臺北市立大學111學年度第一學期

「資訊推動委員會」會議記錄

時　　間：111年11月25日(星期五)上午10時00分

地　　點：本校博愛校區行政大樓201會議室

主　　席：邱校長英浩

出 席 者:如簽到表

壹、 主席報告：

(一)未來請計中、總務處及相關單位合作，將現有教室規劃為行動教室。

(二)現有建築物重建將影響教學，未來規劃新空間為教室，舊建築穩定維持考慮作為教師研究室使用。

貳、報告事項：

（一）宣讀上次會議決議：

案由一：因應Google雲端空間政策調整，校務系統資料庫備份儲存機制調整，提請討論。

決　議：（一）購買Google Education Plus方案，維持Google雲端空間無限容量兩年。第3年起則配合Google 當時政策與優惠方案另訂定相關辦法供各單位申請。

（二）畢業生於畢業仍可使用學生信箱，預設每人5GB，雲端總容量上限規劃為30TB，隨使用者數量增減動態調整；畢業生畢業一年後若未登入使用將予以停用，且不負保管資料責任。

現況說明：已為全校職員生採購Google雲端空間，目前每位在校教職員生皆有無限雲端空間。

案由二：111年度電腦教學軟體採購案，提請討論。

決　議：（一）教學軟體應用於教學使用，不提供個人使用。

（二）各學院所採購之軟體應可授權給院系教師及學生使用。

（三）各院所需採購之軟體不應超過每院預算25萬元。

現況說明：因投標廠商疑似有違反政府採購法之行為，故採購程序暫停，已於111年6月13日北市大總字第

1116014993 號函發台北市政府教育局政風單位調查，至 11 月止仍無調查結果，為避免影響師生權益，簽請續辦招標(如附件 1)。

主席指示：112 年教學軟體請計網中心確認預算，並先對各單位、學院需求進行調查。

(二)工作報告：

1、資訊系統組：

（1）防疫期間配合各項管制之軟硬體協助，包含：校務系統提供網路點名作業，架設自主健康管理回報系統，提供校內疫情調查與管理，配合疫情管制期間持續進行中。

（2）智慧校園門禁系統：已於 4/28 配合中央防疫政策下架，硬體設備留用作為體溫量測使用。

（3）校務系統學生協作計畫：聘請畢業傑出校友擔任業界導師，帶領學生團隊開發手持裝置端校務系統應用，首部作品為學生請假系統。

（4）校務系統資料庫配合網路選課需要，改租用雲端主機測試計畫：擬於 11 月進行第一次壓力測試。

（5）配合總務處資產組規劃，財產系統擬於 11 月進行第一階段上線，可提供教職員在系統進行財產查詢與在系統開立紙本表單。

（6）112 年度資料庫 ASE15.7 維護案採購進行中。

（7）112 年度天母校區電腦機房 UPS 不斷電及空調設備維護服務採購進行中。

（8）112-114 年度 Google 雲端儲存空間採購進行中。

（9）申請加入「教育部全國數位證書及場域建置試辦計畫」第 4 期，目前與教務處合作進行，規劃 112 年 7 月畢業時提供領取數位畢業證書。

2、網路及行政組：

（1）111 年度「博愛校區電腦機房不斷電系統(UPS)汰換」辦理完成。

（2）111 年度「資訊安全管理制度(ISMS)驗證及個資保護管理顧問服務案」辦理完成。

（3）111 年度「資訊安全設備使用授權暨智慧型流量調整服務」辦理完成。

（4）111 年 1 月初至 10 月底、硬體維護 464、軟體維護 268、網路維護 63、系統維護 99、帳號/權限 29、印表

機 33、郵件維護 9、其它及特別勤務 20、電腦教室 26 共計 1011 件。

（5）於 111 年 10 月 16 日完成應用程式防火牆韌體更新，10 月 30 日更新負載平衡器韌體，並於 11 月 1 日更新博愛校區防火牆之韌體。

（6）鑑於開學近三週在上課時間博愛校區對外的學術網路時常接近滿格用量 1G，為優化本校網路服務品質，採取分流方式，獨立出 550 M 頻寬之無線網路直接對外(不經過學術網路)，另外有線網路維持 1G 經由台灣學術網路對外連線(台大)，以改善網路速度。第一次分流設定於 9 月 19 日辦理，第二次設定於 10 月 5 日設定完成。

（7）重申依臺北市政府教育局 109 年 12 月 30 日北市教資字第 1093118386 號函，為避免公務及機敏資料遭不當竊取，全校各單位不得採購及使用大陸廠牌資通訊產品(含軟體、硬體及外包服務使用之設備)，包含有網路功能之設備如無人機、網路攝影機、印表機、相機等，常見大陸品牌產品包括華為、海康威視、大江、小米、紅米、大華……等。如已購買，請勿介接公務系統，並於使用年限期滿逕行報廢。

（8）依 1101 資推會提案決議辦理 111 年度教學軟體採購案，因廠商投標程序瑕疵，故採購程序暫停。

（9）全校 112 年微軟大量授權辦理中。

（10）全校 112 年 Adobe 大量授權辦理中。

（11）全校 112 年 Endnote 書目管理軟體大量授權辦理中。

（12）112 年為師培中心「教育部補助師資培育之大學辦理提升師資生運用數位教學能力計畫」採購平板，預計經費共 7 萬元。

(三)111 年度預算執行結果：請詳見附件 2。

主席指示：

(一)計網中心校務系統開發可多與資訊系學生合作，提供師生參與機會。

(二)選課作業的改善相關同仁都十分努力，請同學們多給予正向建議。

(三)請各單位協助配合落實資訊安全規範。

(四)再次重申各單位請勿購買大陸廠牌資通訊產品。

(五)校務系統學生協作以計網中心為主，配合教務處、學務處建議，提出改善方案。

參、討論事項：

提 案 一：為修正本校「智慧財產權推動委員會設置要點」要點乙案，提請討論。

提案單位：計算機與網路中心　網路及行政組

說　　明：

（1） 擬修正本校「智慧財產權推動委員會設置要點」第 2 條之部分文字。

（2） 檢陳本校「智慧財產權推動委員會設置要點」修正條文對照表、修正草案、現行條文（如附件 3）各 1 份。

決　　議：第二條文字維持各學院院長、其餘照案通過。

提 案 二：為修正本校「資訊安全暨個人資料保護推動執行委員會設置要點」要點乙案，提請討論。

提案單位：計算機與網路中心　網路及行政組

說　　明：

（1） 擬修正本校「資訊安全暨個人資料保護推動執行委員會設置要點」第 2 條之部分文字。

（2） 檢陳本校「資訊安全暨個人資料保護推動執行委員會設置要點」修正條文對照表、修正草案、現行條文（如附件 4）各 1 份。

決　　議：第二條文字維持各學院院長、其餘照案通過。

提 案 三：為修正本校「校園伺服器管理要點」要點乙案，提請討論。

提案單位：計算機與網路中心　網路及行政組

說　　明：

（1） 擬修正本校「校園伺服器管理要點」第 1、3、5、7、9 條之部分文字。

（2） 檢陳本校「校園伺服器管理要點」修正條文對照表、修正草案、現行條文（如附件 5）各 1 份。

決　　議：照案通過。

提 案 四：為修正本校「資訊安全作業要點」要點乙案，提請討論。

提案單位：計算機與網路中心　網路及行政組

說　　明：

（1） 擬修正本校「資訊安全作業要點」第 1 條之部分文字。

（2） 檢陳本校「資訊安全作業要點」修正條文對照表、修正草案、現行條文（如附件 6）各 1 份。

決　　議：照案通過。

提 案 五：為修正本校「網路侵權事件處理要點」要點乙案，提請討論。

提案單位：計算機與網路中心　網路及行政組

說　　明：

（1） 擬修正本校「網路侵權事件處理要點」第 4 條之部分文字。

（2） 檢陳本校「網路侵權事件處理要點」修正條文對照表、修正草案、現行條文（如附件 7）各 1 份。

決　　議：照案通過。

提 案 六：為維護全校網路安全，擬全校性盤點各單位及系所之伺服器，提請討論。

提案單位：計算機與網路中心　網路及行政組

說　　明：

（一）本中心已盤點於主機房內部之伺服器清單，惟各單位及系所之伺服器，擬發全校公告盤點伺服器設備進行列管，並惠請各單位付起相關資安之責任，提請討論。

（二）盤點資料參考格式：

位置	品名	品牌 型號	用途	保管人	IP	購買日期

決　　議：照案通過。

肆、臨時動議：無

伍、散　　會：　11　時　00　分

臺北市立大學智慧財產權推動委員會設置要點 修正/現行 條文對照表		
修正條文	**現行條文**	**說明**
第二條　委員會置委員十九**至二十一人**，委員包括學術副校長、行政副校長、教務長、學生事務長、總務長、研發長、進修推廣處處長、師資培育及職涯發展中心主任、圖書館館長、人事室主任、計算機與網路中心主任、各學院院長、學生會會長、學生議會會長、研究生學會會長，由學術副校長擔任召集人。**委員任期一年，由校長遴聘之。**	第二條　委員會置委員**十七至**十九人，委員包括學術副校長、行政副校長、教務長、學生事務長、總務長、研發長、進修推廣處處長、師資培育及職涯發展中心主任、圖書館館長、人事室主任、計算機與網路中心主任、各學院院長、學生會會長、學生議會會長、研究生學會會長，由學術副校長擔任召集人。	委員人數及文字修正，新增委員任期為一年。

臺北市立大學智慧財產權推動委員會設置要點(草案)

102 年 12 月 9 日資訊推動委員會會議通過
106 年 3 月 28 日 105 學年度第 2 次資訊推動委員會會議通過修正第二、六、八點
111 年 oo 月 oo 日資訊推動委員會會議通過

一、臺北市立大學為積極宣導及執行校園保護智慧財產權工作，特成立智慧財產權推動委員會(以下簡稱本委員會)。

二、委員會置委員十九人，委員包括學術副校長、行政副校長、教務長、學生事務長、總務長、研發長、進修推廣處處長、師資培育及職涯發展中心主任、圖書館館長、人事室主任、計算機與網路中心主任、各學院院長、學生會會長、學生議會會長、研究生學會會長，由學術副校長擔任召集人。委員任期一年，由校長遴聘之。

三、本委員會下置宣導小組及執行小組，其組長分由學生事務長及計算機與網路中心主任擔任之。

四、本委員會之工作執掌：

(一)規劃並推動有關智慧財產權相關法令規定之宣導活動。

(二)落實執行檢視校園合法軟體、教科書、影音光碟等之使用。

(三)訂定教職員工生違反智慧財產權相關規範措施。

(四)其他保護校園智慧財產權相關措施之規劃與執行。

五、本委員會成員均為無給職，視工作需要不定時召開會議，每學期至少召開一次會議，開會時得邀請有關單位人員列席。

六、依「教育部大專校院校園保護智慧財產權行動方案執行自評表」，填報權責單位如下：

(一)行政督導：秘書室、計算機與網路中心。

(二)課程規劃：教務處、進修推廣處、師資培育及職涯發展中心、教學發展中心、通識教育中心、各系所。

(三)教育推廣：教務處、學生事務處、研究發展處、進修推廣處、圖書館、人事室、教學發展中心、通識教育中心、計算機與網路中心、各系所。

(四)校園影印管理：教務處、學生事務處、總務處、研究發展處、進修推廣處、圖書館、各系所。

(五)校園網路管理：計算機與網路中心。

（六)輔導評鑑：行政副校長室、計算機與網路中心。

七、本校權責單位為計算機與網路中心，於每學年初(每年九月中旬前)擬訂活動規劃表，並於每學年末(每年六月底前)會同上條權責單位辦理自評，填報校園保護智慧財產權行動方案自評表，並檢討與考核執行成效。

