管理系統文件

文 件 類 別	第 三 階 文 件	
文 件 編 號	IMS-W-003	
文 件 名 稱	個人資料安全控管作業標準	
發 行 單 位	國立虎尾科技大學	
發 行 日 期	109 年 06 月 12 日	
版　　次	3.0	
訂修廢單位	審　　查	核　　准

（原版簽名頁保存於 IMS 推動小組）

訂　　修　　廢　　記　　錄		
版次	發行日期	訂 修 廢 內 容 摘 要
1.0	106/01/11	初版發行
2.0	108/08/21	因應資通安全管理法施行及配合法規用詞，將「資訊」一詞修改為「資通」。
3.0	109/06/12	1.根據「教育體系電子郵件服務與安全管理指引」內規範新增 5.9.1.11、5.9.1.12、5.9.11.13、5.9.11.14 條文。 2.新增 5.11.社交通訊軟體使用規範

1. 目的

依據「個人資料保護法」、「個人資料保護法施行細則」及本校「個人資料保護管理政策」等相關規定，制訂本校個人資料安全控管程序，以確保個人資料受適當的控管與監視，防止不當管控而造成資料外洩之風險。

2. 適用範圍

本校個人資料（含實體及數位的個人資料）之安全管理。

3. 參考文件

3.1. IMS-P-025 個人資料事件管理程序。

3.2. IMS-P-010 人力資源安全與訓練管理程序書。

3.3. 教育體系電子郵件服務與安全管理指引。

4. 名詞定義

4.1. 可攜式資通設備

包含筆記型電腦、平板電腦、智慧型手機、個人數位助理（PDA）、數位播放器、數位相機、錄音筆、燒錄設備或其他具存取數位資料功能之可攜式資通設備及其周邊設備等。

4.2. 可攜式儲存媒體

可供使用者透過資通設備之通信埠，如 Ethernet、USB 埠、1394 埠等進行大量資料存取之媒體，包含 USB 隨身碟、可攜式硬碟、磁片、光碟片、Compact Flash（CF 卡）、Secure Digital card（SD 卡）等數位相機記憶卡或其他具存取數位資料功能之媒體。

4.3. 一般資通設備

意指桌上型個人電腦、可攜式資通設備、可攜式儲存媒體、印表機、影印機、傳真機及掃描器等一般性資通設備。

5. 作業內容

5.1. 人力資源安全與教育訓練之管理

5.1.1. 為維持重要（核心）業務之營運與管理，不致因員工休假而耽誤本校業務之正常運作，應建立職務代理人制度或人力備援機制。

5.1.2. 本校同仁於到職時應簽署保密切結，於業務上所獲知之機敏資訊非經主管授權不得對外透露，並恪盡保密之責。

5.1.3. 本校同仁、接觸個人資料之外部人員、委外廠商人員於在職及離、退職後，均不得洩漏所知悉之機敏資訊，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。

5.1.4. 本校員工應恪遵「個人資料保護法」，保護本校個人資料使用之合法性、機密性與完整性。

5.1.5. 本校同仁若發現個人資料事故時，應依據「IMS-P-025 個人資料事件管理程序」之相關規定進行通報，並由該事故權責單位進行後續處理改善。

5.1.6. 本校同仁若違反個人資料管理政策、相關法令法規或發生任何危及本校聲譽之行為（如電腦洩密、盜取個人資料…等），都將依正式懲戒程序處置相關違紀人員或訴諸法律行動。

