臺北市立興福國民中學

資通安全維護計畫

第 1.0 版

生效日期：108 年 1 月

壹、 資通安全推動小組成員及分工表

臺北市立興福國民中學資通安全推動小組成員及分工表

單位職級	組別	職掌事項
教務主任	策略規劃組	資通安全長。執掌事項詳列於本校資通安全管理計畫中。
學務主任		1.資通安全政策及目標之研議。 2.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。 3.依據資通安全目標擬定機關年度工作計畫。 4.傳達機關資通安全政策與目標。其他資通安全事項之規劃。 5.辦理資通安全內部稽核
總務主任		
輔導主任		
教師兼任 資訊組長	資安管理組	1.資通安全相關規章與程序、制度之執行。 2.資訊及資通業務之盤點。 3.資料及資通業務之安全防護事項之執行。 4.資通安全事件之通報及應變機制之執行。 5.其他資通安全事項之辦理與推動。
人事主任	績效管理組	辦理資通安全內部稽核

貳、 實施計畫

一、 依據及目的

本計畫依據資通安全管理法第 10 條及施行細則第 6 條訂定。

本計畫依據下列法規訂定：

(一)資通安全管理法第 10 條及其施行細則第 6 條。

(二)其他業務法規名稱。

二、 適用範圍

本計畫適用範圍涵蓋本機關。

三、 核心業務及重要性

(一)核心業務及重要性：

本機關之核心業務及重要性如下表：

核心業務	核心資通系統	重要性說明	業務失效影響說明	最大可容忍中斷時間
無	無	不適用	不適用	不適用

(二)非核心業務及說明：

本機關之非核心業務及說明如下表：

非核心業務	業務失效影響說明	最大可容忍中斷時間
AD 網域伺服器	無法登入電腦作業系統	4 小時
防火牆	對外網路中斷	8 小時
DNS	校園無法連外,外界亦無法連內	24 小時
校園官方網站	外界無法得知校園訊息	24 小時

四、 資通安全政策及目標

(一)資通安全政策

為使本機關業務順利運作，防止資訊或資通業務受未經授權之存取、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），特制訂本政策如下，以供全體同仁共同遵循：

1. 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. 針對各資料的機密性與完整性應妥善保護，避免資料遭竄改。
3. 建立資通安全防護(如:防火牆、防毒軟體)。
4. 辦理資通安全教育訓練(一般使用者與主管，每人每年三小時以上之一般資通安全教育訓練)，提升同仁資通安全意識。
5. 針對辦理資通安全業務有功相關人員應依資通安全管理法子法之「公務機關所屬人員資通安全事項獎懲辦法」進行獎勵。
6. 禁止多人共用同一帳號。
7. 落實資通安全通報機制。

(二)資通安全目標

1. 資安事件發生，於規定的時間完成通報、應變及復原作業。
2. 配合上級機關辦理之電子郵件社交工程演練。
3. 全年度資安通報平臺之資安事件等級第 1、2 級發生件數少於 3 件(含)以下，等級第 3、4 級不得發生。
4. 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。

(三)資通安全政策及目標核定程序

資通安全政策由資訊教育推動委員會議通過後實施。

(四)資通安全政策及目標之宣導

資通安全政策及目標應每年透過教育訓練、內部會議、張貼公告等方式，向機關內所有人員進行宣導，並檢視執行成效。

(五)資通安全政策及目標定期檢討程序

資通安全政策及目標應定期於資訊教育推動委員會議中檢討其適切性。

五、 資通安全推動組織

(一)資通安全長

依本法第 11 條之規定，本機關訂定教務主任（副首長）為資通安全長，負責督導機關資通安全相關事項，其任務包括：

1. 資通安全管理政策及目標之核定、核轉及督導。
2. 資通安全責任之分配及協調。
3. 資通安全資源分配。
4. 資通安全防護措施之監督。
5. 資通安全事件之檢討及監督。
6. 資通安全相關規章與程序、制度文件核定。
7. 資通安全管理年度工作計畫之核定。
8. 資通安全相關工作事項督導及績效管理。
9. 其他資通安全事項之核定。

