

臺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：顏嘉鴻

會議名稱	教育體系個人資料保護安全管理施行計畫 教育訓練	主辦單位	教育部
		承辦單位	國立中興大學
日期	2014/9/18 (四) 14:00-17:00 2014/11/4 (二) 14:00-17:00	地點	成功大學

一、研習目的：

為加強提升教育體系個資保護與管理之意識，使受訓者可擔任各級單位個資業務的負責人，並具備個資國際標準知識及稽核實務應用之能力同時扮演個資種子角色，為教育體系帶來個資管理新觀念，協助教育體系有效推行個資管理制度，用以確保教育體系下之學校落實個資管理制度的有效性。

二、研習內容：

➤ 個人資料管理文件宣導教育訓練

BS 10012 標準暨個人資料保護法文件控管要求、個人資料管理制度文件架構、個人資料文件生命週期、個資侵害事故之緊急應變

➤ 個人資料管理制度稽核暨委外管理教育訓練

個人資料安全稽核機制、教育體系作業查核重點、委外管理暨查核要項

三、心得感想：

這次的教育訓練，原有 5 場次，分別是：

- 個人資料管理制度暨盤點
- 個人資料隱私衝擊分析與風險評鑑
- 個人資料管理文件宣導教育訓練
- 個人資訊管理系統內部稽核規劃與管理教育訓練
- 個人資料管理制度稽核暨委外管理

因接到會辦公文時，有報名過期也有報名額滿，所以只有報到 2 場，致使課程難連貫；然總歸重點在於「經濟合作暨發展組織」(OECD) 所揭示之保護個人資料八大原則

- ✧ 限制蒐集原則 (Collection Limitation)：經本人同意，以合法、公正手段於適當場所蒐集。
- ✧ 資料內容原則 (Data Quality)：符合資料使用之目的，並確保資料之正確性、完整性和時效性。
- ✧ 目的明確化原則 (Purpose Specification)：進行蒐集的目的必須在蒐集的當時就闡述明確，爾後使用也必須受限於當初所訂目的，不得他用。
- ✧ 限制使用原則 (Use Limitation)：若非經資料本人之同意或經法令規定許可，個人資料不得揭露、販售或用於明訂於第三條明確目的以外的用途。
- ✧ 安全保護原則 (Security Safeguards)：資料必須採取合理安全保護措施，以免資料遭遺失、盜用、毀損、竄改或揭露的風險。
- ✧ 公開原則 (Openness)：對個人資料之開發、運用、政策等必須採取一般的公開政策。

◇ 個人參與原則 (Individual Participation) :

個人有權利：

- (a).向資料管理人確認是否保有自己資料，保有哪些相關資料；
- (b).資料管理人在合理時間內、以合理價格、可接受的態度及可理解的形式，向本人聯絡溝通協調其資料之保有與使用；
- (c).如果本人提出以上(a).(b).兩樣請求被資料管理人拒絕，儘可要求合理解釋，並有權質詢此拒絕；
- (d).有權質詢個人相關資料之外，若質詢不滿意可以要求刪除、校正、修改資料直到完整無誤為止。

◇ 責任義務原則 (Accountability) : 資料管理者必須確保落實公司政策與執行措施以遵守上述各項原則。

經審視本校目前狀況，發現校內公用網路硬碟的檔案資料內容較有疑慮，或許大家以為那只是校內能存取，校外無法連結，所以就常把那空間當作自己的檔案備份空間，或分享給他人後置之不理，故不難找到一些個人資料，如班級、座號、姓名、學號甚至身份證字號等，就如我每學期初的校園資訊安全報告中，最後一句話都是「資訊安全—人人有責」，任何一個人有心無心的作為，就有可能影響大家的個資安全。

而個人資料管理制度稽核，必須先建置個人資訊管理系統 (PIMS) 架構，訂定相關規範：管理要點・標準作業流程及書面表格；再建立專業職責：個人資料管理團隊・個人資料聯絡窗口；並訂定控管措施：層級化的安全控管措施・最小化的蒐集、處理及利用・評估個人資料風險・訂定個人資料安全事件及控管程序・定期教育訓練。

稽核常見問題，一般作業：

- ◆ 資料變更處理方式
- ◆ 資訊系統的個資分布、盤點狀況
- ◆ 所有系統的帳號權限 授權規定、然後還會當場調出帳號一個一個問 USER 是誰、帳號盤點
- ◆ 問資料庫內的個資是否掌握清楚？
- ◆ 問 EMAIL 管控作法，如果使用者把個資文件寄出 學校有什麼管理方式？
- ◆ 可攜式媒體管控作法
- ◆ 還有共用資料夾的管理
- ◆ 報表輸出權限
- ◆ 辦公室安全管理方式？
- ◆ 學校是否有個資教育訓練以及宣導？

說來從建立個人資料管理制度到稽核，實在不是一個人力可以負擔，還有很長遠的路要走！

科 (學程) 主任：

教務主任：

校長：

教務主任 張樹仁

光華高中 校長 張淑霞