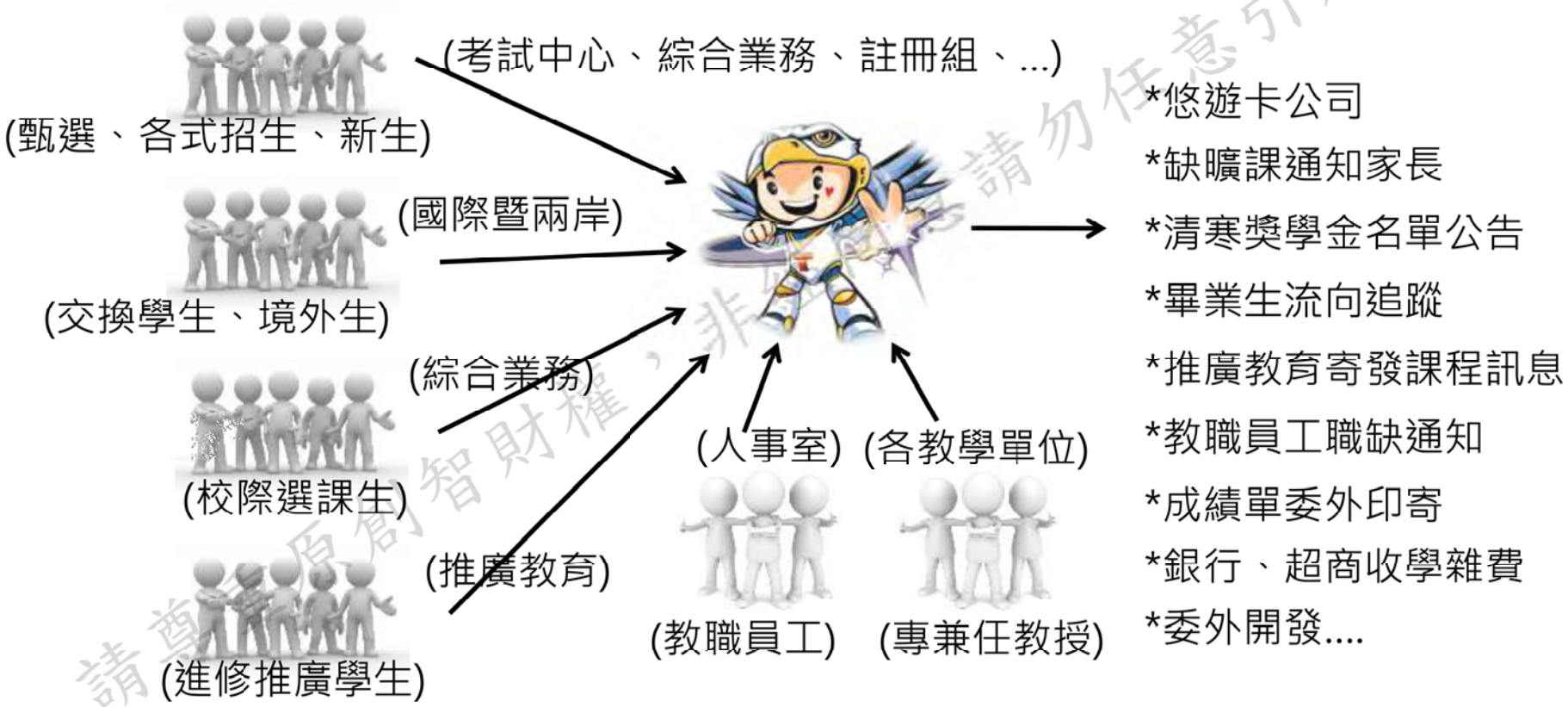
再一次認識-個人資料

107學年度資訊安全暨個資保護管理講習

107.09.06 14:00~17:00

