# 苗栗縣僑樂國小資訊安全政策

## 壹、前言：

鑑於近年來電腦及網際網路應用之普及，為確保本校有關資料、資訊系統、設備及網際網路之安全，特訂定資訊安全管理作業規範，作為本校全體員工資訊安全方面之依據。

## 貳、依據：

「行政院及所屬各機關資訊安全管理要點」、「行政院及所屬各機關資訊安全管理規範」及「苗栗縣政府資訊安全政策」等相關規定。

## 參、資訊安全之定義：

為確保資訊處理之正確性、作業人員之忠誠度、所使用事物機器(包括電腦硬體、軟體、週邊)及網路系統之可靠性，並確保各項資源免受任何因素之干擾、破壞、入侵或任何不利之行為，經由適當的系統規劃、程序規範及行政管理的相互配合，以防範來自內、外部的威脅，達到維護系統安全的目的。

## 肆、資訊安全目標：

為避免系統資料及應用軟體有遭受破壞或不當使用之虞，或當已遭受破壞、不當使用等緊急事故發生時，能迅速應變處置以在最短時間內回復正常運作，降低該事故可能帶來之損害。

## 伍、資訊安全範圍：

一、人員：涵概本校正式人員、約聘雇人員及其他使用本校資訊資源之臨時人員、委外廠商人員等。
二、各行政系統：包括公文系統及各業務單位自行開發或由中央開發移撥使用之重要業務系統等。
三、硬體設備：各主機伺服器及個人電腦等。
四、網路及其設施：本校辦公室之區域網路、網際網路之數據專線及相關網路設施。

## 陸、資訊安全之組織、權責及分工

### 一、資訊安全組織

1. 為統籌本校資訊安全管理等事項之協調、規劃、稽核及推動，成立資通安全處理小組。

## 柒、人員安全管理、責任及教育訓練

### 一、人員安全管理

1. 對資訊相關職務及工作，應進行安全評估，並於人員進用、工作及任務指派時，審慎評估人員之適任性，並進行必要的考核。

2. 各單位對於存取重要性與敏感性資訊或系統操作之人員應依相關法令課予軟硬體保管及資料機密維護責任，並加強工作評估、考核，於人員離（休）職時，並應將重要業務最新備份檔案移交列入機關人員職務異動之必要手續。
3. 為降低因人為疏忽或故意，導致資料或系統遭不法或不當之使用或破壞，各業務單位應建立資訊安全稽核制度，必要時，應針對業務性質明定各項資訊業務檢查項目，由單位主管人員及資訊人員偕同進行定期或不定期查考

## 二、人員責任

1. 本校資訊安全政策應以書面、電子或其他方式告知員工，員工應遵守所訂定之相關規範及其他相關資訊安全規定。員工若違反資訊安全相關規定，得依情節輕重予以處分。
2. 本校員工應遵守維護公務機密之相關法令規定；在職及離退職後，均不得洩漏所知悉之業務機密，或為不當之使用，否則得視其情節輕重予以處分或追究其民、刑事責任。

## 三、教育訓練

1. 依員工角色及職務層級，進行適當的資訊安全講習(如：資訊安全、病毒介紹等)，促使教師瞭解資訊安全的重要性，各種可能的安全風險，以提高教師資訊安全意識，促其遵守資訊安全規定。
2. 隨時公告資訊安全相關訊息。

## 捌、電腦系統安全管理

一、電腦主機、各應用伺服器等設備應設置於專用機房，並指定專人負責管理。
二、個人電腦及各項周邊設備等應依業務性質及場地空間等因素做妥適的配置，並應連接不斷電設備系統之電腦專用插座以確保供電之穩定，以防設備受損。
三、資源使用、設備維護狀況應做成紀錄，設備故障並應儘速排除或聯繫維護廠商處理。
四、各單位使用有智慧財產權的軟體，應遵守相關法令及契約規定，非經合法授權及與業務無關之軟體，不得安裝使用，否則除應負有關法律責任外，倘導致各單位設備毀損，並應負相關損害賠償責任。
五、各單位應定期執行必要的資料及軟體備援作業，以便發生災害或是儲存媒體失效時，可迅速回復正常作業。儲存媒體應存放於安全之環境，並定期更換以確保資料之完整可用。
六、資訊業務委外時，應於事前審慎評估可能的潛在安全風險（例如資料或使用者通行碼被破解、系統被破壞或資料損失等風險），並與廠商簽訂適當的資訊安全協定，以及課予相關的安全管理責任，並納入契約條款。

