

高雄市立前鎮國民中學
資訊安全政策與管理要點



中華民國 112 年 01 月 11 日

高雄市立前鎮國民中學資訊安全政策與管理要點

101年9月4日高雄市立前鎮國中校務會議通過
103年9月19日高雄市立前鎮國中校務會議第1次修訂通過
104年4月9日高雄市立前鎮國中校務會議第2次修訂通過

壹、依據：

- 一、教育部96年5月30日頒定「國中、小學資通安全管理系統實施原則」訂定。
- 二、教育部103年2月7日頒布「國中、小學資通安全管理系統實施原則」修訂。

貳、目標：

有效降低校園資訊安全事件發生、落實資訊安全事件回報機制及處理、提高資訊安全素養。校園資訊安全事件如資訊設備失竊、機敏資料外洩、違反智財權相關法令或電腦處理個人資料保護法規定、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。

參、實施原則

一、網路安全

1.1 網路控制措施

- 學校與外界連線，應僅限於經由高雄市教育網路中心之管控，以符合一致性與單一性之安全要求。
- 應禁止以私人架設網路(如：電話線、2G 或 3G 網路等)連線機房內之主機電腦或網路設備。
- 對於開放提供外部使用者或廠商存取之服務，必須限制使用者之來源 IP 及網路連線埠(Port)，以確保安全。

1.2 無線網路存取

- 應禁止使用者私自將無線網路存取設備介接至校園網路；若有介接之必要應經權責管理人員同意並設定帳號通行碼或加密金鑰以防未經許可之盜用。
- 校園內應提供無線網路存取服務，並採取適當安全管控措施：
 - 專供行政使用之無線網路熱點建議設定加密金鑰防護，並避免使用開放之無線網路存取重要資訊系統及處理敏感性資料。
 - 於教學區域、會議室等場所佈建之無線網路熱點應具有使用者身分認證機制，並經由校園無線路漫遊服務系統提供外校來賓使用。
 - 專供師生教學活動使用之無線網路熱點，若採用其他管理方式確有不便時，應採取限定開放時間及限制開放區域等管理措施，減少遭受不當利用之機會。

- 開放校外人士出入之公共空間可視需要提供民眾無線上網服務，其網段應與校園網路隔離，或委由網路服務業者提供。

二、系統安全

2.1 職責區隔

- 學校行政電腦依個別應用系統之需要，設置專屬電腦，由各行政人員自行負責保管。

2.2 對抗惡意軟體、隱密通道及特洛伊木馬程式

- 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（至少每季）進行如「Windows Update」之程式更新作業，以防範作業系統之漏洞
 - 電腦教室若已安裝還原系統（需設定為開機還原），為因應教學特殊需求，可不安裝防毒軟體，但各種系統更新、漏洞修補程式（如Windows Update）至少每學期更新一次。
- 學校內個人電腦所使用的軟體應有授權。
- 行政用電腦設定開機密碼及螢幕保護程式，以防資料不慎外洩。

2.3 資料備份

- 學校各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。

2.4 資訊存取限制

- 學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、禁止安裝 P2P 軟體等）。

2.5 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，記錄表[文件編號：A-7]由系統或檔案保管人保管。

2.6 通報安全事件與處理

- 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。
- 學校應建立資訊安全事件通報程序[文件編號 A-3]以及安全事件通報單[文件編號 A-4]；通報程序應包括學校內部通報，以及學校與高雄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，應通報高雄市教育網路中心。
- 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。

三、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，應至少於出入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、電腦教室區域內應避免明佈線。

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由學校人員陪同或簽訂安全保密切結書[文件編號 A-1、A-6]。

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，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，如密碼以及螢幕保護[文件編號 A-2]。

