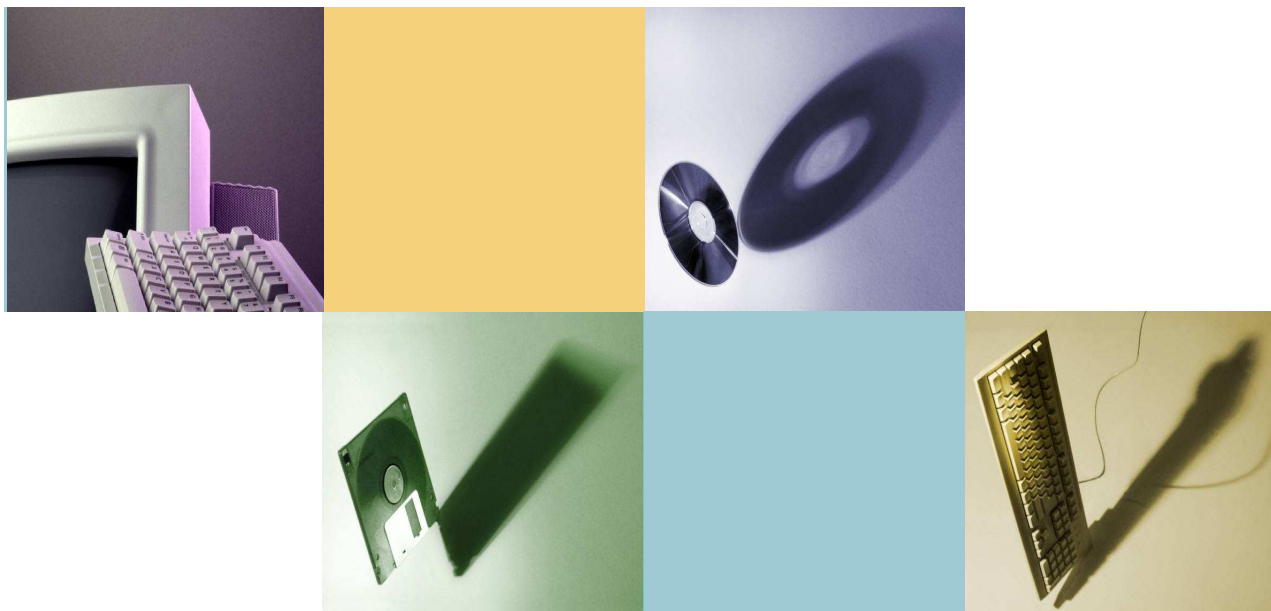


個人資料保護法宣導與學校因應措施

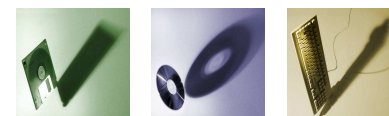


宜蘭大學資訊網路組 曾國旭

Monday, Mar 11 2013

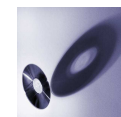
大綱

- 個人資料保護法現況說明
- 個人資料保護法介紹
- 因應個人資料保護法相關安全維護作法
- 案例討論
- 附錄
 - 個人資料保護法的特定目的及個人資料之類別
 - 個人資料蒐集同意書範例



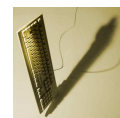
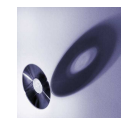
個資法施行現況

- 立法院於**99年4月27日**，將「**電腦處理個人資料保護法**」(84年8月11日公佈)修訂，並三讀通過為「**個人資料保護法**」
- 總統於**99年5月26日**公佈
- 法務部於**101年9月26日**公告**個人資料保護法施行細則**，除規範特種個資不得利用的**第6條**，以及間接蒐集個資1年內告知的**第54條**，暫緩實施，等待修法以外，其餘條文於**101年10月1日**正式實施



