花蓮縣新城國小校園網路使用規範

一、一般保密責任

1、學校提供教職員工或學生使用的個人電腦應設定保護裝置，如個人密碼以及螢幕保護，人員因故離開座位中斷作業時，必須設定保護裝置，防止帳號被盜用或資料被竊取。

2、結束工作時，所有學校教職員工應將其所經辦或使用具有機密或敏感性質的文件（例如公文、學籍資料等）及儲存媒體（如 USB 隨身碟、光碟等），妥善存放，並將桌面收拾乾淨。

3、每部電腦應定期（至少每個月 1 次）進行系統更新漏洞修補作業。

4、每部電腦應安裝防毒軟體，並常駐防毒監控功能，將軟體設定為自動定期更新病毒碼；或由伺服器端進行病毒碼更新的管理。

5、同仁應保持高度之警覺心，防範不法人士以偽裝、騙術獲取帳號及通行碼入侵系統。並應具備高度之危機意識，如有發現疑似系統安全危機時，應迅速通知校園資訊安全管理人員。

二、網路系統存取控制 網路系統存取控制

1. 校內所共用的個人電腦應以特定功能為目的，所有電腦禁止從網路非法下載檔案的行為。

2. 利用檔案分享功能，提供他人存取檔案時，應僅針對必要對象開放使用權限，避免將權限完全開放。

3. 使用者應於授權範圍內存取網路資源，如有違反以下情事，將依相關法規查處。

(1)不得以任何方式竊取他人之帳號、通行碼。

(2)不得使用任何軟體、設備竊聽網路上之通訊(校園資訊安全管理人員因執行業務需要除外)。

(3)不得以任何方式干擾或妨礙網路之正常運作。

(4)不得嘗試入侵網路或電腦設備。

(5)不得於學校網路上儲存、建置或傳播色情文字、圖片、影像、聲音等資訊。

(6)未經核准，不得私設或更改校園網路上任何資訊設備之網際網 路位址(IP Address，簡稱 IP)，如有使用特定 IP 之需求請事先提出申請。

(7)為維護網路安全，禁止在校園網路內架設路由器、無線網路 AP 或 IP 分享器等網路設備。

4. 專供師生教學活動使用之無線網路熱點，若採用其他管理方式確有不便時，應採取限定開放時間及限制開放區域等管理措施，減少遭受不當利用之機會。

三、電子郵件安全管理規定 電子郵件安全管理規定

1. 所有使用者禁止以電子郵件騷擾他人、發送匿名郵件、偽造他人名義發送郵件或惡意發送大量不當郵件，導致其他網路使用者之不安與不便。如有違反之情事，將依相關法規查處。
2. 勿開啟來路不明的電子郵件，避免啟動惡意程式，造成校園網路系統遭受感染與破壞。

四、通行碼使用與保密責任 通行碼使用與保密責任

1. 使用者應該對其個人所持有通行碼善盡保密責任。
2. 要求使用者的通行碼設定，應該包含英文字、數字、特殊符號，長度為 8 碼（含）以上。
3. 至少每三個月更改一次通行碼。
4. 其他部分參考優質通行碼設定原則與使用原則。

五、個人電腦使用規定 個人電腦使用規定

1. 所有電腦禁止下載、安裝、使用、散播非法軟體。
2. 多人使用之個人電腦，使用者不可存放機敏資料，亦不可設定記憶個人帳號與通行碼。
3. 存放於個人電腦上的重要資料應自行定期備份。
4. 個人電腦除作業系統本身所預設安裝之軟體、公務用之資訊系統、合法授權之辦公室軟體、防毒軟體外，使用者不得自行安裝應用軟體。若因公務或教學需要，應向校園資訊安全管理人員提出申請，且該軟體應具有合法之授權。
5. 在使用由外部交換得來之檔案之前，應先以防毒軟體掃瞄檢查，若發現異常，應停止使用該檔案。
6. 操作電腦系統如發現病毒時應立即清除，並通報校園資訊安全管理人員告知病毒或惡意程式名稱。無法自行清除病毒時，儘速通知校園資訊安全管理人員協助處理。

六、儲存媒體使用規定 儲存媒體使用規定

1. 使用光碟片、外接式儲存媒體（如：隨身碟、外接式硬碟…）時，應先以防毒軟體掃瞄檢查，若發現異常，應停止使用該儲存媒體。
2. 所有包含儲存媒體的設備，在報廢前，應先確保已將任何機敏資料和授權軟體刪除及格式化該儲存媒體。
3. 為防止外接式儲存媒體病毒交叉感染，個人電腦應設定關閉自動撥放功能及 Shell Hardware Detection 服務。

七、遵守規範

使用者應遵守智慧財產權、電腦處理個人資料保護法相關法令規定，遵守校園網

路使用規範。如有違反之情事，將依相關法規查處。

八、本規範實施要點，經校長核定後施行，修正時亦同。

資訊組長：資訊組長李宜容　　主任：教務主任葉又寧　　校長：校長張世璿