5.1.7. 有關個人資料保護人員教育訓練之管理作業，應依據「IMS-P-010 人力資源安全與訓練管理程序書」之規定辦理。

5.2. 實體與環境安全之管理

5.2.1. 各單位公務文書及紙本郵件應有專人負責收發。

5.2.2. 未經授權不得將機敏文件攜出辦公環境區域。若有需要，須經主管人員核准，始得進行。

5.2.3. 處理完之個人資料檔案(紙本、電子)，若無需保留應立即絞碎或刪除(電子檔案應確實清除「資源回收筒」)，含有個人資料之報廢紙張不得回收及再利用。

5.2.4. 針對存有個人資料之紙本文件及可攜式儲存媒體，不使用或下班時，應遵守桌面淨空政策，放置於抽屜或儲櫃並上鎖，以避免個人資料外洩。

5.2.5. 為確保本校相關資通設施及資料保護之安全，非業管權責單位指定或授權之人員，不得擅自進入處理與存放機敏資訊之場所。

5.2.6. 本校同仁應保持警覺，留意陌生人員進出辦公環境，若發現身分不明或可疑的人員，應主動詢問其身分並視需要通知權責單位進行處理。

5.2.7. 委外廠商及訪客應於本校各單位指定之區域內活動。

5.2.8. 存放機敏資訊之儲存空間應建立門禁管理，如透過鑰匙或門禁卡等方式進行管控。

5.3. 網路連線安全之管理

5.3.1. 一般規範

5.3.1.1. 使用者需經授權並賦予相關存取權限後，始得使用本校所提供之各項網路服務，已授權的使用者，僅能在授權範圍內存取網路資源。

5.3.1.2. 使用瀏覽器應先評估所瀏覽網頁之安全性，並適度調整瀏覽器安全性設定（如設定「網際網路」之安全層級為「中」以上）。

5.3.1.3. 使用者不得將個人之網路登入身分識別與密碼交付他人使用，亦禁止以任何方法竊取他人的登入身分識別與密碼。

5.3.1.4. 禁止以任何儀器設備或軟體工具竊聽網路上的通訊，也不得以任何手段，蓄意干擾或妨害網路的正常運作。

5.3.1.5. 使用者如發現網路出現異常時，應立即將電腦關閉或將網路斷線，並通報專責人員處理。

5.3.1.6. 嚴禁利用本校網路散布機敏性或違反法令法規之個人資料及檔案。

5.3.1.7. 禁止瀏覽不當之網站（如暴力、色情、賭博、惡意網站等）及散播色情文字、圖片、影像、聲音等不法或不當的資訊，並不得使用與工作無關之串流媒體、MP3、圖片、檔案等傳輸，以避免造成網路壅塞。

5.3.1.8. 禁止使用點對點（Peer to Peer, P2P）類型的傳輸軟體（如ezPeer、KURO、FOXY、e-Donkey、BT…等類型軟體）下載檔案及提供檔案分享。

5.3.1.9. 除因公務需要且經權責主管核可外，禁止傳送機敏性資料檔案給他人或傳送至網際網路上（如他人之郵件信箱或個人外部郵件信箱、網路硬碟、雲端儲存空間、FTP 站及即時通訊軟體之傳送等）。

5.3.1.10. 禁止使用民間業者（如：Google、Dropbox 等）提供之雲端儲存空間、FTP 站及個人外部郵件信箱等進行公務機敏資料交換或儲存，或傳送予業務無關之他人，以免造成本校機敏資料外洩風險。

5.3.1.11. 因業務需要須開啟網路芳鄰分享檔案時，應將存放機密資料的資料夾或是檔案本身加密或是加密碼保護，以確保資料存取之安全。

5.3.1.12. 機敏資訊未經加密或啟動密碼保護，一律禁止使用公眾網路進行傳送。

5.3.1.13. 開放提供委外廠商進行遠端存取服務時，必須由專責人員進行安全評估，確定可行且無安全顧慮，經權責主管核准後方得開放，開放時必須限制網路功能以確保網路安全。

5.3.2. 智慧財產權

5.3.2.1. 禁止下載或安裝來路不明、非公務使用及有違反法令疑慮（如智慧財產權等）的資訊檔案、電腦程式與軟體，以防止被植入後門或木馬程式。若需安裝軟體，須取得合法授權後，始可進行相關作業。