(二)資通安全推動小組

1. 組織

為推動本機關之資通安全相關政策、落實資通安全事件通報及相關應變處理，由資通安全長召集各處室主任成立資通安全推動小組，其任務包括：

(1) 跨處室資通安全事項權責分工之協調。

(2) 應採用之資通安全技術、方法及程序之協調研議。

(3) 整體資通安全措施之協調研議。

(4) 資通安全計畫之協調研議。

(5) 其他重要資通安全事項之協調研議。

2. 分工及職掌

本機關之資通安全推動小組依下列分工進行責任分組，並依資通安全長之指示負責下列事項，本機關資通安全推動小組分組人員名單及職掌應列冊，並適時更新之 ：

(1) 策略規劃組：

i. 資通安全政策及目標之研議。

ii. 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。

iii. 依據資通安全目標擬定機關年度工作計畫。

iv. 傳達機關資通安全政策與目標。

v. 其他資通安全事項之規劃。

(2) 資安防護組：

i. 資通安全技術之研究、建置及評估相關事項。

ii. 資通安全相關規章與程序、制度之執行。

iii. 資訊及資通系統之盤點及風險評估。

iv. 資料及資通系統之安全防護事項之執行。

v. 資通安全事件之通報及應變機制之執行。

vi. 其他資通安全事項之辦理與推動。

(3) 績效管理組：

i. 辦理資通安全內部稽核。

ii. 依教育局規定之時程召開資通安全管理審查會議，提報資通安全事項執行情形，以利教育部稽核審查使用。

六、 人力及經費配置

(一)人力及資源配置

1. 本機關依資通安全責任等級分級辦法之規定，屬資通安全責任等級 D 級，最低應設置資通安全兼辦人員 1 人。

(1) 負責資通系統分級、內部資通安全稽核、防護基準及教育訓練業務之推動。

(2) 負責資通安全防護設施建置及資通安全事件通報及應變業務之推動。

2. 本機關之承辦單位於辦理資通安全人力資源業務時，應加強資通安全人員之培訓，並提升機關內資通安全專業人員之資通安全管理能力。本機關之相關單位於辦理資通安全業務時，如資通安全人力或經驗不足，得洽請相關學者專家或專業機關（構）提供顧問諮詢服務。

3. 本機關負責重要資通設備之管理、維護、設計及操作之人員，應妥適分工，分散權責，若負有機密維護責任者，應簽屬書面約定 ，並視需要實施人員輪調，

建立人力備援制度。

4. 本機關之首長及各級業務主管人員，應負責督導所屬人員之資通安全作業，防範不法及不當行為。
5. 專業人力資源之配置情形應每年定期檢討，並納入資通安全維護計畫持續改善機制之管理審查。

(二)經費配置

1. 規劃配置相關經費及資源時，應考量資通安全政策及目標，並提供建立、實行、維持及持續改善資通安全維護計畫所需之資源 。
2. 每年視整體資通安全資源進行分配，並經資通安全長(資通安全管理代表)核定後，進行相關之建置。
3. 資通安全經費、資源之配置情形應每年定期檢討，並納入資通安全維護計畫持續改善機制之管理審查。

七、 資訊及資通系統之盤點

(一)資訊及資通系統盤點

1. 本機關每年辦理資訊及資通系統資產盤點，依管理責任指定對應之資產管理人，配合校內年度盤點作業清查。
2. 資訊及資通系統資產應以標籤標示於設備明顯處，並載明財產編號、保管人、廠牌、型號等資訊。

(二)機關資通安全責任等級分級

本機關自行辦理資通業務，未維運自行或委外開發之資通系統者，其資通安全責任等級為 D 級。

八、 資通安全風險評估

(一)本機關應每年針對資訊及資通設備資產進行風險評估。

(二)執行風險評估時應參考臺北市政府教育局「資訊資產風險評鑑管理辦法」執行相關作業。

(三)本機關應每年依據資通安全責任等級分級辦法之規定，分別就機密性、完整性、可用性、法律遵循性等構面評估。

九、 資通安全防護及控制措施

本機關依據前章資通安全風險評估結果、自身資通安全責任等級之應辦事項，全機關之防護及控制措施詳如本機關資通安全維護計畫，採行相關之防護及控制措施如下:

