新竹縣寶山鄉新城國民小學資通安全管理辦法

一、 依據

- 教育部 96 年 5 月 30 日函頒國中、小學資通安全管理系統實施原則。
- 個人資料保護法

  中華民國 101 年 9 月 21 日行政院院臺法字第 1010056845 號令發布除第 6、54 條條文外，其餘條文定自一百零一年十月一日施行。
- 個人資料保護法施行細則

  中華民國 101 年 9 月 26 日法務部法令字第 10103107360 號令修正發布名稱及全文 33 條；並自一百零一年十月一日施行。

二、 目的

確保新竹縣寶山鄉新城國民小學（以下簡稱本校）所屬之資訊資產機密性、完整性及可用性，並符合相關法規之要求，使其免於遭受內、外部的蓄意或意外之威脅。

三、 適用範圍

本校校內電腦、資訊與網路服務相關的系統、設備、程序及人員，包含合約廠商及其它經授權使用之人員。

四、 組織與職權

為強化本校資通安全暨個資保護需求，健全資通安全管理制度，特設立「新竹縣寶山鄉新城國民小學資通安全委員會」(以下簡稱本委員會)，以推動本校資通安全管理業務之運作。本委員會之成員為校長、各處室主任及行政組長，由校長兼任召集人，資訊聯絡人為資通安全長，行政及技術相關事宜由資訊組負責。

本委員會權責如下：

1. 訂定本校資通安全政策及資通安全管控機制。
2. 督導資通安全政策之實施。
3. 資通安全事件通報、緊急應變及危機處理。
4. 規劃並督導資通安全教育訓練。
5. 督導個人資料保護工作之落實。

本委員會，必要時得召開臨時會議。會議須有應出席委員半數(含)以上出席始得開會，並得邀請相關人員列席。

五、 資安政策

維護本校資訊之機密性、完整性與可用性，保障使用者資料隱私。

保護本校網路資訊，避免未經授權的存取與修改。

- 本校業務執行須符合相關法令及法規之要求。
- 建立資訊業務永續運作計畫，確保本校業務永續運作。

六、 實施原則

1. 網路安全

1.1 網路控制措施

- 學校與外界連線，應僅限於經由教網中心之管控，以符合一致性與單一性之安全要求。
- 學校內特殊系統（例如會計系統、學生學籍、成績原始資料系統等）之資料，當有必要透過網路進行傳輸時，建議透過虛擬私有網路(Virtual Private Network, VPN）或同等連線方式進行；若無透過網路進行傳輸需求，則建議區隔於網路之外。
- 應禁止以電話線連結主機電腦或網路設備。

1.2 網路安全管理服務委外廠商合約之安全要求

- 委外開發或維護廠商必須簽訂安全保密切結書（參考切結書範本，文件編號 A-1）。

2. 系統安全

2.1 職責區隔

- 學校主機電腦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）。

2.2 對抗惡意軟體、隱密通道及特洛依木馬程式

- 學校內的個人電腦應：
  - 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
  - 定期（至少每個月）進行如「Windows Update」之程式更新作業，以防範作業系統之漏洞
- 學校內個人電腦所使用的軟體應有授權。
- 新系統啟用前，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。

2.3 資料備份

- 學校(或委託)系統管理人員需針對學校重要系統（例如系統檔案、應用系統、資料庫等）定期進行備份工作，或採用自動備份機制；建議週期為每週進行一次。

2.4 操作員日誌

- 學校(或委託)系統管理人員需針對敏感度高、或包含特殊資訊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日誌予以紀錄，作為未來需要時之檢查。
- 日誌內容可包含以下各項：
  - 系統例行檢查、維護、更新活動的起始時間
  - 系統錯誤內容和採取的改正措施。[*參考日誌範本，文件編號 A-2*]
  - 紀錄日誌項目人員姓名與簽名欄

2.5 資訊存取限制

- 學校內開放空間且供教職員工之外人員使用的電腦（不含有教師任課之電腦教室內之電腦）應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）。

2.6 使用者註冊

- 本校新進人員，資訊人員將會以教育局資訊中心郵件系統之帳號，註冊至本校各應用系統上，再由使用者自訂其密碼。若使用者有其特殊需求，也可另行單獨申請變更。
- 本校人員離職後，資訊人員應立即註銷該員在各應用系統的帳號及使用權。
- 本校資訊人員，必須妥善管理各應用系統之使用者帳號。
  - 每人使用唯一的使用者識別碼（ID）。
  - 檢查使用者是否經過系統管理單位之授權使用資訊系統或服務。
  - 保存一份包含所有識別碼註冊的記錄。
  - 使用者調職或離職後，應移除其識別碼的存取權限。
  - 定期（建議每學期）檢查並取消多餘的使用者識別碼和帳號。
  - 定期（建議每學期）檢查新增之帳號，若有莫名帳號產生，應關閉帳號權限，並依通報程序請求處理。