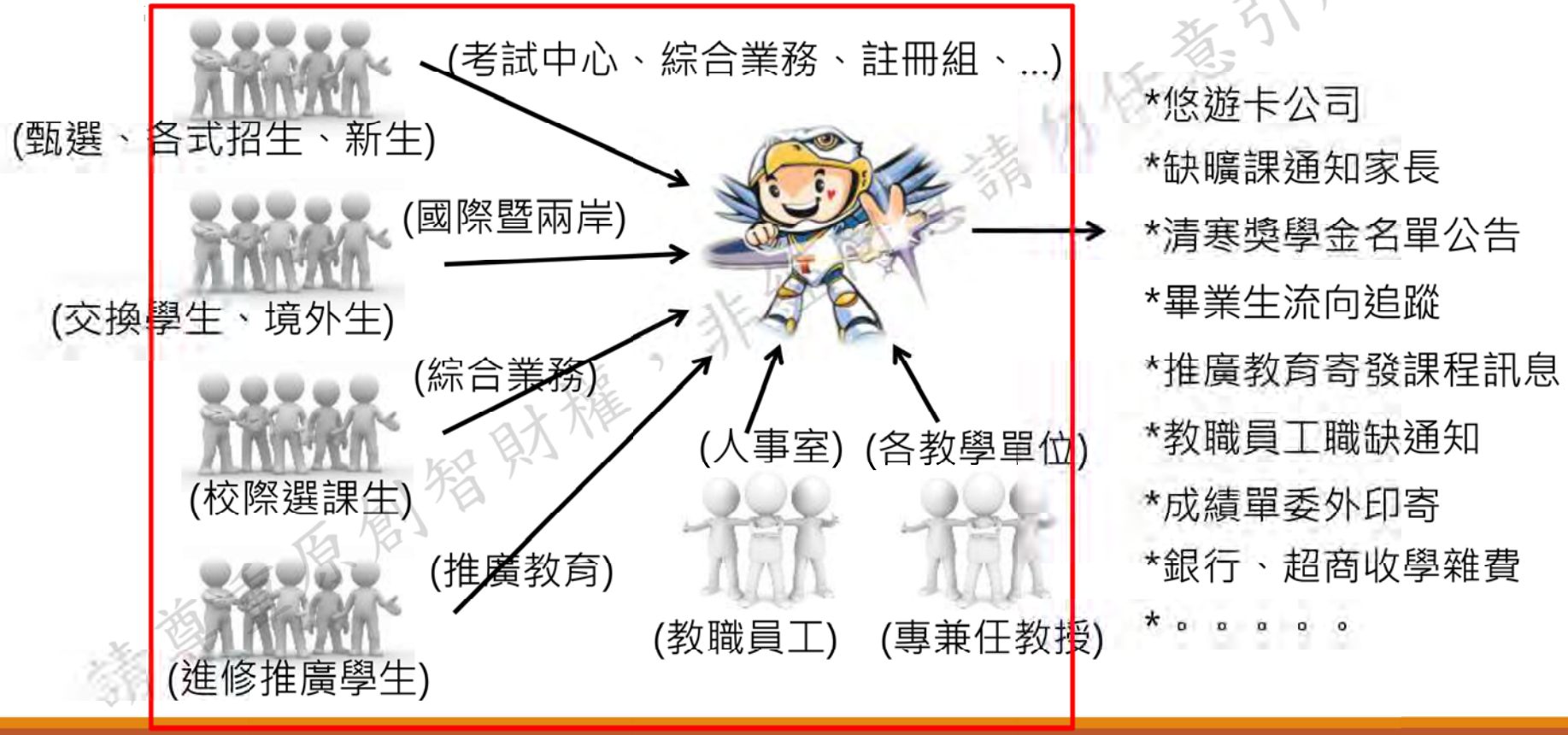
107.09.12 14:00~17:00

大學常見的個資法問題



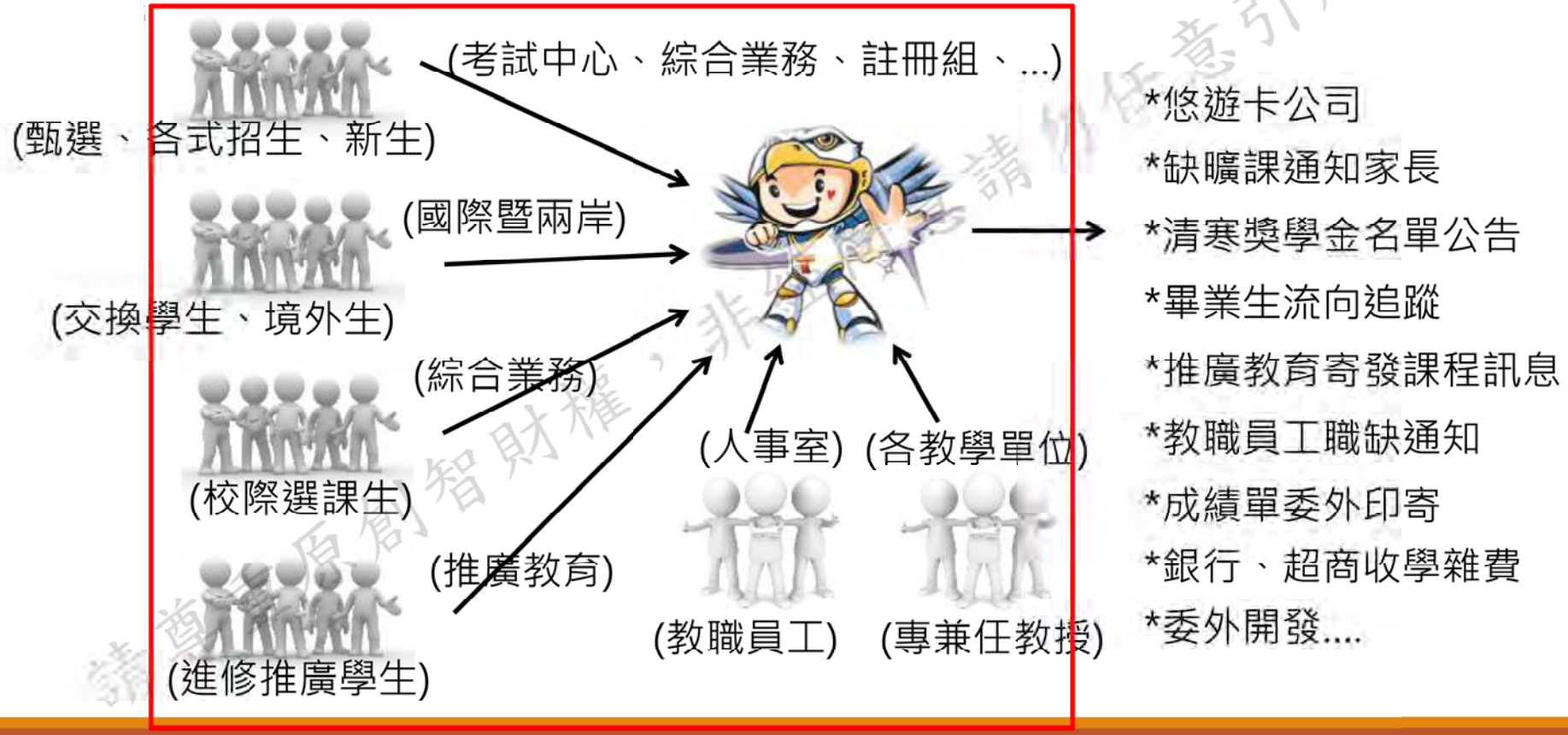
