新北市私立竹林高級中學資通安全管理計畫

機密等級：一般

承辦單位(資訊組)	單位主管(圖書館主任)	校長
資訊組長何宗達	圖書館主任黃琳玲	校長顏麗珠

中 華 民 國 一 〇 九 年 六 月 八 日 星 期 一

新北市私立竹林高級中學資通安全管理計畫

機密等級：一般

承辦單位(資訊組)	單位主管(圖書館主任)	校長

中 華 民 國 一 〇 九 年 六 月 八 日 星 期 一

壹、依　據

一、依行政院八十八年九月十五日台八十八經字第 34735 號函訂頒『行政院及所屬各機關資訊安全管理要點』。
二、依據資通安全管理法第 10 條及施行細則第 6 條規則訂定。

貳、目的及適用範圍

本計畫適用全機關範圍，強化本校資訊安全管理，建立安全及可信賴之數位化校園，確保資料處理、系統、設備及網路安全，保障教職員工權益，特訂此管理計劃。

參、資通安全政策及目標

一、資訊安全政策內容訂定

為使本機關業務順利運作，防止資訊或資通系統受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，並確保其機密性(Confidentiality)、完整性（Integrity）及可用性 （Availability）並，特制訂本政策如下，以供全體同仁共同遵循：

1.應建立資通安全風險管理機制，定期因應內外在資通安全情勢變化， 檢討資通安全風險管理之有效性。
2.應保護機敏資訊及資通系統之機密性與完整性，避免未經授權的存 取與竄改。
3.應強固核心資通系統之韌性，確保機關業務持續營運。
4.應因應資通安全威脅情勢變化，辦理資通安全教育訓練，以提高本 機關同仁之資通安全意識，本機關同仁亦應確實參與訓練。
5.針對辦理資通安全業務有功人員應進行獎勵。
6.勿開啟來路不明或無法明確辨識寄件人之電子郵件。
7.禁止多人共用單一資通系統帳號。

二、核定程序

本辦法經各處室主任、校長核示後，得實施並公告。

三、宣導程序

透過教學研究會及教師工作會報提請討論，加入宣達事項，所訂定之資訊安全管理政策，以書面公告、資訊研習、教育訓練、內部會議等其他方式告知本校教職員工、提供資訊服務之廠商共同遵行。

四、定期檢討

資訊安全管理政策實施後，資通安全政策及目標應定期於資通安全管理審查會議中檢討其適切性，資訊組須定期評估一次，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。

五、資安目標

量化指標：

1. 核心資通系統可用性達 85%以上。
2. 知悉資安事件發生，能於規定的時間完成通報、應變及復原作業。
3. 電子郵件社交工程演練之郵件開啟率及附件點閱率分別低於 6%及 3%。

質化指標：

1. 適時因應法令與技術之變動，調整資通安全維護之內容，以避免資通系統或資訊遭受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，以確保其機密性、完整性及可用性。
2. 達成資通安全責任等級分級之要求，並降低遭受資通安全風險之威脅。
3. 提升人員資安防護意識、有效偵測與預防外部攻擊等。

肆、資通安全推動組織架構

一、職務權責說明

1. 資通安全長：圖書館主任

(1)資訊安全政策、計畫及技術規範之研議、建置及評估等事項。

(2)資料及資訊系統之安全需求研議、使用管理及保護等事項。

(3)成立跨處室之資通安全推動小組，負責協調及推動，統籌資訊安全政策、計畫、資源調度等事項之協調、研議。

2. 資通安全推動小組：負責資通安全規劃及推動、執行實施作業。

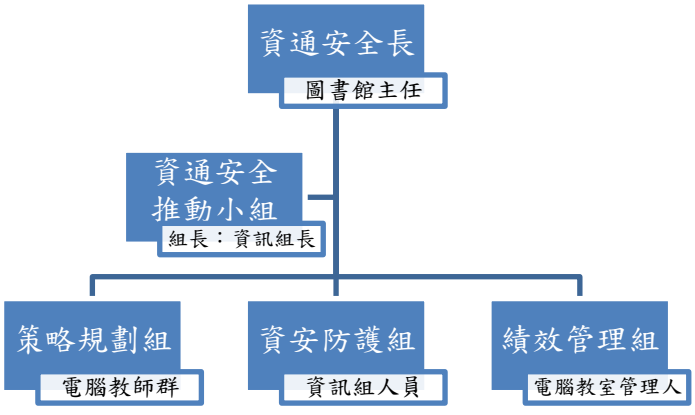
(1)資通安全推動小組組長：資訊組長，統籌管理小組執行業務。

(2)策略規劃組：資通安全政策及目標之研議，訂定機關資通安全相關規章與程序、制度文件，並確保相關規章與程序、制度合乎法令及契約之要求，依據資通安全目標擬定機關年度工作計畫，資通安全技術之研究、建置及評估相關事項。