八、本要點經資訊推動委員會通過，陳請校長核定後實施。

臺北市立大學智慧財產權推動委員會設置要點

102 年 12 月 9 日資訊推動委員會會議通過
106 年 3 月 28 日 105 學年度第 2 次資訊推動委員會會議通過修正第二、六、八點

九、臺北市立大學為積極宣導及執行校園保護智慧財產權工作，特成立智慧財產權推動委員會(以下簡稱本委員會)。

十、委員會置委員十七至十九人，委員包括學術副校長、行政副校長、教務長、學生事務長、總務長、研發長、進修推廣處處長、師資培育及職涯發展中心主任、圖書館館長、人事室主任、計算機與網路中心主任、各學院院長、學生會會長、學生議會會長、研究生學會會長，由學術副校長擔任召集人。

十一、　本委員會下置宣導小組及執行小組，其組長分由學生事務長及計算機與網路中心主任擔任之。

十二、　本委員會之工作執掌：

(一)規劃並推動有關智慧財產權相關法令規定之宣導活動。

(二)落實執行檢視校園合法軟體、教科書、影音光碟等之使用。

(三)訂定教職員工生違反智慧財產權相關規範措施。

(四)其他保護校園智慧財產權相關措施之規劃與執行。

十三、　本委員會成員均為無給職，視工作需要不定時召開會議，每學期至少召開一次會議，開會時得邀請有關單位人員列席。

十四、　依「教育部大專校院校園保護智慧財產權行動方案執行自評表」，填報權責單位如下：

(一)行政督導：秘書室、計算機與網路中心。

(二)課程規劃：教務處、進修推廣處、師資培育及職涯發展中心、教學發展中心、通識教育中心、各系所。

(三)教育推廣：教務處、學生事務處、研究發展處、進修推廣處、圖書館、人事室、教學發展中心、通識教育中心、計算機與網路中心、各系所。

(四)校園影印管理：教務處、學生事務處、總務處、研究發展處、進修推廣處、圖書館、各系所。

(五)校園網路管理：計算機與網路中心。

(六)輔導評鑑：行政副校長室、計算機與網路中心。

十五、 本校權責單位為計算機與網路中心，於每學年初(每年九月中旬前)擬訂活動規劃表，並於每學年末(每年六月底前)會同上條權責單位辦理自評，填報校園保護智慧財產權行動方案自評表，並檢討與考核執行成效。

十六、 本要點經資訊推動委員會通過，陳請校長核定後實施。

臺北市立大學資訊安全暨個人資料保護推動執行委員會設置要點

修正
現行 條文對照表

修正條文	現行條文	說明
第二條　本委員會置委員十九人**至二十一人**，委員包括學術副校長、行政副校長、教務長、學生事務長、總務長、研發長、進修推廣處處長、師資培育及職涯發展中心主任、圖書館館長、人事室主任、計算機與網路中心主任、各學院院長、學生會會長、學生議會會長、研究生學會會長。本委員會置召集人一人，由學術副校長擔任；執行秘書一人，由計算機與網路中心主任擔任，並得視需要聘任顧問**一至二人**。**委員任期一年，由校長遴聘之。**	第二條　本委員會置委員**十七人至**十九人，委員包括學術副校長、行政副校長、教務長、學生事務長、總務長、研發長、進修推廣處處長、師資培育及職涯發展中心主任、圖書館館長、人事室主任、計算機與網路中心主任、各學院院長、學生會會長、學生議會會長、研究生學會會長。本委員會置召集人一人，由學術副校長擔任；執行秘書一人，由計算機與網路中心主任擔任，並得視需要聘任顧問**若干**人。	委員人數修正及酌作文字修正，新增委員任期為一年。

臺北市立大學

資訊安全暨個人資料保護推動執行委員會設置要點(草案)

102 年 12 月 9 日資訊推動委員會會議通過
104 年 10 月 14 日資訊推動委員會會議修正通過
104 年 11 月 10 日 104 學年度第 3 次行政修正通過
106 年 3 月 28 日資訊推動委員會會議修正通過

一、臺北市立大學(以下簡稱本校)為配合行政院資訊安全管理制度之推動與落實個人資料之保護及管理，特設置本校資訊安全暨個人資料保護推動執行委員會(以下簡稱本委員會)，並訂定設置要點(以下簡稱本要點)。

二、本委員會置委員十九人至二十一人，委員包括學術副校長、行政副校長、教務長、學生事務長、總務長、研發長、進修推廣處處長、師資培育及職涯發展中心主任、圖書館館長、人事室主任、計算機與網路中心主任、各學院院長、市政管理學院院長、學生會會長、學生議會會長、研究生學會會長。本委員會置召集人一人，由學術副校長擔任；執行秘書一人，由計算機與網路中心主任擔任，並得視需要聘任顧問一至二人。委員任期一年，由校長遴聘之。

三、本委員會之任務如下：

(一)本校資通安全政策之研議。

(二)跨單位資訊安全事項權責分工之協調。

(三)資訊資產價值及風險評估之研議。

(四)資訊安全事件之危機通報、緊急應變檢討與監督。

(五)整體資訊安全措施之協調與研議。

(六)應採用之資訊安全技術方法或程序之協調與研議。

(七)資訊安全計畫之協調與研議。

(八)辦理資訊安全相關教育訓練及稽核業務。

(九)擬訂本校個人資料保護管理制度及配套措施。

(十)辦理個人資料保護相關法規專業訓練及宣導作業。

(十一) 本校個人資料管理制度之推展。

(十二) 本校個人資料管理制度適法性與合宜性之檢視、審議及評估。

(十三) 個資外洩事件通報暨危機處理。

(十四) 辦理個人資料保護管理作業相關稽核作業。

(十五) 其他重要資訊安全事項之協調與研議及個人資料保護執行事項。

(十六) 本委員會置執行小組由執行秘書指定專人擔任，辦理本委員會各項任務。

(十七) 各單位設聯絡窗口，由教學單位、行政單位指定專人擔任，協助推動單位內資訊安全及個人資料保護業務。

四、本委員會每學期開會一次，必要時得召開臨時會議。

五、本委員會會議應有委員二分之一以上之出席始得開會，會議決議應有出席委員過半數之同意行之。

六、本委員會委員為無給職，諮詢顧問出席會議時，依相關規定支領出席費。

七、本要點未規範事項，依照相關法令辦理。

八、本要點經資訊推動委員會通過，陳請校長核定後實施。

臺北市立大學

資訊安全暨個人資料保護推動執行委員會設置要點

102 年 12 月 9 日資訊推動委員會會議通過
104 年 10 月 14 日資訊推動委員會會議修正通過
104 年 11 月 10 日 104 學年度第 3 次行政修正通過
106 年 3 月 28 日資訊推動委員會會議修正通過