大學常見的個資法問題

蒐集個資有無超過必要範圍？



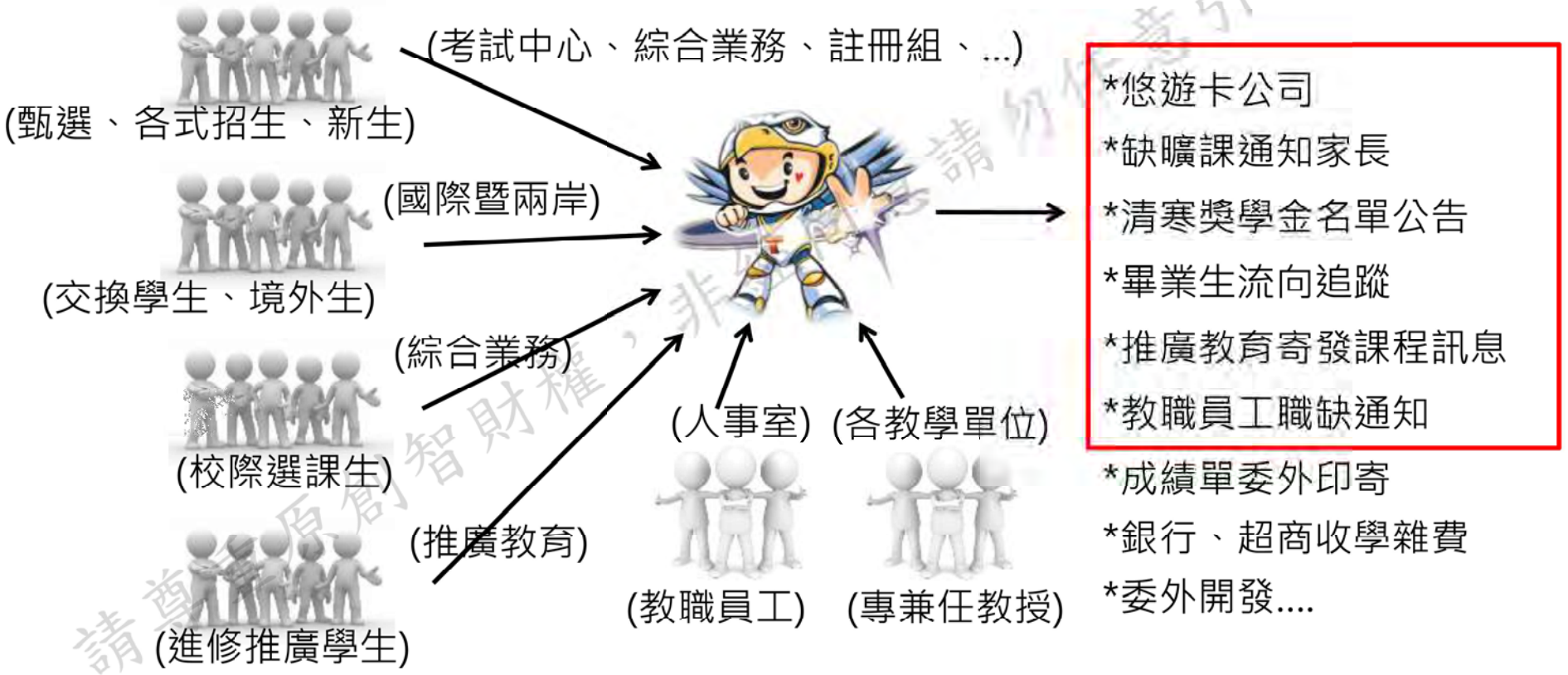
大學常見的個資法問題

蒐集個資有無告知法定事項？(個資蒐集告知聲明)



