**臺南市茄拔國民小學校園資訊設備與網路使用安全規範**

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,如個人鑰匙、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特性的資料(例如公文、學籍資料等)及資料的儲存媒體(如USB隨身碟、磁碟片、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)進行程式更新漏洞修補作業。

4. 每部電腦應安裝防毒系統,並隨時啟動防毒監控程式,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戒心,防範不法人士以偽裝、騙術獲取帳號及通行碼入侵。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工作小組人員。

二、 網路系統存取控制

1. 學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行為。

2. 利用微軟視窗作業系統之檔案分享功能,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登入帳號、通行碼。

(2) 不得使用任何軟體、設備竊聽網路上之通訊(校園資訊安全工作小組人員因執行業務除外)。

(3) 不得使用任何手段干擾或妨害網路之正常運作。

(4) 不得嘗試入侵網路設備及其他電腦。

(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) 不得未經核准,私自安裝網路服務或裝置。

三、 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. 不開啟來路不明或非關校務的電子郵件,避免啟動惡意程式,造成校園網路系統遭受感染與破壞。

3. 關閉郵件預覽功能。

四、 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. 至少每三個月改一次密碼。

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

1. 所有電腦禁止下載、安裝、使用、散播FOXY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、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,應向校園資訊安全工作小組提出申請,且該軟體應具有合法之版權。

5. 使用由外部交換得來之資料前,應先以防毒軟體掃瞄,若發現異常,應停止使用該資料。

6. 同仁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工作小組告知病毒或惡意程式名稱。無法自行清除病毒時通知校園資訊安全工作小組協助處理。

六、 儲存媒體使用規定

1. 使用者使用磁碟片、光碟片、外接式儲存媒體(如:隨身碟、硬碟機...)時,應先以防毒軟體掃瞄,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,應先確保已將任何敏感資料和授權軟體刪除或覆寫。

3. 為防止外接式儲存媒體病毒交叉感染,電腦應設定關閉自動撥放功能及Shell HardwareDetection服務。

七、 遵守規範

使用者應遵智慧財產權相關法令規定,遵守電腦處理個人資料保護法規定,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。

承辦人: 主任: 校長: