國立東華大學 103 學年度保護智慧財產權宣導及執行小組與
資通安全暨個人資料保護宣導及執行小組第 1 次會議－－會議紀錄

時 間：103 年 12 月 3 日 11:00~12:00
地 點：行政大樓 303 會議室
主 席:楊副校長維邦　　紀錄:何銘俊
出席委員：
鄭委員嘉良(請假)　　劉委員瑩三
白委員亦方 李委員大興 高委員傳正
王委員立中 褚委員志鵬 黃委員振榮
羅委員寶鳳 陳委員艷凰 林委員信鋒
林委員穎芬 黃委員宣衛 高委員德義(請假)
張委員德勝 潘委員小雪 夏委員禹九
徐委員揮彥(請假)
學生代表：
梁委員嘉晉 廖委員治權
列席人員：
張組長繼元 何組長銘俊 李組長宇峰
葉惠雯 楊志偉 陳惠汝 何振揚

壹、主席致詞：(略)

貳、確認上次會議紀錄：
【第 3 案】修正：
提案單位：圖書資訊中心
案 由：推動全校進行個資盤點及風險評鑑等工作。
說 明：
3.原預計明年寒假進行教學單位的個資盤點與風險評鑑，因考量明年系所評鑑業務仍持續中，工作繁重，決議改至明年暑假進行。

參、報告事項：
一、報告統合視導事項。(黃振榮主任)
二、資通安全與個人資料保護業務執行狀況。(葉惠雯技術師)
三、主席裁示：
1.校內舉辦的資安教育課程可製作教學錄影，並置於學校 e-Learning 平台。
2.每年圖資週時，可對資安教育課程的內容進行有獎徵答活動，也藉此鼓勵本校同仁多參與相關課程。

肆、提案討論：

【第 1 案】提案單位：圖書資訊中心

案 由：擬訂定本校個人資料安全保護管理基本措施，提請討論。

說明:

一、依據教育部 102 年 10 月 18 日臺教資(四)字第 1020143505 號函辦理。

二、依據 104 年大專校院統合視導之「校園保護智慧財產權與資訊安全（含個資保護)」訪視表，第三項個資保護的第二細項『(二)教育部頒訂「教育體系個人資料安全保護基本措施及作法」配合度(12%)』，訂定本校個人資料安全保護管理基本措施（草案)。

決 議：

1. 照案通過。
2. 應針對個人製做 Tips(小叮嚀)方便自我檢視，以符合個人資料保護工作基本要求。
3. 配合個人資料保護的要求，各單位應檢討於人員異動時有哪些該注意的事項，並於人員離職單上增列相關的檢核欄位。

【第 2 案】提案單位：圖書資訊中心

案 由：擬辦理本校個人資料保護管理內部與委外廠商稽核作業，提請討論。

說明:

一、依據 104 年大專校院統合視導之「校園保護智慧財產權與資訊安全（含個資保護)」訪視表，第三項個資保護的第二細項 『(三)個人資料保護持續改善管理流程(8%)』辦理，包含內部及委外廠商稽核。

二、內部稽核作業：行政單位已於本(103)年暑假完成的個資盤點與風險評鑑，擬於本(12)月請行政單位進行自我檢核後，由圖資中心複檢，檢核表如附件二之一。

三、委外廠商稽核作業:本校將個資業務委外監督管理機制納入合約條款的單位，目前有教務處註冊組及總務處出納組，擬於本(12)月請委外廠商進行自我檢核後，委任單位（註冊組及出納組）複檢，檢核表如附件二之二。

四、每年定期進行內部稽核及委外廠商稽核。

決 議：照案通過。

伍、臨時動議

【第 3 案】提案單位：圖書資訊中心

案 由：制定「非法影印教課書之學生輔導機制標準作業處理流程」，提請討論。

說明:

依據 104 年大專校院統合視導之「校園保護智慧財產權與資訊安全（含個資保護)」訪視表，訪視項目：第一項校園保護智慧財產權，訪視細項：第四細項影印管理(12%) 『3.學校針對進行不法影印教科書之學生建全輔導機制』辦理。

決 議：修正後通過，如附件三。

陸、散會

【附件一】

國立東華大學個人資料安全保護基本措施

壹、人員管理

一、本校教職員工職務如有異動，其保管之個人資料（以下簡稱個資）檔案應列入移交，相關資訊系統存取權限應重新設定。

二、單位接觸個資檔案人員應依照本校個資政策要求，執行相關規定之程序，負擔個資保密義務，並於離職或合約終止時停用資訊系統使用者識別帳號，及繳回通行證及相關證件。

三、禁止使用 LINE、FB、Skype 或其他即時通訊軟體傳輸業務所知悉之個資。

四、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資。

貳、作業管理

一、個資蒐集應秉持「適當、相當且不過度」，只蒐集必要個資，以降低個資外洩風險。

二、針對所保有之個資，部份甚為敏感的欄位內容，譬如：密碼、身分證號等，於蒐集、處理或利用時，加上適宜之遮蔽措施。

三、個資檔案使用完畢後，應立即退出應用程式。

四、個資檔案禁止存放網路共用目錄。

五、網路傳送個資檔案時，應對資料檔案加密，並再確認傳送對象無誤及請對方收到後回覆確認。

六、使用可攜式電腦儲存媒體時，遵循以下的使用規範：

1.確定電腦安裝之防毒程式及病毒碼都有定時更新，足以偵測隱藏之病毒後，方可~~去~~讀取可攜式電腦儲存媒體內的檔案。

2.暫存的個資檔案，使用後應確認刪除。

3.電腦使用應設登入密碼且符合密碼複雜難度要求。

七、影印、列印、傳真使用後須確認設備內並未遺留個資資料及原稿。

八、應定期備份含有個資電腦資料，及確認備份資料的可用性與安全性。

九、個人電腦報廢須對硬碟做低階格式化；移作他用時，應格式化硬碟後再重新安裝系統。

十、報廢之個資文件須用碎紙機銷毀；電子檔須確實刪除與清空資源回收桶。

十一、委託他人執行上述行為時，需對受委託人依個資法施行細則第八條規定為適當之監督，並明確約定相關事項、方式、義務及責任。

參、物理環境管理

一、圖資中心主機房

1.為確保相關設施之安全，非權責單位指定之人員不得擅自進入或使用相關資訊設備。

2.若外部人員或未具進出權限之人員，因執行業務需求進入時，必須指派人員隨行並填寫「人員進出登記表」後方可進出，並遵守相關設備管理之規定。

3.機房之門禁紀錄，應適當保存與定期審閱。

二、校內各單位保有個資之辦公室、檔案室、電腦主機室

1.無人或下班最後一人離開時，需將辦公室關門上鎖。

2.下班時記得將敏感之文件與可攜式資訊設備存放於儲存櫃並上鎖。

3.辦公室內需隨時注意身分不明或可疑的人員。發現不明身分之人員時，需主動詢問並儘速通知相關部門進行處理。

4.重要的辦公室、檔案室或電腦主機室應加裝監視器。

三、個人資料儲存媒體的保管

1.應對儲存媒體內重要的個資檔案加強安全管控，例如加密。

2.應有備份機制，以免重要資料遺失。

3.隨身碟只適宜儲存暫時性檔案，重要的個資檔案使用後應儘快刪除，以免因隨身碟遺失造成個資檔案外洩。

肆、技術管理

一、重要資訊系統主機應做防火牆設定。

二、重要資訊系統應適宜的限制存取 IP。

三、電腦作業系統及相關應用程式之漏洞，應常做修補。資訊系統主機必要時

需定時做弱點掃描，讓主機維持在不易入侵狀態。

四、公務個人電腦應安裝防毒程式並設定自動更新病毒碼及Windows Update。

五、存有個資的個人電腦及伺服器，應設定登入密碼，且其密碼要符合安全之複雜度，至少 6 碼以上，且定期需更換密碼一次。

六、個人電腦應設定螢幕保護密碼，且螢幕保護啟動時間定在 15 分鐘以內。

七、應維持個資存取權限的正確性，且原則上不得共用存取權限，並留意個資被存取的情形。

八、於入侵偵防設備上，設定禁止人員使用點對點(P2P)軟體提供分享檔案。

九、每年執行個資盤點，檢查個資之使用狀況及存取情形。

伍、認知宣導及教育訓練

一、本校應鼓勵教職員工生參與校內外資訊安全與個資保護之教育訓練，並定期宣導個資保護之重要性。

二、每年本校校內至少舉辦 2 場(含)以上的個資保護相關宣導及教育訓練，以養成教職員工生個資保護的警覺性。

三、本校個資窗口負責單位應時常注意個資保護相關知識與訊息，並摘要彙整於「個人資料保護專區」網站，以作為教職員工生獲取個資保護資訊的重要管道。

六、紀錄機制

一、個資交付、傳輸之紀錄

1.以 Email 方式，交付人應保留相關紀錄。

2.系統提供授權人連線下載方式，系統應有連線紀錄可供查閱。

二、確認個人資料正確性及更正紀錄

1.資訊系統設計上應提供個人查核本人的基本資料，並允許做適宜之資料更新，以維持個資正確性。

2.個人以異於上述的其它方式請求更正時，如電話、Email、信函等，處理人員除做必要的查核身份程序外，尚應設法留存事件紀錄。

三、提供當事人行使權利之紀錄

本校「個人資料保護專區」網站中「提供當事人行使權利」應清楚說明，