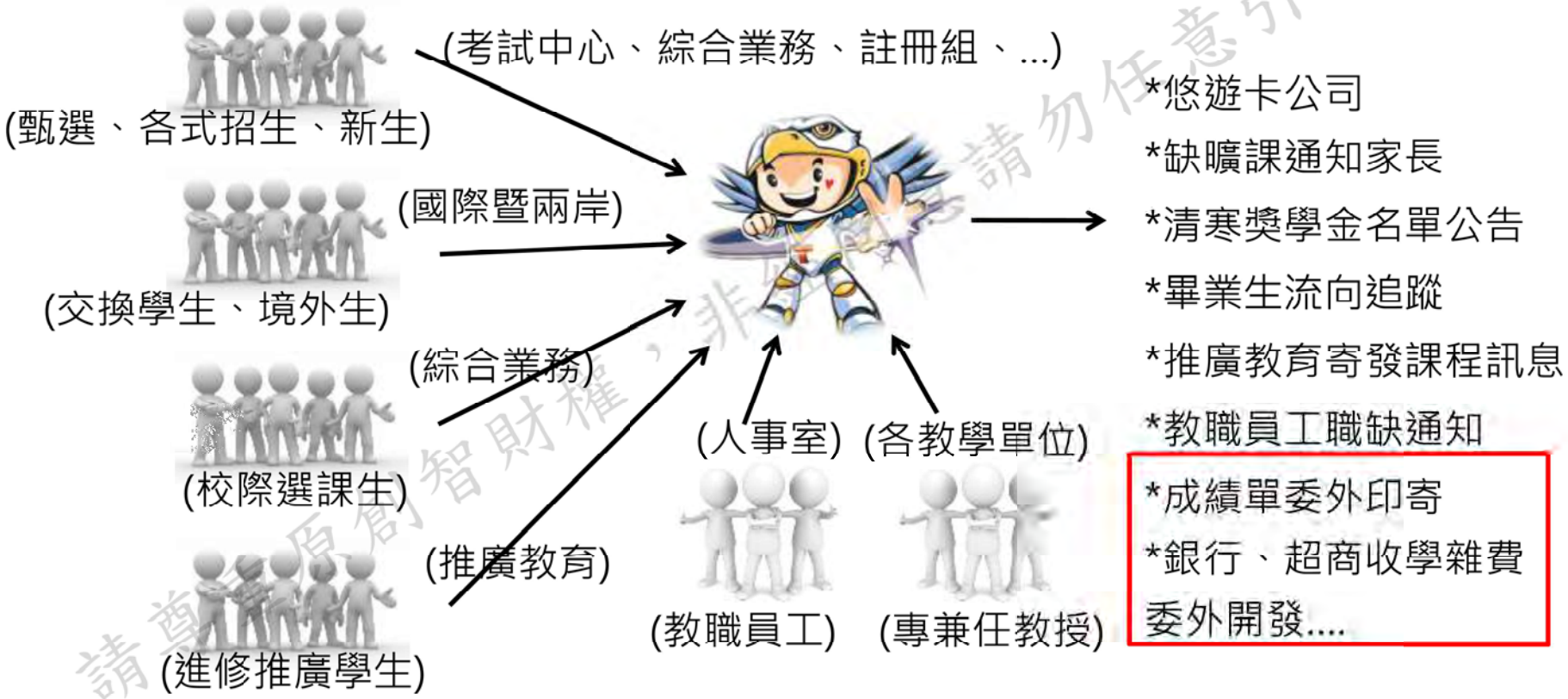
大學常見的個資法問題

利用個資有無超出蒐集目的？



大學常見的個資法問題

委外處理、利用個資有無監督？



永遠搞不清的...直接/間接

- 直接蒐集與間接蒐集...
  - ✓ 若非直接向當事人蒐集個人資料，而是透過第三方所提供的資料，因而蒐集到了個人資料，屬於間接蒐集個資
  - ✓ 反之則為”直接蒐集” (直接蒐集則於蒐集時立即告知)

▶間接蒐集個人資料的告知義務

非直接向當事人蒐集個資，而是透過第三方取得個資，必須在處理或利用前，或首次利用時告知當事人。

在處理或利用前告知 或 在首次利用時告知

非自當事人處蒐集個資，應告知事項：

1. 個人資料來源
2. 蒐集者的名稱（公務機關或非公務機關的名稱）
3. 蒐集的目的
4. 個人資料的類別
5. 個人資料利用的期間、地區、對象及方式
6. 個資當事人擁有的權利：查詢、請求閱覽、製給複製本、補充、更正、「停止蒐集、處理或利用」、刪除。

iThome

https://www.ithome.com.tw/article/88048

https://www.ithome.com.tw/article/91041

間接蒐集不須告知...

不須告知的例外情形

有以下任一情形，可不須告知：

1. 依法律規定得免告知
2. 個人資料的蒐集係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
3. 告知將妨害公務機關執行法定職務
4. 告知將妨害第三人的重大利益
5. 當事人明知應告知的內容
6. 當事人自行公開或其他已合法公開的個人資料
7. 不能向當事人或其法定代理人為告知
8. 學術研究機構基於公共利益，有必要做為統計或學術研究之用，且資料經處理後無從識別特定的當事人。
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

https://www.ithome.com.tw/article/91041

https://www.ithome.com.tw/article/88048

如何檢視...

- ✓拿出各位單位的業務職掌或自己的業務/工作文件
- ✓查看作業流程
- ✓交互核對
- ✓重覆檢核
- ✓個資盤點須配合作業流程與業務職執行逐一核對
- ✓法令法規的符合性/過度收蒐集(未符合特定目的)

看到這新聞，您想到什麼?

個資管理心法543

5個方向

4大原則

3不3要

資料來源：達文西個資暨科技法律事務所

5個方向

1) 資訊自主
2) 違法蒐集
3) 違法利用
4) 黑箱作業
5) 個資意外

4大原則

1) 資料減量
   1) 個資欄位減量
   2) 個資數量減量
   3) 到期個資銷毀
2) 公開透明
   1) 該告知的告知　隱私權聲明、個資告知聲明
   2) 該通知的通知　個資侵害事故
3) 從一而終
   1) 在蒐集目的內利用個資
   2) 檢視有無符合例外
      1) 法律明文規定
      2) 增進公共利益
      3) 免除當事人危險
      4) 防止他人重大危害
      5) 為公共利益做統計+無從識別當事人
      6) 當事人書面同意-明確告知目的、範圍及同意與否的影響
4) 妥善保管

4)妥善保管

適當安全維護

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。

非公務機關保有個人資料檔案者，應採行適當之安全措施。

得採取下列措施

- 組織資源配置
- 通報應變機制
- 認知教育訓練
- 資料紀錄保存
- 個人資料範圍
- 內部管理程序
- 設備安全管理
- 安全維護計畫
- 風險評估機制
- 安全人員管理
- 安全稽核機制

3不3要

- ✓不蒐集、不保存用不到的個資
- ✓不在蒐集目的外利用個資
- ✓不掉以輕心

- ☑要攤在陽光下
- ☑要顧及當事人權利
- ☑要定期檢視個資法律遵循

個資管理-良善管理之責的建立

1) 了解個資相關規範的要求（含個資法、民法、刑法、單位內法令法規...）
   ➔適法性
2) 必要的安全措施
   ➔持續...管理程序及安全符法性作為檢視（如蒐集之特定目的...182...）
3) 個資檔案盤點
   ➔持續執行與檢核-個資盤點及風險評鑑
4) 持續維運
   ➔每年至少一次之審核與查檢

沒有最好、只有更好

一直滾動下去...