個資法修正重點

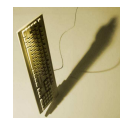
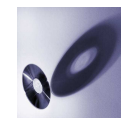
- 範圍與主體普遍化
 - 新版個資法將舊法**規範的對象**從原來公務機關與非公務機關(醫院、學校、電信、金融、證券、保險、大眾傳播、徵信等8大行業)**擴大至各行各業及個人**
 - **保護的範圍**由使用電腦或類似設備處理之個人資料**擴大為以任何方式(包含紙本)留存的資料**



個資法修正重點(續)

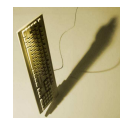
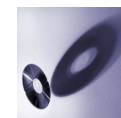
- 強化行為規範

- **特定目的**：個人資料之蒐集、處理或利用，不得逾越特定目的之必要範圍，並應與蒐集之目的具有正當合理之關聯
- **公開及專人維護**：應將所蒐集、處理及利用之個資類別、檔案名稱、保有之依據及目的，保有機關名稱及聯絡方式加以公開，並指定專人維護
- **告知及書面同意**：向當事人蒐集個人資料時，應明確告知當事人蒐集機關的名稱、目的、個資類別、個資利用的期間、地區、對象及方式、當事人得行使之權利及方式等，並取得當事人之書面同意



個資法修正重點(續)

- 加重罰則及團體訴訟
 - **民事賠償**：二千萬元→二億元
 - **刑事處罰**：五萬元→一百萬元，三年以下有期徒刑→五年以下有期徒刑
- 擴及海外及委外單位
 - 公務機關及非公務機關，在中華民國領域外對中華民國人民個人資料蒐集、處理或利用者，亦適用本法(第51條)
 - 受公務機關或非公務機關委託蒐集、處理或利用個人資料者，於本法適用範圍內，視同委託機關(第4條)



個資法第6條(暫緩)

- 有關醫療、基因、性生活、健康檢查及犯罪前科之個人資料，不得蒐集、處理或利用。但有下列情形之一者，不在此限：

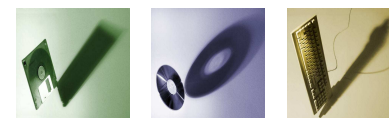
一、法律明文規定

二、公務機關執行法定職務或非公務機關履行法定義務所必要，且有適當安全維護措施

三、當事人自行公開或其他已合法公開之個人資料

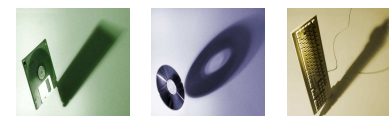
四、公務機關或學術研究機構基於醫療、衛生或犯罪預防之目的，為統計或學術研究而有必要，且經一定程序所為蒐集、處理或利用之個人資料

前項第四款個人資料蒐集、處理或利用之範圍、程序及其他應遵行事項之辦法，由中央目的事業主管機關會同法務部定之



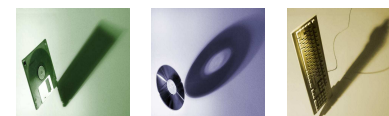
個資法第6條修法方向

- 增列得蒐集、處理或利用之例外情形
 - 為增進公共利益所必要
 - 取得當事人書面同意
- 公務機關或學術研究機構蒐集、處理或利用須去識別化
- 病歷改為特種個資



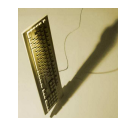
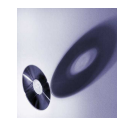
個資法第54條(暫緩)

- 本法修正**施行前非由當事人提供之個人資料**，依第九條規定應於處理或利用前向當事人為告知者，**應自本法修正施行之日起一年內完成告知**逾期未告知而處理或利用者，以違反第九條規定論處



