# 教育部「提升校園資訊安全服務計畫(101年至102年)」
# 區縣網顧問服務-成大區網
# 教育機構如何因應個資法

**102 年 9 月 12 日(四)**

<下午場>

資料準備：NII產業發展協進會

吳昭儀資深經理

# 大綱

一、個資法現況說明

二、因應個資法相關安全維護作法

三、教育機構個人資料保護工作事項及檢核表重點說明

四、常見的稽核發現

五、問題與討論

# 一、個資法現況說明

# 個人資料，無所不在

帳單地址
電子郵件信箱
帳戶資料

電信/網路
服務提供業者

開立帳戶資料
保單資料
貸款徵信資料
會員資料
周年慶抽獎券


銀行/證券/保險公司
百貨公司/大賣場

信用卡資料
客戶資料
宅配地址
教育程度

線上購物/網拍
社群網站

身分證號碼
結婚登記
報稅資料
駕照申請/換發

監理/戶政
財稅等政府單位

健檢報告
病歷資料
診斷書

醫院/診所
健康檢查中心

學籍資料
人事資料
註冊/報名資料
家長會聯絡


學校/補習班
社區活動中心

# 個資法從101年10月1日開始正式實施

- 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，這兩條暫緩實施，等待修法以外，其餘條文都正式實施。
- 現在不分產業，公家機關、私人企業、學校機構，甚至是每一個個人，也不管儲存在紙本或是電子形式的個人資料，都需受到個資法的規範。
- 法務部在101年9月26日公告個資法施行細則，並同步於101年10月1日實施，沒有緩衝期。

# 個資法過頭？學校榮譽榜變ＯＯ榜！

## 個資法過頭？學校榮譽榜變○○榜！

2012-11-09


中天新聞》「個資法」上路後人名打圈的怪象，從法院地檢署蔓延到校園！南投縣府發文各校，要求學校必須榮譽榜學生的名字中間要打圈，學生們聽到消息都覺得很失落，好不容易得了獎，卻不能公開全名。

## 即時新聞》個資法施行 大學行政傷腦筋

Breaking news

【中央社／台北6日電】 2012.11.06 04:50 pm

個人資料保護法今年10月上路，對大學行政產生不小衝擊，包括榜單、獎懲公告等都要改變作法，使用學生個資時更要小心再三。

教育部今天舉辦「大專校院外國學生輔導人員研習會」，議題集中在個資法的衝擊，邀請智慧財產法院法官林洲富、成功大學法律系教授王毓正分別於台北、台南演講，幫來自97所大專、108位行政人員上課。

教育部國際文化教育事業處承辦人員表示，個資法上路後，學校一些習以為常的作法，都必須改變。例如以前公告錄取榜單時，往往會連同姓名、國籍一併公布，現在恐怕就不適當，建議姓名不能全登，或乾脆只用流水號。

獎懲公告時，也要注意學生的隱私，教育部建議秉持「隱惡揚善」的原則，記過時不要公告個資，且本國生、外籍生的處理方式要一致，避免引起爭議。

國際文教處承辦人員說，另一個行政人員易犯的錯誤是通訊錄，以前學生社團、同鄉會向學校要名單，大都會給予。個資法上路後，就只能幫忙傳遞資訊，讓有興趣的學生自行參加。

# 學校機構屬公務或非公務機關？

- 公務與非公務機關之定義：
  - §2&7 公務機關
    - 依法行使公權力之中央或地方機關或行政法人
  - §2&8 非公務機關
    - 指前款以外之自然人、法人或其他團體

- 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。

# 私立學校於實施教育之範圍內，為個人資料保護法所稱公務機關或非公務機關？

- 個資法所定之公務機關，係指依法行使公權力之中央或地方機關或行政法人。因此，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。至於私立學校，雖然由法律在特定範圍內授與行使公權力，惟私立學校在適用個資法時，為避免其割裂適用個資法，並使其有一致性規範，私立學校應屬個資法所稱之非公務機關。
- (摘自「法務部102年6月24日法律字第10200571790號書函」-本函全文可於本部全球資訊網點選「法務部主管法規查詢系統」查詢）

# 如何降低個資法之風險？

## 公務機關（公立學校）

- §18 公務機關保有個人資料檔案者，應指定專人辦理安全維護事項，防止個人資料被竊取、竄改、毀損、滅失或洩漏。
- §28 公務機關違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權力者，負損害賠償責任。但損害因天災、事變或其他不可抗力所致者，不在此限。
- §31 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。
- 施行細則第十二條第二項說明「落實安全維護措施」有十一項。

# 如何降低個資法之風險？

## 非公務機關（私立學校）

- §27-1 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。
- §29 非公務機關違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權力者，負損害賠償責任。但能證明其無故意或過失者，不在此限。
- §50 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。
- §31 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。
- 施行細則第十二條第二項說明「落實安全維護措施」有十一項。

# 施行細則第十二條第二項的來源

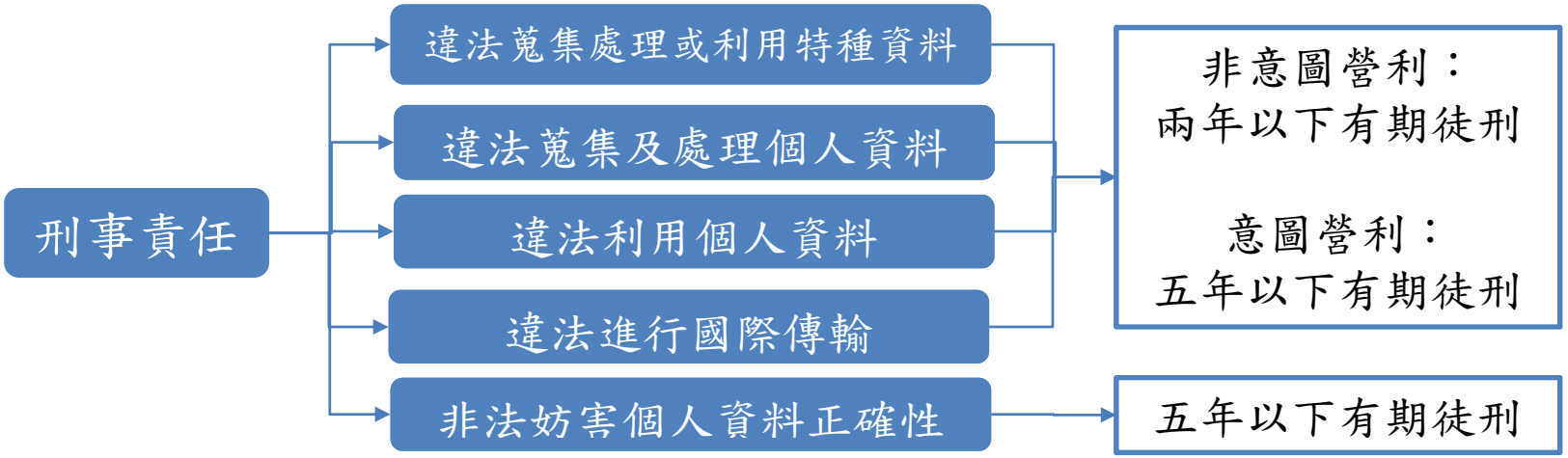
- 法務部施行細則第十二條說明了「適當安全防護措施」，基本上就是英國BS 10012的做法。為了避免違反個資法，透過機制來建立防護措施，不是為驗證而已。（過去ISO 27001只集中於資訊部門）
- 個資法第2條第2款：「個人資料檔案：指依系統建立而得以自動化機器或其他非自動化方式檢索、整理之個人資料之集合。」：個資盤點不能只在資訊部門（資訊部門可以協助確認），因為個資法客體含「各種形式含個資的檔案（如紙張等）」
- 盤點個資時應注意個資生命週期（蒐集、處理、利用、傳輸、銷毀）的關聯性：各階段的合法性，必須回到蒐集時的特定目的與範圍。「蒐集合法」，不表示其他階段合法