5.3.2.2. 未經著作權人之同意，使用者不得將受保護的著作上傳於公開之網站上。

5.3.2.3. 使用者不得利用本校網路進行其他可能涉及侵害智慧財產權之行為。

5.4. 帳號密碼及存取控制之管理

5.4.1. 存取控制政策

5.4.1.1. 個人資料之存取應與本身業務範圍相關，任何人未經授權不得存取與個人業務無關之個人資料。

5.4.1.2. 權責主管應審慎評估重要系統特殊權限之授權管理。

5.4.1.3. 因處理系統當機與異常狀況需視狀況授與適當之存取權限，並避免共用帳號，如特殊情況，需共用帳號時，應建立可歸責性之機制，以利識別身分。

5.4.1.4. 可攜式設備及儲存媒體，如筆記型電腦、隨身碟、光碟、磁帶等，應採取適當控管措施，避免個人資料未經授權存取。

5.4.1.5. 個人資料之存取必須符合「個人資料保護法」、「個人資料保護法施行細則」等相關法令之要求與規定，或契約對資料保護及資料存取使用控管之權責規定。

5.4.1.6. 針對無人看管的資通設備，應有適當控管程序，以防未經授權之存取或濫用。公共使用之影印機、印表機、傳真機或多功能事務機每日應檢視有無個人資料遺留。

5.4.1.7. 為確保個人資料之安全，對敏感性系統或處理大量個人資料之資通設備，應採取適當控管程序或隔離措施。

5.4.1.8. 伺服器、個人電腦及筆記型電腦應設定螢幕保護程式，並設定密碼或採取登出鎖定方式保護；自行啟動螢幕保護程式的時間設定應不超過 10 分鐘。

5.4.2. 使用者帳號管理

5.4.2.1. 使用者帳號申請

5.4.2.1.1. 新進同仁報到後，由人事部門建立人事資料，由新進同仁向權責單位提出申請，權責單位再依工作職掌所需開立帳號並授予適當之權限。

5.4.2.1.2. 本校具機敏性資料之應用系統帳號須經申請並核可後，方可建立帳號使用。非業務權責單位人員如需使用其資通系統時，須經業務權責單位主管核可後方得使用。