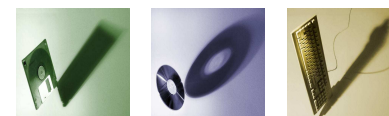
個資法第54條修法方向

- 刪除新法施行1年內完成告知的期限
- 改為處理或利用前告知當事人

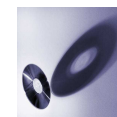


提醒您

- 不要因為擔心違反個資法，導致過度地「避免或迴避」必要資料之蒐集與使用
- 個人資料保護的重點在於「保持個人資料的正確性，並且告知當事人所蒐集資料的特定目的，以及安全處理與使用方式與範圍，並作好適當的刪除與銷毀工作」

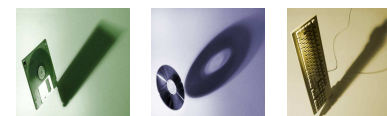


Q & A



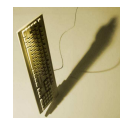
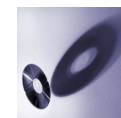
大綱

- 個人資料保護法現況說明
- 個人資料保護法介紹
- 因應個人資料保護法相關安全維護作法
- 案例討論
- 附錄
 - 個人資料保護法的特定目的及個人資料之類別
 - 個人資料蒐集同意書範例



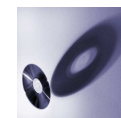
個人資料保護法

- 共六章，56條
 - 第一章：總則(第1條至第14條)
 - 第二章：公務機關對個人資料之蒐集、處理及利用(第15條至第18條)
 - 第三章：非公務機關對個人資料之蒐集、處理及利用(第19條至第27條)
 - 第四章：損害賠償及團體訴訟(第28條至第40條)
 - 第五章：罰則(第41條至第50條)
 - 第六章：附則(第51條至第56條)



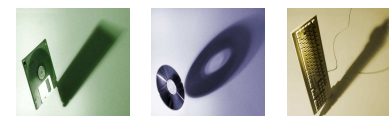
個人資料保護法(續)

- 立法目的與精神
 - 為**規範個人資料之蒐集、處理及利用**，**以避免人格權受侵害**，並促進個人資料之合理利用，特制定本法(第1條)
- 什麼是個人資料？
 - 指**自然人**之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料(第2條第1款)



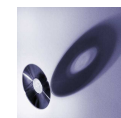
個人資料保護法(續)

- 學校屬公務機關或非公務機關？
 - 公務機關：指依法行使公權力之中央或地方機關或行政法人(第2條第7款)
 - 非公務機關：指前款以外之自然人、法人或其他團體(第2條第8款)
 - 依據教育部函，公立學校如係各級政府依法令設置實施教育之機構，而具有機關之地位，應屬個資法之公務機關。非由各級政府設置之私立學校，則屬本法之非公務機關



個人資料保護法(續)

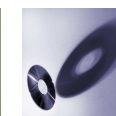
- 個人資料之蒐集、處理或利用，應尊重當事人之權益，依誠實及信用方法為之，不得逾越特定目的之必要範圍，並應與蒐集之目的具有正當合理之關聯(第5條)



個人資料保護法(續)

- 直接蒐集個人資料的告知義務--向當事人蒐集之前告知(第8條)

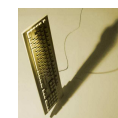
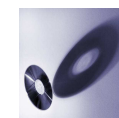
應告知事項	得免為告知之情況
1 機關名稱。	1 依法律規定得免告知
2 蒐集目的。	2 個人資料之蒐集係公務機關執行法定職務所必要
3 個人資料類別。	3 告知將妨害公務機關執行法定職務
4 利用期間、地區、對象及方式。	4 告知將妨害第三人之重大利益
5 當事人依第3條規定得行使之權利及方式： (1) 查詢或請求閱覽。 (2) 請求製給複製本。 (3) 請求補充或更正。 (4) 請求停止蒐集、處理或利用。 (5) 請求刪除。 上述權利，不得預先拋棄或以特約限制。	5 當事人明知應告知之內容
6 如當事人得自由選擇提供個人資料，不提供將對其權益之影響。	



個人資料保護法(續)

- 間接蒐集個人資料的告知義務--處理或利用當事人的個資之前告知(第9條)