(一)資訊及資通設備之管理

1. 資訊及資通設備之使用

(1) 本機關同仁使用資訊及資通設備須遵守設備管理機關相關規範。

(2) 本機關同仁使用資訊及資通設備時，應留意其資通安全要求事項，並負對應之責任。

(3) 本機關同仁使用資訊及資通設備後，應依規定之程序歸還。資訊類資訊之歸還應確保相關資訊已正確移轉，並安全地自原設備上抹除。

(4) 非本機關同仁使用本機關之資訊及資通設備，應確實遵守本機關之相關資通安全要求，且未經授權不得任意複製資訊。

(5) 對於資訊及資通設備，宜識別並以文件記錄及實作可被接受使用之規則。

(二)存取控制與加密機制管理

1. 網路安全控管

(1) 本機關之防火牆由本機關自行管理，區域劃分如下：

I. 外部網路：對外網路區域，連接外部廣網路(Wide Area Network, WAN)。

II. 內部區域網路 (Local Area Network, LAN) ：機關內部單位人員及內部伺服器使用之網路區段。

(2) 外部網路及內部區域網路間連線需經防火牆進行存取控制，非允許的服務與來源不能進入其他區域。

(3) 本機關應定期檢視防火牆政策是否適當。

(4) 本機關內部網路之區域應做合理之區隔，使用者應經授權後在授權之範圍內存取網路資源。

(5) 對網路系統管理人員或資通安全主管人員的操作，均應建立詳細的紀錄。並應定期檢視網路安全相關設備設定規則與其日誌紀錄，並檢討執行情形。

(6) 使用者應依機關規定之方式存取網路服務。

(7) 網域名稱系統(DNS)防護

I. 一般伺服器應關閉 DNS 服務，防火牆政策亦應針對 DNS 進行控管，關閉不需要的 DNS 服務存取。

II. DNS 伺服器應經常性進行弱點漏洞管理與修補、落實存取管控機制。

III. 內部主機位置查詢應指向機關內部 DNS 伺服器。

(8) 無線網路防護

I. 機密資料原則不得透過無線網路及設備存取、處理或傳送。

II. 無線設備應具備安全防護機制以降低阻斷式攻擊風險，且無線網路之安全防護機制應包含外來威脅及預防內部潛在干擾。

III. 行動通訊或紅外線傳輸等無線設備原則不得攜入涉及或處理機密資料之區域。

IV. 用以儲存或傳輸資料且具無線傳輸功能之個人電子設備與工作站，應安裝防毒軟體，並定期更新病毒碼。

2. 資通業務權限管理

(1) 本機關之資通業務應設置通行碼管理，通行碼之要求需滿足：

I. 通行碼長度 8 碼以上。

II. 通行碼複雜度應包含英文大寫小寫、特殊符號或數字三種以上。

III. 使用者每 90 天應更換一次通行碼。

(2) 使用者辦理資通業務前應經授權，並使用唯一之使用者 ID，除有特殊營運或作業必要經核准並紀錄外，不得共用 ID。

(3) 使用者無繼續辦理資通業務時，應立即停用或移除使用者 ID，資通業務管理者應定期清查使用者之權限。

3. 特權帳號之存取管理

(1) 資通設備之特權帳號請應經正式申請授權方能使用，特權帳號授權前應妥善審查其必要性，其授權及審查記錄應留存。

(2) 資通設備之特權帳號不得共用。

(3) 對於特權帳號，宜指派與該使用者日常公務使用之不同使用者 ID。

(4) 資通設備之特權帳號應妥善管理，並應留存特殊權限帳號之使用軌跡。

(5) 資通設備之管理者每季應清查系統特權帳號並劃定特權帳號逾期之處理方式。

4. 加密管理

(1) 本機關之機密資訊於儲存或傳輸時應進行加密。

(2) 本機關之加密保護措施應遵守下列規定：

I. 應落實使用者更新加密裝置並備份金鑰。

II. 應避免留存解密資訊。

III. 一旦加密資訊具遭破解跡象，應立即更改之。

(三)作業與通訊安全管理

1. 防範惡意軟體之控制措施

(1) 本機關之主機及個人電腦應安裝防毒軟體，並時進行軟、硬體之必要更新或升級。

I. 經任何形式之儲存媒體所取得之檔案，於使用前應先掃描有無惡意軟體。