5.4.2.2. 使用者帳號異動

5.4.2.2.1. 除特殊規定外，員工離、退職時，系統管理人員於收到相關單位通知後，應進行帳號註銷或停用。

5.4.2.2.2. 員工內部調職時，應提出異動申請，系統管理人員應確實刪除其原單位之存取權限。

5.4.2.2.3. 員工留職停薪時，系統管理人員於收到人事單位通知後，應停用其權限範圍以外的帳號。

5.4.2.3. 特殊權限帳號管理

5.4.2.3.1. 系統管理人員應避免共用管理者帳號，記載重要系統管理者帳號與密碼之文件，應密封並存放於上鎖之安全處所。

5.4.2.3.2. 具機敏性資料之伺服器及資料庫，其特殊權限帳號應每年清查，並留下查核結果紀錄陳權責主管審核。

5.4.2.3.3. 新購置之資通設備或系統，應於安裝完成後刪除或關閉不必要之帳號及更改預設密碼。

5.4.3. 密碼安全使用規範

5.4.3.1. 使用者首次登入系統時，應立即變更預設密碼，並妥善保管帳號與維持密碼之機密性。

5.4.3.2. 應用系統或個人建立之帳號密碼檔案，應加密碼方式保護。

5.4.3.3. 密碼長度設定
一般資通設備使用者之密碼長度設定至少 8 碼（含）以上，且須每隔 6 個月更換密碼一次，密碼變更時應避免重複或循環使用舊密碼。

5.4.3.4. 密碼內容設置原則

5.4.3.4.1. 密碼內容之設定，應包含阿拉伯數字及英文字母，建議包含特殊符號。另重要資通系統（如：網域及含有個人資料等系統）的密碼建議採複雜性原則。

5.4.3.4.2. 複雜性原則

A. 密碼必須包含英文大寫字母、英文小寫字母、阿拉伯數字及特殊符號四個類別中至少兩種。

B. 密碼內容之設定，避免使用與個人有關之資料做為密碼，如下說明：

(a) 使用者識別碼、出生年月日、身分證字號。

(b) 汽機車牌照號碼、機關單位簡稱。

(c) 電腦主機名稱、作業系統名稱。

(d) 電話號碼、空白、字典字彙（具有意義的英文單字，例如：flower、eagle、birthday 等）。

5.4.3.5. 使用者須負密碼保護之責，不得對任何人透露或以任何形式公開自己帳號及密碼，以避免密碼外洩。

5.4.3.6. 本校人員及委外廠商有保護通行碼之責，應避免將帳號密碼張貼或放置於伺服器、網路設備、個人電腦、螢幕或其他無任何防護措施之場所。

5.4.3.7. 使用者若懷疑密碼被他人知悉或發現密碼疑遭盜用或破解時，應立即更改密碼。

5.4.3.8. 除特殊需求外，禁止使用者與他人共用自己或他人的帳號及

密碼，且帳號與密碼應存放於安全之處，保存帳號、密碼之檔案應以加密或加密碼之方式保護。

5.4.3.9. 禁止盜用或冒用他人帳號及密碼使用網路資源，或將個人帳號及密碼借予他人使用。

5.4.3.10. 使用者忘記密碼時，應依帳號及密碼申請規定向系統管理者提出申請，由系統管理者確認身分後，重新設定新密碼。

5.4.3.11. 使用者登入系統時應避免使用記錄密碼之功能，以免開機時自動登入系統。

5.4.4. 使用者存取權限

5.4.4.1. 對於職務異動如調、離職、留職停薪人員等，依本程序書之使用者帳號異動辦理，據以異動、註銷或停用存取權限。

5.4.4.2. 使用者存取業務相關之個人資料須經授權，其帳號應為唯一之識別碼，禁止借用他人之帳號或共用帳號。

5.4.4.3. 久未登入系統之帳號應妥善管理，經確認無須使用後，應予以刪除。

5.4.5. 作業系統存取控制

5.4.5.1. 除因老舊系統或特殊情形外，應啟動系統紀錄功能。

5.4.5.2. 系統紀錄存取，應限定僅由系統管理人員或被授權者存取。

5.4.5.3. 帳號名稱應避免顯示任何足以辨識為特殊權限的訊息，如管理者或監督者。

5.4.6. 應用系統之存取控制

5.4.6.1. 應用系統資訊之使用，僅限業務相關之授權使用者，並應適當控制。

5.4.6.2. 應用系統之「機敏」等級以上資訊，應與一般資訊作適當區隔，並加強權限控管措施。

5.4.6.3. 會談期逾時之控制

使用者登入應用系統後，若超過所規定的閒置時間而無任何動作時，系統會啟動會談期逾時(Session timeout)控制，將其帳號登出，以防止未經授權使用者的存取及阻絕服務之攻擊(若屬功能限制或系統老舊無法提供此功能，待版本升級或更新系統時改善)。

5.4.7. 網路存取控制

5.4.7.1. 網路系統應依安全需求區隔不同區域，並設置網路安全設備如防火牆及網路閘門等加以保護。

5.4.7.2. 網路之存取活動，應定期檢視，並留存日誌備查。

5.4.7.3. 對於開放提供外部客戶或廠商存取之服務，必須限制使用者之網路功能以確保網路安全。

5.4.7.4. 網路路由之規劃必須確保任何網路連線或資訊傳輸符合網路存取之安全需求。

5.4.8. 遠端存取之限制

5.4.8.1. 委外廠商及本校員工非經授權許可，一律禁止執行遠端存取作業。

5.4.8.2. 須進行遠端連線存取個人資料時，應限定標的範圍及來源 IP 位址，並陳權責主管審核。

5.4.9. 資料庫存取控制

5.4.9.1. 資料庫帳號管理

5.4.9.1.1. 進行資料庫存取作業時，應啟動作業系統或資料庫系統之身分識別機制。

5.4.9.1.2. 具機敏性資料之資料庫系統存取帳號，應依功能區分為應用系統及資料庫管理之帳號，並給予適當之權限。

5.4.9.1.3. 具機敏性資料之資料庫系統存取授權，應以執行業務及

職務所需者為限，當使用者職務異動時，須依照本程序書 5.6 之使用者存取管理原則辦理。

5.4.9.1.4. 具個人資料之資料庫系統帳號之密碼，須為英文大小寫、數字及特殊符號混合使用，且不得與帳號名稱相同，密碼長度至少為 8 碼，並嚴禁管理人員轉知他人。