九、臺北市立大學(以下簡稱本校)為配合行政院資訊安全管理制度之推動與落實個人資料之保護及管理，特設置本校資訊安全暨個人資料保護推動執行委員會(以下簡稱本委員會)，並訂定設置要點(以下簡稱本要點)。

十、本委員會置委員十七人至十九人，委員包括學術副校長、行政副校長、教務長、學生事務長、總務長、研發長、進修推廣處處長、師資培育及職涯發展中心主任、圖書館館長、人事室主任、計算機與網路中心主任、各學院院長、學生會會長、學生議會會長、研究生學會會長。本委員會置召集人一人，由學術副校長擔任；執行秘書一人，由計算機與網路中心主任擔任，並得視需要聘任顧問若干人。

十一、　本委員會之任務如下：

（十八）　本校資通安全政策之研議。

（十九）　跨單位資訊安全事項權責分工之協調。

（二十）　資訊資產價值及風險評估之研議。

（二十一）資訊安全事件之危機通報、緊急應變檢討與監督。

（二十二）整體資訊安全措施之協調與研議。

（二十三）應採用之資訊安全技術方法或程序之協調與研議。

（二十四）資訊安全計畫之協調與研議。

（二十五）辦理資訊安全相關教育訓練及稽核業務。

（二十六）擬訂本校個人資料保護管理制度及配套措施。

（二十七）辦理個人資料保護相關法規專業訓練及宣導作業。

（二十八）本校個人資料管理制度之推展。

（二十九）本校個人資料管理制度適法性與合宜性之檢視、審議及評估。

（三十）　個資外洩事件通報暨危機處理。

（三十一）辦理個人資料保護管理作業相關稽核作業。

（三十二）其他重要資訊安全事項之協調與研議及個人資料保護執行事項。

（三十三）本委員會置執行小組由執行秘書指定專人擔任，辦理本委員會各項任務。

（三十四）各單位設聯絡窗口，由教學單位、行政單位指定專人擔任，協助推動單位內資訊安全及個人資料保護業務。

十二、　本委員會每學期開會一次，必要時得召開臨時會議。

十三、　本委員會會議應有委員二分之一以上之出席始得開會，會議決議應有出席委員過半數之同意行之。

十四、　本委員會委員為無給職，諮詢顧問出席會議時，依相關規定支領出席費。

十五、　本要點未規範事項，依照相關法令辦理。

十六、　本要點經資訊推動委員會通過，陳請校長核定後實施。

臺北市立大學校園伺服器管理要點修正現行條文對照表

修正條文	現行條文	說明
第一條　依據**「臺灣學術網路管理規範」及「臺北市立大學網路使用要點」**，針對臺北市立大學(以下簡稱本校)伺服器之管理與使用，訂定「校園伺服器管理辦法」(以下稱本辦法)。	第一條　依據**本校校園網路使用辦法第四條**，針對臺北市立大學(以下簡稱本校)伺服器之管理與使用，訂定「校園伺服器管理辦法」(以下稱本辦法)。	修正依據為臺灣學術網路管理規範及臺北市立大學網路使用要點第三條。
第三條　**各單位**架設伺服器主機，須**指派專責伺服器管理人員**負責維護管理，並事先填具**「伺服器架設申請單」或「虛擬主機申請單」**，向計算機與網路管理中心申請(以下稱本中心)，經審查核准後方可運作**，異動時亦同**。	第三條　**本單位或個人**架設伺服器主機，須**有專人**負責維護管理，並事先填具**申請表**，向計算機與網路管理中心申請(以下稱本中心)，經審查核准後方可運作。	新增表單名稱及異動規定，並進行文字修正。
第五條	第五條　學生個人架設之主機應先行向所屬系所提出申請，再轉交計算機與網路中心並由該系所管理之。	本條刪除。
第六條　伺服器**其內容及使用需符合「臺灣學術網路管理規範」及「臺北市立大學網路使用要點」，且不得安裝違反智慧財產權之軟體及違法操作。**	第七條　伺服器**不得安裝違反著作權法之軟體及違法操作。**	新增伺服器使用須符合「臺灣學術網路管理規範」及「臺北市立大學網路使用要點」規範。
第八條　各單位之伺服主機，**伺服器管理人員需**定期(每學期不得少於壹次)清查伺服器資訊內容並記錄、追蹤處理情況。**伺服器管理者應為其伺服器建置安全防護機制，**計算機與網路中心每學期對列管伺服器進行資訊安全檢測，不合格之伺服器將暫停其連線直至改善為止。	第九條　各單位之伺服主機，**須有專人**定期(每學期不得少於壹次)清查伺服器資訊內容並記錄、追蹤處理情況。計算機與網路中心每學期對列管伺服器進行資訊安全檢測，不合格之伺服器將暫停其連線直至改善為止。	因應資安需求新增伺服器管理者應為其伺服器建置安全防護機制及文字修正。

臺北市立大學校園伺服器管理要點(草案)

98 年 02 月 17 日第 6 次行政會議通過
104 年 10 月 13 日資訊推動委員會會議修正通過
111 年 oo 月 oo 日資訊推動委員會會議修正通過

一、依據「臺灣學術網路管理規範」及「臺北市立大學網路使用要點」，針對臺北市立大學(以下簡稱本校)伺服器之管理與使用，訂定「校園伺服器管理辦法」(以下稱本辦法)。

二、 本辦法對象為使用本校 IP 並對外開放服務伺服器之單位或個人。

三、本校各單位架設伺服器主機，須指派專責伺服器管理人員負責維護管理，並事先填具「伺服器架設申請單」或「虛擬主機申請單」，向計算機與網路管理中心申請(以下稱本中心)，經審查核准後方可運作，異動時亦同。

四、 申請伺服器各行政或教學單位主管應負單位內伺服主機督導之責，並禁止未申請核准及遭列管之伺服器於單位內運作。

五、 臺灣學術網路系提供各學校及研究單位作為學術用途，於校園網路內不得提供商業性網路服務，亦不可提供具商業廣告性質之免費網路服務(包含郵件伺服器、網頁伺服器及其他種類伺服器等)。

六、伺服器其內容及使用需符合「臺灣學術網路管理規範」及「臺北市立大學網路使用要點」，且不得安裝違反智慧財產權之軟體及違法操作。

七、 退(離)職人員及畢業學生應依資訊安全規定及程序，由伺服器管理人員取消存取網路權利。

八、各單位之伺服主機，伺服器管理人需員定期(每學期不得少於壹次)清查伺服器資訊內容並記錄、追蹤處理情況。伺服器管理者應為其伺服器建置安全防護機制，計算機與網路中心每學期對列管伺服器進行資訊安全檢測，不合格之伺服器將暫停其連線直至改善為止。

九、計算機與網路中心得暫停伺服器對外之連線，有涉及下列情形之一伺服器者：

(一)各單位之伺服器因管理不當，違反本辦法者。

(二)伺服器管理人員未參加本中心每年不定期舉辦之資訊安全講習。

(三)伺服器管理人員未參加或配合本校資訊安全處理小組不定期之演練。

(四)伺服器負責人員連絡三次以上無回應。

十、 伺服器被暫停對外連線一個月仍無法恢復者，本中心得撤銷該伺服器之設立許可，該伺服器可於問題排除後重新提出申請。

十一、 本要點經資訊推動委員會通過，陳請校長核定後實施。

臺北市立大學校園伺服器管理要點

98 年 02 月 17 日第 6 次行政會議通過
104 年 10 月 13 日資訊推動委員會會議修正通過

一、 依據本校校園網路使用辦法第四條，針對本校伺服器之管理與使用，訂定「校園伺服器管理辦法」(以下稱本辦法)

二、 本辦法對象為使用本校 IP 並對外開放服務伺服器之單位或個人。

三、 本單位或個人架設伺服器主機，須有專人負責維護管理，並事先填具申請表，向計算機與網路管理中心申請(以下稱本中心)，經審查核准後方可運作。

四、 申請伺服器各行政或教學單位主管應負單位內伺服主機督導之責，並禁止未申請核准及遭列管之伺服器於單位內運作。

五、 學生個人架設之主機應先行向所屬系所提出申請，再轉交計算機與網路中心並由該系所管理之。

六、 臺灣學術網路系提供各學校及研究單位作為學術用途，於校園網路內不得提供商業性網路服務，亦不可提供具商業廣告性質之免費網路服務(包含郵件伺服器、網頁伺服器及其他種類伺服器等)。

七、 伺服器不得安裝違反著作權法之軟體及違法操作。

八、 退(離)職人員及畢業學生應依資訊安全規定及程序，由伺服器管理人員取消存取網路權利。

九、 各單位之伺服主機，須有專人定期(每學期不得少於壹次)清查伺服器資訊內容並記錄、追蹤處理情況。計算機與網路中心每學期對列管伺服器進行資訊安全檢測，不合格之伺服器將暫停其連線直至改善為止。

十、 計算機與網路中心得暫停伺服器對外之連線，有涉及下列情形之一伺服器者：

(一)各單位之伺服器因管理不當，違反本辦法者。

(二)伺服器管理人員未參加本中心每年不定期舉辦之資訊安全講習。

(三)伺服器管理人員未參加或配合本校資訊安全處理小組不定期之演練。

(四)伺服器負責人員連絡三次以上無回應。

十一、 伺服器被暫停對外連線一個月仍無法恢復者，本中心得撤銷該伺服器之設立許可，該伺服器可於問題排除後重新提出申請。

十二、 本要點經資訊推動委員會通過，陳請校長核定後實施。

臺北市立大學資訊安全作業要點 修正/現行 條文對照表

修正條文	現行條文	說明
第一條　臺北市立大學(以下簡稱本大學)為確保本大學各單位各項資訊蒐集、處理、傳送、儲存及流通之安全，並保障本大學教職員工生之權益，特依「**個人資料保護法**」、「**資通安全管理法**」訂定本要點。	第一條　臺北市立大學(以下簡稱本大學)為確保本大學各單位各項資訊蒐集、處理、傳送、儲存及流通之安全，並保障本大學教職員工生之權益，特依「**電腦處理個人資料保護法**」、「**行政院及所屬各機關資訊安全管理要點**」訂定本要點。	電腦處理個人資料保護法於九十九年五月二十六日已廢止修正為個人資料保護法。行政院及所屬各機關資訊安全管理要點已於一百一十一年一月十七日廢止。

臺北市立大學資訊安全作業要點(草案)

95 年 9 月 25 日資訊推動委員會第二次會議通過
95 年 11 月 30 日核定後實施
104 年 10 月 13 日資訊推動委員會會議修正通過
111 年 oo 月 oo 日資訊推動委員會會議修正通過

壹、目的

一、臺北市立大學(以下簡稱本大學)為確保本大學各單位各項資訊蒐集、處理、傳送、儲存及流通之安全，並保障本大學教職員工生之權益，特依「個人資料保護法」、「資通安全管理法」訂定本要點。

貳、通則

二、本要點應以書面、電子或其他方式告知本大學全體教職員工生、連線作業之公私機構及提供資訊服務之廠商共同遵行。

三、本要點應至少每年評估一次，以順應技術、業務等相關環境之趨勢，確保實務作業之有效性。

四、本要點實施時如有必要，各單位應訂定說明文件，如管理規範、作業程序、資訊安全控管文件等。

五、資訊安全應定期或不定期進行稽核。

參、權責分工

六、於實施本要點時，其權責分工如下：

(一)為統籌、協調、研議本大學各項資訊安全之政策、計畫及資源調度，特成立「資訊安全推行小組」。「資訊安全推行小組」由教務長、學生事務長、總務長三長、主任秘書、人事、會計室主任、計算機與網路中心主任共同組成；由教務長擔任召集人，計算機與網路中心為業務承辦單位。

(二)各項電腦軟硬體設備、應用系統、網路通訊之安全計畫及技術規範之研議、建置及評估等，由所屬資訊或管理單位或人員負責辦理。

(三)各項資料之安全需求、使用管理及保護等事項，由業務承辦單位或人員負責辦理。

(四)資訊機密維護及稽核使用管理事項，由秘書室會同相關單位負責辦理。

肆、人員管理

七、本大學各單位對資訊相關職務及工作，應進行安全評估，並於人員進用、任務指派及工作時，審慎評估人員之適任性，並進行必要之考核。

八、各單位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存取特別權限之人員，應加強評估及考核。

九、各單位應針對管理、業務及資訊等不同工作類別之需求，定期辦理資訊

安全教育訓練及宣導，建立資訊安全認知，提升單位資訊安全水準。

十、單位應加強資訊安全人力之培訓，提升資訊安全管理能力。

十一、各單位資訊安全人力或經驗如有不足，得洽請學者專家或專業機關(構)提供顧問諮詢服務。

十二、各單位負責重要資訊系統之管理、維護、設計及操作之人員，應妥適分散權責，並視需要建立制衡機制，實施人員輪調，建立人力備援制度。

十三、各相關單位主管應負責所屬員工之資訊安全作業，防範不法及不當行為。

伍、電腦系統安全管理

十四、各單位辦理資訊業務委外作業，應於事前研提資訊安全需求，明定廠商之資訊安全責任及保密規定，並列入契約，要求廠商遵守並定期考核。

十五、各單位自行開發或委外發展系統，應在系統生命週期之初始階段，即將資訊安全需求納入考量；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。

十六、各單位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。各單位基於實際作業需要，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。各單位委託廠商建置及維護重要軟硬體設施時，應在單位相關人員監督及陪同下始得為之。

十七、各單位對系統變更作業，應建立控管制度，並建立紀錄，以備查考。

十八、各單位使用軟體之權利及義務應依著作權法及有關議定之合約辦理。各單位應依據「政府所屬各級行政機關電腦軟體管理作業要點」，建立軟體使用管理制度。

十九、各單位應採行必要之事前預防及保護措施，偵測及防制電腦病毒及其他惡意軟體，確保系統正常運作。

陸、網路安全管理

二十、各單位利用公眾網路傳送資訊或進行交易處理，應遵守「台灣學術網路使用規範」；並應評估可能之安全風險，確定資料傳輸具完整性、機密性、身分鑑別及不可否認性等安全需求。

二十一、各單位應針對資料傳輸、撥接線路、網路線路與設備、對外連接介面及路由器等事項，研擬妥適安全控管措施。

二十二、各單位與外界網路連接之網點，必要時得以防火牆或其他安全設施，控管外界與單位內部網路之資料傳輸及資源存取。

二十三、各單位開放外界連線作業之資訊系統，必要時得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。

二十四、各單位開放外界連線作業之資訊系統，必要時得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。

二十五、各單位利用網際網路及全球資訊網公布及流通資訊，應實施資料安全等級評估，機密性、敏感性及未經當事人同意之個人隱私資料及文件，不得上網公布。

二十六、單位網站存有個人資料及檔案者，應加強安全保護措施，防止個人隱私資料遭違法或不當之竊取使用。

二十七、本大學應訂定電子郵件使用規定，機密性資料及文件，不得以電子郵件或其他電子方式傳送。機密性資料以外之敏感性資料及文件，如有電子傳送之需要，本大學應視需要以適當之加密或電子簽章等安全技術處理。單位業務性質特殊，須利用電子郵件或其他電子方式傳送機密性資料及文件者，得採用權責主管機關認可之加密或電子簽章等安全技術處理。

二十八、各單位採購資訊軟硬體設施，應依國家標準或權責主管機關訂定之政府資訊安全規範，研提資訊安全需求，並列入採購規格。各單位發展及應用加密技術，應採用權責主管機關認可之密碼模組產品。各單位採購外國產製之密碼模組產品，應請廠商提出輸出許可或相關授權文件，確保密碼模組之安全性，並避免採購金鑰代管或金鑰回復功能之產品。

柒、系統存取控制

二十九、各單位應訂定系統存取政策及授權規定，並以書面、電子或其他方式告知教職員工生及使用者之相關權限及責任。

三十、各單位應依資訊安全政策，賦予各級人員必要之系統存取權限；賦予之系統存取權限，應以執行法定任務所必要者為限。對被賦予系統管理最高權限之人員及掌理重要技術及作業控制之特定人員，應經審慎之授權評估。

三十一、本大學各單位離(休)職人員，學生應立即取消使用校內各項資訊資源之所有權限，老師則保留各項資訊資源之權限。各單位人員職務調整及調動，應依系統存取授權規定，限期調整其權限。

三十二、各單位應建立教職員工生及使用者註冊管理制度，加強通行密碼管理，並要求定期更新；其通行密碼之更新週期，由各單位視作業系統及安全管理需求決定，最長以不超過六個月為原則。對單位內外擁有系統存取特別權限之人員，應建立使用人員名冊，加強安全控管，並縮短密碼更新週期。

三十三、各單位開放外界連線作業，應事前簽訂契約或協定，明定其應遵守之資訊安全規定、標準、程序及應負之責任。

三十四、各單位對系統服務廠商以遠端登入方式進行系統維護者，應加強安全控管，並建立人員名冊，課其相關安全保密責任。

三十五、各單位資料需委外建檔者，不論在單位內外執行，均應採取適當及必要之安全管制措施，防止資料被竊取、竄改、販售、洩漏及不當備份等情

形發生。

三十六、各單位應確立系統稽核項目，建立資訊安全稽核制度，定期或不定期進行資訊安全稽核作業；系統中之稽核紀錄檔案，應禁止任意刪除及修改。

捌、業務永續運作之規劃

三十七、各單位應訂定業務永續運作計畫，評估各種人為及天然災害對單位正常業務運作之影響，訂定緊急應變與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。

三十八、各單位應建立資訊安全事件緊急處理機制，在發生資訊安全事件時，應依規定之處理程序，立即向該單位權責人員通報，於採取反應措施後，並由本大學聯繫檢警調機關偵查。

玖、其他安全措施

三十九、各單位應依相關法規，訂定及區分資料安全等級，並依不同安全等級，採取適當及必要之資訊安全措施。

四十、各單位應就設備安置、周邊環境及人員進出管制等，訂定妥善之設備及環境安全管理措施。

拾、附則

四十一、本要點經資訊推動委員會通過，陳請校長核定後公布施行。

臺北市立大學資訊安全作業要點

95 年 9 月 25 日資訊推動委員會第二次會議通過
95 年 11 月 30 日核定後實施
104 年 10 月 13 日資訊推動委員會會議修正通過

壹、目的

一、臺北市立大學(以下簡稱本大學)為確保本大學各單位各項資訊蒐集、處理、傳送、儲存及流通之安全，並保障本大學教職員工生之權益，特依「電腦處理個人資料保護法」、「行政院及所屬各機關資訊安全管理要點」訂定本要點。

貳、通則

二、本要點應以書面、電子或其他方式告知本大學全體教職員工生、連線作業之公私機構及提供資訊服務之廠商共同遵行。

三、本要點應至少每年評估一次，以順應技術、業務等相關環境之趨勢，確保實務作業之有效性。

四、本要點實施時如有必要，各單位應訂定說明文件，如管理規範、作業程序、資訊安全控管文件等。

五、資訊安全應定期或不定期進行稽核。

參、權責分工

六、於實施本要點時，其權責分工如下：

(一)為統籌、協調、研議本大學各項資訊安全之政策、計畫及資源調度，特成立「資訊安全推行小組」。「資訊安全推行小組」由教務長、學生事務長、總務長三長、主任秘書、人事、會計室主任、計算機與網路中心主任共同組成；由教務長擔任召集人，計算機與網路中心為業務承辦單位。

(二)各項電腦軟硬體設備、應用系統、網路通訊之安全計畫及技術規範之研議、建置及評估等，由所屬資訊或管理單位或人員負責辦理。

(三)各項資料之安全需求、使用管理及保護等事項，由業務承辦單位或人員負責辦理。

(四)資訊機密維護及稽核使用管理事項，由秘書室會同相關單位負責辦理。

肆、人員管理

七、本大學各單位對資訊相關職務及工作，應進行安全評估，並於人員進用、任務指派及工作時，審慎評估人員之適任性，並進行必要之考核。

八、各單位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存取特別權限之人員，應加強評估及考核。

九、各單位應針對管理、業務及資訊等不同工作類別之需求，定期辦理資訊安全教育訓練及宣導，建立資訊安全認知，提升單位資訊安全水準。

十、單位應加強資訊安全人力之培訓，提升資訊安全管理能力。

十一、各單位資訊安全人力或經驗如有不足，得洽請學者專家或專業機關(構)提供顧問諮詢服務。

十二、各單位負責重要資訊系統之管理、維護、設計及操作之人員，應妥適分散權責，並視需要建立制衡機制，實施人員輪調，建立人力備援制度。

十三、各相關單位主管應負責所屬員工之資訊安全作業，防範不法及不當行為。

伍、電腦系統安全管理

十四、各單位辦理資訊業務委外作業，應於事前研提資訊安全需求，明定廠商之資訊安全責任及保密規定，並列入契約，要求廠商遵守並定期考核。

十五、各單位自行開發或委外發展系統，應在系統生命週期之初始階段，即將資訊安全需求納入考量；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。

十六、各單位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。各單位基於實際作業需要，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。各單位委託廠商建置及維護重要軟硬體設施時，應在單位相關人員監督及陪同下始得為之。

十七、各單位對系統變更作業，應建立控管制度，並建立紀錄，以備查考。

十八、各單位使用軟體之權利及義務應依著作權法及有關議定之合約辦理。各單位應依據「政府所屬各級行政機關電腦軟體管理作業要點」，建立軟體使用管理制度。

十九、各單位應採行必要之事前預防及保護措施，偵測及防制電腦病毒及其他惡意軟體，確保系統正常運作。

陸、網路安全管理

二十、各單位利用公眾網路傳送資訊或進行交易處理，應遵守「台灣學術網路使用規範」；並應評估可能之安全風險，確定資料傳輸具完整性、機密性、身分鑑別及不可否認性等安全需求。

二十一、各單位應針對資料傳輸、撥接線路、網路線路與設備、對外連接介面及路由器等事項，研擬妥適安全控管措施。

二十二、各單位與外界網路連接之網點，必要時得以防火牆或其他安全設施，控管外界與單位內部網路之資料傳輸及資源存取。

二十三、各單位開放外界連線作業之資訊系統，必要時得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。

二十四、各單位開放外界連線作業之資訊系統，必要時得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。

二十五、各單位利用網際網路及全球資訊網公布及流通資訊，應實施資料安全等級評估，機密性、敏感性及未經當事人同意之個人隱私資料及文件，不得上網公布。

二十六、單位網站存有個人資料及檔案者，應加強安全保護措施，防止個人隱私資料遭違法或不當之竊取使用。

二十七、本大學應訂定電子郵件使用規定，機密性資料及文件，不得以電子郵件或其他電子方式傳送。機密性資料以外之敏感性資料及文件，如有電子傳送之需要，本大學應視需要以適當之加密或電子簽章等安全技術處理。單位業務性質特殊，須利用電子郵件或其他電子方式傳送機密性資料及文件者，得採用權責主管機關認可之加密或電子簽章等安全技術處理。