II. 電子郵件附件及下載檔案於使用前，宜於他處先掃描有無惡意軟體。

III. 確實執行網頁惡意軟體掃描。

(2) 管理者並應每年定期針對管理之設備進行軟體清查。

(3) 使用者不得私自使用已知或有嫌疑惡意之網站。

(4) 使用者應定期進行作業系統及軟體更新，以避免惡意軟體利用系統或軟體漏洞進行攻擊。

2. 遠距工作之安全措施

(1) 本機關資通業務之操作及維護以現場操作為原則，避免使用遠距工作，如有緊急需求時，應申請並經資通安全推動小組同意後始可開通。

(2) 資通安全推動小組應定期審查已授權之遠距工作需求是否適當。

(3) 針對遠距工作之連線應採適當之防護措施(並包含伺服器端之集中過濾機制檢查使用者之授權)，並且記錄其登入情形。

I. 提供適當通訊設備，並指定遠端存取之方式。

II. 提供虛擬桌面存取，以防止於私有設備上處理及儲存資訊。

III. 遠距工作終止時之存取權限撤銷，並應返還相關設備。

3. 電子郵件安全管理

(1) 使用者使用電子郵件時應提高警覺，並使用純文字模式瀏覽，避免讀取來歷不明之郵件或含有巨集檔案之郵件。

(2) 原則不得電子郵件傳送機密性或敏感性之資料，如有業務需求者應依相關規定進行加密或其他之防護措施。

(3) 使用者不得利用機關所提供電子郵件服務從事侵害他人權益或違法之行為。

(4) 使用者應確保電子郵件傳送時之傳遞正確性。

(5) 本機關應配合上級機關辦理電子郵件社交工程演練，並檢討執行情形。

4. 確保實體與環境安全措施

(1) 通訊機房(機櫃)之管理

I. 通訊機房(機櫃)應進行實體隔離。

II. 機關人員或來訪人員應申請及授權後方可進入通訊機房，通訊機房管理者並應定期檢視授權人員之名單。

III. 人員進入管制區應配載身分識別之標示，並隨時注意身分不明或可疑人員。

IV. 僅於必要時，得准許外部支援人員進入通訊機房(機櫃)。

V. 人員及設備進出通訊機房(機櫃)應留存記錄。

(2) 通訊機房(機櫃)之環境控制

I. 通訊機房(機櫃)之空調、電力得建立備援措施。

II. 通訊機房(機櫃)得安裝之安全偵測及防護措施，包括熱度及煙霧偵測設備、火災警報設備、溫濕度監控設備、漏水偵測設備、入侵者偵測系統，以減少環境不安全引發之危險。

III. 各項安全設備應定期執行檢查、維修，並應定時針對設備之管理者進行適當之安全設備使用訓練。

(3) 辦公室區域之實體與環境安全措施

I. 應考量採用辦公桌面的淨空政策，以減少文件及可移除式媒體等在辦公時間之外遭未被授權的人員取用、遺失或是被破壞的機會。

II. 文件及可移除式媒體在不使用或不上班時，應存放在櫃子內。

III. 機密性及敏感性資訊，不使用或下班時應該上鎖。

IV. 機密資訊或處理機密資訊之資通業務應避免存放或設置於公眾可接觸之場域。

V. 顯示存放機密資訊或具處理機密資訊之資通業務地點之通訊錄及內部人員電話簿，不宜讓未經授權者輕易取得。

VI. 資訊或資通業務相關設備，未經管理人授權，不得被帶離辦公室。

5. 資料備份

(1) 重要資料應進行資料備份，其備份之頻率應滿足復原時間點目標之要求，並執行異地存放。

(2) 本機關應每季確認重要資料備份之有效性。且測試該等資料備份時，宜於專屬之測試系統上執行，而非直接於覆寫回原資通設備。

(3) 敏感或機密性資訊之備份應加密保護。

6. 媒體防護措施

(1) 使用隨身碟或磁片等存放資料時，具機密性、敏感性之資料應與一般資料分開儲存，不得混用並妥善保管。

(2) 資訊如以實體儲存媒體方式傳送，應留意實體儲存媒體之包裝，選擇適當人員進行傳送，並應保留傳送及簽收之記錄。

(3) 為降低媒體劣化之風險，宜於所儲存資訊因相關原因而無法讀取前，將其傳送至其他媒體。

(4) 對機密與敏感性資料之儲存媒體實施防護措施，包含機密與敏感之紙本或備份磁帶，應保存於上鎖之櫃子，且需由專人管理鑰匙。

7. 電腦使用之安全管理