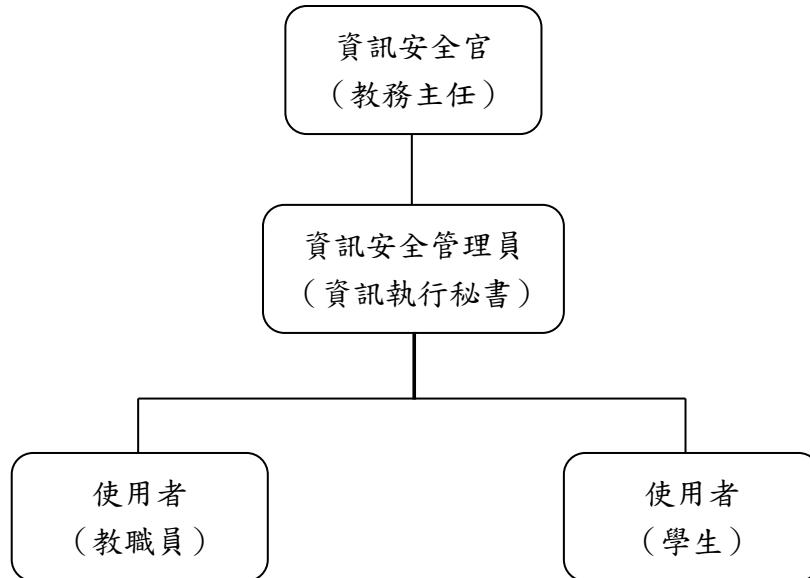
四、可攜式電腦設備與媒體

- 公務用可攜式電腦設備(如：筆記型電腦、平板電腦、智慧型手機等)應設定保護機制，如設定通行碼、圖形辨識、臉孔辨識或指紋辨識等。
- 公務用可攜式電腦設備應執行安全相關程序（如：掃毒、預設通行碼更新、系統更新等），以防範可能隱藏的病毒或後門程式。

- 公務用可攜式儲存媒體(如：隨身碟、光碟、磁帶等)應依儲存資料的機敏性實施安全控管措施，如檔案加密儲存或將該儲存媒體存放於上鎖儲櫃或安全處所。

五、人員安全

5.1 組織架構簡圖



資訊安全組織成員表詳如[文件編號 A-6]

5.2 資訊安全教育與訓練

- 使學校(或委託)系統管理人員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。
- 學校鼓勵或安排資訊組長/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。若全學年參與資訊安全教育相關訓練或宣導活動時數為零者，且無正當理由，得限制其使用校內資訊設備，以維護全校資訊安全。
- 將資訊安全教育納入學校電腦課程中。

六、資訊業務委外管理

- 服務委外廠商合約之安全要求
 - 在資訊業務委外合約中，應訂定委外廠商的資訊安全責任及保密規定。
 - 應要求委外廠商簽訂安全保密切結書[文件編號 A-1]。
 - 委外廠商人員到校服務時，應請其簽署委外廠商人員保密切結書[文件編號 A-6]。

- 委外廠商服務異動或終止時，應中止或刪除其系統上的帳號與權限[文件編號 A-11]。

七、應對以下各項相關法令有基礎之認知，

7.1 智慧財產權

- 經濟部智慧財產局 <http://www.tipo.gov.tw/>
- 著作權相關法規
http://www.tipo.gov.tw/ch/Download_DownloadPage.aspx?path=2173&Language=1&UID=9&ClsID=35&ClsTwoID=71&ClsThreeID=0
- 著作權法
http://www.tipo.gov.tw/ch/AllInOne_Show.aspx?path=1362&guid=a71977ea-6478-4e37-a46a-15497ba7c275&lang=zh-tw

7.2 個人資訊的資料保護及隱私

- 電腦處理個人資料保護法
<http://law.moj.gov.tw/LawClass/LawContent.aspx?PCODE=I0050021>

7.3 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/Scripts/newsdetail.asp?no=1J0080039>
- 核可憑證機構名單
http://www.moea.gov.tw/~meco/doc/ndoc/s5_p07_p03.htm

文件編號：A-1

資訊服務委外單位服務暨保密切結書範本

_____公司(以下簡稱為本公司)為配合_____學校(以下簡稱為貴校)之資訊應用業務需求，進行相關資訊系統或軟體開發、測試、建置及維護等工作。本公司提供資訊服務項目如下：

- 一、
- 二、
- 三、

(註：列出貴公司將會在健保資訊網上提供予醫事服務機構之服務項目)

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。若所提供之資訊業務服務，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