依據個人資料保護法第三條，當事人得行使之相關權利，例如請求閱覽等，並提供本校個資窗口之詳細連絡資訊，例如連絡電話、Email及郵寄地址。

四、工作人員權限新增、變動及刪除紀錄

人員工作異動時，重要資訊系統負責人應即對系統使用權限重新做設定，並保留相關紀錄。

五、個人資料刪除、廢棄紀錄

執行個資盤點與風險評鑑時，個資保管人應對已超過保留期限的部份，列表記錄後依規定銷毀及確認無誤，如碎紙與刪除電子檔。

六、教育訓練紀錄

1.將取得授權之研習課程講義或簡報檔公告「個人資料保護專區」網站。

2.應保留教育訓練舉辦紀錄。

柒、本措施經資通安全暨個人資料保護宣導及執行小組通過，陳請校長核定後公布實施，修正時亦同。

【附件二之一】

國立東華大學個人資料保護管理制度檢核表

說明：

1.依據本校「個人資料保護管理政策」及「個人資料安全保護管理基本措施」辦理。

2.執行流程：各單位定期自我檢核後，由本校個資窗口單位進行複檢。

一級單位		二級單位	
填表人		填表日	年　　月　　日
e-mail	@mail.ndhu.edu.tw	校內分機	

編號	檢核項目	符合	部分符合	未符合	不適用	**勾選「部分符合」、「未符合」「不適用」**者，請於本欄填寫原因
人員管理						
1	單位是否設置「個資保護聯絡窗口」，協調聯繫個資事宜？					
2	處理個資是否採取權限區隔，非專責處理特定個資者不得具有存取或查閱個資之權限？					
3	處理個資檔案之人員職務異動時，是否列冊移交相關儲存媒體及資料？					
4	處理個資檔案之人員職務異動時，接替人員是否於相關系統重置通行碼，並視需要更換使用者識別帳號？					
5	處理個資檔案之外部人員，是否簽訂保密切結書相關文件？					
6	處理個資檔案之人員離職或合約終止時，是否取消或停用其使用者識別帳號？					
作業管理						
7	單位是否遵循相關法令，進行蒐集、利用或處理進行個資（含特種個資）？					
8	單位向當事人直接蒐集個資時，是否明確說明蒐集單位名稱、目的、個資類別、期間、地區、對象、處理方式、當事人行使權利及方式，以及不提供資料之影響？					
9	單位是否有蒐集、利用或處理特種個資（醫療、基因、性生活、健康檢查、犯罪前科）？					
10	單位是否已針對委外單位，於契約上訂有明確的監督要求，並執行監督？					
11	交換紙本個資時，是否採取彌封或其他具備保密機制之傳遞方式？					
12	交換個資檔案時，是否對資料檔案加密，或是透過加密通道、機制傳送？					
13	個資檔案使用完畢後，是否立即退出應用程式？					
14	是否已具備利用事務機器(例影印機、印表機或傳真機)列印、傳真或使用個資後，應立即取走之安全觀念？					
15	個資檔案處理完畢，是否定期進行銷毀或刪除？					

16	儲存個資檔案之電腦或相關設備如需報廢或移轉他用，是否刪除其內所儲存之個資檔案？					
17	處理個資檔案之應用系統，是否設置使用者帳號及通行碼？					
物理環境管理						
18	是否依據各業務屬性，指定人員負責管理儲存個資檔案之資訊設備與其他相關設施，並檢視、處理其錯誤或異常事件等訊息？					
19	儲存個資之資訊設備是否置放於實體安全的環境（如：具門禁控管、監視設備之 辦公區域或機房）？					
20	儲存個資檔案之紙本或可攜式設備(例 USB、磁碟)等相關儲存媒體，是否置於實體保護之環境？(例具門禁控管、監視設備之辦公區域、上鎖的櫃子)					
21	儲存個資檔案之媒體是否有攜出、拷貝或複製的管控機制？					
技術管理						
22	重要資訊系統主機是否設定防火牆與限制存取IP?					
23	處理個資檔案之個人電腦，是否設置使用者帳號及通行碼？					
24	是否將存放敏感性個資的電腦與外部網路隔絕（如：防火牆）？					
25	處理個資檔案之電腦或相關設備，是否設定電腦螢幕保護程式？					
26	公務個人電腦應安裝防毒程式並設定自動更新病毒碼及Windows Update?					
27	是否已完成個資盤點並建立清冊？					
認知宣導與教育訓練						
28	單位是否已清楚了解單位內有關個資之蒐集、處理、利用之範圍？					
29	單位若有蒐集特種個資，是否清楚了解單位內有關特種個資之用途？					
30	單位是否派員參加個資及資安相關教育課程？					
31	是否已辨識單位保有個資之適法性？					
紀錄機制						
32	交換個資時，是否記錄轉交或傳輸行為之流向？					
33	單位是否有設計個資蒐集目的消失或屆滿之資料刪除程序？					
34	是否針對先前查檢不符合事項進行提出討論並找出原因？					
35	是否針對先前查檢不符合事項進行改善？					
36	是否擬定預防措施，避免先前查檢不符合事項再發生？					
37	是否每年至少一次審視矯正預防落實度與後續改善？					