(3)資安防護組：由資通安全人員負責傳達機關資通安全政策與目標，資通安全相關規章與程序、制度之執行，資訊及資通系統之盤點及風險評估，資料及資通系統之安全防護事項之執行，資通安全事件之通報及應變機制之執行。

(4)績效管理組：辦理資通安全內部稽核，定期召開資通安全管理審查會議，提報資通安全事項執行情形。

二、資通安全推動小組組織圖



三、資通安全推動小組經費規劃

資通安全推動小組定期規劃防毒軟體、軟硬體及系統維護費、資訊及資安相關教育訓練及研習。

例行性經費項目：

1.伺服器防毒軟體授權規劃。

2.防火牆維運及租用經費規劃。

3.依照每學年計畫補助或學校經費辦理資訊及資安相關研習。

4.學校官網系統維護費用規劃。

5.欣河學籍系統維護費用規劃。

6.清江圖書館系統維護費用規劃。

7.網路系統及資訊設備維修經費規劃。

伍、資訊及資通系統之盤點

每年度辦理資訊及資通系統資產盤點，並製作「資訊設備清冊」，資產如有異動，由資通安全推動小組更新資產清冊，資訊清冊內容含電腦、印表機、網路硬體設備、防火牆等資料，註明其規格、年度、名稱項目、存置地點等資料，並建檔於雲端儲存強化其安全性。

陸、資通安全防護及控制措施

一、資訊及資通系統之保管：

1.資訊及資通系統管理人應確保資訊及資通系統已盤點造冊並適切分級、持續更新。

2.資訊及資通系統管理人應確保資訊及資通系統被妥善保存或備份。

3. 資訊及資通系統管理人應確保屬重要者，已採取適當之存取控制政策。

二、資訊及資通系統之管理：

1.使用資訊及資通系統前應經其管理人授權。

2.使用資訊及資通系統時，應留意其資通安全要求事項，並負對應之責任。

3.資通系統刪除或汰除前應評估機關是否已無需使用該等資訊。

4.資通系統刪除或汰除時宜加以清查，以確保所有機敏性資訊及具使用授權軟體已被移除或安全覆寫。

5.具機敏性之資訊或具授權軟體之資通系統，採取實體銷毀，或以毀損、刪除或覆寫之技術，使原始資訊無法被讀取，並避免僅使用標準刪除或格式化功能。

三、資通安全防護設備

1.建置防毒軟體、網路防火牆、電子郵件過濾裝置，持續使用並適時進行軟、硬體之必要更新或升級。

2.資安設備定期備份，定期檢視並由主管檢討執行情形。

3.由資安推動小組負責防火牆規則操作、基本功能控管及廠商聯繫事宜。

四、電腦系統安全管理。

1. 辦理資訊業務委外作業，須明定廠商之資訊安全責任及保密規定並簽立保密切結書，並列入契約，要求廠商遵守並定期考核。
2. 對於系統變更作業或更新功能，由資訊組執行控管並詳細紀錄，以備查考。
3. 各系統伺服器所存放之機房須由資訊組專人專責管理，並嚴禁無關人員進出。
4. 本校存放機密性及敏感性資料之大型主機或伺服器主機(如 Domain Name Server 等),除作業系統既有的安全設定外,應強化身份辨識之安全機制，防止遠端撥接或遠端登入資料經由電話線路或網際網路傳送時，被偷窺或截取(如一般網路服務 HTTP、Telnet、FTP 等的登入密碼)，及防制非法使用者假冒合法使用者身分登入主機進行偷竊、破壞等情事。

五.網路安全管理

1. 系統的最高使用權限，應經權責主管人員審慎評估後，交付可信賴的人員管理。
2. 網路系統管理人員應負責製發帳號，供授權的人員使用。
3. 提供給內部人員使用的網路服務，與開放業務有關人員從遠端登入內部網路系統的網路服務，應執行嚴謹的身分辨識作業，或使用防火牆代理伺服器(Proxy Server)進行安全控管。
4. 離（休）職人員應依資訊安全規定及程序，取銷其存取網路之權利。
5. 網路系統管理人員未經權責主管人員許可，不得閱覽使用者之私人檔案；但如發現有可疑的網路安全情事，網路系統管理人員得依授權規定檢查其檔案。
6. 網路系統中各主要主機伺服器應有備援主機，以備主要作業主機無法正常運作時之用。
7. 網路硬體設備應加裝不斷電系統，以防止不正常的斷電狀況。
8. 系統與網路入侵之處理
   (1) 立即拒絕入侵者任何存取動作，防止災害繼續擴大;當防護網被突破時，系統應設定拒絕任何存取;或入侵者已被嚴密監控，在不危害內部網路安全的前題下，得適度允許入侵者存取動作，以利追查入侵者。
   (2) 切斷入侵者的連接。或為達到追查入侵者的目的，可考慮讓入侵者做有條件的連接，一旦入侵者危害到內部網路安全，則必須立即切斷入侵者的連接。
   (3) 應全面檢討網路安全措施及修正防火牆的設定，以防禦類似的入侵與攻擊。
   (4) 對入侵者的追查，除利用稽核檔案提供的資料外，得使用系統指令執行反向查詢，並連合相關單位(如網路服務公司)，追蹤入侵者。
   (5) 入侵者之行為若觸犯法律規定，構成犯罪事實，應立即告知檢警憲調單位，請其處理入侵者之犯罪事實調查各系統伺服器與外界網路連接

