新竹市東區新竹國民小學校園網路使用規範

中華民國 105 年 6 月 22 日核定

壹、目的

為充分發揮校園網路（以下簡稱網路）功能，以支援教學研究、行政活動及線上學習之功能，普及尊重法治觀念，以促進教育及學習，並提供網路使用者可資遵循之準據，特依教育部「校園網路使用規範」訂定新竹市東區新竹國民小學校園網路使用規範（以下簡稱本規範）。

貳、適用範圍

凡使用本校校園網路者(含通訊電路及網路服務之使用者)，皆應遵守本規範。本校校園網路包括：本校校園內之資訊設備，及利用本校校園網路連線之所有資訊設備、教學網路、行政網路、無線網路、宿舍網路、校外遠端連線（如撥接、ADSL、FTTB… 等）及遠端擷取（PPTP、SSL-VPN… 等）。

參、實施方式

一、網路規範

為維護校園網路正常使用，應辦理下列事項：

（一）向市府教育處尋求協助處理網路相關法律問題。

（二）採取適當之措施以維護網路安全。

（三）宣導網路使用之相關規範，並引導網路使用者正確使用網路資源、重視網路相關法令及禮節。

（四）其他與網路有關之事項。

二、尊重智慧財產權

（一）不得安裝使用未經授權之電腦程式。

（二）不得私自下載、拷貝受著作權法保護之著作。

（三）不得未經著作權人之同意，將受保護之著作上傳於公開之網站上。

（四）不得私自於校內架設網站。

（五）不得於個人網頁中提供下載未經授權之資料。

（六）網路線上討論區上之文章，若作者已明示禁止轉載，不得任意轉載。

（七）不得利用網站或點對點網路工具，提供公眾下載受保護之著作。

（八）其他可能涉及侵害智慧財產權之行為。

三、禁止濫用或干擾網路系統

（一）不得私設或竄改校園網路上任何電腦之網際網路位址(IP Address，簡稱 IP)。

(二)不得入侵他人主機或資料庫，進行盜拷竄改毀損資料、攻擊破壞干擾系統作業。

（三）不得散布電腦病毒或其他干擾、破壞系統機能之程式，進而導致流量異常 。

（四）不得擅自截取、竊聽網路傳輸訊息。

（五）不得以破解、盜用或冒用他人帳號及密碼等方式，未經授權使用電腦或網路資

源，或洩漏他人之帳號及密碼。

（六）不得擅自將帳號借予他人使用。

（七）不得窺視他人之電子郵件或檔案。

（八）不得以任何方式濫用網路資源，包括以電子郵件大量傳送廣告信、連鎖信或無用之信息，或以灌爆信箱、掠奪或佔用資源等方式，影響系統之正常運作。

（九）不得以任何形式從事散佈、詐欺、誹謗、侮辱、猥褻、騷擾、威脅、攻擊、毀謗、非法交易或其他違法之行為。

（十）不得利用網路大量下載程式、影片或音樂等非教學研究目的之相關活動。

（十一）不得在公眾討論區討論私人事務，發佈文章時請尊重他人的權益和隱私。

（十二）不得嘗試侵入未經授權之電腦系統。

（十三）禁止使用者私自將無線網路存取設備介接至校園網路；若有介接之必要應經權責管理人員同意並設定帳號通行碼或加密金鑰以防未經許可之盜用。

（十四）不得利用學校之網路資源從事非教學研究等相關之活動或其他違法行為。

（十五）不得利用學校之網路資源從事未經本校許可的商業或違法、不當行為。

四、網路之管理

為執行本規範之內容，其有關網路之管理事項如下：

（一）協助校內教職員工及學生建立自律機制。

（二）為維護網路資源之妥善分配，管理單位得對網路流量做適當區隔與管控。

（三）對於違反本規範或影響網路正常運作者，管理單位得與採用流量管制或暫停該使用者之權利。經確認恢復正常狀態，始恢復其網路連線。

（四）各類應用伺服器（如電子佈告欄、網站等）應設置專人負責管理、維護。違反網站使用規則者，負責人得暫停其使用權。

（五）使用者若發現系統安全有任何缺陷或漏洞，應儘速通知管理單位處理。

（六）限制內部資訊系統只允許從校園內部 IP 位址，或經由本市教育處教育網路中心虛擬私有網路（VPN）連結及存取。(新竹市人事差勤系統、教師新竹市教育雲……等非本單位管轄，請遵守各單位管理規定)