高雄市立前鎮國民中學

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_____公司以及前鎮國民中學保存

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

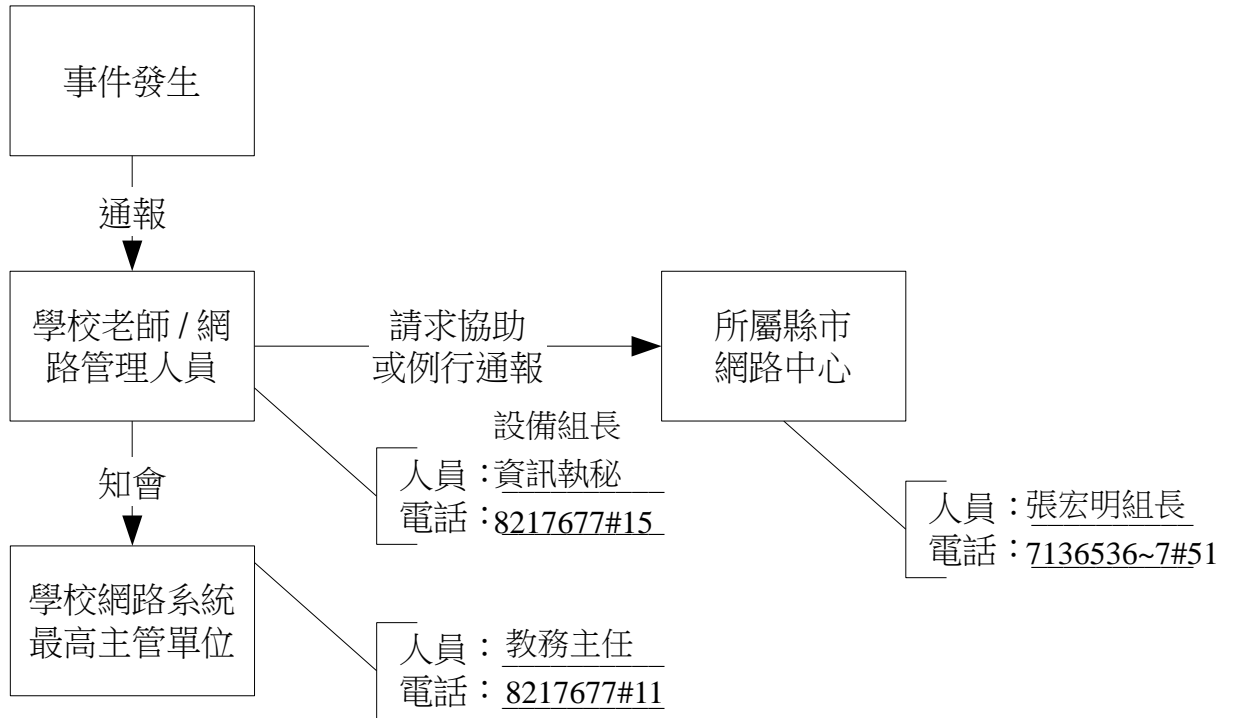
1. 嚴禁不設通行碼
2. 通行碼嚴禁與帳號相同
3. 通行碼嚴禁與主機名稱相同
4. 不要使用與自己有關的資訊，例如學校或家裡電話、親朋好友姓名、身份證號碼、生日等。
5. 不重覆電腦鍵盤上的字母，例如 6666rrrr 或 qwertyui 或 zxcvbnm。
6. 不使用連續或簡單的組合的字母或數字，例如 abcdefgh 或 12345678 或 24681024
7. 避免全部使用數字，例如 52526565
8. 不使用難記以至必須寫下來的通行碼。
9. 避免使用字典找得到的英文單字或詞語，如 TomCruz、superman
10. 不要使用電腦的登入畫面上任何出現的字。
11.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