2.7 特權管理

- 學校的電腦與網路系統資訊具有存取特權人員清單、及其所持有的權限說明，應予以文件化記錄備查。

2.8 密碼(Password)之使用

- 本校各資訊系統與服務應避免使用共同帳號及密碼。
- 設定各應用系統的帳號密碼時，請遵循以下原則：
  - 混合大寫與小寫字母、數字，特殊符號。
  - 密碼越長越好，最短也應該在 8 個字以上。

- 至少每三個月改一次密碼。
- 使用技巧記住密碼
  - 使用字首字尾記憶法：
    a. My favorite student is named Sophie Chen，取字頭成為 mFSinsC
    b. There are 26 lovely kids in my English class，取字尾成為 Ee6ysnMEc
  - 中文輸入按鍵記憶法：
    a. 例如「密碼」的注音輸入為「wj/ vu/6a83」

- 應該避免的作法
  - 嚴禁不設密碼、與帳號相同或與主機名稱相同。
  - 不要使用與自己有關的資訊，例如學校或家裡電話、親朋好友姓名、身份證號碼、生日等。
  - 不重覆電腦鍵盤上的字母，例如 6666rrrr 或 qwertyui 或 zxcvbnm。
  - 不使用連續或簡單的組合的字母或數字，例如 abcdefgh 或 12345678 或 24681024
  - 避免全部使用數字，例如 52526565。
  - 不使用難記以至必須寫下來的密碼。
  - 避免使用字典找得到的英文單字或詞語，如 TomCruz 、superman
  - 不要使用電腦的登入畫面上任何出現的字。
  - 不分享密碼內容給任何人，包括男女朋友、職務代理人、上司等。

因特殊需要擁有多個帳號時，可考慮使用一組複雜但相同的密碼。

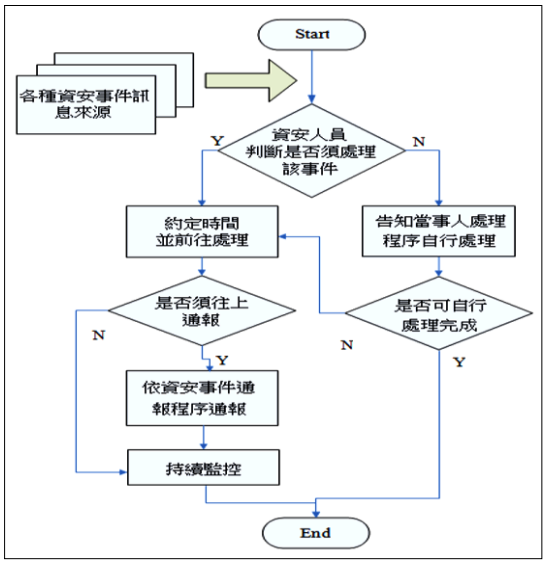
2.9 原始程式庫之存取控制

- 學校與系統廠商間的合約應加註對原始程式庫安全之要求，並防範資料庫隱碼(SQL-injection)問題，針對存取資料庫程式碼之輸入欄位進行字元合理性檢查。

2.10 通報安全事件與處理

- 本校發生資安事件之處理流程如右圖所示。
- 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。

- 資訊安全事件通報程序[*參照安全事件通報程序，編號 A-4*]以及安全事件通報單[*參考安全事件通報單，文件編號 A-5*]；通報程序應包括學校內部通報，以及學校與所屬縣市教育網路中心的通報。
- 當學校內部無法處理之資通安全事件，應通報新竹縣網路中心。
- 所訂出資訊安全事件通報程序應公布於校園內使用電腦與網路之場所，提供使用者瞭解。



3. 實體安全

3.1 設備安置及保護

- 學校重要的資訊設備（如主機機房）應置於設有空調空間。
- 學校資訊設備主機機房、電腦教室區域，應設置滅火設備，並禁止擺放易燃物、或飲食。
- 學校資訊設備主機機房、電腦教室區域內的電源線插頭應有接地的連結、或有避雷針等裝置，避免如雷擊事件所造成損害情況。
- 學校資訊設備主機機房、電腦教室區域，應至少於入出口處加裝門鎖或其他同等裝置。