之網點，須設立防火牆以控管外界與內部網路之資料傳輸及資源存取，必要時應以代理伺服器等方式提供外界存取資料，避免外界直接進入資訊系統或資料庫存取資料。

六、系統存取控制管理。

1. 登入各作業系統時，依各級人員執行法定任務所必要之系統存取權限，由資訊組系統管理人員設定應賦予權限之帳號與密碼，並於一個學期內須更換一次。
2. 對離（休）職人員，須立即取消使用各項資訊資源所有權限，並列入人員離（休）職之必要手續。
3. 對學校內外擁有系統存取特別權限之人員，由資訊組建立使用人員名冊，加強安全控管，並縮短密碼更新周期為兩個月。
4. 學校之重要資料如需委外建檔者，不論在學校內外執行，均由資訊組與委外廠商簽訂適當之安全管制合約，防止資料被竊取、竄改、販售、洩漏及不當備份等情形發生。

七、系統發展及維護安全管理。

1. 學校自行開發或委外發展系統，須在系統開發初期階段，即將資訊安全納入考量；系統之維護、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、暗門及電腦病毒等危害系統安全。
2. 對委外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，並嚴禁資訊組核發長期性之系統辨識碼及通行密碼。
3. 對委外廠商或系統維護人員基於實際作業需要，資訊組得核發短期性及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。
4. 各處室委託廠商建置及維護重要軟硬體設施時，應在學校系統管理人員與資訊組人員監督及陪同下始得為之。

八、資訊資產安全管理。

1. 電腦病毒及惡意軟體之防範
   (1) 建立軟體管理政策，規定使用者應遵守軟體授權規定，禁止使用未取得授權的軟體。
   (2) 電腦病毒防制軟體應定期更新。
   (3) 使用防毒軟體事前掃瞄電腦系統及資料儲存媒體，偵測有無感染電腦病毒。
   (4) 對來路不明及內容不確定的磁片，應在使用前詳加檢查是否感染電腦病毒。
   (5) 應遵守智慧財產權相關規定。
   (6) 對所收電子郵件之附加檔案更須先經過掃瞄確定安全後始得開啟。
2. 個人資料之保護
   (1) 應依據電腦處理個人資料保護法等相關規定，審慎處理個人資訊。

(2)應建立個人資料控制及管理機制，並視需要指定負責個人資料保護之人員，以便協調管理人員、使用者及系統服務提供者，促使相關人員瞭解各部門應負的個人資料保護責任，以及應遵守之作業程序。

3. 日常作業之安全管理

(1)應準備足夠的備援設施，定期執行必要的資料及軟體備份及備援作業，以便發生災害或是儲存媒體失效時，可迅速回復正常作業。

(2)系統發生作業錯誤時，應正式記錄下來，並報告權責主管人員，並採取必要的更正行動。

(3)電腦作業環境如溫度、溼度及電源供應之品質等，應隨時監測，並採取必要的補救措施。

4. 電腦媒體與資料文件之安全管理

(1)可重複使用的資料儲存媒體，不再繼續使用時，應將儲存的內容消除。

(2)須離辦公場所的儲存媒體，應建立書面的授權規定，並建立使用紀錄。

(3)儲存媒體應依製造廠商提供的保存規格，存放在安全的環境。

(4)系統文件應鎖在安全的儲櫃或其他安全場所。

(5)委外處理的電腦文具、設備、媒體蒐集及委外處理資料，應慎選有足夠安全管理能力及經驗的機構作為委辦對象。

(6)應保護重要的資料檔案，以防止遺失、毀壞、被偽造或竄改。

(7)與他單位進行電子資料交換，應採行保護措施，以防止資料受損及未經授權的資料存取及竄改。

(8)個人文件檔案存檔時須養成加密保護習慣，若檔案需提供網路共享則必須加密保護。

5. 為防斷電時造成系統毀損或資料流失，主機房須配置不斷電系統因應斷電時有足夠時間做存檔與正常關機。

九、實體及環境安全管理。

1. 資訊組就系統伺服器主機設備安置於主機房，並由資訊組專責管理，並管制非相關人員隨意進出。
2. 主機房須設置空調恆溫控制，並配置適量之化學消防設施。
3. 若非資訊單位人員或維修人員，不得自行拆卸電腦機殼及更換內部零組件。