文件編號：A-3

安全事件通報程序範本



文件編號：A-4

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

承辦人員：

資訊安全長：

校長：

學校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：_____

文件編號：A-5

資訊安全組織成員表

記錄編號：101-0001

日期：101年*月*日

職務	職稱	姓名	電話	手機	電子郵件
資訊安全委員會					
委員兼召集人	校長	柯○○	07-8217677 轉 10		
委員	教務主任	陳○○	07-8217677 轉 11		
委員	學務主任	洪○○	07-8217677 轉 21		
資訊安全官					
資安官	教務主任	陳○○	07-8217677 轉 11		
資訊安全小組					
組長	設備組長	魏○○	07-8217677 轉 15		
組員	資訊執秘	陳○○	07-8217677 轉 15		
組員	註冊組長	陳○○	07-8217677 轉 14		
資訊安全稽核小組（校安）					
組長	學務主任	洪○○	07-8217677 轉 21		
組員	總務主任	陳○○	07-8217677 轉 31		
組員	生教組長	范○○	07-8217677 轉 23		
緊急處理組（發言）					
召集人	教務主任	陳○○	07-8217677 轉 11		
組員	人事主任	張○○	07-8217677 轉 51		
組員	總務主任	陳○○	07-8217677 轉 31		
組員	輔導主任	吳○○	07-8217677 轉 41		
組員	會計主任	薛○○	07-8217677 轉 61		

文件編號：A-6

保密切結書

紀錄編號：日期： 年 月 日

本人 _____ 將嚴守工作保密規定與國家相關法令對業務機密負完全保密之責，並尊重智慧財產權。絕不擅自洩漏、傳播職務上任何業務相關資料及任職期間經辦、保管或接觸之所有須保密訊息資料；絕不擅自複製、傳播任何侵害智慧財產權之任何程式、軟體，違者願負法律責任。

此致

資訊安全管理小組

立同意書人： _____

身分證字號： _____

所屬單位別： _____

中 華 民 國 年 月 日

文件編號：A-7

特權閱讀紀錄單

檔案保管人：_____

序號	日期	閱讀者	事由	備註
1	年 月 日		<input type="checkbox"/> 公務：依據文號_____	
			<input type="checkbox"/> 其他：_____	
2	年 月 日		<input type="checkbox"/> 公務：依據文號_____	
			<input type="checkbox"/> 其他：_____	
3	年 月 日		<input type="checkbox"/> 公務：依據文號_____	
			<input type="checkbox"/> 其他：_____	
4	年 月 日		<input type="checkbox"/> 公務：依據文號_____	
			<input type="checkbox"/> 其他：_____	
5	年 月 日		<input type="checkbox"/> 公務：依據文號_____	
			<input type="checkbox"/> 其他：_____	
6	年 月 日		<input type="checkbox"/> 公務：依據文號_____	
			<input type="checkbox"/> 其他：_____	
7	年 月 日		<input type="checkbox"/> 公務：依據文號_____	
			<input type="checkbox"/> 其他：_____	
8	年 月 日		<input type="checkbox"/> 公務：依據文號_____	
			<input type="checkbox"/> 其他：_____	
9	年 月 日		<input type="checkbox"/> 公務：依據文號_____	
			<input type="checkbox"/> 其他：_____	
10	年 月 日		<input type="checkbox"/> 公務：依據文號_____	
			<input type="checkbox"/> 其他：_____	
11	年 月 日		<input type="checkbox"/> 公務：依據文號_____	
			<input type="checkbox"/> 其他：_____	
12	年 月 日		<input type="checkbox"/> 公務：依據文號_____	
			<input type="checkbox"/> 其他：_____	
13	年 月 日		<input type="checkbox"/> 公務：依據文號_____	
			<input type="checkbox"/> 其他：_____	
14	年 月 日		<input type="checkbox"/> 公務：依據文號_____	
			<input type="checkbox"/> 其他：_____	
15	年 月 日		<input type="checkbox"/> 公務：依據文號_____	
			<input type="checkbox"/> 其他：_____	