資料違法外洩時，一定要和當事人說嗎？

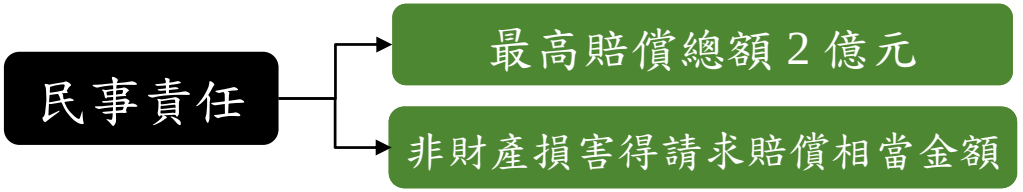
- 公務機關或非公務機關違反本法規定，致個人資料被竊取、洩漏、竄改或 其他侵害者，應查明後以適當方式通知當事人。(§12)

若違反個資法，只要罰錢就可以了嗎？

# 公務機關之法律責任

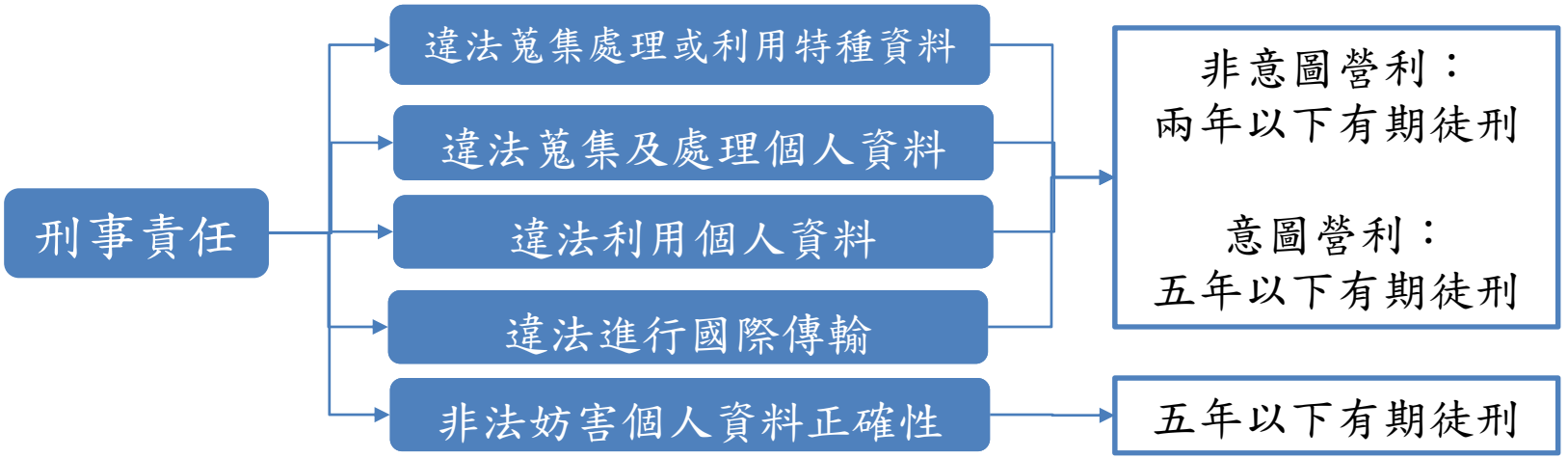



公務員假借職務上之權力、機會或方法，犯本章之罪者，加重其刑至二分之一。(§44)




公務機關違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。但損害因天災、事變或其他不可抗力所致者，不在此限。被害人雖非財產上之損害，亦得請求賠償相當之金額；其名譽被侵害者，並得請求為回復名譽之適當處份。依前二項情形，如被害人不易或不能證明其實際損害額時，得請求法院依侵害情節，以每人每一事件新臺幣五百元以上二萬元以下計算。(§28)

