個人電腦資訊安全自我檢查表

紀錄編號：_____ 填表日期： 年 月 日

編號	檢查項目	檢查結果	檢查說明
1	已完成電腦系統帳號密碼設定	□是 □否	個人電腦設備應設定帳號密碼，密碼建議至少每六個月更換一次密碼長度應至少8 碼及穿插特殊字元以符合複雜度。
2	已完成螢幕保護密碼設定	□是 □否	電腦應使用螢幕保護程式，設定螢幕保護密碼，並將螢幕保護啟動時間設定為10 分鐘以內。
3	已關閉資源分享	□是 □否	請勿開啟網路芳鄰分享目錄與檔案，並停用 Guest 帳號。
4	無來路不明或未授權軟體	□是 □否	1.嚴禁下載、安裝或使用來路不明、有違法疑慮（如版權、智慧財產權等）、未經授權或影響電腦網路環境安全之軟體。 檢查重點: .未公告授權使用軟體 .來路不明軟體。 2. 檢查未授權檔案： a. 搜尋:**dat,**mp3,avi,mpg,ape,rm,rmvb 等副檔名。 b. 檢查重點:查看歌曲,影片及其他檔案是否合法授權, 3. 如有發現來路不明或未授權檔案,請立即移除。
5	已安裝防毒軟體	□是 □否	進行下載、複製、使用不明來源檔案前，請確認檔案安全無虞，應先完成掃毒，嚴禁任意移除或關閉防毒軟體。
6	已完成瀏覽器安全設定	□是 □否	IE、Firefox 等相關瀏覽器安全等級應設定為中級或更高，並關閉快顯功能、ActiveX 等主動執行功能及封鎖彈跳視窗，執行特殊程式如須降低安全性或需加裝外掛功能，請先進行安全檢查及管理。
7	郵件軟體已關閉信件預覽	□是 □否	電子郵件軟體應關閉收信預覽功能，請勿任意開啟不明來源的電子郵件，爲避免惡意連結及圖片危害請使用文字模式閱讀信件。
8	無 eDonkey、BT 等 P2P 軟體	□是 □否	禁止使用點對點互連(P2P)、tunnel 相關工具或任何有危害本校網路、設備及造成網路壅塞佔用頻寬等軟體。 檢查重點: p2p 軟體例: (PPstream，eDonkey ， eMule ， ezPeer ， BitTorrent(BT) ， Kuro ， BitComet , WinMX, Kazaa, uTorrent , Azureus(JAVA) , BitABC , BitTornado , eXeem , Shareaza)等名稱。
9	無 Web、FTP、Mail 等網路設站服務	□是 □否	電腦設備不可任意架站或做私人、營利用途。
10	已完成 MS-Office 軟體巨集安全設定	□是 □否	使用文書處理軟體(包括 Word、Excel、Powerpoint 等)應將巨集安全性設定為高級或更高，執行特殊程式如須降低安全性，請先進行安全檢查及管理。
11	Guest 帳號已關閉	□是 □否	請勿開啟網路芳鄰分享目錄與檔案，並停用 Guest 帳號。
12	開啟 WINDOWS 系統自動更新程式	□是 □否	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。

個人電腦資訊安全自我檢查表			
文件編號	NPSS-ISMS-D-001	版次	1.0

編號	檢查項目	檢查結果	檢查說明
13	網路位置設定	□是 □否	安裝 Win10 作業系統之電腦連線至網路時，網路位置應設定為公用網路。保護電腦不受網際網路上任何惡意軟體的危害
14	關閉 Autorun	□是 □否	個人電腦請關閉插入可攜式儲存媒體或光碟時之自動執行功能
15	重要業務文件已備份	□是 □否	1.應定期備份個人電腦設備內重要文件及資訊，使用個人電腦設備處理機密資料或公文時，應作加密處理且勿存放於個人電腦中，應存放於實體隔離媒體並完成加密。 2.應避免使用非本校防護範圍內(本校各辦公室)之網路及電腦設施辦理公務，若確有必要使用外部(如住家、公共場所)資訊環境，務請確認資訊使用環境是否具備下列防護措施: (一)儲存於攜帶式儲存媒體(如行動碟)之公務相關電子檔案應予加密。 (二)使用之連網電腦設備應安裝防毒軟體(含最新版之病毒碼更新)及防火牆，並應保持啟動運作狀態。 (三)處理公務之電腦設備以不連上網路為原則(使用本部網路應用系統除外)，同時於處理完畢後應將公務相關電子檔案移除，且不得存放於主機。
16	機密資訊加密儲存於實體隔離媒體	□是 □否	

單位：_____職稱：_____姓名：_____ (簽章)