金門縣學術網路使用及資通安全防護作業要點

一、金門縣政府(以下簡稱本府)為維護學術網路環境之資通訊安全，特訂定本要點。

二、本府教育網路中心（以下簡稱教網中心）網際網路及區域網路之建立，係以提供金門縣(以下簡稱本縣)教職員工生，從事教學輔助、學術研究、行政業務等相關活動為目的。

三、下列單位得申請連線學術網路：

(一)依法設立之各級學校及研究機構。

(二)輔導設置之數位機會中心。

(三)其他符合臺灣學術網路設置目的，並經臺灣學術網路管理委員會通過之單位。

四、利用學術網路之個人或單位皆為教網中心網際網路連線單位之使用者。

五、連線單位於新申請或變更申請所屬網路介接至骨幹網路者，應檢具經單位首長核定之「與臺灣學術網路骨幹網路介接計畫書」(以下簡稱介接計畫書)，向教網中心提出申請，經審查同意後辦理介接事宜。

六、介接計畫書應包括下列項目：

(一)所屬網路及應用系統相關伺服主機之現況與架構說明。

(二)內部網路使用規範：應參照臺灣學術網路管理規範之相關規定，納入各該連線單位之網路使用相關規範，並經行政程序核定及公告於學校或機關（構）之對外網站首頁。

(三)所屬網路之整體使用流量統計：應建置與骨幹網路介接之網路使用流量情形統計資訊網頁(包括以日、週、月為單位之即時及歷史流量)。

(四)所屬 IP 之每日使用流量排序分析：就服務範圍使用之 IP 位址，統計分析其對骨幹網路之個別 IP 使用流量排名並紀錄，紀錄內容包括流入、流出及總量等之使用流量資訊。紀錄至少應保留一個月。

(五)建立連線單位處理網路管理、資通安全之聯繫機制，並指派專人管理該帳號及負責相關事宜之訊息處理。

(六)建立 IP 位址管理機制：包括 IP 位址分配之主機用途及管理人之相關資料，登記資料如涉及個人資料，應依個人資料保護法及其相關法規規定辦理。

(七)建立網路攻擊等資安事件之處理機制：包括來自單位內部或外部之異常事件，並提出具體之管理規定及改善措施。

(八)連線單位(高級中等以下學校)應建立不適合存取網站內容之過濾防護機制：說明所建立之過濾防護機制相關軟硬體設施架構。

(九)上述第 8 點提及之連線單位除外，得建立不適合存取網站內容之過濾防護機制：說明所建立之過濾防護機制相關軟硬體設施架構。

七、教網中心每年至少一次，以書面或實地訪查方式檢核連線單位之執行狀況，連線單位如未依介接計畫書確實執行，經通知限期改善，屆期仍未改善者，教網中心得限制或暫停連線單位必要範圍之網路服務。

八、連線單位應自備連接骨幹網路連接點之電路及兩端必要光纖模組或相關設備，頻寬超過 100Mpbs 者須使用乙太介面 GE(Gigabit Etherent)介面介接。

九、連線單位必須依照介接計畫書或教網中心原規劃之網路架構使用，不得任意更動教網中心設置之網路架構，如連線單位須調整變動整體網路架構，須重新提交介接計畫書，向教網中心提出申請，經審查同意後始可辦理調整變動事宜。

十、連線單位整體架構應如附件所示。

十一、教網中心對於本縣校園網路管理範圍:

(一)國中(小)：管理終端防火牆、路由交換器設備、網路連線品質、點對點網路狀況。

(二)高中(職)、大專校院及其他單位：管理網路連線品質、點對點網路狀況。

十二、網路使用者應隨時注意在使用資訊設備時，不得影響他人生活及共同使用者之權益。

十三、網路之使用者禁止於網路上從事下列活動：

(一)傳送違反著作權法及違反相關法律規章之資訊。

(二)以任何方式偷窺、竊取、更改、干擾、破壞他人資訊。

(三)蓄意散佈電腦病毒或其他未經授權資訊。

(四)侵入未經授權使用之電腦系統。

(五)將個人登入身份識別帳號及密碼借予他人使用。

(六)盜用或冒名使用他人身份申請登入識別帳號或網際網路位址（IP Address)。

(七)蓄意破壞或不正當使用資訊設備（電腦主機、個人電腦、網路設備等)。

(八)使用校園網路散佈廣告信、販售違禁品、非法軟體或資料。

(九)任何未經授權許可之商業行為。

(十)散佈不實文字、毀謗他人名譽。

(十一)危害或干擾系統安全或網路通信安全。

(十二)其他國家及教網中心相關法律規章明訂違法者。

十四、校園網路安全控制措施如下：

(一)與外界連線，應僅限於經由教網中心之管控，以符合一致性與單一性之安全要求。

(二)轄下單位禁止以私人架設網路(如：電話線、4G 或 5G 網路、光世代等)連結機房內之主機電腦或網路設備，禁止任何私人、廠商網路設備取代教網中心建置終端、防護設備等。