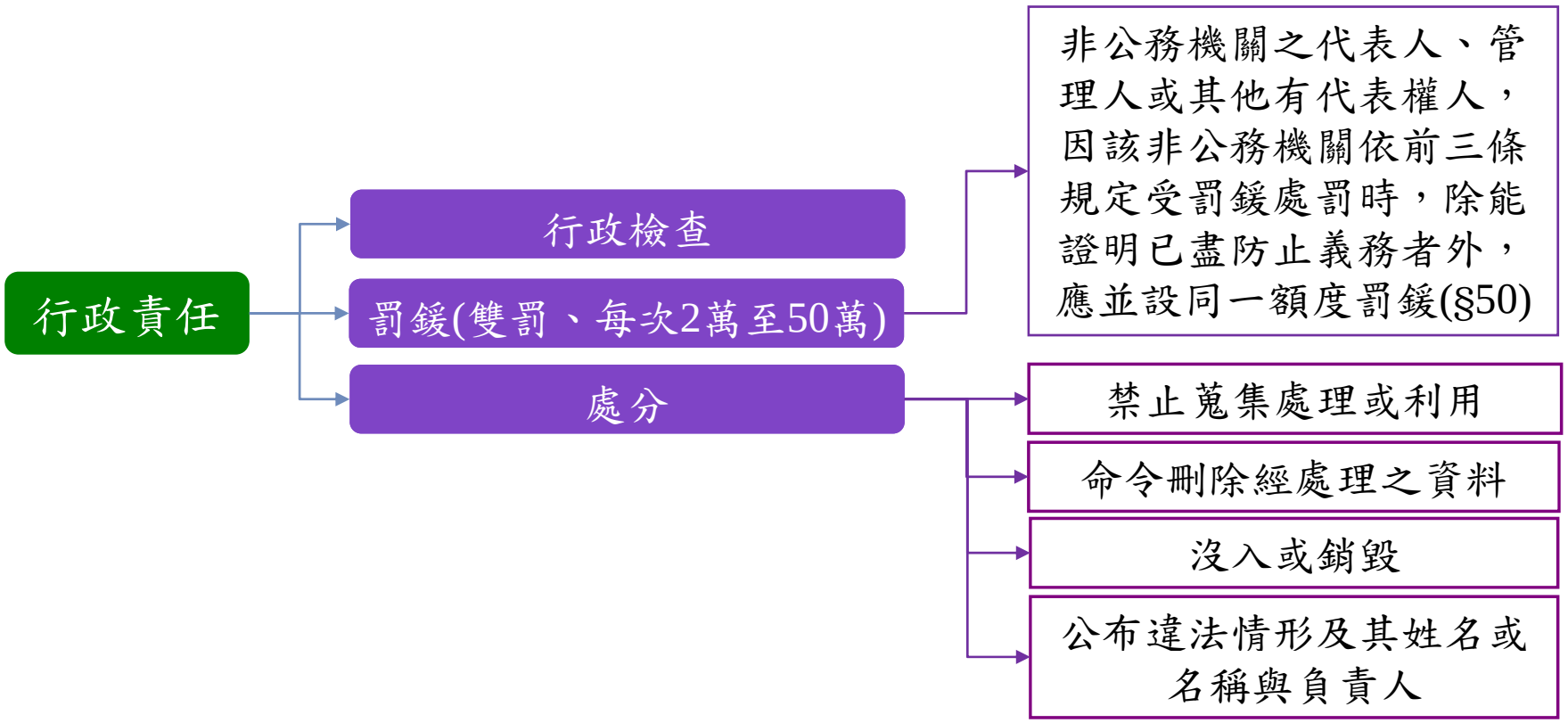
# 非公務機關之法律責任





非公務機關違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵 害當事人權利者，負損害賠償責任。但能證明其無故意或過失者，不在此限。 (§29)

# 非公務機關之法律責任(續)



# 保護個人資料的其他律法

- **民法18、195（侵害人格權）**
  - 財產上的損害賠償
  - 精神慰撫金
  - 回復名譽的適當處分
- **刑法315、315-1、318-1（妨害秘密罪）**
  - 有期徒刑 → 三年以下
  - 罰金 → 三萬元以下
- **通訊保障及監察法19、24、25（秘密通信自由）**
  - 損害賠償
  - 有期徒刑 → 五年以下

# 個人資料的生命週期

# 個資法 V.S 個人資料管理制度

1. 個資法與“PIMS”：協助建立機制來面對個資法，而不只是建立制度通過驗證。（過去ISO 27001只集中於資訊部門）
2. 個資法第2條第2款：「個人資料檔案：指依系統建立而得以自動化機器或其他非自動化方式檢索、整理之個人資料之集合。」：個資盤點不能過度集中在資訊部門（但資訊部門彙集的資訊可以協助確認），因為個資法客體包含「各種形式含有個資的檔案（如紙張等）」
3. 盤點個資時應注意個資生命週期（蒐集、處理、利用、傳輸、銷毀）的關聯性：各階段的合法性，必須回到蒐集時的特定目的與範圍。若誤以為「蒐集合法」，其他階段就合法，恐怕會在個資盤點時造成疏忽，而後續制度的建立與法律的連結將產生「法律疏漏」之處

# 二、因應個資法相關安全維護作法

# 必要安全措施包括(細則§12)

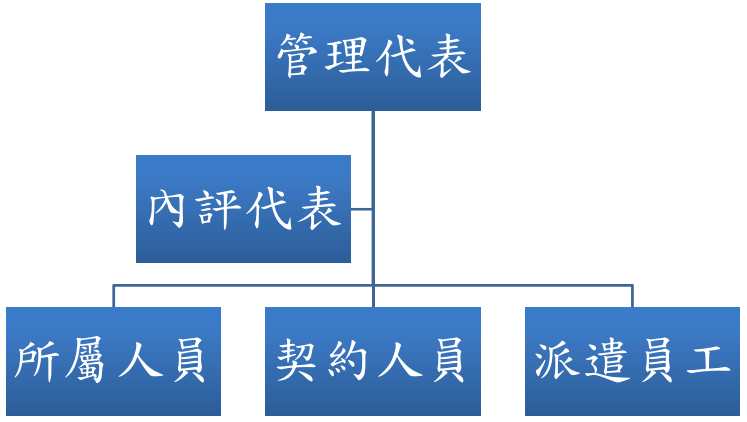
- 配置管理之人員及相當資源
- 界定個人資料之範圍
- 個人資料之風險評估及管理機制
- 事故之預防、通報及應變機制
- 個人資料蒐集、處理及利用之內部管理程序
- 資料安全管理及人員管理
- 認知宣導及教育訓練
- 設備安全管理
- 資料安全稽核機制
- 使用紀錄、軌跡資料及證據保存

個人資料安全維護之整體持續改善

# 管理組織

1. 個人資料管理代表：負責人或負責人直接授權，擔任督導本計畫之規劃、訂定、執行、修訂及相關決策之人員。
2. 個人資料內評代表：由負責人授權，負責評核本計畫之執行成效之人員。
3. 所屬人員：執行業務之過程必須接觸個人資料之人員，包括公司之定期或不定期契約人員及派遣員工。

**配置管理之人員及相當資源**



# 管理組織

- 為訂定並執行本計畫，應建立個人資料檔案安全維護管理組織，並配置相當資源。
- 前項管理組織之任務如下：
  1. 規劃、訂定、執行與修訂安全維護計畫相關程序。
  2. 管理代表應定期向事業之負責人就前款事項提出書面報告。
  3. 管理組織至少應包括個人資料管理代表與個人資料內評代表。

配置管理之人員及相當資源

# 一般程序（1/4）（政策）

- 應依據組織與事業特性訂定個人資料保護管理政策，經負責人核可，並公開周知，使所屬人員均明確瞭解。
- 政策至少應包括下列事項：

界定個人資料之範圍

1. 將遵守我國個人資料保護相關之法令規定。
2. 將以合理安全之方式，於特定目的範圍內，蒐集、處理及利用個人資料。
3. 將以可期待之合理安全水準技術保護其所蒐集、處理、利用之個人資料檔案。
4. 將會設置聯絡窗口，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。
5. 將以處理個人資料被竊取、竄改、毀損、滅失或洩漏等事故。
6. 如有委託蒐集、處理及利用個人資料時，將妥善監督受託機關。
7. 將持續維運本計畫，以確保個人資料檔案之安全。