① 尿液檢查
檢查項目
酸鹼度
蛋白質
葡萄糖
紅血球
白血球

② 血液檢查
檢查項目
血紅素
紅血球
白血球
白小板

③ 生化檢查
檢查項目
白蛋白
球蛋白
尿素氮
膽固醇
三酸甘油酯
尿酸

作業經歷
既往病歷
自覺症狀
呼吸系統
血液循環系統
泌尿系統
消化系統
神經系統
皮膚系統
頭頸部
四肢及關節
身高
體重
色盲
視力(右/左)裸視
視力(右/左)矯正
聽力(右/左)
血壓(收縮壓)
血壓(舒張壓)
S.P尿比重
PH酸鹼值
Protein尿蛋白
Glucose尿糖
O.B尿潛血
NIT尿硝酸鹽
胸部X光攝影
應處理及注意事
【體重_異常】需注
【收縮壓_異常】血

健檢項目	健檢結果		
	98年度	97年度	96年度
檢查日期	2007/12/19	2006/11/15	2004/12/21
檢查編號	大安_61219S007	951115大安G056_B034	大安_412211213
部門名稱	軟體設計部	軟體設計部	軟體設計部
身高	174.5 cm	174 cm	174 cm
體重	75.4【60～73】Kg	68【59～72】Kg	71.8【59～72】Kg
右耳聽力檢查	正常	正常	正常
左耳聽力檢查	正常	正常	正常
色盲	正常	正常	正常
右眼裸視			0.9【0.8～1.5】
左眼裸視			0.9【0.8～1.5】
右眼矯正	0.7【0.7～1.5】	0.9【0.8～1.5】	
左眼矯正	0.6【0.7～1.5】	0.8【0.8～1.5】	
收縮壓	116【100～140】mmHg	112【100～135】mmHg	114【100～135】mmHg
舒張壓	66【60～90】mmHg	69【60～85】mmHg	72【60～85】mmHg
尿酸鹼值(PH)	6【5～8】	6.5【4.5～8】	6【4.5～8】
尿蛋白(Protein)	(-)	(-)	(-)
尿潛血(OB)	(-)	(-)	(-)
尿糖	(-)	(-)	(-)
膽紅素(Bilirubin)	(-)	(-)	(-)
尿膽素(Urobilinogen)	0.1【0.1～1】Eu/dl	0.1【0.1～1】Eu/dl	0.1【0.1～1】Eu/dl
酮體(Ketone body)	(-)	(-)	(-)
尿硝酸鹽(NIT)	(-)	(-)	(-)
比重(SP_GR)	1.01【1.005～1.03】	1.025【1.005～1.03】	1.02【1.005～1.03】
尿白血球酯	(-)	(-)	(-)
胸部X光檢查異常狀況	正常	正常	正常
骨質密度	-0.1【-0.9～10】	-0.7【-1～5】	

- 健康檢查....
  - ✓全黑
  - ✓有紅字
  - ✓每年比較...

看到這新聞，您想到什麼?

https://tw.news.appledaily.com/headline/daily/20180627/38054604/

大學常見的個資違法問題

- ✓當事人**權利行使管道**未建立
- ✓個資保存期限未統一
- ✓院系研討會報名資料由老師或承辦人員負責，無法控管
- ✓學校與校友會非同一機關，但學校直接提供畢業學生個資給校友會
- ✓境外生、學分班學生相關申請資料各自保管，未建立統一管理機制
- ✓銷毀未落實....

持續的適法性查檢...以矯正違法

- ✓持續自我檢視與落實自我要求
- ✓個資盤點清查宜定期執行與定期自我抽核
- ✓個資蒐集、處理、利用適法性查檢以宜複核
- ✓個資查檢缺失項目矯正宜落實
- ✓適法性複檢不宜由承辦人自行檢核

別把稽核當找碴，借由他人之手，更容易看到被自己忽略的事....

凡住過必留下．．．鄰居
凡考過必留下．．．成績
凡吃過必留下．．．體積
所以．．．
凡走過必留下．．．痕跡

沒有跌倒．．．　就不知道撞到是會痛的

面對...

凡走過必留下痕跡...（告知、軌跡、存錄）

必要且不過度的蒐集...（必要性，且與特定目的相符）

有做就是有，沒做到的..就持續改善或調整...（管理制度與可行性）

時時注意.....

必須隨時注意時事與法令法規的更動

新知心知...