（七）校園網路原則禁止使用 P2P 軟體。

（八）違反網站使用規則者，得刪除其文章或暫停其使用。情節重大、違反校規或法令者，並應轉請學校處置。

（九）其他有關校園網路管理之事項。

五、網路隱私權之保護

學校應尊重網路隱私權，不得任意窺視使用者之個人資料或有其他侵犯隱私權之行為。但有下列情形之一者，不在此限，設備管理人或使用人應配合提供必要之系統權限：

（一）為維護或檢查系統安全。

（二）依合理之根據，懷疑有違反本規範之二、三大項(尊重智慧財產權、禁止濫用或干擾網路系統)之情事時，為取得證據或調查不當行為。

（三）為配合司法機關之調查。若校外單位有偵查犯罪之必要，應先知會本校校園網路管理單位且出示相關法律函（ 證 ）件。各處室於接獲本校校園網路管理單位通知後，應依「台灣學術網路連線單位配合防治網路犯罪處理要點」、「個人資料保護法」、「公務人員服務法」配合提供相關資料。

（四）若遇緊急危難之情事，為取得相關之資料，以利及時防治或處置（例如：生命財產遭重大變故)。

（五）其他依法令之行為。

六、私人電腦

（一）私人電腦區域網路設定請使用自動取得 IP，並不得擅自指定或更改。

（二）使用校園網路，視同接受本規則所有條款，並須受本規則約束。

七、資安事件管理

網路使用者應隨時留意任何疑似資安問題，以保網路使用安全。舉凡經教育機構資安通報平台及正式函文提報之資安事件，大致可分為以下類別：

（一）INT(入侵攻擊)：

1. 系統入侵(資訊設備遭惡意使用者入侵)
2. 對外攻擊(對外部主機進行攻擊行為)
3. 針對性攻擊(針對特定個人的資訊洩漏與身分盜取)
4. 散播惡意程式(主機對外進行惡意程式散播)
5. 中繼站(主機成駭客之中繼站，接收惡意程式連線)
6. 社交工程攻擊(帳號遭盜用對外發動社交工程攻擊)
7. Spam(資訊設備從事大量廣告信件、垃圾郵件散播行為)
8. C&C(主機疑似為駭客之殭屍電腦 Host 伺服器)
9. Bot(資訊設備疑似成為駭客所控制之殭屍網路成員)

（二）DEF(網頁攻擊)：

1. 惡意網頁(網頁遭駭客置換或放置不當內容)
2. 惡意留言(網頁遭駭客放上惡意留言)
3. 網頁置換(網頁遭駭客置換)
4. 釣魚網站(主機遭駭客置入釣魚網站)

資安事件處理原則：

1. 經教育機構資安通報平台提報之 IP，經查證屬實，暫時停止使用網路資源。
2. 檢警正式來文，因校方無檢調權，若查案有此需求，應請檢警人員提出搜索票，校方才能全力配合調查。

肆、違規處置

網路使用者如違反本規範者，將受到下列之處分：

（一）暫時停止使用網路資源。

（二）若情節嚴重者，接受校規之處分或其他相關之法律責任。

（三）依前兩項規定之處分者，其另有違反法令行為時，行為人尚應依民法、刑法、著作權法或其他相關法令，自負法律責任。

伍、本辦法經校長核定後公告實施，並得隨時檢討補充修正。