新北市立明德高級中學校園網路使用規範

109 年 10 月 13 日資通安全小組會議通過

一、目的及依據

基於充分發揮校園網路，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， 並提供網路使用者可資遵循之依據，依據教育部 90 年 12 月 26 日公布的「教育部校園網路使用規範」及 99 年 1 月 11 日公布之「台灣學術網路管理規範」訂定「新北市立明德高級中學校園網路使用規範」（以下簡稱本規範）。

二、適用範圍

本校校園網路主要提供行政業務與教學研究及學生學習使用，凡利用各式可上網之裝置（含各式電腦、行動裝置、手機及其他可存取網路之裝置）接取本校校園網路(含通訊電路及網路服務)相關設備，即為本校校園網路之使用者(以下簡稱使用者)，皆應遵守「台灣學術網路使用規範」、「教育部校園網路使用規範」及本規範相關規定。

三、使用者之責任與義務

（一） 善盡各項資料、系統和帳號密碼之保管和保密

1、 使用者應善盡保管自身身份識別帳號與密碼、各項資料之責任，並自負因該帳號及密碼、各項資料使用時所衍生之一切法律責任。

2、 本校各系統管理者及使用者，對系統內所有之各項資料，負有保密義務，不得任意提供他人使用、亦不得洩漏所擁有的帳號及密碼資料、各項資料，造成系統安全、他人安全可能的重大威脅。

（二） 尊重智慧財產權

網路使用者應尊重智慧財產權，不得為下列行為：

1、 使用未經授權之電腦軟體。

2、 違法下載、複製受著作權法保護之著作。

3、 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。

4、 網路線上討論區上之文章，若作者已明示禁止轉載，仍然任意轉載。

5、 利用網站或點對點網路工具，提供公眾下載受保護之著作。

6、 其他涉及侵害智慧財產權之行為。

（三） 禁止濫用或干擾網路系統，網路使用者不得為下列行為：

1、 散布電腦病毒，或其他干擾，或破壞系統機能之程式，進而導致流量異常。

2、 擅自截取網路傳輸訊息。

3、 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。

4、 任意將帳號借予他人使用，或故意洩漏他人之帳號及密碼。

5、 隱藏帳號或使用虛假帳號。但經明確授權得匿名使用者不在此限。

6、 擅自窺視他人之電子郵件或檔案。

7、 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、佔用資源等方式，影響系統之正常運作。
8、 以電子郵件、線上談話、電子佈告欄或類似功能之方法散佈詐欺、誹謗、侮辱、猥褻、騷擾、非法軟體交易或其他違法之訊息。
9、 其他利用校園網路資源從事非教學研究等相關之活動或違法行為。

（四） 網路管理

為執行本規範之內容，有關網路管理之分工及管理事項如下：

1、 全校對外網路及連接各單位之骨幹網路由圖書館資訊組(以下簡稱管理單位)管理。
2、 為維護網路資源之妥善分配，管理單位得對網路資源做適當區隔與管控。
3、 對於無故佔用大量網路資源或流量異常者，致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。
4、 對於散布內容有不當或涉及違法者，管理單位得逕行刪除其內容或強制停止運作。
5、 各類應用網路資源（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。
6、 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。
7、 為降低本校資訊系統的安全威脅，阻擋源自校外網路(非本校內部的 IP 位址)流量，除已開放的服務外，若有其他需求，須提出申請。
8、 限制內部行政校務資訊系統只允許從校園內部 IP 位址，或經由本校虛擬私有網路 (VPN) 連結及存取。

四、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)

五、隱私權保護

網路管理應尊重個人隱私權，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，管理單位或相關設備系統管理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。
(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。
(五)其他依本國法令之行為。