文件編號：A-9

資訊資產清單

一、資訊設備類

序號	財產編號	財產名稱	權責 保管人	放置地點
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				

二、資訊系統、文件類

序號	財產編號	財產名稱	權責 保管人	放置地點
1				
2				
3				
4				
5				
6				

各處室文件依權責由各處室主任、組長留存備查

文件編號：A-10

三、國中小學資安管理系統實施原則自我檢測表

本查檢表以「國中小學資安管理系統實施原則」所擬定，作為國中小學就其資通安全實施現況進行自我評量之用途。

學校名稱：_____

填寫單位：_____

填寫者：_____

填寫日期：_____

編號	檢測項目	符合與否	補充說明
網路安全			
1.	本校對外網際網路連線只透過縣網中心進行。	<input type="checkbox"/> 是 <input type="checkbox"/> 否	
2.	學校自行管理的資訊應用系統包括？	<input type="checkbox"/> 會計系統 <input type="checkbox"/> 人事系統 <input type="checkbox"/> 學籍系統 <input type="checkbox"/> 網站服務 <input type="checkbox"/> 電子郵件 <input type="checkbox"/> 教學系統 <input type="checkbox"/> 視訊系統	
3.	所勾選之系統所儲存的資訊當有必要和縣(市)網路中心進行網路傳輸時，傳輸連線是否透過專屬線路(如VPN)完成？	<input type="checkbox"/> 是 <input type="checkbox"/> 否	
4.	學校是否與其資訊系統或設備維護及委外廠商，簽訂適當的資訊安全協定或切結書？	<input type="checkbox"/> 是 <input type="checkbox"/> 否	
系統安全			
5.	請列舉學校內所使用的電腦設備場所或類別。	<input type="checkbox"/> 行政辦公室電腦 <input type="checkbox"/> 教師辦公室公用電腦 <input type="checkbox"/> 電腦教室 <input type="checkbox"/> 實驗室教學電腦 <input type="checkbox"/> 一般教室之電腦 <input type="checkbox"/> 伺服器等重要資訊服務提供之電腦設備 <input type="checkbox"/> 其他_____	

編號	檢測項目	符合與否	補充說明
6.	學校所有電腦均安裝防毒軟體?	<input type="checkbox"/> 是 <input type="checkbox"/> 否	
7.	是否針對防毒軟體進行自動更新病毒碼之設定?	<input type="checkbox"/> 是 <input type="checkbox"/> 否	
8.	是否定期針對學校所有電腦系統進行全面病毒掃描?	<input type="checkbox"/> 是 <input type="checkbox"/> 否	
9.	電子郵件是否執行過濾(防範)處理?	<input type="checkbox"/> 是 <input type="checkbox"/> 否 <input type="checkbox"/> 不適用	
10.	學校是否訂定教職員電子郵件使用安全政策	<input type="checkbox"/> 是 <input type="checkbox"/> 否 <input type="checkbox"/> 不適用	
11.	是否瞭解使用未取得授權或盜版軟體的資訊安全風險?	<input type="checkbox"/> 是 <input type="checkbox"/> 否	
12.	請列舉學校內部須保存且重要性高之資料。	<input type="checkbox"/> 學籍資料 <input type="checkbox"/> 教學資料 <input type="checkbox"/> 其他	
13.	上提所列出的重要資料是否定期進行備份?	<input type="checkbox"/> 是 <input type="checkbox"/> 否 <input type="checkbox"/> 不適用 備份頻率：每_____	
14.	備份資料是否存放於機房外之安全區域場所?	<input type="checkbox"/> 是 <input type="checkbox"/> 否 <input type="checkbox"/> 不適用	
15.	是否備有系統維護日誌?	<input type="checkbox"/> 是 <input type="checkbox"/> 否 <input type="checkbox"/> 不適用	
16.	學校的資訊系統之使用是否訂定使用者帳號註冊及註銷政策?	<input type="checkbox"/> 是 <input type="checkbox"/> 否 <input type="checkbox"/> 不適用	
17.	使用者帳號註冊及註銷政策內，是否包含右列各項目?	<input type="checkbox"/> 規定使用唯一的使用者識別碼 <input type="checkbox"/> 檢查使用者是否經過系統所有人之授權 <input type="checkbox"/> 初次登入系統之預設通行碼更改 <input type="checkbox"/> 人員調、離職或退休之帳號註銷流程 <input type="checkbox"/> 保存包含所有識別碼註冊的記錄	
18.	基於作業需要，需提供特定人員設定系統存取特權時，是否記錄具有存取特權者身分以及其特權之權限?	<input type="checkbox"/> 是 <input type="checkbox"/> 否 <input type="checkbox"/> 不適用	
19.	上提存取特權紀錄文件是否妥善保存?	<input type="checkbox"/> 是 <input type="checkbox"/> 否 <input type="checkbox"/> 不適用	

