教育體系遠距教學之資訊安全指引

一、 目的

近年因為疫情因素，遠距教學需求大增。為讓各級學校在遠距教學時對於所使用之軟體與設備能有資安措施保護，故訂定「教育體系遠距教學之資訊安全指引」，以作為各校實施遠距教學時考量網路安全因素與預防措施之參考原則。

二、 適用對象

教育部轄下各級機關學校。

三、 視訊教學處理原則

（一）使用安全軟體及工具進行視訊教學，應避免使用具有資安疑慮之視訊軟體。軟體相關資訊可參考教育部教育雲「線上教學便利包」之「工具與資源」https://learning.cloud.edu.tw/onlinelearning/support.html。

（二）視訊教學之課程僅開放予預定之參與者，對於開啟課程，需要密碼並使用等候室等功能以控制入場。為增加安全性，建議使用隨機生成之密碼，且不重複使用。

（三）為保障參與者之資訊安全，課程主持人應注意分享課程連結對象是否為參與者，並於課程開啟時應確認參與者之身分才能加入課程。

（四）為避免敏感資訊外洩，應確保視訊環境安全（例如:確認牆上之白板和其他物品已清除敏感或個人資訊）；如需開啟視訊鏡頭時，建議使用模糊背景選項(如有教學平臺或軟體具有此功能)。

(五) 如使用 Web 瀏覽器登錄教學平臺，應注意輸入網站之網址正確性，以及避免點擊不明來源之連結網址。

四、 線上資料傳遞與分享原則

（一）課程進行期間應確保螢幕共享、線上課程錄製及教材文件共享之內容，未涉及個人敏感資訊或個人隱私。

（二）分享檔案時建議使用加密方式，並使用另一個管道分享密碼(例如:另一個信箱或其它通訊軟體)。

五、 遠距參與者之資通安全責任

（一） 參與者應確認所使用資通訊設備之資通安全，建議連線之資通設備進行資訊安全檢測(例如:防毒軟體之掃描)。當安裝軟體工具至參與遠距教學之資通設備時，建議至官網下載軟體，勿安裝不明來源之軟體。

（二） 檢查網路連線環境之安全性，如使用無線網路請確認網路來源是否合宜，建議避免使用無使用者身份認證之無線網路環境。如使用家庭網路，建議修改網路設備之預設密碼並避免使用弱密碼，且僅與信任的人共享此資訊。

（三） 使用資通設備或系統建議保持最新軟體與韌體版本。

（四） 仔細查看為課程發送之課程邀請，是否來自課程主持人。

六、 各校或其主管機關得參考本指引，訂定各校相關作業流程規定。