3.2 電源供應

- 學校重要的資訊設備（如主機機房）應有適當的電力設施，例如設置UPS、電源保護措施，以免斷電或過負載而造成損失。

3.3 纜線安全

- 學校資訊設備主機機房、電腦教室區域內佈線應加以整理。

3.4 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。

3.5 設備維護

- 應與設備廠商建立維護合約。
- 廠商進入安全區域需簽訂安全保密切結書。

3.6 財產攜出

- 未經授權不應將學校的資訊設備、資訊或軟體攜出所在地。

- 當有必要將設備移出，應檢視相關授權，如主任層級（含）以上核章，並實施登記與歸還記錄。
- 相關財產之攜出應依教育部或學校既有之相關規定處理。

3.7 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(例如公文、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。
- 學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。

4. 人員安全

4.1 每學年至少要於校務會議上宣導一次本管理辦法，以及重要資通安全消息，以加強教職員工的資安意識。將安全列入工作執掌中

4.2 資訊安全教育與訓練

- 本校資通安全長，每年至少要有十八小時的資通安全相關教育訓練，使其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。
- 其他教職員工每年至少要有六小時，參與資通安全教育訓練或宣導活動，以提昇資通安全認知。

5. 個資保護要求

5.1 本校應就法律允許下，因公務需求所蒐集、處理及保存的個人資料，公佈以下項目至學校網站上。

- 個人資料檔案名稱。
- 保有機關名稱及聯絡方式。
- 個人資料檔案保有之依據及特定目的。
- 個人資料之類別。

5.2 本校教職員工必須遵守個資法規定，不得以任何理由，在沒有法源依據或違反當事人的意願下任意蒐集或洩露他人個資。

5.3 個資法實施後，本校辦理各項活動之因應措施

- 本校在辦理任何公開活動，會有蒐集、處理甚至公佈部份個資(例：姓名）時，必須在活動辦法及報名表中，陳述「本校之機關名稱」、「蒐集用途」及「使用地區和期限」，在經「當事人同意」並報名後始得蒐集。若有公佈的需求時，必須加註「將會公佈本活動優勝人（學）員名單」字樣。所蒐集的個資，必須於宣告期限後予以銷毀。
- 本校承辦業務人員，必須妥善保護各項個人資料，並在活動辦法及報名表中註明「本校將會善盡保管之責」字樣。

6.　應對以下各項相關法令有基礎之認知

6.1智慧財產權

- 經濟部智慧財產局

  http://www.tipo.gov.tw/

- 著作權法

  http://law.moj.gov.tw/LawClass/LawContent.aspx?PCODE=J0070017

6.2個人資料保護及隱私

- 個人資料保護法

  http://law.moj.gov.tw/LawClass/LawAll.aspx?PCode=I0050021

- 個人資料保護法施行細則

  http://law.moj.gov.tw/LawClass/LawAll.aspx?PCode=I0050022

6.3電子簽章法

- 電子簽章法

  http://law.moj.gov.tw/LawClass/LawContent.aspx?PCODE=J0080037

- 電子簽章法施行細則

  http://law.moj.gov.tw/LawClass/LawContent.aspx?PCODE=J0080039

- 核可憑證機構名單

  http://gcis.nat.gov.tw/eclaw/bbs.asp

本辦法經校長核准後實施

文件編號：A-1

新竹縣寶山鄉新城國民小學服務委外單位服務暨保密切結書

公司(以下簡稱為本公司)為配合新竹縣寶山鄉新城國民小學（以下簡稱為貴校）之業務需求，進行相關工作。本公司提供服務項目如下：

一、

二、

三、

(註：列出貴公司將會提供之服務項目)

本公司願意在對貴校提供上述服務項目範圍內之服務時,保證因提供業務服務需存取貴校資訊系統中所存放，凡屬與公文機密、個人及事業單位權益相關之資料，無論其內容之一部或全部，均負保密之責；相關資料均以留在貴校內部範疇內處理，倘須由本公司攜至校外處理，應簽奉貴校核可。

本公司亦不私自蒐集貴校所擁有之任何資訊。若所提供之業務服務，不符合上述之規定或經營之服務項目超出上述範圍，或違犯法令，本公司同意無異議接受接受法律制裁與及其訴訟費用，並負責所引發之各項損失賠償。此致