5.4.9.1.5. 具機敏性資料之資料庫最高權限帳號存取授權，應僅限於資料庫管理人員或職務代理人。

5.4.9.1.6. 應變更資料庫預設帳號之密碼或關閉使用。

5.4.9.2. 資料庫異動與測試

5.4.9.2.1. 應用系統測試及正式作業所需資料庫管理系統，宜分別在不同伺服器下執行，並避免資料遭意外竄改或不當使用。

5.4.9.2.2. 具機敏性之測試資料，應僅由系統管理人員進行存取，且應將個人資料內容轉換為虛擬資料、模糊化或遮蔽。

5.4.9.2.3. 正式資料庫系統變更作業前，如資料庫系統版本更新、安裝修補程式等，應先評估對現行系統之影響後始得變更，重大變更作業須經權責主管核准後始可實施。

5.4.9.2.4. 資料庫變更作業應經由權責主管同意後授權進行。資料庫公用程式存取權限應適當控管，禁止一般使用者存取。

5.4.9.2.5. 對外提供服務之重要應用系統，其後端資料庫應考量連接可限制存取之網路設備統一控管，避免資料庫遭入侵。

5.5. 系統開發與維護之管理

5.5.1. 資通系統應保護「機敏」等級以上之資料，防止洩漏或被竄改，必要時應使用資料加密相關機制保護。

5.5.2. 系統測試環境所使用之設備環境應予獨立，不應與提供服務之設備環境共用。

5.5.3. 具機敏性資訊之應用系統，應設計加密傳輸機制(如 SSL 或 https 等)，必要時應針對資料內容加以保護(如資料庫加密)，並記錄傳輸的相關資訊，包含傳輸來源、接收目的位址、傳送時間與傳輸成功或失敗等資訊。

5.5.4. 系統伺服主機須由系統管理者評估其需要，若不會影響系統效能且有安全防護需求，則必須安裝防毒軟體，避免受到病毒的感染。

5.5.5. 應用系統安裝及佈署時，應評估執行下列安全檢測：

5.5.5.1. 資料庫伺服器檢測
檢測內容含：Patch 更新考量、不必要之通訊協定、服務及通訊埠關閉、預設資料庫移除、使用者與系統管理員帳號密碼安全強度、安全稽核功能設定及日誌檔備份等。

5.5.5.2. 網站及應用伺服器檢測
檢測內容含：跨網站指令碼(Cross Site Scripting，XSS)、注入缺失(Injection Flaw)、Patch 更新考量、不必要之通訊協定、服務及通訊埠關閉、使用者與系統管理員帳號密碼安全強度及日誌檔備份、每個網頁之安全控管等。

5.5.6. 應對具個人資料之重要資通系統定期實施弱點掃描或滲透測試，以鑑別各單位應用系統與作業環境之風險，並針對弱點部分實施修補與改善，並保留相關紀錄以備查核。