# 一般程序（2/4）

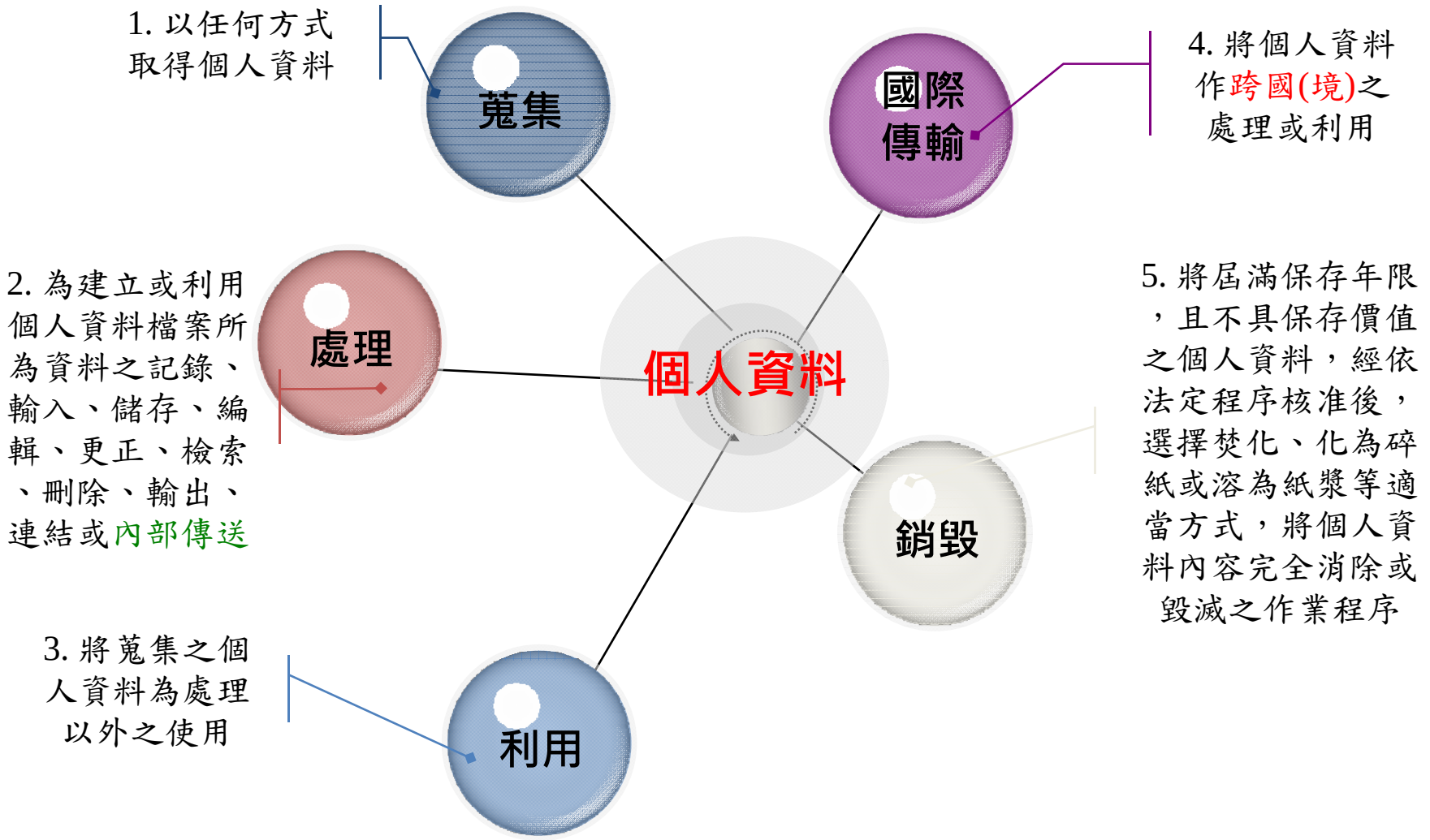
- 應依據個人資料保護相關法令，清查所保有之個人資料，界定其納入本計畫之範圍並建立清冊，且定期確認其是否有所變動。

| 項目編號 | 個人資料檔案名稱 | 保有依據 | 個人資料類別 | 保有單位 |
|---|---|---|---|---|
| | | | | |
| | | | | |

界定個人資料之範圍

個人資料之風險評估及管理機制

# 個人資料檔案盤點作業




**個人資料檔案盤點重點在於個資之生命週期**

# 一般程序（3/4）

- 應根據前條所界定之個人資料，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，應訂定下列程序：
  1. 採取適當之應變措施，以控制事故對當事人之損害擴大。
  2. 查明事故之狀況並適時通知當事人。
  3. 避免類似事故再次發生。

界定個人資料之範圍

個人資料之風險評估及管理機制

# 一般程序（4/4）

- 委託他人蒐集、處理或利用個人資料之全部或一部時，為對受託人為適當之監督，應建立下列程序：
  1. 確認所委託蒐集、處理或利用之個人資料之範圍、類別、特定目的及其期間。
  2. 確認受託人應採取必要安全措施。
  3. 有複委託者，確認其複委託之對象。
  4. 受託人或其受僱人違反個人資料保護法令或委託契約條款時，要求其向委託人通知相關事項。
  5. 與受託人約定委託人所保留指示之事項。
  6. 委託關係終止或解除時，要求受託人返還或銷毀因委託事項所交付之個人資料載體，及刪除因委託事項所儲存於受託人之個人資料。
  7. 確認受託人執行上述要求事項之狀況。