新竹縣寶山鄉新城國民小學

申請單位及負責人蓋章：

日期：　　年　　月　　日

本服務暨保密切結書一式兩份，分別由_____公司以及新竹縣寶山鄉新城國民小學保存

文件編號：A-2

操作員日誌範本

填寫日期：　　民國　　年　　月　　日
系統操作起始時間：　上（下）午　　時　　分
系統操作結束時間：　上（下）午　　時　　分

操作事項	□　系統例行檢查 □　系統維護 □　系統更新操作
系統錯誤說明	
採取改正措施說明	

操作人員：　　簽名欄

日誌填寫人員：　　簽名欄

文件編號：A-3

優質通行碼設定原則與使用原則

一、 良好的通行碼設定原則

1. 混合大寫與小寫字母、數字，特殊符號。
2. 通行碼越長越好，最短也應該在 8 個字以上。
3. 至少每三個月改一次密碼。
4. 使用技巧記住通行碼
   - 使用字首字尾記憶法：
     a. My favorite student is named Sophie Chen，取字頭成為 mFSinsC
     b. There are 26 lovely kids in my English class，取字尾成為 Ee6ysnMEc
   - 中文輸入按鍵記憶法：
     a. 例如「通行碼」的注音輸入為「wj/ vu/6a83」

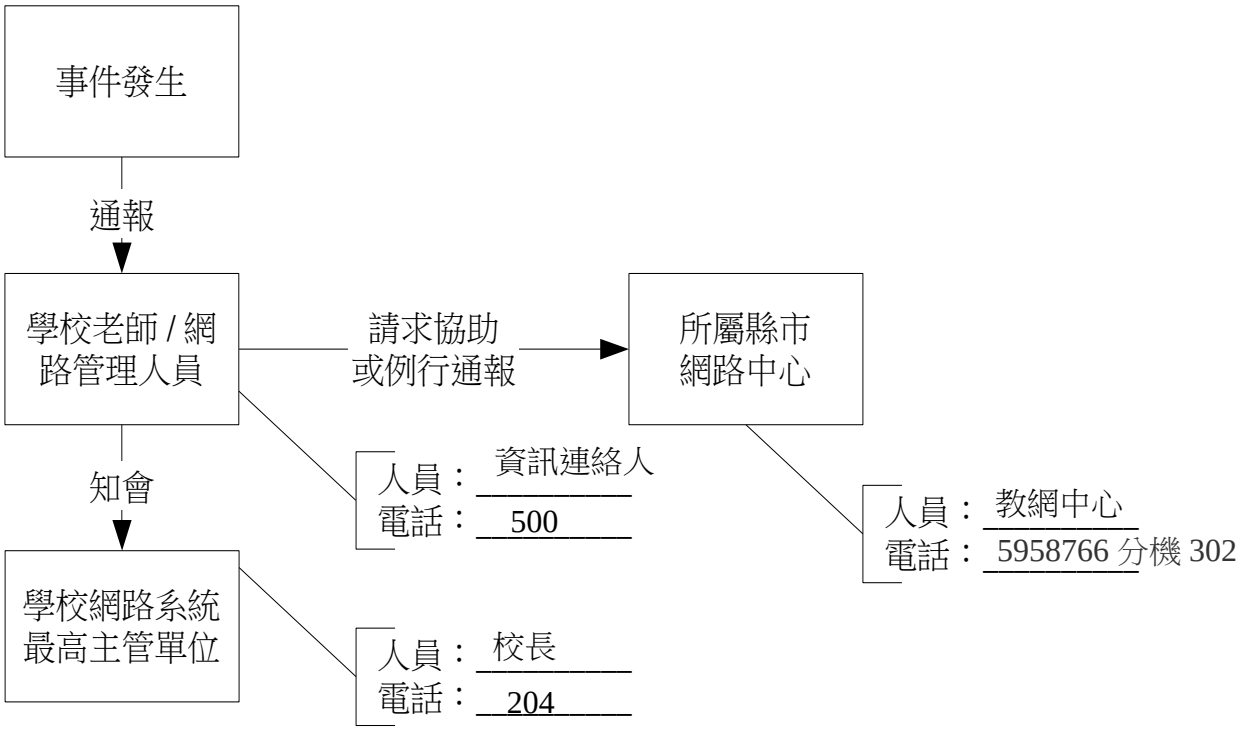
二、 應該避免的作法

1. 嚴禁不設通行碼
2. 通行碼嚴禁與帳號相同
3. 通行碼嚴禁與主機名稱相同
4. 不要使用與自己有關的資訊，例如學校或家裡電話、親朋好友姓名、身份證號碼、生日等。
5. 不重覆電腦鍵盤上的字母，例如 6666rrrr 或 qwertyui 或 zxcvbnm。
6. 不使用連續或簡單的組合的字母或數字，例如 abcdefgh 或 12345678 或 24681024
7. 避免全部使用數字，例如 52526565
8. 不使用難記以至必須寫下來的通行碼。
9. 避免使用字典找得到的英文單字或詞語，如 TomCruz 、superman
10. 不要使用電腦的登入畫面上任何出現的字。
11. 不分享通行碼內容給任何人，包括男女朋友、職務代理人、上司等。