應告知事項	得免為告知之情況
1 機關名稱。	1 依法律規定得免告知。
2 蒐集目的。	2 個人資料之蒐集係公務機關執行法定職務所必要。
3 個人資料類別。	3 告知將妨害公務機關執行法定職務。
4 利用期間、地區、對象及方式。	4 告知將妨害第三人之重大利益。
5 當事人依第3條規定得行使之權利及方式： (1) 查詢或請求閱覽。 (2) 請求製給複製本。 (3) 請求補充或更正。 (4) 請求停止蒐集、處理或利用。 (5) 請求刪除。 上述權利，不得預先拋棄或以特約限制。	5 當事人明知應告知之內容。
6 個人資料來源。	6 當事人自行公開或其他已合法公開之個人資料
	7 不能向當事人或其法定代理人為告知。
	8 基於公共利益為統計或學術研究之目的而有必要，且該資料須經提供者處理後或蒐集者依其揭露方式，無從識別特定當事人者為限。
	9 大眾傳播業者基於新聞報導之公益目的而蒐集個人資料。



個人資料保護法(續)

- 非公務機關對**特定目的內個人資料之蒐集、處理** (第19條)

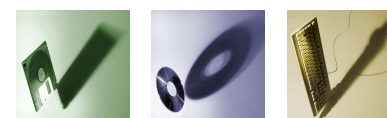
- 非公務機關對個人資料之蒐集或處理，除第六條第一項所規定資料外，應有特定目的，並符合下列情形之一者：

- 一、法律明文規定

- 二、與當事人有契約或類似契約之關係

- 三、當事人自行公開或其他已合法公開之個人資料

- 四、學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或蒐集者依其揭露方式無從識別特定之當事人



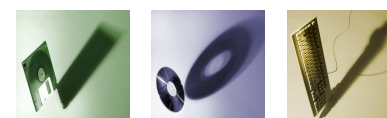
個人資料保護法(續)

五、經當事人書面同意

六、與公共利益有關

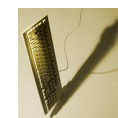
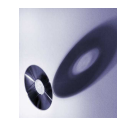
七、個人資料取自於一般可得之來源。但當事人對該資料之禁止處理或利用，顯有更值得保護之重大利益者，不在此限

蒐集或處理者知悉或經當事人通知依前項第七款但書規定禁止對該資料之處理或利用時，應主動或依當事人之請求，刪除、停止處理或利用該個人資料



個人資料保護法(續)

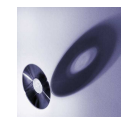
- 非公務機關對**特定目的外個人資料之利用**(第20條)
 - 非公務機關對個人資料之利用，除第六條第一項所規定資料外，應於執行法定職務必要範圍內為之，並與蒐集之特定目的相符。但有下列情形之一者，得為特定目的外之利用：
 - 一、法律明文規定
 - 二、為增進公共利益
 - 三、為免除當事人之生命、身體、自由或財產上之危險
 - 四、為防止他人權益之重大危害
 - 五、公務機關或學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或蒐集者依其揭露方式無從識別特定之當事人
 - 六、經當事人書面同意



個人資料保護法(續)

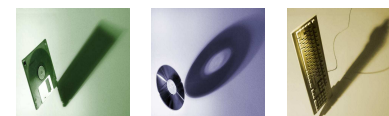
非公務機關依前項規定利用個人資料行銷者，當事人表示拒絕接受行銷時，應即停止利用其個人資料行銷

非公務機關於首次行銷時，應提供當事人表示拒絕接受行銷之方式，並支付所需費用。



個人資料保護法(續)

- 個人資料之安全保護相關規定
 - 非公務機關保有個人資料檔案者，**應採行適當之安全措施**，防止個人資料被竊取、竄改、毀損、滅失或洩漏
 - 中央目的事業主管機關得指定非公務機關訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法
 - 前項計畫及處理方法之標準等相關事項之辦法，由中央目的事業主管機關定之(第27條)