## 玖、網路安全管理

一、開放外界連線作業之資訊系統，應視資料及系統之重要性及價值，採用資料加密、身分鑑別、電子簽章、防火牆及安全漏洞偵測等不同安全等級之技術或措施，防止資料及系統被侵入、破壞、竄改、刪除及未經授權之存取。
二、與外界網路連接之網點，應以防火牆及其他必要安全設施，控管外界與內部網路之資料傳輸與資源存取。
三、應安裝校園版之防毒軟體，建置入侵偵測、弱點分析等防駭軟體以保護機關內部網路免於受病毒感染及惡意軟體或駭客入侵之情事發生，此外設備應隨時上網下載、更新最新病毒碼、主機作業系統漏洞修補等。
四、網路如發現有被入侵或有疑似被侵入情形，應依資通安全處理小組作業要點等相關規定及處理程序，採取必要的行動。

## 壹拾、系統存取控制：

一、使用者新進、調整職務及離（休）職時，應以書面通知人事及各應用系統之作業單位或負責人，各應用系統負責人並應依通知及連線作業使用者申請，新增、調整或刪除其使用權限，確保系統安全。
二、任何帳號皆必須設定通行密碼，使用者通行密碼應符合安全原則，建議使用最少六位長度的通行密碼並應定期更改通行密碼(建議至少三個月一次為原則，最長不宜超過六個月）。
三、人員暫時離開時應使用鍵盤鎖或其他控管措施保護電腦設備，不使用電腦設備時，必須完全登出電腦系統或離線。
四、對系統服務廠商以遠端登入方式進行系統維修者，應加強安全控管，並課其相關安全保密責任。

## 壹拾壹、系統發展及維護之安全管理

一、系統之開發建置、維護、更新、上線執行及版本異動作業，應予安全管制，避免不當軟體、後門及電腦病毒等危害系統安全。
二、對廠商之軟硬體系統建置及維護人員，應規範及限制其可接觸之系統與資料範圍，並嚴禁核發長期性之系統辨識碼及通行密碼。如基於實際作業需要，得核發短期或臨時性之系統辨識及通行密碼供廠商使用，但使用完畢後應立即取消其使用權限。
三、委託廠商建置及維護重要之軟硬體設施，應在本機關相關人員監督及陪同下始得為之。

## 壹拾貳、資訊資產之安全管理

一、建立與資訊系統有關的資訊資產清冊，訂定資訊資產的項目、擁有者及安全等級分類等，由資訊及財產單位負責。
二、依據國家機密保護、電腦處理個人資料保護及政府資訊公開等相關法規，建立資訊安全等級之分類標準，以及相對應的保護措施。
三、已列入安全等級分類的資訊及系統之輸出資料，應標示適當的安全等級以利使用者遵循。

## 壹拾參、實體及環境安全管理

一、支援重要業務運作的資料中心及電腦機房，應設立良好的實體安全措施，地點的選定，應考量火災、水災、地震等自然及人為災害的可能性，並考量鄰近空間的可能安全威脅。

二、電腦設備之設置，應予保護，以防止斷電或其他電力不正常導致的傷害。

三、就設備安置、周邊環境及人員進出管制等，訂定實體及環境安全管理措施。

## 壹拾肆、業務永續運作計畫之規劃與管理

一、評估各種人為及天然災害對業務運作之影響，訂定緊急應變及回復作業程序及相關人員之權責，並定期演練及調整更新計畫。

二、如發生資訊安全事件（包括系統有安全漏洞、遭受非法入侵及破壞、遭遇阻斷服務攻擊及功能不正常事件等），致電腦系統無法運作或影響執行效率時，應迅速通報電腦中心人員及單位主管，本校資安聯絡人並應視情節依行政院國家資通安全會報相關規定向上通報。

三、通報後應立即停止使用受影響之電腦系統或設備，並保留現況，電腦中心人員獲通報後應記錄相關的訊息。

## 壹拾伍、附則

一、資訊安全政策與相關規範應不定期檢討評估，以反映政府法令、技術及業務等最新發展現況，確保資訊安全實務作業之有效性。

二、本資訊安全政策奉　校長核可後實施，修正時亦同。