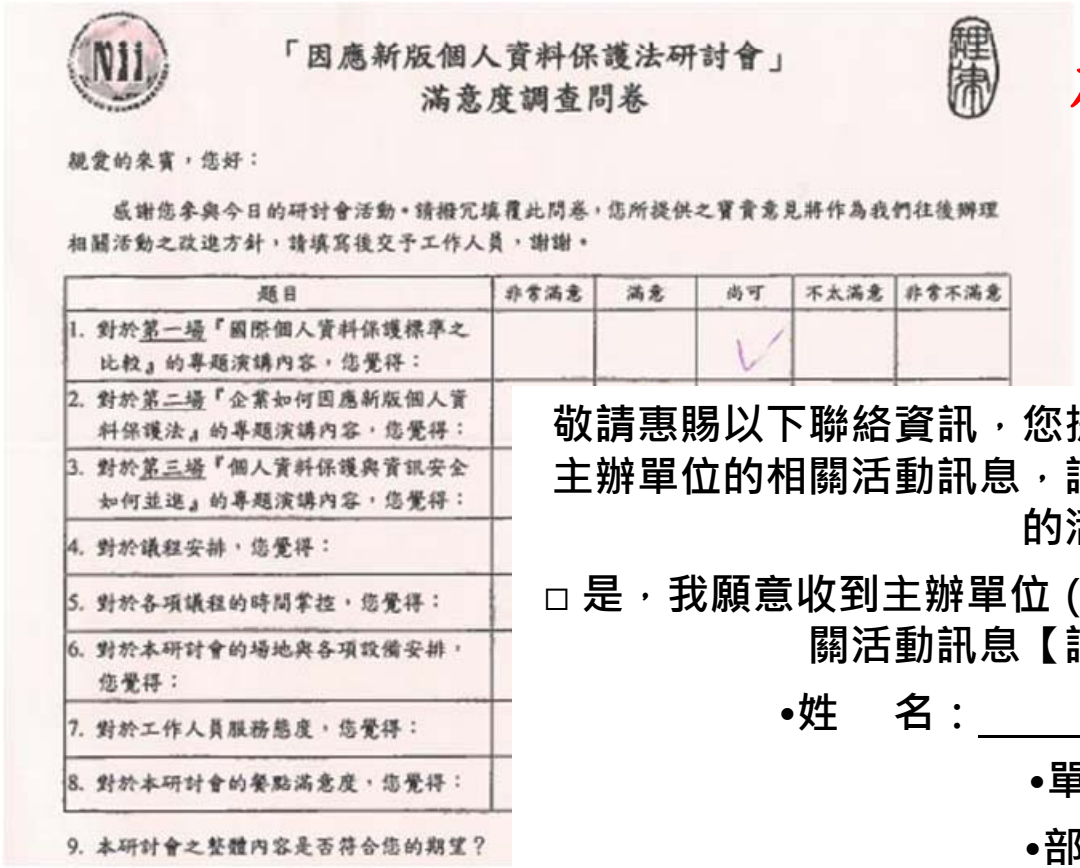
**個人資料蒐集、處理及利用之內部管理程序**

# 法令遵循程序（1/3）

- 為確保個人資料之蒐集符合個人資料保護相關法令要求，應建立下列程序：
  1. 確認蒐集個人資料之特定目的。
  2. 確認具備法令所要求之特定情形或其他要件。
- 為遵守本法第八條及第九條關於告知義務之規定，應建立下列程序：
  1. 確認是否得免告知。
  2. 依據資料蒐集之情況，採取適當之告知方式。
- 為確保個人資料之利用符合個人資料保護相關法令要求，應建立下列程序：
  1. 確保資料之利用符合特定目的。
  2. 確認是否得進行及如何進行特定目的外利用。
- 如欲新增或變更特定目的時，應依下列程序為之：
  1. 確認是否得新增或變更特定目的。
  2. 再次依本辦法第十三條、第十四條之程序為之。

**個人資料蒐集、處理及利用之內部管理程序**

# 簡單說，就是你可以這樣做…



「因應新版個人資料保護法研討會」
滿意度調查問卷

親愛的來賓，您好：

感謝您參與今日的研討會活動，請撥冗填覆此問卷，您所提供之寶貴意見將作為我們往後辦理相關活動之改進方針，請填寫後交予工作人員，謝謝。

| 題目 | 非常滿意 | 滿意 | 尚可 | 不太滿意 | 非常不滿意 |
|---|---|---|---|---|---|
| 1. 對於第一場『國際個人資料保護標準之比較』的專題演講內容，您覺得： | | | ✓ | | |
| 2. 對於第二場『企業如何因應新版個人資料保護法』的專題演講內容，您覺得： | | | | | |
| 3. 對於第三場『個人資料保護與資訊安全如何並進』的專題演講內容，您覺得： | | | | | |
| 4. 對於議程安排，您覺得： | | | | | |
| 5. 對於各項議程的時間掌控，您覺得： | | | | | |
| 6. 對於本研討會的場地與各項設備安排，您覺得： | | | | | |
| 7. 對於工作人員服務態度，您覺得： | | | | | |
| 8. 對於本研討會的餐點滿意度，您覺得： | | | | | |

9. 本研討會之整體內容是否符合您的期望？

## 研討會的會員資料

敬請惠賜以下聯絡資訊，您提供的訊息未來將用於發送本研討會主辦單位的相關活動訊息，請確認您未來是否願意接到前述單位的活動通知：

□ 是，我願意收到主辦單位（NII協進會與理律法律事務所）的相關活動訊息【請續填以下聯絡資訊】

- 姓　　名：_____ [簽名]
- 單位名稱 ：
- 部門/職稱 ：
- 電　　話：_____ 分機：
- E-MAIL：

□ 否，我不願意收到主辦單位的任何活動訊息。

# 同意書內容範例

- **5.1.2 本會蒐集個人資料時，應明確告知當事人以下事項：**
  - 公司名稱、聯繫方式。
  - 蒐集目的。
  - 個人資料的類別。
  - 個人資料利用期間、地區、對象及方式，應向當事人說明資料使用期間、保存期限、使用範圍及使用方式。
  - 當事人可以行使之權利及方式，例如當事人可請求查詢、閱覽、製給複製本、補充、更正、刪除、停止蒐集、處理或利用。
  - 應說明當事人可自行判斷是否提供個人資料，若為本會提供服務時所必需的資訊，因而造成無法提供該服務之情形時，應說明對其個人權益之影響。
  - 本會於網站上蒐集個人資料時，應說明採用之相關技術，如cookies等。
  - 本會蒐集之個人資料若使用於行銷目的，應明確告知當事人拒絕接受行銷之方式。

# 法令遵循程序（2/3）

- 於利用個人資料行銷時，應建立下列程序：
  1. 確保當事人表示拒絕接受後，立即停止利用其個人資料行銷。
  2. 於首次行銷時，提供當事人免費表示拒絕接受行銷之方式。
- 針對本法第六條之特種個人資料，應建立以下程序：
  1. 確認所蒐集、處理及利用之個人資料是否包含特種個人資料。
  2. 確保蒐集、處理及利用特種個人資料，符合相關法令之要求。
- 為國際傳輸個人資料時，應建立是否受中央目的事業主管機關限制之確認程序，如有限制，並應遵守之。
- 應定期確認其所保有個人資料之特定目的是否消失，或期限是否屆滿，若特定目的消失或期限屆滿時，應遵守本法第十一條第三項規定。