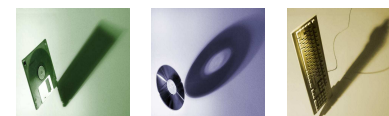


個人資料保護法(續)

- 損害賠償

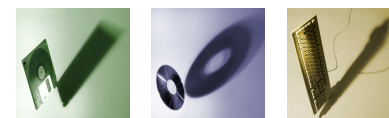
- 非公務機關違反個資法規定，致個人資料遭不法蒐集、處理、利用或其他當事人權利者，負損害賠償責任。但能證明其無故意或過失者，不在此限

被害人不易或不能證明其實際損害額時，法院得依侵害情節，以每人每一事件新台幣五百元以上二萬元以下計算。如同一原因事實造成多數當事人權利受侵害事件，賠償金額最高以新台幣二億元為限。但若該原因事實所涉利益超過新台幣二億元者，以該所涉利益為限(第28、29條)



個人資料保護法(續)

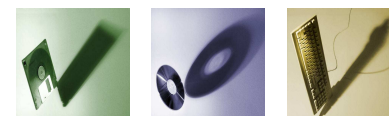
- 損害賠償請求權，自請求權人知有損害及賠償義務人時起，因二年間不行使而消滅；自損害發生時起，逾五年者，亦同(第30條)
- 損害賠償，除依本法規定外，公務機關適用國家賠償法之規定，非公務機關適用民法之規定(第31條)



個人資料保護法(續)

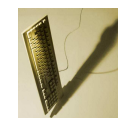
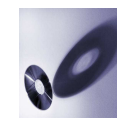
- 罰則

- 非公務機關違反個資法相關規定，足生損害於他人者，處二年以下有期徒刑、拘役或科或併科新台幣二十萬元以下罰金。意圖營利犯前項之罪者，處五年以下有期徒刑、拘役或科或併科新台幣一百萬元以下罰金(第41條)
- 妨害個人資料檔案之正確而足生損害於他人者，處五年以下有期徒刑、拘役或科或併科新台幣一百萬元以下罰金(第42條)



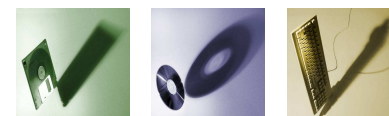
個人資料保護法(續)

- 非公務機關有下列情事之一者，由中央目的事業主管機關或直轄市、縣（市）政府處新臺幣五萬元以上五十萬元以下罰鍰，並令限期改正，屆期未改正者，按次處罰之：
 - 一、違反第六條第一項規定
 - 二、違反第十九條規定
 - 三、違反第二十條第一項規定
 - 四、違反中央目的事業主管機關依第二十一條規定限制國際傳輸之命令或處分(第47條)



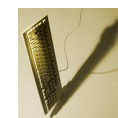
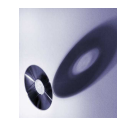
個人資料保護法(續)

- 一、非公務機關有下列情事之一者，由中央目的事業主管機關或直轄市、縣（市）政府限期改正，屆期未改正者，按次處新臺幣二萬元以上二十萬元以下罰鍰：
 - 一、違反第八條或第九條規定
 - 二、違反第十條、第十一條、第十二條或第十三條規定
 - 三、違反第二十條第二項或第三項規定
 - 四、違反第二十七條第一項或未依第二項訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法（第48條）

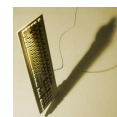
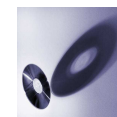


個人資料保護法(續)

- 非公務機關無正當理由違反第二十二條第四項規定者，由中央目的事業主管機關或直轄市、縣（市）政府處新臺幣二萬元以上二十萬元以下罰鍰（第49條）
- 非公務機關之代表人、管理人或其他有代表權人，因該非公務機關依前三條規定受罰鍰處罰時，除能證明已盡防止義務者外，應並受同一額度罰鍰之處罰（第50條）