5.5.7. 系統開發委外安全控管
為確保應用系統之安全性與可靠性，應於契約書中明訂下列安全管理事項：

5.5.7.1. 系統需求分析時，應考量現況及未來應用系統之運作環境配置、資料之重要性及遭受攻擊之可能性，據以發展應用系統之安全需求及系統功能。

5.5.7.2. 程式測試時，應進行相關安全性檢測，並提供相關測試報告與紀錄。

5.5.7.3. 委外廠商每次交付之應用程式版本，應進行應用程式安全弱

點掃描，若有弱點存在，委外廠商須負責修改。

5.5.7.4. 契約期間如發生程式錯誤或資料漏失，經確認屬委外廠商責任者，應由委外廠商負責更正；另損及他人權益時，亦由委外廠商負責。

5.5.7.5. 委外廠商對業務上所接觸之資料，應採必要之保密措施。委外廠商及專案相關人員均應依本校規定填具保密切結。

5.5.7.6. 委外廠商應配合本校安全控管要求，辦理應用系統弱點修補、異常排除、事件通報及進行相關演練作業事宜。

5.6. 資訊備份之管理

5.6.1. 個人電腦使用者應定期將重要的資料進行備份，確保備份資料之安全性，以避免非授權的存取。

5.6.2. 備份資料至少每年執行資料回復測試，以確認備份資料之可用性。

5.6.3. 存放重要機敏資料之備份媒體應存放於安全場所。備份媒體運送過程中應存放於上鎖之媒體保護箱由專人親送。

5.6.4. 各單位應對存有個人資料之系統伺服器進行備份。備份作業應儘量於離峰時段進行。

5.7. 一般資通設備安全使用規範

5.7.1. 本校所配發之一般資通設備以公務使用為原則，使用者須合理的使用個人電腦資源，且符合本校使用規範並接受相關稽查管考。

5.7.2. 個人電腦、筆記型電腦或平板電腦等應依正常開（關）機操作程序使用及保管，下班或長時間不用時應關機並關閉相關電源，可攜式儲存媒體應上鎖保護。

5.7.3. 離開座位時，應將電腦鎖定及啟用螢幕保護程式，並啟動密碼以保護電腦資料安全，並將螢幕保護啟動時間設定在 10 分鐘以內，以避免他人偷窺及使用電腦。

5.7.4. 筆記型電腦及平板電腦等須攜出使用時，請妥善保管，且應先評

估外部網路環境之安全性，不可隨意連線至不明或不安全之無線或有線網路環境。

5.7.5. 個人電腦之軟、硬體安裝後，使用者在使用時如發生任何問題，應立即向專責人員反應處理。

5.7.6. 電腦使用者非經授權嚴禁擅自拆卸或加裝電腦週邊設備或更改系統環境設定（如 IP、GATEWAY、DNS 等）與設定檔，若發生故障或是有異常情況時，使用者應通報專責人員處理。

5.7.7. 存放於一般資通設備之機敏性檔案非經核可不得攜出，且應加密或設密碼保護，以防止資料外洩。

5.7.8. 因業務需要須開啟網路芳鄰分享檔案時，應將存放機密資料的資料夾或是檔案本身加密或是加密碼保護，以確保資料存取之安全性。

5.7.9. 使用影印機、印表機、傳真機、掃描機或多功能事務機處理機敏性文件後，應立即將文件資料取走，並予以適當保存。

5.7.10. 個人電腦須設定校時（時間同步）功能，以維持系統時間的一致性，確保系統稽核紀錄的正確性及可信度，作為事後法律上或是紀律處理上的重要依據。

5.7.11. 含有機敏資料之儲存媒體(如硬碟、隨身碟或光碟片)在進行報廢前，必須實體破壞或利用工具進行消磁，確保資料已被完全銷毀防止資料外洩。

5.8. 電腦防毒及惡意軟體入侵保護管理

5.8.1. 本校個人電腦應安裝防毒軟體，電腦使用者或管理者應注意病毒碼更新狀況並定期執行個人電腦、筆記型電腦病毒掃描。本校電腦所安裝之防毒軟體，不得擅自卸載或移除。

5.8.2. 與其他外部電腦、可攜式資通設備及可攜式儲存媒體交換檔案資料時，必須先經過病毒掃描方可進行。

5.8.3. 電腦使用者或管理者應定期更新作業系統及其它應用程式之弱點

修補程式，並保持更新至最新狀態。

5.8.4. 如遇疑似惡意程式或病毒感染情況，防毒軟體無法處理或作業仍不正常時，使用者應立即通報資訊人員處理。

5.8.5. 如需使用外來(非本校提供)的可攜式設備或儲存媒體，必須先進行掃毒的動作，以避免電腦、系統與網路受到惡意程式威脅。

5.8.6. 如遇疑似惡意程式感染情況，防毒軟體無法處理或作業仍不正常時，使用者應立即通報專責人員處理，若確認為惡意程式感染事件後，由專責人員判斷感染途徑及其惡意程式名稱，並協助使用者將惡意程式移除或隔離。

