

新北市鄧公國小資通安全管理辦法

中 華 民 國 102 年 3 月 27 日資訊會議通過

- 一、目標：本規範為規定鄧公國小（以下簡稱本校）資通安全管理作業實施方式，以增進資訊作業之安全性，確保學校資料之機密性、完整性與可用性。
- 二、適用範圍：本校電腦、資訊與網路服務相關的系統、設備、程序、及人員。
- 三、實施規定：
 - (一)網路安全：
 - 1、網路控制措施：
 - (1)本校與外界連線，應僅限於經由教育局網路管理單位之管控，以符合一致性與單一性之安全要求。
 - (2)應禁止以電話線連結主機電腦或網路設備。
 - 2、服務委外廠商合約之安全要求：
 - (1)委外開發或維護廠商必須簽訂安全保密切結書。
 - (二)系統安全：
 - 1、職責區隔：
 - (1)本校伺服器主機可依個別應用系統之需要，設置專屬電腦，例如網路服務主機（電子郵件、網站主機）、教學系統主機（例如隨選視訊主機）。
 - (2)本校的行政系統主機（例如財務、人事、公文系統等）電腦，由教育局或市政府等單位統籌管理。
 - 2、對抗惡意軟體、隱密通道及特洛伊木馬程式。
 - (1)本校內的個人電腦應：裝置防毒軟體，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。
 - (2)本校內個人電腦所使用的軟體應有授權。
 - (3)新伺服器系統啟用前，應經過掃毒與更新系統密碼程序，以防範可能隱藏的病毒或後門程式。
 - 3、資料備份：本校系統管理人員需針對學校重要系統（例如系統檔案、網站、資料庫等）定期進行備份工作或採用自動備份機制；並應使用設備執行異地備份或使用光碟、隨身碟或外接式硬碟執行異地存放。
 - 4、操作員紀錄：本校系統管理人員需針對重要的電腦系統進行檢查、維護、更新等動作時，應針對這些活動填寫紀錄，作為未來需要時之檢查。
 - 5、資訊存取限制：本校內所共用的個人電腦應以特定功能為目的，並設定特定安全管控機制（例如限制從網路非法下載檔案行為、限制自行安裝軟體行為、限制特定資料的存取等）。
 - 6、使用者註冊：人員報到或離退職應會辦資訊組長（教師），資訊組長（教師）應執行電腦系統使用的使用者註冊及註銷程序，透過該註冊及註銷程序來控制使用者資訊服務的存取。

- 7、特權管理：本校的電腦與網路系統資訊具有存取特權人員清單。
- 8、通行碼之使用：管制使用者第一次登入系統時，必須立即更改預設通行碼，預設通行碼應設定有效期限。
- 9、通報安全事件與處理。本校任何人於校內發現異常情況或疑似資安事件及應立即向資訊組長（教師）通報，資訊組長（教師）應儘速進行處理並研判事件等級。

(三)實體安全

- 1、設備安置及保護：本校重要的資訊設備（如主機機房）應置於設有空調空間。本校資訊設備主機機房及電腦教室區域。本校資訊設備主機機房及電腦教室區域，應於出入口處設置門禁的機制。
- 2、溫濕度控制：本校重要的資訊設備（如主機機房）應有溫濕度控制措施，以防止資訊設備意外損壞，溫度最好控制在 20℃~25℃，濕度最好控制在相對濕度 50 度~70 度。機房內應懸掛溫濕度計，以觀察實際之溫濕度情況。
- 3、電源供應：本校重要的資訊設備（如主機機房）應有適當的電力設施。
- 4、纜線安全：本校資訊設備主機機房及電腦教室區域內網路線應建佈於高架地板或需設置保護設施。
- 5、設備與儲存媒體之安全報廢或再使用：所有包括儲存媒體的設備項目，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。
- 6、設備維護：若有需要，宜與設備廠商建立維護合約。
- 7、桌面淨空與螢幕淨空政策：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（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。
- 8、本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。

(四)人員安全

- 1、人員安全責任：利用各種場合宣導各層級人員應負之資訊安全責任，以強化工作上之資訊安全意識。
- 2、因業務需要將機敏資料交付委外廠商時（如辦理保險、校外教學等），廠商必須簽訂安全保密切結書。
- 3、資訊安全教育與訓練：本校系統管理人員應有足夠能力執行日常基礎之資安管理系統維護工作，並使其瞭解資安事件通報之程序。
- 4、本校鼓勵資訊組長/老師/系統管理人員以及所有教職員參與資訊安全教育訓練或宣導活動，以提昇資訊安全認知。
- 5、應對以下各項相關法令有基礎之認知：智慧財產權、著作權法、個人資料保護法、個人資料保護法施行細則

四、本辦法經鄧公國小資訊教育委員會議決，校長核定後公布施行，修正時亦同。