止個人資料被偷看、改掉、損壞、遺失或外洩，本校人員處理個人資料時，必須依照本計畫執行，包含工作結束後的資料處理。

**三、計畫成員**

1. **主任管理人**：由校長擔任，負責指導和評估整體執行狀況。
2. **個人資料管理人（簡稱管理人）**：由各處室主任擔任，負責部門內的個資安全，並將工作流程與重點納入部門的管理制度。

(1)若發生資料外洩或損壞，需立刻處理並寫報告給主任管理人。

(2)配合稽核後的建議做修正，並報告主任管理人。

1. **稽核人員**：由校內內部稽核人員負責，在例行稽核時一併檢查個資安全計畫的執行情況。
2. **所屬人員**：指在工作中接觸個資的人員，包括全職、兼職或派遣員工。

**四、資料安全管理措施**

1. 沒有公務需要時，不得將存有機密資料的隨身儲存裝置帶離辦公室。
2. 共同使用的隨身儲存裝置，使用後請將資料刪除。
3. 個資要經過授權才能提供，若用網路傳送，須加密。
4. 個資要備份，備份資料須和原件一樣被妥善保護。
5. 到期的個資需記錄後報請校長核准再銷毀，紙本資料需用碎紙或焚燒處理，電子媒體要消磁、剪斷或敲碎處理。
6. 委外處理時，需簽訂合約保護個資，並派人監督處理過程並保留證明。

**五、人員管理措施**

1. 根據工作內容設定不同權限的帳號密碼登入系統使用個資。
2. 若需使用非自己權限範圍內的個資，需事前申請並經主管核可。
3. 所有人員在校工作期間接觸到的個資，都需保密。

**六、設備安全管理措施**

1. 紙本資料要放在鎖起來的櫃子或檔案室中，僅限授權人員使用；電腦主機要放在受控的機房中。
2. 員工應保管好電腦與資料設備，設定登入與螢幕保護密碼；下班前應關閉電腦，並鎖好資料。
3. 保管資料的地點需有防火與防盜措施；主機要有防火牆，機房需有門禁、監視器與防火設備。

**七、工作結束後資料處理方式**

1. 若因工作結束、契約到期或法律規定需要銷毀資料時，紙本資料需碎紙或焚燒處理，電子媒體需消磁、剪斷或敲碎。
2. 銷毀前須報主任管理人核准，並記錄時間、地點，拍照或錄影備存。

**八、本計畫經行政會議通過，陳請校長核定後實施，修訂時亦同。**