5.9. 電子郵件安全使用規範

5.9.1. 一般規範

5.9.1.1. 電子郵件使用者需經授權並賦予相關存取權限後，始得使用本校電子郵件系統收發電子郵件。

5.9.1.2. 為避免遭他人冒用個人電子郵件信箱，使用者應妥善保管密碼且定期更改密碼，並不得將個人帳號借予他人使用。

5.9.1.3. 禁止使用帳號傳送或轉發煽動性、毀謗性、威脅性、猥褻性、商業性及違法的電子郵件。

5.9.1.4. 內部互傳或對外的每封電子郵件傳送時，不應超過規定之大小限制，並禁止傳送垃圾郵件，以免影響頻寬，浪費網路資源。

5.9.1.5. 禁止電子郵件使用者發送電子郵件騷擾他人，或偽造他人名義發送電子郵件，導致其他使用者之不安與不便。

5.9.1.6. 若收到來路不明之電子郵件，應立即刪除。禁止開啟或轉寄來路不明的電子郵件及其附件檔案或連結，以免遭受惡意程式或病毒的感染。

5.9.1.7. 電子郵件使用者如發現疑似電子郵件病毒事件，應立即關閉個人之電子郵件收發軟體，並通報專責人員處理。

5.9.1.8. 非公務需求且未經權責主管核可，禁止透過電子郵件寄送未加密或未啟用密碼保護之機密性資料,且勿將密碼寫在 E-mail 內容中。

5.9.1.9. 若公務需要需透過電子郵件傳送機敏性資料時，需經權責主管核可後，於傳送之前將檔案以加密、加密碼保護或電子簽章等安全技術處理。

5.9.1.10. 郵件收發軟體應設定關閉郵件預覽及不自動下載 HTML 郵件中的圖片功能。

5.9.1.11. 本校使用者使用電子郵件服務時，應尊重網路隱私權，不得任意窺視其他使用者之個人資料或有其他侵犯隱私權之行為。不得盜用他人或系統資源，或以任何方式影響系統正常運作。

5.9.1.12. 本校使用者辦理公務、及重要（或敏感）專案使用之電子郵件信箱（可規劃專用電子郵件信箱），不得轉至外部私人信箱收發公務資訊。

5.9.1.13. 教職員如轉任或借調至公務機關服務者，不得使用學校電子郵件信箱收發公務機關相關電子郵件。

5.9.1.14. 使用者如因故無法使用公務信箱讀取訊息，以致影響公務執行，得由直屬單位主管指定代理人提出申請，並經郵件維護負責單位審核必要性後，授權代理人讀取公務信箱相關內容。

5.9.2. 智慧財產權

5.9.2.1. 不得引用來源不明的電子郵件或檔案內容。

5.9.2.2. 禁止以電子郵件傳遞或交換非法之應用軟體。

5.10. 可攜式設備及儲存媒體之安全使用規範

5.10.1. 員工一律禁用可攜式設備及可攜式儲存媒體等設施，如公務上須使用則須提出申請經權責主管核准後方可使用。

5.10.2. 可攜式設備及可攜式儲存媒體僅限於公務使用，禁止使用於私人

用途，使用時應謹防資訊外洩或中毒。

5.10.3. 使用可攜式儲存媒體時須先進行掃毒以確認其不含病毒與惡意程式，掃毒後方可進行資料之上傳及寫入作業。

5.10.4. 將機密資料存放於可攜式儲存媒體上時，得採取適當加密處理或設定密碼保護（如 Word、Excel 或壓縮軟體之密碼功能），避免可攜式儲存媒體遺失時造成資訊外洩。

5.10.5. 筆記型電腦應安裝防毒軟體，並定期檢查作業系統修正程式與更新病毒碼為最新版本。

5.10.6. 存有重要機密性資訊之可攜式資通設備或儲存媒體攜出時，設備管理人員應負保護之責不得離身，且針對相關檔案資料須執行加密或先清除其機密資訊，以避免資料洩露，另作業完成後須徹底抹去媒體上相關資料。