柒、資通安全教育訓練

一、資通安全教育訓練辦理方式：

擬定資通安全認知宣導及教育訓練計畫，以建立員工資通安全認知，提升機關資通安全水準，並應保存相關之資通安全認知宣導及教育訓練之紀錄。

二、認知宣導及教育訓練之內容得包含：

1.資通安全政策。

2.資通安全法令規定。

3.資通安全作業內容。

4.資通安全技術訓練。

三、人員管理及資訊安全教育訓練

1.被授權的網路使用者，只能在授權範圍內存取網路資源。

2.使用人員應遵守「臺灣學術網路使用規範」及相關規定。

3.使用者應遵守相關安全規定，如有違反，應撤消其網路資源存取權利，並依相關法規處理。

4.網路使用者不得將自己的登入身份識別與登入網路的密碼交付他人使用。

5.應禁止網路使用者以任何方法竊取他人的登入身份與登入網路通行碼。

6.應禁止及防範網路使用者以任何儀器設備或軟體工具竊聽網路上的通訊。

7.對資訊相關職務及工作人員，應進行安全評估，並依其任務之適任性進行必要之考核。

8.對可存取機密性與敏感性資訊或系統之人員，及因工作需要須配賦系統管理權限之人員，應加強評估及考核。

9.資訊組得視實際需要辦理資訊安全教育訓練及宣導，建立業務人員資訊安全認知，提升學校資訊安全水準。

10.加強資訊安全管理人力之培訓提升資訊安全管理能力。

11.對負責重要資訊系統之管理、維護、設計及操作之人員，應妥適分工，分散權責，並視需要建立人力備援制度。

12.校長及各處室主任，負責督導所屬員工之資訊作業安全，防範不法及不當行為。

捌、其他未定事項以「行政院所屬各機關資訊安全管理規範」及相關規定規範之。

附件

新北市私立竹林高級中學

委外廠商暨執行人員保密切結書

立切結書人----------（簽署人姓名）等，受新北市私立竹林高級中學委派至**圖書館資訊組**處理業務，謹聲明恪遵機關下列工作規定，對工作中所持有、知悉之資訊系統作業機密或敏感性業務檔案資料，均保證善盡保密義務與責任，非經機關權責人員之書面核准，不得擷取、持有、傳遞或以任何方式提供給無業務關係之第三人，如有違反願賠償一切因此所生之損害，並擔負相關民、刑事責任，絕無異議。

一、 未經申請核准，不得私自將機關之資訊設備、媒體檔案及公務文書攜出。

二、 未經機關業務相關人員之確認並代為申請核准，不得任意將攜入之資訊設備連接機關網路。若經申請獲准連接機關網路，嚴禁使用數據機或無線傳輸等網路設備連接外部網路。

三、 經核准攜入之資訊設備欲連接機關網路或其他資訊設備時，須經電腦主機房掃毒專責人員進行病毒、漏洞或後門程式檢測，通過後發給合格標籤，並將其粘貼在設備外觀醒目處以備稽查。

四、 廠商駐點服務及專責維護人員原則應使用機關配發之個人電腦與週邊設備，並僅開放使用機關內部網路。若因業務需要使用機關電子郵件、目錄服務，應經機關業務相關人員之確認並代為申請核准，另欲連接網際網路亦應經機關業務相關人員之確認並代為申請核准。

五、 機關得定期或不定期派員檢查或稽核立切結書人是否符合上列工作規定。

六、 本保密切結書不因立切結書人離職而失效。

七、 立切結書人因違反本保密切結書應盡之保密義務與責任致生之一切損害，立切結書人所屬公司或廠商應負連帶賠償責任。

八、

立切結書人：

姓名及簽章	身分證字號	聯絡電話及戶籍地址

立切結書人所屬廠商或單位：圖書館資訊組

廠商名稱及蓋章	廠商負責人姓名及簽章	廠商聯絡電話及地址

填表說明：

一、 廠商駐點服務人員、專責維護人員，或逗留時間超過三天以上之突發性維護增援、臨時性系統測試或教育訓練人員（以授課時需連結機關網路者為限）及經常到機關洽公之業務人員皆須簽署本切結書。

二、 廠商駐點服務人員、專責維護人員及經常到機關洽公之業務人員每年簽署本切結書乙次。

中 華 民 國 年 月 日