日期：　年　月　日

國立興大附中電腦安全自我檢查暨個資保護檢查表

1121017 版

請檢查個人電腦、公用電腦(保管人)及筆記型電腦，並於檢查結果欄位勾選是否完成簽名，經單位主管核章後，送交稽核單位彙整，本表確實檢查，以維安全。

單位：＿＿＿＿＿＿職稱：＿＿＿姓名：＿＿＿＿單位主管：＿＿＿＿＿

編號	檢查項目	檢查說明	檢查結果	個人電腦資訊安全設定操作手冊
1	已完成電腦系統帳號密碼設定	1.行政人員及公用電腦均應設置密碼。查看是否需要登入帳號，密碼是否為 8 碼以上。 2.密碼之設定不得與帳號相同。 3.密碼勿記載在他人垂手可得的地方。如：螢幕上	□是 □否	同時按下 Win + I 鍵以便進入 Windows 設定，然後點選「帳戶」-登入選項-右下-密碼。
2	完成螢幕保護密碼設定	電腦螢幕桌面逾時自動進入密碼保護。	□是 □否	電腦的桌面按右鍵-個人化-鎖定畫面-右側-螢幕保護程式設定，等候設定 10 分鐘，勾選「繼續執行後顯示登入畫面」
3	無來路不明或未授權軟體	檢查程式:查看控制台->新增/移除程式或應用程式。如發現來路不明或未授權軟體，請立即移除。	□是 □否	檢查新增移除程式
4	已安裝防毒軟體，並定期更新病毒碼與掃描	檢查電腦是否有安裝正版防毒軟體。定期更新病毒碼與掃描。	□是 □否	可安裝學校防毒軟體(校內安裝)
5	無 eDonkey、BT 等 P2P 軟體及挖礦軟體、遠端遙控軟體	P2P 軟體例如：eDonkey、eMule、ezPeer、BitTorrent(BT)、uTorrent 等名稱。 挖礦軟體執行時會產生高熱，風扇狂轉現象。 遠端遙控軟體：Teamviewer、AnyDesk…等。	□是 □否	檢查新增移除程式
6	開啟 WINDOWS 系統自動更新程式	同仁應配合進行軟體更新，修補漏洞，保持更新至最新狀態，勿自行關閉系統自動更新程式。	□是 □否	設定-更新與安全性-Windows Update
7	無閱覽不當之網站	禁止於上班時間閱覽不當之網路(如暴力、色情、賭博、駭客、惡意網站等)及瀏覽非公務用途網站，以避免內部頻寬壅塞。	□是 □否	
8	機敏性文件安全性	機敏性資料不需使用時置放於上鎖之安全儲櫃或其他安全場所內。 影印機、印表機、傳真機上不留存機敏性文件，應立即取走。 應考量採用辦公桌面的淨空政策，以減少文件及儲存媒體等在正常的辦公時間之外遭未被授權的人員取用、遺失、竄改或是被破壞的機會。	□是 □否	

9	無保存包含學生或教師個資之資料	檢查電腦資料是否曾下載學生資料，例如：通訊錄、辦理保險資料。 以下常見個資來源：校務所需取得教職員工生的相關基本資料時、教職員工生問卷調查、招募教職員工、學生入學登記、學生成績通知、學生輔導作業、繳交相關費用或撥發薪資時。	□是 □否	使用關鍵字查詢，「保險、通訊錄、名冊…」等
10	學校公告欄及個人網站無含有個資之資料	查看學校公告欄及個人經營的網路媒體，例如：個人教學網頁、IGT、BLOG 部落格、FB 臉書…等，上傳含有個資之資料，尤其是 EXCEL 檔容易夾帶其它分頁。	□是 □否	應轉成 PDF 檔後再上傳或傳播，在轉檔時會提醒你有其它的分頁，可避免夾帶含有個資之分頁。