(1) 電腦、業務系統或自然人憑證，若超過十五分鐘不使用時，應立即登出或啟動螢幕保護功能並取出自然人憑證。

(2) 禁止私自安裝點對點檔案分享軟體及未經合法授權軟體。

(3) 連網電腦應隨時配合更新作業系統、應用程式漏洞修補程式及防毒病毒碼等。

(4) 筆記型電腦及實體隔離電腦應定期以人工方式更新作業系統、應用程式漏洞修補程式及防毒病毒碼等。

(5) 下班時應關閉電腦及螢幕電源。

(6) 如發現資安問題，應主動循機關之通報程序通報。

(7) 支援資訊作業的相關設施如影印機、傳真機等，應安置在適當地點，以降低未經授權之人員進入管制區的風險，及減少敏感性資訊遭破解或洩漏之機會。

8. 行動設備之安全管理

(1) 機密資料不得由未經許可之行動設備存取、處理或傳送。

(2) 機敏會議或場所不得攜帶未經許可之行動設備進入

(四)資通安全防護設備

(3) 本機關應建置防毒軟體、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。

(4) 資安設備應定期備份日誌紀錄，定期檢視並由主管複核執行成果，並檢討執行情形。

十、 資通安全事件通報、應變及演練相關機制

為即時掌控資通安全事件，並有效降低其所造成之損害，訂定資通安全事件通報、應變及演練相關機制，詳**資通安全事件通報應變程序**[2]。

十一、 資通安全情資之評估及因應

本機關接獲資通安全情資，應評估該情資之內容，並視其對本機關之影響、本機關可接受之風險及本機關之資源，決定最適當之因應方式，必要時得調整資通安全維護計畫之控制措施，並做成紀錄。

1. 資通安全情資之分類評估

本機關接受資通安全情資後，應指定資通安全專責(兼職)人員進行情資分析，並依據情資之性質進行分類及評估，情資分類評估如下：

(1) 資通安全相關之訊息情資

資通安全情資之內容如包括重大威脅指標情資、資安威脅漏洞與攻擊手法情資、重大資安事件分析報告、資安相關技術或議題之經驗分享、疑似存在系統弱點或可疑程式等內容，屬資通安全相關之訊息情資。

(2) 入侵攻擊情資

資通安全情資之內容如包含特定網頁遭受攻擊且證據明確、特定網頁內容不當且證據明確、特定網頁發生個資外洩且證據明確、特定系統遭受入侵且證據明確、特定系統進行網路攻擊活動且證據明確等內容，屬入侵攻擊情資。

(3) 機敏性之情資

資通安全情資之內容如包含姓名、出生年月日、國民身份證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病例、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接識別之個人資料，或涉及個人、法人或團體營業上秘密或經營事業有關之資訊，或情資之公開或提供有侵害公務機關、個人、法人或團體之權利或其他正當利益，或涉及一般公務機密、敏感資訊或國家機密等內容，屬機敏性之情資。

(4) 涉及核心業務、核心資通系統之情資

資通安全情資之內容如包含機關內部之核心業務資訊、核心資通系統、涉及關鍵基礎設施維運之核心業務或核心資通系統之運作等內容，屬涉及核心業務、核心資通系統之情資。

2. 資通安全情資之因應措施

本機關於進行資通安全情資分類評估後，應針對情資之性質進行相應之措施，必要時得調整資通安全維護計畫之控制措施。

(1) 資通安全相關之訊息情資

由資通安全推動小組彙整情資後進行風險評估，並依據資通安全維護計畫之控制措施採行相應之風險預防機制。

(2) 入侵攻擊情資

由資通安全專責(兼職)人員判斷有無立即之危險，必要時採取立即之通報應變措施，並依據資通安全維護計畫採行相應之風險防護措施，另通知各單位進行相關之預防。

3. 機敏性之情資

就涉及個人資料、營業秘密、一般公務機密、敏感資訊或國家機密之內容，應採取遮蔽或刪除之方式排除，例如個人資料及營業秘密，應以遮蔽或刪除該特定區段或文字，或採取去識別化之方式排除之。