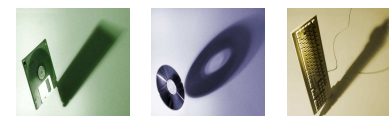


Q & A



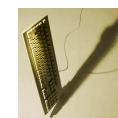
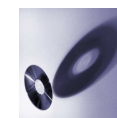
大綱

- 個人資料保護法現況說明
- 個人資料保護法介紹
- 因應個人資料保護法相關安全維護作法
- 案例討論
- 附錄
 - 個人資料保護法的特定目的及個人資料之類別
 - 個人資料蒐集同意書範例



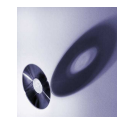
必要安全措施（施行細則第12條）

- 公務機關或非公務機關，**為防止個人資料被竊取、竄改、毀損、滅失或洩漏，採取技術上及組織上之措施。包括下列事項：**
 - 一、配置管理之人員及相當資源。
 - 二、界定個人資料之範圍。
 - 三、個人資料之風險評估及管理機制。
 - 四、事故之預防、通報及應變機制。
 - 五、個人資料蒐集、處理及利用之內部管理程序。
 - 六、資料安全管理及人員管理。
 - 七、認知宣導及教育訓練。
 - 八、設備安全管理。
 - 九、資料安全稽核機制。
 - 十、使用紀錄、軌跡資料及證據保存。
 - 十一、個人資料安全維護之整體持續改善。



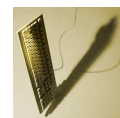
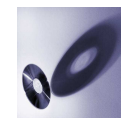
學校的因應措施

- 成立**個資保護專責組織**
 - 規劃、訂定、執行與修訂安全維護計畫相關程序
 - 應包括個人資料管理代表與內稽人員
- 訂定**個資保護政策**，至少應包括下列事項
 - 遵守我國個人資料保護相關之法令規定
 - 以合理安全之方式，於特定目的範圍內，蒐集、處理及利用個人資料
 - 以可期待之合理安全水準技術，保護其所蒐集、處理及利用個人資料
 - 設置聯絡窗口，供當事人行使關於個人資料之權利或提出相關之申訴與諮詢
 - 處理個人資料被竊取、竄改、毀損、滅失或洩漏等事故
 - 如有委託蒐集、處理及利用個人資料，將妥善監督受託單位
 - 持續維運本政策，以確保個人資料的安全



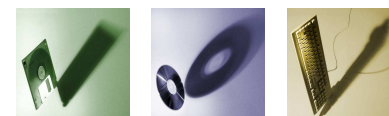
學校的因應措施(續)

- **清查組織內所有個資**，並加以公告
 - 依據個人資料保護相關法令，清查所保有之個人資料，界定其範圍並建立清冊，並定期確認是否有所變動
- 根據所界定之個人資料，及其相關業務流程，分析可能產生之風險，並根據風險之高低，訂定不同層級之管控措施，且確認受管控之風險在可接受範圍內
- 為因應所保有之個人資料被竊取、竄改、毀損、滅失或洩漏等事故，應訂定事故通報管理程序



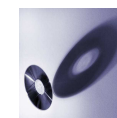
學校的因應措施(續)

- 進行必要的資訊安全與個資教育訓練及安全管理措施，包含人員管理、資料安全管理及設備安全管理
- 為確保個資保護之有效性，應定期檢查是否落實執行，並建立下列程序
 - 發生未落實執行之情形時，協助改善之程序
 - 有變更之需要時，其變更之程序

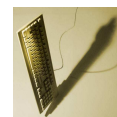
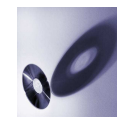


學校的因應措施(續)

- 各項程序執行時，至少應保存下列紀錄
 - 因應事故發生所採取行為之紀錄
 - 確認受託人執行委託人要求事項之紀錄
 - 提供當事人行使權利之紀錄
 - 確認資料正確性及更正之紀錄
 - 權限新增、變動及刪除之紀錄
 - 違反權限行為之紀錄
 - 備份及還原測試之紀錄
 - 個人資料交付、傳輸、刪除、廢棄之紀錄
 - 存取個人資料系統之紀錄
 - 教育訓練之紀錄
 - 稽核及改善程序執行之紀錄