編號	檢測項目	符合與否	補充說明
20.	系統或設備委外廠商因需要必須具備存取權限時，是否另行開設臨時帳號(臨時識別碼與通行碼)，並於委外人員結束服務後，取消該臨時帳號？	<input type="checkbox"/> 是 <input type="checkbox"/> 否 <input type="checkbox"/> 不適用	
21.	是否每一個獨立的系統均設定獨立的帳號？	<input type="checkbox"/> 是 <input type="checkbox"/> 否 <input type="checkbox"/> 不適用	
22.	是否要求使用者對其個人通行碼應盡保密責任？	<input type="checkbox"/> 是 <input type="checkbox"/> 否 <input type="checkbox"/> 不適用	
23.	是否要求使用者初次登入系統後必須立即更改預設之通行碼？	<input type="checkbox"/> 是 <input type="checkbox"/> 否 <input type="checkbox"/> 不適用	
24.	系統安裝後是否管制原始程式？	<input type="checkbox"/> 是 <input type="checkbox"/> 否 <input type="checkbox"/> 不適用	
25.	學校是否定有資訊安全事件通程序？	<input type="checkbox"/> 是 <input type="checkbox"/> 否 <input type="checkbox"/> 不適用	
26.	學校相關人員是否知悉安全事件之通報程序？	<input type="checkbox"/> 是 <input type="checkbox"/> 否 <input type="checkbox"/> 不適用	
27.	宣導學校人員知悉安全事件之通報程序的方式。	<input type="checkbox"/> 公告 <input type="checkbox"/> 通報程序張貼於電腦使用場所 <input type="checkbox"/> 其他_____	
實體安全			
28.	學校電腦機房區域是否獨立或隔離？	<input type="checkbox"/> 是 <input type="checkbox"/> 否 <input type="checkbox"/> 不適用	
29.	學校電腦機房區域進出口是否加強門鎖或其他防範侵入之裝置？	<input type="checkbox"/> 是 <input type="checkbox"/> 否 <input type="checkbox"/> 不適用	
30.	學校電腦機房區域之人員進出是否予以管制？	<input type="checkbox"/> 是 <input type="checkbox"/> 否 <input type="checkbox"/> 不適用	
31.	請說明學校機房區域之人員進出管制方法或限制條件。	<input type="checkbox"/> 只有授權進入機房之人員擁有機房門禁鑰匙 <input type="checkbox"/> 門口設立禁止進入標示 <input type="checkbox"/> 保持門禁的封鎖狀態 <input type="checkbox"/> 其他	
32.	電腦機房內是否嚴禁存放易燃物及未經核准之電器或其他物品？	<input type="checkbox"/> 是 <input type="checkbox"/> 否 <input type="checkbox"/> 不適用	
33.	電腦作業區(含機房)是否執行禁止抽菸及飲用食物？	<input type="checkbox"/> 是 <input type="checkbox"/> 否 <input type="checkbox"/> 不適用	