**個人資料蒐集、處理及利用之內部管理程序**

# 法令遵循程序（3/3）

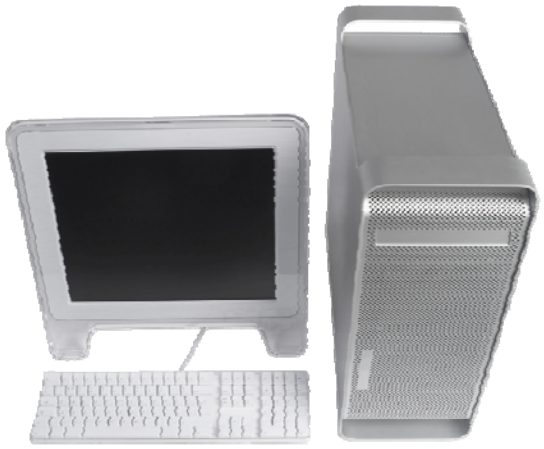
- 為確認其所保有之個人資料處於正確且最新之狀態，應建立下列程序：
  1. 確保資料於處理過程中，正確性不受影響。
  2. 當確認資料有錯誤時，應適時更正。
  3. 定期檢查資料為正確且最新。
  4. 因可歸責於非公務機關之事由，未為更正或補充之個人資料，應建立於更正或補充後，通知曾提供利用對象之程序。

個人資料蒐集、處理及利用之內部管理程序

- 為提供資料當事人行使個人資料保護法第三條所規定之權利，應建立下列程序：
  1. 提供當事人行使權利之方式。
  2. 確認當事人身分之方式。
  3. 確認是否有本法第十條及第十一條得拒絕當事人行使權利之情況。
  4. 適時回覆當事人請求。

# 安全管理措施（1/5）

- **應採取下列人員管理措施：**
  1. 確認蒐集、處理及利用個人資料之各相關業務流程之負責人員。
  2. 依據作業之必要，設定所屬人員不同之權限並控管之，以一定認證機制管理其權限，且定期確認權限內容設定之適當與必要性。
  3. 與所屬人員簽訂保密契約，契約內容至少包含所屬人員應負之保密義務與保密範圍，及違反保密義務之效果。
- **應採取下列物理環境管理措施**
  1. 依據作業內容之不同，實施必要之門禁管理。
  2. 妥善保管個人資料之儲存媒體。
  3. 針對不同作業環境，建置必要之防災設備。



資料安全管理及人員管理

# 安全管理措施（2/5）

- **應採取下列作業管理措施：**
  1. 訂定蒐集、處理及利用之作業注意事項。
  2. 運用電腦及相關設備處理個人資料時，應訂定使用可攜式儲存媒體之規範。
  3. 針對所保有之個人資料內容，確認是否有加密之必要，如有必要，應採取適當之加密機制。
  4. 傳輸個人資料時，因應不同之傳輸方式，確認是否有加密之必要，如有必要，應採取適當之加密機制，並確認資料收受者之正確性。
  5. 應依據所保有資料之重要性，評估個人資料是否有備份必要，如有必要應予備份。對於備份資料應確認是否有加密之必要，如有必要，採取適當之加密機制，儲存備份資料之媒體亦應以適當方式保管，且定期進行備份資料之還原測試，以確保備份之有效性。

設備安全管理

# 安全管理措施（3/5）

- 應採取下列作業管理措施：
  6. 儲存個人資料之媒體於廢棄或移轉與他人前，應確實刪除媒體中所儲存之資料，或以物理方式破壞之。
  7. 妥善保存認證機制及加密機制中所運用之密碼，如有交付他人之必要，亦應妥善為之。

設備安全管理

# 安全管理措施（4/5）

資料安全管理及人員管理

- **利用電腦或相關設備蒐集、處理或利用個人資料時，應採取下列技術管理措施：**
  1. 於電腦、相關設備或系統上設定認證機制，對有存取個人資料權限之人員進行識別與控管。
  2. 認證機制使用帳號及密碼之方式時，使其具備一定安全之複雜度並定期更換密碼。
  3. 於電腦、相關設備或系統上設定警示與相關反應機制，以對不正常之存取為適當之反應與處理。
  4. 對於存取個人資料之終端機進行身分認證，以識別並控管之。
  5. 個人資料存取權限之數量及範圍，於作業必要之限度內設定之，且原則上不得共用存取權限。
  6. 採用防火牆或路由器等設定，避免儲存個人資料之系統遭受無權限之存取。
  7. 欲使用能存取個人資料之應用程式時，確認使用者具備使用權限。

# 安全管理措施（5/5）

- **利用電腦或相關設備蒐集、處理或利用個人資料時，應採取下列技術管理措施：**

8.定期測試權限認證機制之有效性。

9.定期檢視個人資料之存取權限設定正當與否。

10.於處理個人資料之電腦系統中安裝防毒軟體，並定期更新病毒碼。

11.對於電腦作業系統及相關應用程式之漏洞，定期安裝修補之程式。

12.定期瞭解惡意程式之威脅，並確認安裝防毒軟體及修補程式後之電腦系統之穩定性。

13.具備存取權限之終端機不得安裝檔案分享軟體。

14.測試處理個人資料之資訊系統時，不使用真實之個人資料，如有使用真實之個人資料之情形時，明確規定其使用之程序。

15.處理個人資料之資訊系統如有變更時，確認其安全性並未降低。

16.定期檢查處理個人資料之資訊系統之使用狀況及個人資料存取之情形。

**設備安全管理**

# 計畫稽核及改善程序

- 為確保本計畫之有效性，應定期檢查本計畫是否落實執行。
- 為持續改善本計畫，應建立下列程序：
  1. 計畫發生未落實執行之情形時，協助改善之程序。
  2. 如計畫有變更之需要時，其變更之程序。

資料安全稽核機制

# 記錄機制

- 關於本計畫各項程序之執行，至少應保存下列紀錄：
  1. 因應事故發生所採取行為之紀錄。
  2. 確認受託人執行委託人要求事項之紀錄。
  3. 提供當事人行使權利之紀錄。
  4. 確認資料正確性及更正之紀錄。
  5. 權限新增、變動及刪除之紀錄。
  6. 違反權限行為之紀錄。
  7. 備份及還原測試之紀錄。
  8. 個人資料交付、傳輸之紀錄。
  9. 個人資料刪除、廢棄之紀錄。
  10. 存取個人資料系統之紀錄。
  11. 定期檢查處理個人資料之資訊系統之紀錄。
  12. 教育訓練之紀錄。
  13. 計畫稽核及改善程序執行之紀錄。

**必要之使用紀錄、軌跡資料及證據之保存**

# 三、教育機構個人資料保護工作事項及檢核表重點說明

# 本次稽核項目

| | |
|---|---|
| 1 | 成立管理織人員及相當資源 |
| 2 | 界定個人資料之範圍 |
| 3 | 個人資料之風險評估及管理機制 |
| 4 | 事故之預防、通報及應變機制 |
| 5 | 個人資料蒐集、處理及利用之內部管理程序 |
| 6 | 資料安全管理及人員管理 |
| 7 | 認知宣導及教育訓練 |
| 8 | 設備安全管理 |
| 9 | 資料安全稽核機制 |
| 10 | 使用紀錄、軌跡資料及證據保存 |
| 11 | 個人資料安全維護之整體持續改善 |