歐盟個資保護新法　嚴格護衛隱私

|20180127 公視全球現場深度週報 |GDPR的衝擊....2018/05/25正式施行

何謂GDPR

- 一般資料保護規範（General Data Protection Regulation，簡稱GDPR）
  - 根據GDRP官網描述，這條法規是「保護以及加強歐盟成員國人民的資料隱私，以及重塑整個地區內的組織處理資料隱私的方法。」雖是這麼說，但正因為網路無遠弗屆的特性，讓資料本身根本沒有地域性可言。
  - 這項法規的基礎，是「被遺忘權（right to be forgotten）」，是一種在歐盟已經付諸實踐的人權概念，可以要求控制資料的一方，刪除所有個人資料的任何連結（link）、副本（copies）或複製品（replication）；還有「資料可攜權（Right to data portability）」，意思是用戶可以將A服務的資料，轉移到B服務上，這也就是為什麼Instagram最近推出資料打包備份功能、蘋果推出管理個資工具。

什麼是GDPR？不可不知的歐盟資料保護規則
General Data Protection Regulation
https://www.youtube.com/watch?v=-jNxv447qKI

資料來源：數位時代-https://www.bnext.com.tw/article/49249/gdpr-general-data-protection-regulation-eu-

誰受GDPR的規範...

您的公司有歐盟顧客上門，就適用 GDPR

如餐廳、旅館、旅行社、計程車、電商購物平台...，擁有顧客的信用卡資料、會員資料等

您的企業有歐盟員工，或歐盟供應商，就適用 GDPR

包括正職與兼職員工、供應商、協力廠商、合作夥伴...，您可能擁有他們的保險資料、薪資紀錄、聯絡資訊等

非營利組織與政府機構，也適用 GDPR

如果組織的志願工作者、會員、贊助者、捐款人、顧問...是歐盟公民，您擁有他們的聯絡資訊、稅捐資料等，就受 GDPR 規範

什麼是GDPR？不可不知的歐盟資料保護規則 General Data Protection Regulation
https://www.youtube.com/watch?v=-jNxv447gKI

資料來源：Microsoft 網站

我做錯什麼，會違反 GDPR？

企業對歐盟公民個資保護不周，如資料外洩或遭到勒索軟體攻擊

導致個資被竊取、被非法存取、或被分享給無權利使用的第三方

企業使用歐盟公民個資，脫離約定目的，或缺乏正當性

例如某活動蒐集的個資，被轉給另一個無關的活動使用

未給予個資當事人應有的權利

權利包括當事人有權要求更正或刪除其個人資料等

沒有採取足夠的安全技術保護個人資料，或未保存使用個資的歷史記錄

就算個資並未外洩，只要資料防護的水準不夠高，就不符合規範

資料來源：Microsoft 網站

GDPR 10大重點

1. 以資料為主體
2. 必須設置資料保護長且需負起法律責任
3. 必須先徵求當事人的同意
4. 強化個人資料可攜權權利
5. 新增被遺忘權(資料抹除)
6. 外洩，必須在72小時內通報
7. 個資保護系統預設要納入隱私保護
8. 賦予當事人有權*反對*-被自動化剖析（Profiling）
9. 落實資料保護影響評估
10. 提高罰則金額，甚至以全球營業額計算

GDPR十大重點-1

- **以資料為主體**
  - GDPR除了適用在歐盟地區註冊的企業，或者是不是歐盟註冊的企業，但在歐盟營運，或者是，有蒐集、處理或利用歐盟民眾個人資料的企業或組織等，都在GDPR的規範中。

GDPR十大重點-2

- **企業必須設置資料保護長，且需負起法律責任**
  - 全球所有企業的核心業務，只要涉及歐洲民眾個資的蒐集、處理和利用時，不論公司規模大小，都必須設置***資料保護長***。這個資料保護長必須要有效依法履行職責，一旦企業有違反GDPR的規範，這個資料保護長需要被追究相關的法律責任。

GDPR十大重點-3

- **個資的蒐集、處理和利用，必須先徵求當事人的同意**
  - 歐盟要求企業必須強化同意書的條件，**不可以**使用充滿法律術語和難以理解的文字，且必須和其他事項內容有區隔，可以更容易獲得民眾的了解和同意。
  - GDPR不僅要求要提供**簡明易懂**的個資使用同意書，連撤銷個資使用的同意書，也必須一樣簡明易懂且容易撤銷。
  - GDPR也賦予歐洲民眾**可以選擇「不共用資料」的權利**，也就是說，歐洲民眾可以拒絕企業共同行銷。

GDPR十大重點-4

- **強化個人資料可攜權權利**
  - 資料可攜權就是讓歐洲民眾在不同服務業者之間，具有自由搬動個資的權利，例如，歐洲民眾可以從某個ISP業者，**輕易**搬到另外一個ISP業者的服務上。

GDPR十大重點-5

- **新增被遺忘權(資料抹除)**
  - 「被遺忘權」是近年來歐洲對於隱私保護一再強調的重點項目之一，像是，歐洲法院過去已經有不少的判例要求，包括Google在內的搜尋引擎業者，必須把「不相關」或「過期」的個人資訊結果中，移除相關的連結。
  - 被遺忘權也被稱為「資料抹除」，就是要讓資料的當事人可以要求包括資料控制者以及資料處理者，必須協助抹除當事人個人資料、停止使用當事人個資，這包括供應商和其他的**第三方業者**在內。他指出，抹除資料的前提條件包括：資料利用與處理目的不同、非法處理個資，或者是資料當事人撤銷同意書等，都可以要求刪除。
  - GDPR上規範的被遺忘權，在現階段比較偏向**「搜尋不到相關資訊」**。