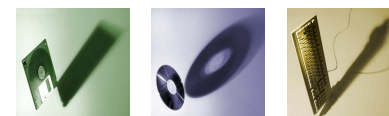


Q & A



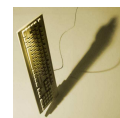
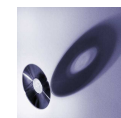
大綱

- 個人資料保護法現況說明
- 個人資料保護法介紹
- 因應個人資料保護法相關安全維護作法
- 案例討論
- 附錄
 - 個人資料保護法的特定目的及個人資料之類別
 - 個人資料蒐集同意書範例



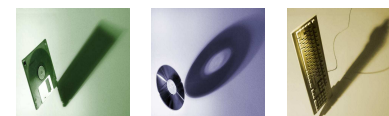
案例討論

- 學生入學時，是否需讓學生知道學校可能利用其資料的狀況，並在新生訓練或註冊時，取得同意的「授權」？
 - 除非學校使用個人資料有可能超過教育行政之特定目的，不然是不需要學生額外授權。不過因為新法增加了「告知」義務，在學生入學時就要立刻履行告知義務。如果學校超過特定目的之利用，就應該及早告知學生，並取得「書面同意」



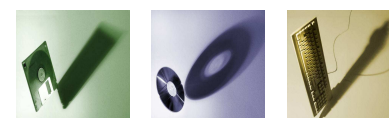
案例討論(續)

- 學校在公告欄上公告獎懲名單（學生姓名、學號）有違反個資嗎？
 - 有關獎懲之公告，符合學校辦理教育行政之目的，並不違反個資法



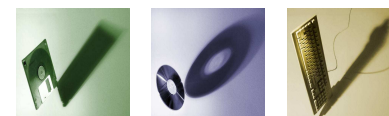
案例討論(續)

- 學校可否提供家長查詢學生考試成績、個人缺曠、操行等資料？
 - 應區分學生為成年或未成年，成年學生的家長應有學生授權，否則無法查詢。未成年的家長是學生的法定代理人，可以查詢



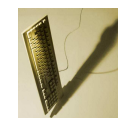
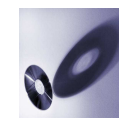
案例討論(續)

- 學校目前的**畢業學生資料**，**如何使用**才是屬於合法使用範圍？
 - 學校**使用校友的資料**還是必須符合「**教育行政**」的特定目的，如果**超過這個目的**還是不能使用，**需要在畢業前取得學生授權**



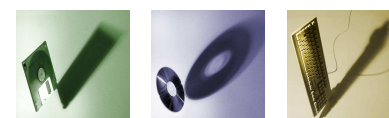
結論

- 學生獎懲資料符合學校辦理教育行政之目的，公佈不違反個資法
- 每位教職員均應檢視自己放在網路上與學校有關業務的資料是否違反個人資料保護法蒐集、處理與利用之規範，若有請立即自行刪除，若無法自行刪除者，應通知學校資訊單位協助處理。如班級網頁中是否有學生的姓名、生日、照片（特別是照片旁有標註可供辨識學生身份的資料）等之資訊揭露
- 學校辦理研習課程等活動之簽到單，須妥善保管並定期或不定期時予以銷毀



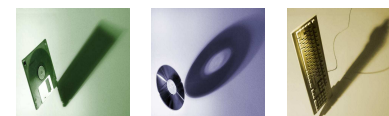
結論(續)

- 學校網站上若出現學生班級、座號、全名、健康狀況、家庭狀況、聯絡方式、輔導紀錄、申請補助進度等資訊，須進一步檢視公開之必要性，或進行必要處理後再公開
- 教師索取學生個資需由業務承辦人判別是否合乎該師之職權，方可給予個資。可透過建立調閱紀錄表並由權責主管簽核等方式進行管控與追蹤