5.10.7. 廠商所交付本校之光碟（含程式、系統文件、手冊或其他業務資料等），其保存應由專人保管。

5.10.8. 筆記型電腦於本校外部環境使用時，應考量以下防護措施：

5.10.8.1. 筆記型電腦須於本校外部環境使用網路時，應先評估網路環境之安全性，並確認電腦內之防毒軟體已更新為最新版本。

5.10.8.2. 筆記型電腦須於本校外部公共空間使用時，若螢幕畫面顯示敏感或機密資訊時，應注意畫面是否有遭旁人窺視之疑慮。

5.10.8.3. 不可將筆記型電腦置於視線以外之處，應隨身攜帶確保實體安全。

5.10.9. 用外來的可攜式設備及可攜式儲存媒體，必須先進行掃毒的動作，以避免本校電腦、系統與網路受到病毒威脅。

5.10.10. 可攜式設備及儲存媒體遺失時應立即通報單位主管，並評估資料遺失是否具有機密性，依情節之重大程度決定是否向上呈報。

5.10.11. 外校可攜式設備或儲存媒體的安全要求

5.10.11.1.非本校之可攜式資通設備如需連接本校網路進行維護或測試作業時，須經權責主管同意後於限定場所內使用。

5.10.11.2.連接本校網路之可攜式資通設備須具備適當之防毒能力，並更新至最新之病毒碼，作業系統及相關應用程式等亦須更新至最新之弱點修正程式。

5.10.11.3.使用者如需使用外來的可攜式設備或儲存媒體，必須先進行掃毒的動作，以避免電腦、系統與網路受到惡意程式威脅。

5.10.11.4.於本校網路使用可攜式資通設備應遵守本校相關管理規範，不可再開啟其他無線網路裝置，未經申請核可，禁止執行封包、收集分析等軟體以及任何網路偵測之行為。

5.10.11.5.如上述該項作業之目的為執行網路偵測或封包收集分析，應由本校相關人員全程陪同。

5.10.11.6.具有照相或錄影功能之可攜式資通設備，未經同意不得進行拍攝，如經本校同意拍攝時應有本校人員陪同。

5.10.11.7.非本校人員欲使用可攜式儲存媒體攜出本校資料時，本校業務承辦人必須詳細記載使用人員之服務單位等相關資訊並說明用途，經業務承辦人員確認可攜式儲存媒體不含病毒與惡意程式，方可進行資料上傳及寫入作業，且業務承辦人員應陪同並確認寫入資料之內容。

5.10.11.8.機密資料檔案的讀取及複製須符合本校各業務單位的規定，並經該單位主管或其授權人員核可。

5.11. 社交通訊軟體使用規範

5.11.1 嚴禁利用社交通訊軟體網路散布機密性或違反法令法規之資料及檔案。

5.11.2 除因公務需要且經權責主管核可外，禁止利用社交通訊軟體傳送機密性資料檔案給他人或傳送至網際網路上。

5.11.3 嚴禁使用社交通訊軟體傳送色情文字、圖片、影像、聲音等不法

或不當的資訊或來源不明、來源未經授權、或自未經信任網路接收或下載檔案與連結。

5.12. 安全查核

5.12.1. 每年由各單位資安及個資保護專責人員，依「IMS-W-003-01 辦公區域安全檢查表」之檢查項目逐一進行查核作業，並於檢查表上簽名，送交單位主管審核。

5.12.2. 每年由各單位資安及個資保護專責人員，將「IMS-W-003-02 個人電腦安全檢查表」發給電腦使用人員，並依檢查表中之各項檢查項目進行自我查核，完成查檢且經單位主管審核後，將檢查表送交個人資料保護專責人員進行抽檢。

5.12.3. 資安及個資保護專責人員如發現不符合項目時，應報請單位主管指定相關人員協助進行異常狀況處理。

5.13. 異常處理

查核結果若屬不符合事項，則由單位主管指派專人進行異常狀況之處理，異常狀況若無法即期處理及改善，則依據「IMS-P-008 矯正預防及持續改善管理程序」之相關規定執行矯正與預防措施，進行問題矯正及風險預防作業。

5.14. 紀錄保存

相關業務承辦人員應參照如下規範，妥善保存各項紀錄。

編號	表單名稱	保存地點	保存期限
1	辦公區域安全檢查表	各單位	至少 3 年
2	個人電腦安全檢查表	各單位	至少 3 年

6. 相關表單

6.1. IMS-W-003-01 辦公區域安全檢查表。

6.2. IMS-W-003-02 個人電腦安全檢查表。