4. 涉及核心業務、核心資通系統之情資

資通安全推動小組應就涉及核心業務、核心資通系統之情資評估其是否對於機關之運作產生影響，並依據資通安全維護計畫採行相應之風險管理機制。

十二、 資通系統或服務委外辦理之管理

本機關無委外辦理資通系統之建置、維運或資通服務之提供，若另有需求時得應考量受託者之專業能力與經驗、委外項目之性質及資通安全需求，選任適當之受託者，並監督其資通安全維護情形。

十三、 資通安全教育訓練

1. 資通安全教育訓練要求

(1) 資安兼任或資訊人員每人每年至少接受 3 小時以上之資安專業課程訓練。

(2) 本機關之一般使用者與主管，每人每年接受 3 小時以上之一般資通安全教育訓練。

2. 資通安全教育訓練辦理方式

承辦單位應於每學年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紀錄。

十四、 公務機關所屬人員辦理業務涉及資通安全事項之考核機制

本機關所屬人員之平時考核或聘用，依據公務機關所屬人員資通安全事項獎懲辦法、臺北市政府及所屬各機關學校公務人員平時獎懲標準表，及臺北市立國民中學組織規程規定辦理之。

十五、 資通安全維護計畫及實施情形之持續精進及績效管理機制

於每年「教育部全國國中小學資訊安全管理系統」填報期限前完成稽核項目之填報。

十六、 資通安全維護計畫實施情形之提出

本機關依據資通安全管理法第 12 條之規定，應於每年向臺北市政府教育局資訊教育科，提出資通安全維護計畫實施情形，使其得瞭解本機關之年度資通安全計畫實施情形。

十七、 附件表單:

1.資通安全保密同意書

2.管制區域人員進出登記表

3.本機最大權限申請書

壹、臺北市立興福國民中學資通安全保密同意書

編號：

立同意書人＿＿＿＿＿＿於民國＿＿＿年＿＿月＿＿＿＿日起於＿＿＿＿＿＿＿＿＿＿任職，因業務涉及單位重要之資訊及資通系統，故同意下列保密事項：

一、於業務上所知悉之機敏資料及運用之資通系統等，應善盡保管及保密之責。二、相關業務之資訊、文件，不得私自洩漏與業務無關之人員。

三、遵守其他本單位資通安全相關之法令及規定。

四、如有危害本單位資通安全之行為，願負相關之責任。

立同意書人：＿＿＿＿＿＿＿＿（簽章）

身份證字號：＿＿＿＿＿＿＿＿ 服務機關：＿＿＿＿＿＿＿＿＿＿ 機關首長：＿＿＿＿＿＿＿＿＿＿

中　　華　　民　　國　　年　　月　　日

貳、臺北市立興福國民中學管制區域人員進出登記表

編號：

製表日期：　　年　　月　　日

編號	姓名	單位	配同人員	日期	進入時間	離開時間	事由	權限	進出設備	攜帶物品

承辦人員：　　單位主管：

參、臺北市立興福國民中學**本機最大權限申請書**

紀錄編號：　　日期：　　年　　月　　日

本人 _____ 茲因工作相關程式 _____，需開放個人電腦本機最大權限，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。絕不安裝使用未經授權之電腦軟體， 並不使用點對點互連(P2P)軟體及其它相關工具下載或提供分享檔案、絕不擅自複製、傳播任何侵害智慧財產權之任何程式、軟體，違者願負一切相關法律責任。

此致

臺北市立興福國民中學

立 同 意 書 人：_____

身 分 證 字 號：_____

所 屬 單 位 別：_____

中　　華　　民　　國　　年　　月　　日