GDPR十大重點-6

- **外洩個資，必須在72小時內通報資料保護主管機關**
  - 不論是資料控制者或者是資料處理者，一旦爆發個資外洩的資安事件時，必須要在72小時內，即刻通報給資料保護主管機關（Data Protection Authority）；但是，如果這個外洩資料對於當事人會造成重要危害時，也應該要及時通知當事人。
  - 歐盟對於應該在多久期間內，將個資外洩的事情通知當事人，並沒有明確規定，但若以公告機制作為通知當事人的作為，是可以的。

  - 不論是資料控制者或者是資料處理者，一旦爆發個資外洩的資安事件時，必須要在72小時內，即刻通報給資料保護主管機關（Data Protection Authority）；但是，如果這個外洩資料對於當事人會造成重要危害時，也應該要及時通知當事人。
  - 歐盟對於應該在多久期間內，將個資外洩的事情通知當事人，並沒有明確規定，但若以公告機制作為通知當事人的作為，是可以的。

GDPR十大重點-8

- **賦予當事人有權反對被自動化剖析（Profiling）權利**
  - 一旦當事人提出反對權，而資料控制者或處理者無其他正當理由反對時，就必須**立即停止處理**當事人個資。
  - GDPR賦予資料當事人有權了解某一項特定服務，是如何利用大數據分析、機器學習、人工智慧等技術，進行資料分析和研判的服務，當然也**有權反對**被如此剖析。

GDPR十大重點-9

- **要求企業必須落實資料保護影響評估**
  - DPIA（Data Protection Impact Assessments 數據保護影響評估）主要是要辨識業務流程中，有哪些涉及個人隱私權利的風險，並加以衡量、管理和因應；而且在進行評估前，也應該先確認相關的業務活動與帶來的隱私風險，是否具有其對稱性和必要性。

GDPR十大重點-10

- **提高罰則金額，甚至以全球營業額計算罰金金額**
  - 為了讓企業更有警覺，GDPR更大幅提高罰金金額，罰款分兩種情境做處罰，第一種是沒有合法理由，拒絕當事人刪除個人資料的請求，也沒有建立對企業或用戶資料保護的文件化管理系統時，最高可以處罰1千萬歐元（約新臺幣3.6億元），或者是全球營業總額的2%作為罰款。
  - 如果是更嚴重的違規，不論是非法處理個資；沒有合法理由，拒絕用戶停止處理個資的情求；在資料外洩事故發生後，沒有及時通知個資監管機構；沒有執行隱私風險評估（DPIA）；沒有任命資料保護長；違法向第三國傳輸個資等違規行為，最高可以處罰2千萬歐元（新臺幣7.2億元）或是全球營業總額4%作為罰款。
  - 不論是定額罰金或是營業總額比例的罰金，哪一個罰款多，就以哪一個為主。

所以...我們**了解**了？？？

賦予權...
告知義務
當事人同意
處理的合宜性
利用的合法性
傳輸的保護力
銷毀的落實性
隨時留意新聞與法令法規的異動
.....以上皆是.....安全維護措施

資安法立院三讀通過

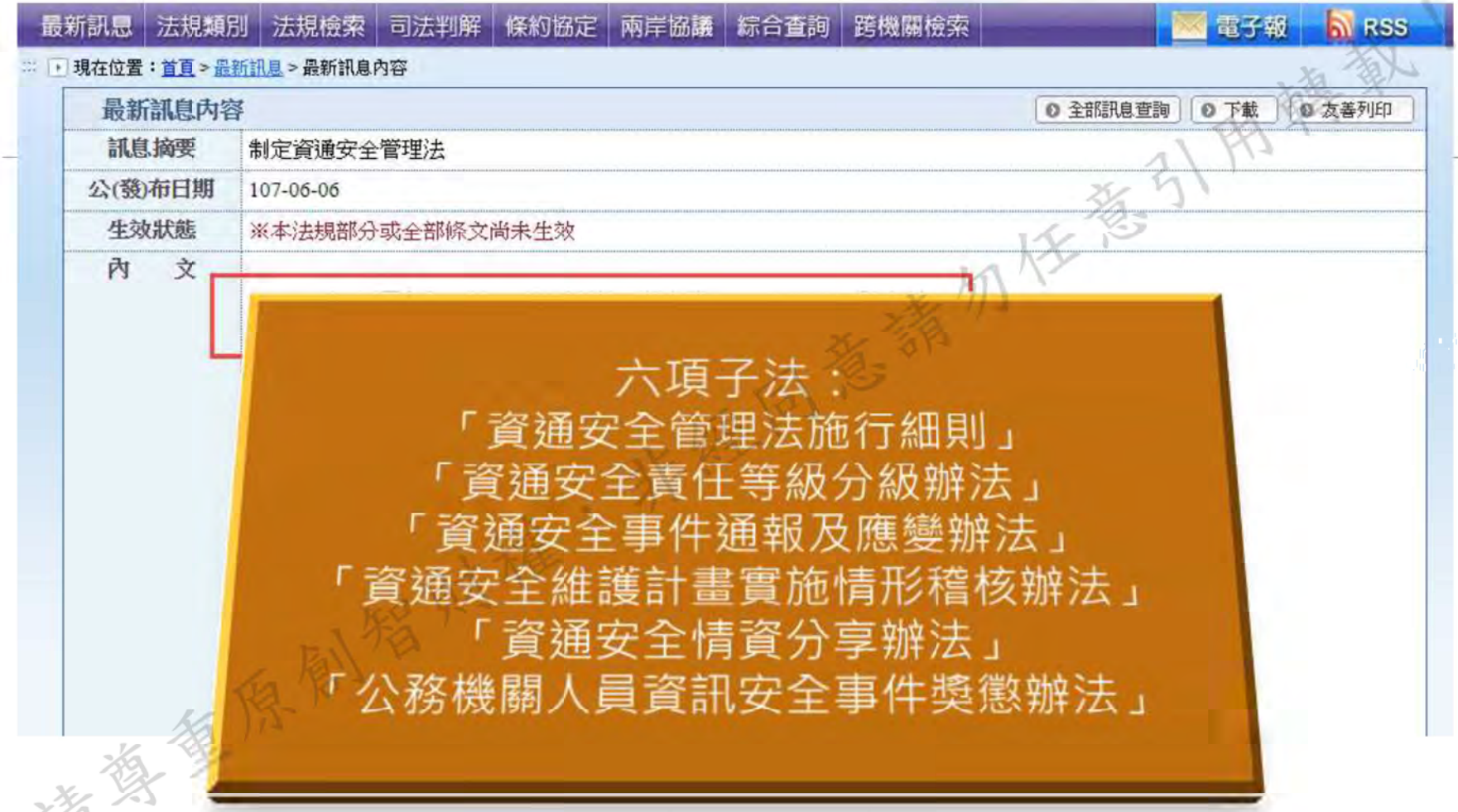
臺灣在5月11日立法院院會中，順利完成《資通安全管理法》三讀，法條經由總統公告後，正式施行日期將由行政院另行公告。接下來，行政院也將陸續完成相關包括《資通安全管理法施行細則》在內的6個子法，期能完善臺灣資通安全的法治基礎