# 1.配置管理之人員及相當資源

1.1 機關學校應建立個人資料保護管理政策。

1.2 機關學校應成立個人資料保護管理小組，由單位副首長擔任召集人，統籌決策與單位內資訊安全與個人資料業務之資源整合運用。

1.3 機關學校應指定專人依相關法令辦理安全維護及保管事項，作為機關內部之個人資料管理代表。機關組織編制較小者，則統一由該機關「個資保護聯絡窗口」兼辦上述專人業務。

1.4 機關學校應決定並提供有關單位規劃與施行個人資料保護工作所需的資源，包含人力、物資或外部諮詢顧問等。

# 2.界定個人資料之範圍

2.1 機關學校應定期執行個人資料檔案鑑別作業，建立與維護個人資料檔案清冊，公務機關並依個資法要求於網站上公開相關資訊。

# 個人資料檔案清查-格式參考

| 項目<br>編號 | 個人資料<br>檔案名稱 | 保有依據 | 特定目的<br>及類別 | 保有單位 |
|---|---|---|---|---|
| | | | | |
| | | | | |

個人資料保護法之特定目的及個人資料之類別 ( 民國 101 年 10 月 1 日 修正 )
http://mojlaw.moj.gov.tw/LawContentDetails.aspx?id=FL010631

# [加分題]
# 3.個人資料保護之風險評估及管理機制

3.1 機關學校應針對「個人資料檔案清冊」內容，訂定個資衝擊影響程度評估準則，並進行個資資產之衝擊影響程度分析。

3.2 個人資料檔案風險評鑑應定期執行，以瞭解處理各種個人資料的可能風險，並針對這些風險訂定處理計畫。

# 4.事故之預防、通報及應變機制

4.1 學校機關的人員應瞭解個人資料保護法之要求，克盡職責保護及管理相關業務所接觸之個人資料。

4.2 當發生個人資料資訊安全事件時，應通報主管機關；若事件發生導致個人資料被竊取、洩漏、竄改或其他侵害者，應依個資法第12條查明後以適當方式通知當事人。

4.3 機關學校應訂定個人資料資訊安全事件處理程序。

4.4 機關學校所設置的「個資保護聯絡窗口」除作為機關學校間個資業務協調聯繫之對口外，也擔任機關學校本身個資安全事件通報之對口，以及重大個資外洩事件之民眾聯繫單一窗口。機關學校應將「個資保護聯絡窗口」之聯繫方式（如：電話、email）置於機關學校網站，以便利民眾提出申訴與救濟。

[加分題]

# 5.個人資料蒐集、處理及利用之內部管理程序

5.1 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。

5.2 蒐集個人資料時，應依個人資料保護法第8條明確告知當事人相關資訊：

(a) 機關名稱。(b) 蒐集目的。(c) 個人資料的類別。

(d) 個人資料利用期間、地區、對象及方式。(e) 當事人行使之權利事項及方式等。

(f) 當事人不提供個人資料對其權益之影響。

5.3 機關學校應於法律允許之範圍內提供資料當事人下列權利：

(a) 查詢或請求閱覽。 (b)請求製給複製本。 (c)請求補充或更正。

(d) 請求停止蒐集、處理或利用。 (e)請求刪除。

5.4 蒐集非由當事人提供之個人資料時，應於處理或利用前，依個人資料保護法第9條，向當事人告知個人資料來源及應告知資訊，如本文件5.2所列之 (a) ~ (e) 項目。

5.5 學校機關應維護個人資料的正確性，並主動依當事人的請求更正或補充之。

5.6 當資料利用範圍超出蒐集的特定目的時，應依個人資料保護法第16條與第20條有關特定目的以外之利用規範。

# 6.資料安全管理及人員管理(1/4)

6.1 機關學校管理之網站或網頁內容，於確有必要公布個人資料時，需經所屬主管核准，且依相關法律及規範處理，始得公布。

6.2 對於個人資料之調閱宜經申請並核准，並加以記錄其調閱身分及行為。調閱紀錄可視機關實際需求存檔，以利後續人員查詢及追蹤。

6.3 處理個人資料時，需核對個人資料之輸入、輸出、編輯或更正是否與原件相符。個人資料提供利用時，對資料相符與否如有疑義，應調閱原檔案查核。

6.4 個人資料檔案應定期備份（例如每個月），並防止備份檔案被竊取、竄改、毀損、滅失或洩露。

6.5 個人資料輸入、輸出、存取、更新、更正或註銷等處理行為，宜釐定使用範圍及調閱或存取權限。

6.6 含有個人資料之紙本報表的申請、讀取、列印、使用、存檔、轉交及銷毀等處理及利用行為，宜建立相關之授權、監督及行為記錄機制。

# 6.資料安全管理及人員管理(2/4)

6.7 個人資料檔案之處理行為應設置使用者代碼及通行碼，使用者代碼不得與他人共用且通行碼須定期更新，並視業務及資料重要性，考量其他輔助安全措施。個人資料檔案使用完畢後，應立即退出應用程式。

6.8 學校機關應訂定處理個人資料檔案資訊設備或系統登入通行碼之更換與設定規則，例如通行碼至少每六個月更換一次，通行碼長度應至少8碼，且包含文數字等。

6.9 針對個人資料檔案之處理，可視需要考量採取權限區隔、資料加密機制，或相關核准程序加以控管，非專責處理特定個人資料者不得具有存取或查閱個人資料之權限，並留存使用者身分、識別帳號與其行為紀錄以供事後稽查。

6.10 個人資料檔案禁止存放於網路芳鄰分享目錄。

6.11 儲存個人資料的資訊設備應使用螢幕保護程式，設定螢幕保護密碼，並將螢幕保護啟動時間設定為15分鐘以內。

6.12 儲存個人資料之資訊設備應安裝防毒軟體，除至少每日更新病毒碼外，並應每週執行排程掃描。

# 6.資料安全管理及人員管理(3/4)

6.13 儲存個人資料之資訊設備應定期檢視、更新作業系統、應用程式漏洞（如：Windows作業系統、Windows Office、Adobe Acrobat等）。

6.14 內部傳遞或與其他機關交換個人資料時，應選擇可靠且具備保密機制之傳遞方式，如於實體文件封袋加上彌封、或對資料檔案壓縮加密，並對轉交或傳輸行為加以記錄流向備查。