(三)依業務性質之不同，區分不同內部網路，例如：教學、行政等，以降低未經授權存取之風險。

(四)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。若有開放之必要，應經教網中心同意並簽訂切結書等保密文件，如發生資安相關事件，單位應自行負責相關後續責任。

(五)校園內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。

(六)校園內各公務資通訊產品，禁止使用大陸廠牌資通訊產品(含軟體、硬體及服務)。

(七)遠端存取服務採「原則禁止、例外允許」方式，並依資通安全管理法施行細則第 4 條、資通安全責任等級分級辦法附表十之遠端存取相關規定辦理。

十五、各校應配合本府資訊資源向上集中計畫，推動其核心資通系統向上集中，並依資通安全責任等級分級辦法第十條第四款，調整其學校資通安全責任等級。

十六、本縣高級中等以下學校應配合辦理下列事項：

(一)資訊資產盤點作業及資安防護作業事項。

(二)檢視其資訊資產盤點結果、核心資通系統向上集中作業事項及期程，並依資通安全責任等級分級辦法辦理資安防護作業。

(三)依資通安全管理法第 13 條規定，配合資通安全維護計畫實施情形之稽核作業，如有缺失或待改善者，應提出改善報告，送交本府審查。

(四)依據呈報之資通安全防護計畫書辦理各項要求事宜。

十七、核心資通系統至少應包含各校官方網站、網域名稱服務（DNS)、電子郵件伺服器、學習歷程檔案系統、校務行政系統等保有教職員生個人資料檔案之資通系統，各校非核心資通系統，

不得持有教職員生之個人資料，且應與核心資通系統有明確網路區隔，不得使用身分證字號或電話等作為帳號依據。

十八、網路使用者若違反本要點或涉嫌侵害他人權益時，除移送學校及相關單位議處外，需自負刑事與民事責任。

十九、任何單位或個人若發現校園網際網路位址之資訊設備發生不正當行為時，可檢附相關行為證明資料提供予教網中心，教網中心於查明該不當資訊設備來源並發現其行為確有不當時，得轉知該資訊設備管理者處理。情節重大者，得移送相關單位處理。

二十、各連線單位若有配合偵查犯罪之必要，應先行文知會本府，各單位於接獲本府同意後，應依臺灣學術網路連線單位配合防治網路犯罪處理要點、電腦處理個人資料保護法、公務人員服務法配合提供相關資料。

二十一、各校校內使用者應善盡保管自身身份識別帳號與密碼之責任。

二十二、網路管理者應尊重網路隱私權、不得任意窺視其他網路使用者之個人資料或有侵犯隱私權之行為。但有下列情形之一者，不在此限：

(一)為維護或檢查系統安全。

(二)依據合理之懷疑，認為有違反校規情事發生時，為取得證據或進行調查所必要之行為。

(三)為配合司法機關之調查。

(四)其他依法令執行之相關網路管理行為。

二十三、網路使用者中之公用電腦管理者應善盡下列管理責任：

(一)保管並維護管理者之身份識別帳號及密碼。

(二)保管並維護公用電腦使用者之身份識別帳號及密碼。

(三)保管並維護使用者之個人資料。

(四)公用電腦服務之維護。

(五)公用電腦安全系統之維護。

(六)保存期限內公用電腦使用者存取紀錄或系統紀錄之維護。

(七)公用電腦系統及使用者重要資料備份之維護。

(八)對不當使用系統資源者在公告相關管理規則後予以停權或適當處分。

(九)配合主管機關處理爭議或偵查犯罪，提供相關資料。

二十四、校園網路使用者中之網路設備管理者應善盡下列管理責任：

(一)維護管理相關校園網路資訊設備中之網路設備及相關資訊設備。

(二)保管並維護網路設備之管理者身分識別帳號及密碼。

(三)對不當使用網路資源者在公告相關管理規則後予以停權或適當處分。

二十五、教網中心各資訊設備管理者在公告管理規則時，得以公函、電子布告欄或教網中心全球資訊網首頁連結之相關網頁公告之。

二十六、為維持本縣校園網路架構永續發展，連線單位(國中小以下連線單位)如需變更、擴充、調整校園網路架構或採購建置校園網路設備，應呈報本府教育網路中心核可後辦理，並須配合本要點第九條之規定辦理相關作業事宜。

附件、連線單位整體架構示意圖: