

台南市光華高級中學教師參加校外各項研習會心得報告

報告人：陳鈺淳

會議名稱	114年度教育部主管高級中等學校及國立特殊教育學校資通安全教育訓練	主辦單位	教育部國民及學前教育署		
日期	114.11.24	承辦單位	國教署特殊育網路中心	地點	集思新烏日會議中心(巴本廳 303 會議室)

壹、研習目的

- (1) 建立教育部、其所主管之高級中等學校及國立特殊教育學校的資通安全認知，提升學校資通安全水準。
- (2) 增進教育部所屬高級中等學校及國立特殊教育學校相關人員之資通安全教育課程知能，瞭解資通安全議題，並能於工作及生活中正確使用資訊設備與有效保護個人資料。
- (3) 配合《資通安全管理法》規定辦理，確保一般使用者及主管每年接受 3 小時以上資通安全通識教育訓練之要求。

貳、研習議題及內容

全球資通安全威脅趨勢分析與案例分享 博創資訊科技股份有限公司 蘇志哲輔導顧問師

參、感想：

在本次有關資通安全威脅趨勢的研習中，我重新檢視了自己在特教行政工作中處理資料的方式，也更清楚明白資安風險其實每天都在我們身邊。特教行政接觸的學生資料非常敏感，不僅包含身心障礙類別、評估報告，也牽涉到家庭狀況、醫療證明等，一旦外洩，對學生與家長的影響遠比一般資料更嚴重。因此，資安的落實不只是程序，而是責任。

研習中提到的六大威脅，首先是個人資料與憑證外洩的風險，過去常以為只要密碼設定複雜就沒問題，但實際上，一旦憑證遭盜用，再好的系統也守不住。這提醒我，多因素驗證、不要共用帳號及三到六個月定期更新密碼都是必須落實的基本動作。

此外，學校大量使用雲端服務，包括共享資料夾、表單調查、補助提交等，看似便利，但若權限設定不嚴謹，就可能讓不相干的人看到學生資料，這部分讓我提醒自己，在建立或分享雲端檔案時一定要再次確認權限，避免因疏忽導致資料外洩。

社交工程的威脅也很重要，行政人員每天收到的信件、訊息很多，一封假冒家長或機關名義的信件若不慎點開，可能讓電腦被植入惡意程式，甚至影響整個處室的資料安全，這讓我更重視辨識陌生連結、可疑附件及假冒公文的重要性。

研習也談到系統弱點、供應鏈風險以及 AI 技術帶來的新型態攻擊，雖然這些看似離行政人員較遠，但其實息息相關。例如：延遲更新系統也可能讓漏洞被攻擊；使用外部服務或補助平台時，必須確認其安全性；甚至如今 AI 可以生成假訊息、假語音，更增加判斷上的困難。

整體來說，此次研習讓我更具備警覺，也提醒自己未來在處理學生資料、與家長聯繫、使用雲端服務時，都要保持謹慎。資安不是資訊組的工作，而是每位行政同仁都必須共同維護的責任。只有透過每個人的小心與落實，才能確保學生與家長的資料不受威脅。

科(程)主任：

輔導主任 吳佩珊

教務主任：

教務主任 陳怡仁

校長：

校長 陳綺雯