6.15 自行開發或委外處理個人資料檔案之資訊系統，應在系統開發生命週期之初始階段，將個人資料檔案的安全需求納入考量（如：邏輯測試）；系統之維護、更新、上線、及版本異動等作業，應予安全管制，避免危害個人資料安全。

6.16 宜避免允許維護人員或系統服務廠商以遠端登入方式進行牽涉個人資料的資訊系統維護或其他有關之運作；若需使用遠端登入方式進行維護，則應透過加密通道進行（如：HTTPS、SSH等）。

6.17 自行開發或委外處理個人資料檔案之資訊系統，應將個人資料（包含測試用個人資料）施予妥善之保護與控管。

# 6.資料安全管理及人員管理(4/4)

6.18 處理個人資料檔案之人員，其職務如有異動，應將所保管之儲存媒體及有關資料列冊移交，接辦人員除應於相關系統重置通行碼外，應視需要更換使用者識別帳號。

6.19 處理個人資料檔案之人員，應簽訂保密切結書，並確認於離職時或合約終止時取消或停用其使用者識別帳號，且收繳其通行證及相關證件。

6.20 針對個人資料檔案處理人員訂定電腦使用規範，例如禁止以下操作行為：

(a) 禁止使用即時通訊軟體傳輸個人資料檔案。
(b) 禁止使用外部網頁式電子郵件(Webmail)傳輸個人資料檔案。
(c) 禁止使用點對點(P2P)軟體及Tunnel相關工具下載或提供分享檔案。
(d) 禁止在社群網站、部落格、公開論壇或其他利用網際網路形式公開業務所知悉之個人資料。

6.21 個人資料檔案若委外建檔，應於委外合約中載明所處理之個人資料保密義務、資訊安全相關責任及違反之罰則。

6.22 與委外廠商所簽訂正式書面協議或契約中，應明確陳述契約終止時，相關個人資料的銷毀或交還程序。

# 7. 認知宣導及教育訓練

7.1 機關學校應對處理個人資料檔案之人員施予資訊安全與個資隱私保護之教育訓練（內、外訓皆可），並定期於單位內宣導個資隱私保護之重要性。

7.2 機關學校全體教職員生及相關經手個人資料之第三人應對以下法令及規範有基礎認知：

(a) 個人資料保護法

(b) 個人資料保護法施行細則

(c) 教育體系資通安全管理規範

(d) 國中、小學資通安全管理系統實施原則

7.3 機關學校辦理個人資料保護認知宣導活動完畢後，應留存相關紀錄備查。

# 8.設備安全管理

8.1 指定專人負責管理儲存個人資料檔案之資訊設備與其他相關設施等，並檢視、處理其錯誤或異常事件等訊息。

8.2 儲存個人資料之資訊設備應置放於實體安全區域（如：門禁控管之辦公區域、機房），或與外部網路隔絕（如：防火牆），避免有心人士或非授權人員存取。

8.3 儲存個人資料檔案之磁碟、磁帶，及紙本等相關儲存媒體，應指定專人管理，並置於實體保護之環境（如：上鎖之防潮箱、書櫃），必要時應建立備援機制，以防止資料損壞、遺失或遭竊取。相關儲存媒體非經權責單位同意並留存紀錄，不得任意攜出或拷貝複製。

8.4 外部團體或個人更新或維修電腦設備時，應指派專人在場，確保個人資料之安全及防止個人資料外洩。

8.5 儲存個人資料檔案之電腦或相關設備如需報廢或移轉他用時，應確實刪除該設備所儲存之個人資料檔案。

[加分題]

## 9.資料安全稽核機制

9.1 機關學校應定期執行稽核作業，以確保相關管理措施之有效性。

9.2 機關學校若業務變更，應立即執行稽核作業，以確保作業變更後的風險。

# [加分題]
# 10.使用紀錄、軌跡資料及證據保存

10.1機關學校可依實際業務狀況及需求與業務評估，針對以下個人資料處理相關活動，進行紀錄的保存，以為未來舉證等用途。

(a) 因應事故發生所採取行為之紀錄。
(b) 確認受託人執行委託人要求事項之紀錄。
(c) 提供當事人行使權利之紀錄。
(d) 確認資料正確性及更正之紀錄。
(e) 權限新增、變動及刪除之紀錄。
(f) 備份及還原測試之紀錄。
(g) 個人資料交付、傳輸之紀錄。
(h) 個人資料刪除、廢棄之紀錄。
(i) 存取個人資料系統之紀錄。
(j) 定期檢查處理個人資料之資訊系統之紀錄。
(k) 教育訓練之紀錄。
(l) 計畫稽核及改善程序執行之紀錄。

# 11.個人資料安全維護之整體持續改善

11.1 針對資訊安全事件及稽核缺失應訂定改善行動或預防措施，以減低事件再次發生機會。

11.2 稽核發現缺失改善情形、風險評估結果及個人資料資訊安全事件等，必須每年定期呈報個人資料保護管理小組。

# 四、常見的稽核發現

# 常見的稽核發現(1/3)

- 建議宜建立個資保護管理政策，並公告予同仁知悉。
- 建議宜建立個人資料檔案清冊，並公布個人資料檔案大綱於網站，以符合個資法之要求。
- 建議宜建立個資內稽、事件管理及矯正預防機制。
- 建議宜對於個人資料之調閱，建立申請及核准程序。
- 建議交換個人資料時須記錄轉交或傳輸行為之流向。
- 建議可再全面落實處理個人資料檔案之人員職務異動時，宜列冊移交相關儲存媒體及資料。
- 建議宜全面對處理個人資料檔案之人員施予資訊安全與個資隱私保護之教育訓練，並定期於單位內宣導個資隱私保護之重要性，且留存紀錄備查。

# 常見的稽核發現(2/3)

- 建議宜再宣導及加強檢查以下事項：
  - 禁止開啟網路芳鄰分享目錄與檔案。
  - 禁止使用MSN或其他即時通訊軟體傳輸個人資料檔案。
  - 禁止使用外部網頁式電子郵件(Webmail)傳輸個人資料檔案。
  - 禁止使用點對點(P2P)軟體及Tunnel相關工具下載或提供分享檔案。
  - 禁止人員在社群網站、部落格、公開論壇或其他利用網際網路形式公開業務所知悉之個人資料。
- 建議個人資料檔案宜採加密儲存及傳送。
- 建議存存放個人資料之資訊設備宜定期檢視、更新作業系統及應用程式漏洞。

# 常見的稽核發現(3/3)

- 個人資料檔案若委外建檔，建議應於委外合約中載明所處理之個人資料保密義務、資訊安全相關責任及違反之罰則。
- 與委外廠商所簽訂正式書面協議或契約中，建議應明確陳述契約終止時，相關個人資料的銷毀或交還程序。


Question
& Answer ...