六、違規處置

網路使用者違反本規範者，將受到下列處分：

1. 暫時停止相關使用者使用網路資源。
2. 學生違反相關規範經查證屬實，經查證屬實，依「新北市立明德高級中學學生獎懲規定」處分，並通知當事人家長到校處理，其另有違法行為時，行為人應依民法、刑法、著作權法或其他相關法令負法律責任外，本校得不經使用者同意，配合司法及相關單位提供相關資料。
3. 教職員工違反相關規範，由相關管理單位以書面通知當事人改善並暫停其網路使用權。如未改善，則簽請校長核可後移送考評委員會處理。其另有違法行為時，行為人應依民法、刑法、著作權法或其他相關法令負法律責任外，本校得不經使用者同意，配合司法及相關單位提供相關資料。
4. 違反本規範之使用者對於懲處有異議時，得依相關程序，提出申訴或救濟。

七、本規範若有未盡事宜，依照相關法令及規定辦理。

八、本規範經本校資通安全小組會議通過後實施，修正時亦同。

新北市立明德高級中學資訊安全管理要點

本要點依據「行政院及所屬各機關資訊安全管理要點」、「教育體系資通安全管理規範」規定訂定。

一、資訊安全權責分工

(一)對處理敏感性、機密性資料之人員及因工作需要須賦於系統管理權限之人員，應妥適分工，分散權責，視需要建立人員相互支援制度。

(二)對離職人員，依據人員離職之處理程序辦理，並立即取消使用各項系統資源所有權限。

(三)針對不同層級人員，視實際需要辦理資訊安全教育訓練及宣導，促使人員瞭解資訊安全的重要性，各種可能的安全風險，以提高人員資訊安全意識，促其遵守資訊安全規定。

(四)各業務主管，須負責督導所屬人員之資訊作業安全，防範不法及不當行為。

二、電腦系統安全管理

(一)使用臺灣學術網路危機處理中心(TACERT)教育機構資安通報平台，建立資訊設施及系統的變更管理通報機制，以免造成系統安全上的漏洞。

(二)依據電腦處理個人資料保護法之相關規定，審慎處理及保護個人資訊。

(三)建立系統備援設施，定期執行必要的資料、軟體備份並存放在不同主機，以便發生災害或儲存媒體失效時，可迅速回復正常作業。

(四)重要的資訊設備、個人電腦均需設定具有密碼管制之銀幕保護程式。

三、網路安全管理

(一)本校與外界網路連接之網點，須設立防火牆控管外界與內部網路之資料傳輸及資源存取。

(二)機密性及敏感性的資料或文件，不得存放在對外開放的資訊系統中，敏感性資訊如有電子傳送之必要，需經加密或電子簽章等安全技術處理後傳送。

(三)審慎評估開放外界連線及本校間資料傳送作業，必要時簽訂契約或協定，限制系統可運作之

權限，並明定應遵守之資訊安全規定、程序及應負之責任。

四、系統存取控制管理

(一)視安全管理需求核發及變更密碼。

(二)登入學校網域或網站時，依各處室人員職掌所必要之系統存取權限，由系統管理人員設定賦予權限之帳號與密碼。

(三)各單位之重要資料如需委外建檔者，不論在所內或所外執行，均須與委外廠商簽訂適當之安全管制條款，防止資料被竊取、竄改、販售、洩漏及不當備份等情形發生。

五、系統發展及維護之安全管理

(一)在資訊系統規劃之需求分析階段，即將資訊安全納入考量；系統之維護、更新、上線執行及版本異動作業，應予安全管制，避免不當軟體、暗門及電腦病毒等危害系統安全。

(二)資訊業務委外時，應於事前審慎評估可能的潛在安全風險，須明定廠商之資訊安全責任及保密規定，並列入契約，要求廠商遵守。

(三)對於委外建置之軟硬體系統及維護人員，應規範及限制其可接觸之系統與資料範圍，並於使用完畢後立即取消其使用權限。

(四)依據智慧財產權之相關規定，規範各種軟體之使用。

六、實體及環境安全管理

(一)系統伺服主機、設備應安置於主機房，並由資訊組專責管理，並管制非相關人員隨意進出。

(二)評估各種人為及天然災害對正常業務運作之影響，並視需要調整更新計畫。