延伸參考：

"Password Management Guideline", by department of defense computer security center, 12 April 1985
http://www.radium.ncsc.mil/tpep/library/rainbow/CSC-STD-002-85.pdf

新竹縣寶山鄉新城國民小學資訊安全事件通報程序



新竹縣寶山鄉新城國民小學學校資通安全事件通報單

編號：

填報時間：　　年　　月　　日　　時　　分

洽詢電話：　　傳真：

E-mail：

或逕送：

一、發生資通安全之機關(機構)聯絡資料：

機關(機構)名稱：　　聯絡人：

E-mail：

電話：　　傳真：

二、資通安全事件通報事項：

1.事件發生時間：　　年　　月　　日　　時　　分

2.主機(伺服器)資料：

◎ IP位址(IP Address)：

◎ 網域名稱(Domain name)：

◎ 主機(伺服器)廠牌、機型：

◎ 作業系統名稱、版本、序號：

◎ 網際網路資訊位址(Web URL)：

◎ 已裝置之安全機制：

3.資通安全事件資料：

◎影響等級：□『A』級：影響公共安全、社會秩序、人民生命財產。

□『B』級：系統停頓，業務無法運作。

□『C』級：業務中斷，影響系統效率。

□『D』級：業務短暫停頓，可立即修復。

◎ 事件說明：

◎ 應變措施：

三、期望支援項目：

四、解決辦法：

五、已解決時間：　　年　　月　　日　　時　　分

校長：　　資訊安全長：　　承辦人員：

新竹縣寶山鄉新城國民小學資通安全事件解除單

編號：

填報時間：　　年　　月　　日　　時　　分

洽詢電話：　　傳真：

E-mail：

或逕送：

一、發生資通安全之機關(機構)聯絡資料：

機關(機構)名稱：　　聯絡人：

E-mail：

電話：　　傳真：

二、資通安全事件通報事項：

1.事件發生時間：　　年　　月　　日　　時　　分

2.主機(伺服器)資料：

◎ IP位址(IP Address)：

◎ 網域名稱(Domain name)：

◎ 主機(伺服器)廠牌、機型：

◎ 作業系統名稱、版本、序號：

◎ 網際網路資訊位址(Web URL)：

◎ 已裝置之安全機制：

3.資通安全事件資料：

◎影響等級：□『A』級：影響公共安全、社會秩序、人民生命財產。

□『B』級：系統停頓，業務無法運作。

□『C』級：業務中斷，影響系統效率。

□『D』級：業務短暫停頓，可立即修復。

◎ 事件說明：

◎ 應變措施：

三、已解決時間：　　年　　月　　日　　時　　分

填寫人：

新竹縣寶山鄉新城國民小學學校教職員工及學生校內電子郵件及網路磁碟帳號管理辦法

中華民國 105 年 8 月

一、 凡本校教職員工及學生均可申請電子郵件信箱及網路磁碟機帳號，教職員工帳號可自訂，但不與他人相同為原則。

二、 為配合新竹縣網郵件集中管理之政策，本校郵件僅做為業務、教學通訊聯絡用途，不做私人使用用途，若需對外通訊用途請自行申請私人信箱。

三、 本校電子郵件之收件位址為 @mail.edu.tw

四、 本帳號密碼的使用範圍包含(1)網路磁碟的存取(2)校內電子郵件收發、(3)線上報修。

五、 教職員工請洽資訊聯絡人申請，學生請由任課老師視上課需求由任課老師洽資訊聯絡人申請。

六、 為維護教職員生權益及系統安全，一旦發現帳號被盜用，立即通報資訊聯絡人並修改密碼。

七、 帳號所有人必須對帳號善盡保管之責，包括：

牢記並定期更改密碼以防止被盜用，密碼需符合優質通行碼設定原則與使用原則。

禁止將帳號借與他人使用，或交換帳號使用。

不得傳送不當之資訊。

嚴禁散佈電腦病毒，發送圾垃信件及大量郵件以避免浪費網路資源。

嚴禁從事任何營利之商業行為。

八、 帳號所有人若有違反上述規定，視情結輕重停止帳號使用權三個月或永久取消系統使用權，若有違反法律之情事，需自負相關法律責任。

九、 本帳號使用期限至離職、畢業或辦理離校手續後，自動失效。

十、 本辦法如有未盡事宜，得隨時修正之。