

臺北市北投國民中學資訊安全管理規範

壹、目標

- 一、維護校園網路環境及電腦設備正常運作。
- 二、防止駭客、病毒等入侵及破壞，提高資安意識、降低資安風險。
- 三、防止不當及不法使用電腦系統及校園網路，避免人為疏失。
- 四、推廣資訊安全教育，提昇全校師生網路禮節及資訊安全素養。

貳、實施範圍

- 一、人員：包括本校師生、職員工及委外維修廠商人員。
- 二、應用系統：包含校園內所有電腦系統及網路服務。
- 三、硬體設備：
 1. 行政專用電腦。
 2. 班級電腦設備。
 3. 教學電腦設備。
 4. 專科教室及其他公用場所電腦設備。
 5. 電腦機房網路伺服器及相關的網路連線設備。
- 四、資訊安全教育訓練：
 1. 研習活動及宣導：每學期安排於全校教職員共同聚會或特定時段，舉行全校教職員資訊安全研習或宣導，宣導資訊安全，提供新知。
 2. 電腦教學：於課程活動中設計必要之資訊安全及資訊素養議題，提昇學生資訊素養能力及資安意識。

參、管理與分工

本校資訊安全工作之權責分工如下：

- 一、資訊安全規範之建置及評估等事項，由資訊組負責辦理。

二、各行政電腦在使用的安全需求、使用管理及保護等事項，由各處室業務承辦人員負責依相關規定辦理，並列入所屬處室主管督考。

三、各業務上的資訊機密維護，由各業務承辦人員依相關規定辦理，並列入所屬處室主管督考。

四、資訊安全的實施由本校全體教職員工共同執行與維護。

肆、安全管理

一、電腦病毒及惡意軟體之防範

1. 定期更新作業系統及防毒軟體之修補程式，以防制電腦病毒及惡意軟體之侵入風險。
2. 對來路不明及內容不確定之媒體及資料，應在使用前詳加檢查是否感染電腦病毒。

二、軟體管理

1. 軟體之使用，應遵守智慧財產權及相關法令規定。
2. 教職員工及學生不得把未得授權的軟體裝設到校園電腦；亦禁止下載未經授權、P2P 或其他與公務無關之軟體。

三、日常電腦安全管理

1. 應定期執行必要的備份，以防發生災害或是儲存媒體失效。
2. 電腦及網路系統更新、維修、問題處理，應迅速報告相關人員，以便儘速維修。
3. 學校電腦主機房、電腦教室區域，應設置滅火設備。
4. 非業務相關人員，嚴禁進出電腦機房。僅資訊人員、受准許之總務人員及必要之維修人員得以進出機房。

四、資料安全管理

1. 內含機密性或敏感性資料的媒體報廢時，應以安全的方式處理，例如格式化，或予以物理性破壞，以確保資料從媒體中完全清除。

2. 所有學校教職員工應將其所經辦或使用具有機密性的資料或儲存媒體，妥善存放，並於專用的電腦執行，防範洩漏或不當的使用。在傳輸、儲存過程中可用加密方法保護。
3. 個人資料的使用，應依「電腦處理個人資料保護法」等有關法令規定辦理。
4. 個人電腦應設定螢幕密碼、個人密碼或是以其他控制措施保護。
5. 超過保存時限的檔案，應依相關規定刪除或銷毀。
6. 對於多人使用的資訊系統(校務行政系統、其他公務系統、班級網站)，必須依循安全的管理權限：
 - (1)依執行業務之需求，賦予使用者系統存取權限。
 - (2)使用者調整職務及離(休)職時，必須儘速註銷其系統存取權限。
 - (3)確認系統存取特別權限之事項以及人員名單，定期檢查及取消閒置不用的帳號。。

伍、資訊安全事件通報處理機制

資訊安全事件包括：任何來自網路的駭客攻擊、病毒感染、垃圾郵件、資料或網頁遭竄改、以及通訊中斷等。因資訊安全事件致電腦系統無法運作或影響執行效率時，相關人員應立即停止使用受影響之電腦系統或設備，並停止或拔除網路連線，迅速通報資訊組，或請維護廠商協助處理，並依安全事件通報機制處理。

陸、本計畫經校長核可後實施，修正時亦同。