編號	檢測項目	符合與否	補充說明
34.	電腦機房內系統是否使用不斷電系統?	<input type="checkbox"/> 是 <input type="checkbox"/> 否 <input type="checkbox"/> 不適用	
35.	電腦機房內系統的不斷電系統使用年限為?	<input type="checkbox"/> 是 <input type="checkbox"/> 否 <input type="checkbox"/> 不適用	
36.	電腦機房內連線纜線是否整理分類清楚?	<input type="checkbox"/> 是 <input type="checkbox"/> 否 <input type="checkbox"/> 不適用	
37.	學校電腦教室內連接纜線是否整理分類清楚?	<input type="checkbox"/> 是 <input type="checkbox"/> 否 <input type="checkbox"/> 不適用	
38.	電腦機房內的設備纜線插頭是否均接地處理?	<input type="checkbox"/> 是 <input type="checkbox"/> 否 <input type="checkbox"/> 不適用	
39.	學校電腦教室內的設備連接纜線是否均有接地處理?	<input type="checkbox"/> 是 <input type="checkbox"/> 否 <input type="checkbox"/> 不適用	
40.	學校報廢電腦及其他儲存媒體之程序中，是否有針對所儲存資料進行刪除或格式化處理之項目?	<input type="checkbox"/> 是 <input type="checkbox"/> 否 <input type="checkbox"/> 不適用	
41.	學校電腦機房或其他重要資訊設備區域，須有第三方支援人員進入進行維護、維修、或測試等工作時，是否簽署資訊安全切結書?	<input type="checkbox"/> 是 <input type="checkbox"/> 否 <input type="checkbox"/> 不適用	
42.	學校的資訊設備是否列於學校資產清單中?	<input type="checkbox"/> 是 <input type="checkbox"/> 否 <input type="checkbox"/> 不適用	
43.	學校的資訊設備是否涵蓋於學校資產攜出管理規範中?	<input type="checkbox"/> 是 <input type="checkbox"/> 否 <input type="checkbox"/> 不適用	
44.	學校重要的資訊設備、個人電腦是否均設定具有通行碼管制之銀幕保護程式?	<input type="checkbox"/> 是 <input type="checkbox"/> 否 <input type="checkbox"/> 不適用	
45.	學校的重要公文、儲存媒體長時間不使用或不使用時，是否存放於加裝鎖保護的場所或保存櫃當中?	<input type="checkbox"/> 是 <input type="checkbox"/> 否 <input type="checkbox"/> 不適用	
人員安全			
46.	學校教職員的工作說明書或職員手冊中是否加註對資訊安全保護之要求?	<input type="checkbox"/> 是 <input type="checkbox"/> 否 <input type="checkbox"/> 不適用	
47.	學校之資訊安全政策是否公佈?	<input type="checkbox"/> 是 <input type="checkbox"/> 否 <input type="checkbox"/> 不適用	
48.	是否針對學校教職員進行資訊安全認知之教育?	<input type="checkbox"/> 是 <input type="checkbox"/> 否	

編號	檢測項目	符合與否	補充說明
49.	學校的網路管理人員是否接受資訊安全教育訓練?	<input type="checkbox"/> 是 <input type="checkbox"/> 否	

資訊管理人員：

教務主任：

總務主任：

校長：

文件編號：A-11

帳號申請單(範本)

申請人：		申請日期：	
所屬單位：		分機：	
系統名稱	帳號	申請項目	說明
<input type="checkbox"/> 1.		<input type="checkbox"/> 新增 <input type="checkbox"/> 刪除 <input type="checkbox"/> 重新啟用 <input type="checkbox"/> 停用 <input type="checkbox"/> 異動 <input type="checkbox"/> 重設通行碼	
<input type="checkbox"/> 2.		<input type="checkbox"/> 新增 <input type="checkbox"/> 刪除 <input type="checkbox"/> 重新啟用 <input type="checkbox"/> 停用 <input type="checkbox"/> 異動 <input type="checkbox"/> 重設通行碼	
<input type="checkbox"/> 3.		<input type="checkbox"/> 新增 <input type="checkbox"/> 刪除 <input type="checkbox"/> 重新啟用 <input type="checkbox"/> 停用 <input type="checkbox"/> 異動 <input type="checkbox"/> 重設通行碼	
<input type="checkbox"/> 4.		<input type="checkbox"/> 新增 <input type="checkbox"/> 刪除 <input type="checkbox"/> 重新啟用 <input type="checkbox"/> 停用 <input type="checkbox"/> 異動 <input type="checkbox"/> 重設通行碼	
<input type="checkbox"/> 5.		<input type="checkbox"/> 新增 <input type="checkbox"/> 刪除 <input type="checkbox"/> 重新啟用 <input type="checkbox"/> 停用 <input type="checkbox"/> 異動 <input type="checkbox"/> 重設通行碼	
備註			
執行紀錄			
資訊組長(教師)：		主管覆核：	

帳號使用注意事項

1. 使用者須妥善保管帳號通行碼，不可告知他人或書寫於他人可取得之處，如便條紙、螢幕或主機外殼等，亦應避免放置於其他易遭他人窺視之場所。
2. 使用者通行碼的長度最少應由 8 個字元組成，並且英文與數字混和。
3. 使用者通行碼應避免包含使用者相關之個人資訊，如電話號碼、生日或姓名。
4. 使用者通行碼宜定期變更，並避免重複使用或循環使用舊通行碼。
5. 使用者離職須移除其系統帳號始完成離職手續。