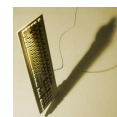
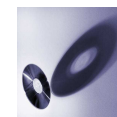


結論(續)

- 向尚未成年之學生取用個資，需取得當事人及監護人同意方可行之
- 保留重要或敏感個資之處所需有門禁等實體安全控管機制。存放個人資料的電腦也需安全控管機制，例如密碼
- 包含個人資料的電腦在報廢前，需將硬碟資料進行完全移除（不只是清空電腦資源回收筒）

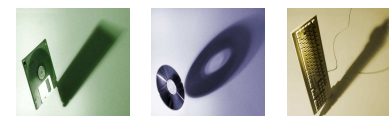


Q & A



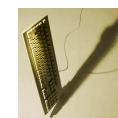
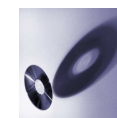
大綱

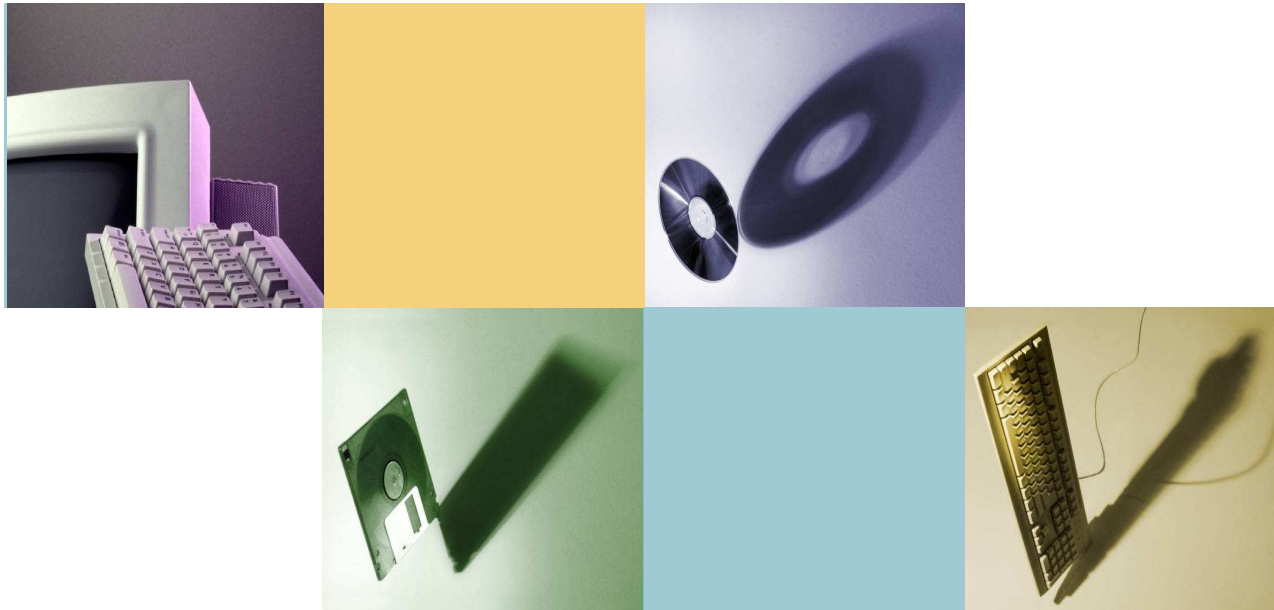
- 個人資料保護法現況說明
- 個人資料保護法介紹
- 因應個人資料保護法相關安全維護作法
- 案例討論
- 附錄
 - 個人資料保護法的特定目的及個人資料之類別
 - 個人資料蒐集同意書範例



附錄

- 個人資料保護法的特定目的及個人資料之類別
 - **101年10月1日公布施行**，共182項特定目的
- 個人資料蒐集同意書範例





THANKS !