新聞

【臺灣資安邁入新紀元】資安法立院三讀通過

臺灣在5月11日立法院院會中，順利完成《資通安全管理法》三讀，法條經由總統公告後，正式施行日期將由行政院另行公告。接下來，行政院也將陸續完成相關包括《資通安全管理法施行細則》在內的6個子法，期能完善臺灣資通安全的法治基礎

文/ 黃泰棻 | 2018-05-22



教育部　函

機關地址：10051臺北市中山南路5號
聯絡人：林文信
電話：02-7712-9092
Email：ansel@mail.moe.gov.tw

裝

受文者:環球學校財團法人環球科技大學

發文日期:中華民國107年7月27日

發文字號：臺教資(四)字1070127841號

速別：普通件

訂

密等及解密條件或保密期限：普通

附件：國家發展委員會函

主旨：轉知國家發展委員會函（如附件），「個人資料保護法」法律主管機關自即日起移由國家發展委員會職掌，請查照並轉知所屬。

線

說明：

正本：部屬機關(構)、各公私立大學校院

副本：

Q&A
感謝您的聆聽

請完成小小的自我檢測並繳回文件...謝謝您~

107學年度個資管理重點工作時程

請各單位參酌並轉達相關作業承辦人員，以利配合並提早規範各事務，謝謝協助！

- 請各單位「個人資料管理執行小組」成員參加107年8月20日13：30於MA305辦理107學年度個資盤點說明會及Google Apps Script教育訓練。
- 請於107年9月4日前完成107學年度個資盤點作業，將盤點結果送單位會議審議通過後，將紙本及電子資料送交圖書資訊處資訊安全維護組。(參與106年度發證稽核單位，請進行次要不符合事項與觀察事項進行矯正作業)
- 預訂107年9月底前召開107學年度第1次個資委員會，進行管理審查及全校個資盤點結果複核，請各單位務必**於期限內**完成相關個資作業調整並完成106年度發證稽核次要不符合事項與觀察事項之矯正作業，**各矯正作為請於107年9月15日將電子資料**寄送圖書資訊處資訊安全維護組。
- 「教育機構資安驗證中心」將於107年11月至本校進行第一年追查稽核，確切日期將待驗證中心通知後，轉知受稽單位

下列事項請大家務必於107年10月底前完成

- 配合個資盤點清冊，完成**必要資料之銷毀**作業或**歸檔處理**（入庫要有清冊）
- 銷毀作業的記錄或照片請**務必完備**
- 過保存年限之資料若不刪除，可於單位會議上***決議後***即可不立即刪除，惟請務必有相關紀錄
- 各單位之倉庫或存放重要資料之檔案櫃，務必有**必要之安全管控**，如進出記錄表、攝影存錄或其它保全措施
- 各項申請表單請務必仔細盤點....
- 日常業務執行之必要原則或僅知原則，對於本校管理程序之認知請務必自我提昇
- 其它....不要怕被查....

參考資料

本校資安管理文件

http://olis.twu.edu.tw/isms_regulation.php

本校個資管理文件

http://olis.twu.edu.tw/pims_regulation.php

教育機構資安驗證中心
https://www.iscb.edu.tw/

教育部-校園資訊安全服務網
https://cissnet.edu.tw/

教育部 主管法規查詢系統
http://edu.law.moe.gov.tw/index.aspx
法務部 個人資料保護專區
http://pipa.moj.gov.tw
探討使用GOOGLE表單蒐集個資之迷思
http://nchu-iscb-casestudy.blogspot.tw/2017/07/ISCB1701.html
利用程式每天自動檢查您的GOOGLE表單狀況並寄發信件
http://nchu-iscb-casestudy.blogspot.tw/2017/07/ISCB1702.html
以GOOGLE表單蒐集個資注意事項 及GOOGLE APPS SCRIPT
http://olis.twu.edu.tw/download/2018/20180820.pdf