二十八、各單位採購資訊軟硬體設施，應依國家標準或權責主管機關訂定之政府資訊安全規範，研提資訊安全需求，並列入採購規格。各單位發展及應用加密技術，應採用權責主管機關認可之密碼模組產品。各單位採購外國產製之密碼模組產品，應請廠商提出輸出許可或相關授權文件，確保密碼模組之安全性，並避免採購金鑰代管或金鑰回復功能之產品。

柒、系統存取控制

二十九、各單位應訂定系統存取政策及授權規定，並以書面、電子或其他方式告知教職員工生及使用者之相關權限及責任。

三十、各單位應依資訊安全政策，賦予各級人員必要之系統存取權限；賦予之系統存取權限，應以執行法定任務所必要者為限。對被賦予系統管理最高權限之人員及掌理重要技術及作業控制之特定人員，應經審慎之授權評估。

三十一、本大學各單位離(休)職人員，學生應立即取消使用校內各項資訊資源之所有權限，老師則保留各項資訊資源之權限。各單位人員職務調整及調動，應依系統存取授權規定，限期調整其權限。

三十二、各單位應建立教職員工生及使用者註冊管理制度，加強通行密碼管理，並要求定期更新；其通行密碼之更新週期，由各單位視作業系統及安全管理需求決定，最長以不超過六個月為原則。對單位內外擁有系統存取特別權限之人員，應建立使用人員名冊，加強安全控管，並縮短密碼更新週期。

三十三、各單位開放外界連線作業，應事前簽訂契約或協定，明定其應遵守之資訊安全規定、標準、程序及應負之責任。

三十四、各單位對系統服務廠商以遠端登入方式進行系統維護者，應加強安全控管，並建立人員名冊，課其相關安全保密責任。

三十五、各單位資料需委外建檔者，不論在單位內外執行，均應採取適當及必要之安全管制措施，防止資料被竊取、竄改、販售、洩漏及不當備份等情形發生。

三十六、各單位應確立系統稽核項目，建立資訊安全稽核制度，定期或不定期進行資訊安全稽核作業；系統中之稽核紀錄檔案，應禁止任意刪除及修改。

捌、業務永續運作之規劃

三十七、各單位應訂定業務永續運作計畫，評估各種人為及天然災害對單位正常業務運作之影響，訂定緊急應變與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。

三十八、各單位應建立資訊安全事件緊急處理機制，在發生資訊安全事件時，應依規定之處理程序，立即向該單位權責人員通報，於採取反應措施後，並由本大學聯繫檢警調機關偵查。

玖、其他安全措施

三十九、各單位應依相關法規，訂定及區分資料安全等級，並依不同安全等級，採取適當及必要之資訊安全措施。

四十、各單位應就設備安置、周邊環境及人員進出管制等，訂定妥善之設備及環境安全管理措施。

拾、附則

四十一、本要點經資訊推動委員會通過，陳請校長核定後公布施行。

網路侵權事件處理要點 修正/現行 條文對照表		
修正條文	**現行條文**	**說明**
第四條　本校受理疑似網路侵權事件後。將先**封鎖該 IP**，並通知該 IP 所屬單位。	第四條　本校受理疑似網路侵權事件後。將先**移除涉有侵權之內容**，並通知該 IP 所屬單位。	因應現有計算機與網路中心技術可行作法，修改為直接封鎖該 IP。

臺北市立大學網路侵權事件處理要點(草案)

99 年 10 月 5 日 99 學年度第 1 次智慧財產權推動委員會通過
102 年 12 月 9 日資訊推動委員會會議修正通過
104 年 10 月 13 日資訊推動委員會會議修正通過
111 年 oo 月 oo 日資訊推動委員會會議修正通過

一、依據教育部校園網路使用規範訂定「網路侵權事件處理要點」(以下簡稱本要點)。

二、本要點適用範圍為全校教職員工生。

三、網路侵權事件乃指校內電腦透過網路進行疑似侵犯智慧財產權之行為。

四、本校受理疑似網路侵權事件後。將先封鎖該 IP，並通知該 IP 所屬單位。

五、各 IP 所屬單位內教職員工生有疑似侵權行為，應立即進行查詢與輔導，並向本校計算機與網路中心(以下簡稱本中心)回報疑似侵權者相關資料。疑似侵權者必須視是否侵權之情況分別填寫「臺北市立大學違反智慧財產權不再犯切結書」或「臺北市立大學違反智慧財產權宣稱原創之切結書」並送至本中心俾利管理。

六、教職員工被檢舉疑似侵權行為，並經查證屬實者，移請人事室或相關單位依法規懲處。

七、學生被檢舉疑似侵權行為，並經查證屬實者，移請學生事務處依校規懲處。

八、本要點經資訊推動委員會通過，陳請校長核定後實施。

臺北市立大學網路侵權事件處理要點

99 年 10 月 5 日 99 學年度第 1 次智慧財產權推動委員會通過
102 年 12 月 9 日資訊推動委員會會議修正通過
104 年 10 月 13 日資訊推動委員會會議修正通過

九、依據教育部校園網路使用規範訂定「網路侵權事件處理要點」(以下簡稱本要點)。

十、本要點適用範圍為全校教職員工生。

十一、　網路侵權事件乃指校內電腦透過網路進行疑似侵犯智慧財產權之行為。

十二、　本校受理疑似網路侵權事件後。將先移除涉有侵權之內容，並通知該 IP 所屬單位。

十三、　各 IP 所屬單位內教職員工生有疑似侵權行為，應立即進行查詢與輔導，並向本校計算機與網路中心(以下簡稱本中心)回報疑似侵權者相關資料。疑似侵權者必須視是否侵權之情況分別填寫「臺北市立大學違反智慧財產權不再犯切結書」或「臺北市立大學違反智慧財產權宣稱原創之切結書」並送至本中心俾利管理。

十四、　教職員工被檢舉疑似侵權行為，並經查證屬實者，移請人事室或相關單位依法規懲處。

十五、　學生被檢舉疑似侵權行為，並經查證屬實者，移請學生事務處依校規懲處。

十六、　本要點經資訊推動委員會通過，陳請校長核定後實施。