臺北市私立再興國民小學資訊安全管理辦法

壹、依據

教育部103年2月7日國中、小學資通安全管理系統實施原則訂定。

貳、目標

一、維持校園網路及電腦正常運作。

二、防止駭客、病毒等入侵及破壞。

三、防止不當及不法使用電腦系統及校園網路，並避免人為疏失。

四、推廣資訊安全教育，培育本校師生、職員工具有網路資訊禮節及素養。

參、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. 班級導師電腦。
3. 教師講桌電腦。
4. 科任教師筆記型電腦。
5. 伺服主機及相關網路設備。

四、資訊安全教育訓練：

1. 研習及宣導：鼓勵教職員參加校外資訊安全研習，汲取新知；並不定期利用各項集會或特闢時段，宣導資訊安全或舉辦資訊相關議題教育訓練，提升資訊素養。
2. 電腦教學：三、四、五、六年級設計所需之資訊安全教育，並於電腦課程中實施。

肆、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。

伍、安全管理

一、電腦病毒及惡意軟體之防範

1. 作業系統及防毒軟體應定期更新，以防範系統漏洞，強化對電腦病毒及惡意軟體的防護。
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、資料安全管理

1. 應定期執行必要的備份，以防發生災害或儲存媒體故障失效。
2. 內含機密性或敏感性資料的儲存媒體報廢時，應以安全的方式處理，例如低階格式化，或予以物理性破壞，以防範資料被不當讀取運用。
3. 教職員工應將個人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。
4. 個人資料的使用，應依「個人資料保護法及施行細則」等有關法令規定辦理。
5. 個人電腦應設定開機登入密碼及螢幕保護機制，當個人電腦暫不使用時，應使用鍵盤鎖或其他控管措施保護個人電腦安全。
6. 超過保存時限的檔案，應依相關規定刪除或銷毀。
7. 對於多人使用的資訊系統，必須依循安全的管理權限：

(1)依執行業務之需求，賦予使用者系統適當存取權限。

(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。

四、網路安全管理

1.校內禁止私自架設網路連結機房內之主機電腦或網路設備。

2.校內禁止私自將無線網路存取設備介接至校園網路。

五、實體安全管理

1.電腦機房、電腦教室區域，應設置偵煙、偵熱或滅火設備。

2.電腦機房應設置溫濕度控制措施，確保設備正常穩定運作。

3.電腦機房資訊設備應有適當的電力保護設施，例如設置不斷電系統、穩壓器等，以免無預警斷電或過負載而造成損失。

4.電腦機房設置門禁管制措施，除資訊組人員及受准許之總務或受准許之廠商維修人員等，其餘未經准許人員不能無故進出機房。

陸、資訊安全事件通報處理機制

資訊安全事件包括：系統被入侵、對外攻擊、針對性攻擊、散播惡意程式、中繼站、電子郵件社交工程攻擊、垃圾郵件、命令或控制伺服器、殭屍電腦、惡意網頁、惡意留言、網頁置換、釣魚網頁、個資外洩等。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，中斷或拔除網路連線，迅速通報資訊組，或請維護廠商協助處理，並依安全事件通報程序處理。

柒、本辦法經校長核可後實施，修正時亦同。