填表人核章		二級單位主管核章		一級單位主管核章	

<table>
<tr><th colspan="4">以下欄位由圖資中心填寫</th></tr>
<tr><td>檢查
項目</td><td colspan="3"></td></tr>
<tr><td>檢查
結果</td><td colspan="3">檢查結果 □符合 □不符本校要求
不符內容：</td></tr>
<tr><td>檢查
日期</td><td>年　　月　　日</td><td rowspan="2">圖資中心
單位主管核章</td><td rowspan="2"></td></tr>
<tr><td>檢查人
核章</td><td></td></tr>
</table>

LICxxx 1031125

【附件二之二】

國立東華大學委外處理個人資料保護管理制度檢核表

說明：

1.依據本校「個人資料保護管理政策」及「個人資料安全保護管理基本措施」辦理。

2.本表參考自「中興大學契約簽訂後符合個人資料保護法規範檢核表(範本)」，由中興大學授權本校使用，請勿外流。

3.執行流程：受任人(廠商)定期自我檢核後，由本校委任單位進行複檢。

受任人(廠商) 名　稱				填表日	年　　月　　日
填表人姓名		電話		e-mail	

編號	檢核項目	符合	部分符合	未符合	不適用	**勾選「部分符合」、「未符合」「不適用」**者，請於本欄填寫原因
人員管理						
1	處理個資是否採取權限區隔，非專責處理特定個資者不得具有存取或查閱個資之權限？					
2	是否已具備利用事務機器(例影印機、印表機或傳真機)列印、傳真或使用個資後，應立即取走之安全觀念？					
3	處理個資檔案之人員職務異動時，是否列冊移交相關儲存媒體及資料？					
4	處理個資檔案之人員職務異動時，接替人員是否於相關系統重置通行碼，並視需要更換使用者識別帳號？					
5	處理個資檔案之外部人員，是否簽訂保密切結書相關文件？					
6	處理個資檔案之人員離職或合約終止時，是否取消或停用其使用者識別帳號？					
作業管理						
7	受任人(廠商)是否遵守個人資料保護法的相關規定？					
8	受任人（廠商）是否依本校個人資料保護管理制度簽訂「委外廠商保密切結書」？					
9	受任人（廠商）是否依本校所列的或其所指示範圍內蒐集、處理、利用個資？					
10	受任人（廠商）有複委託者，其約定是否一併適用於受託者？					
11	交換紙本個資時，是否採取彌封或其他具備保密機制之傳遞方式？					
12	交換個資檔案時，是否對資料檔案加密，或是透過加密通道、機制傳送？					
13	個資檔案使用完畢後，是否立即退出應用程式？					
14	個資檔案處理完畢，是否定期進行銷毀或刪除？					
15	儲存個資檔案之電腦或相關設備如需報廢或移轉他用，是否刪除其內所儲存之個資檔案？					

16	處理個資檔案之應用系統，是否設置使用者帳號及通行碼？					
17	委外建檔的個資檔案，是否於委外合約中載明所處理之個資保密義務、資訊安全相關責任及違反之罰則？					
物理環境管理						
18	是否依據各業務屬性，指定人員負責管理儲存個資檔案之資訊設備與其他相關設施，並檢視、處理其錯誤或異常事件等訊息？					
19	儲存個資之資訊設備是否置放於實體安全的環境（如：具門禁控管、監視設備之辦公區域或機房）？					
20	儲存個資檔案紙本或可攜式設備(例 USB、磁碟)等相關儲存媒體，是否置於實體保護之環境？(例具門禁控管、監視設備之辦公區域、上鎖的櫃子)					
21	儲存個資檔案之媒體是否有攜出、拷貝或複製的管控機制？					
技術管理						
22	處理個資檔案之個人電腦，是否設置使用者帳號及通行碼？					
23	是否將存放敏感性個資的電腦與外部網路隔絕（如：防火牆）？					
認知						
24	受任人（廠商）是否識別個資所涉及的範圍？					
紀錄機制						
25	交換個資時，是否記錄轉交或傳輸行為之流向？					
26	受任人（廠商）是否有設計個資蒐集目的消失或屆滿之資料刪除程序？					
27	是否針對先前查檢不符合事項進行提出討論並找出原因？					
28	是否針對先前查檢不符合事項進行改善？					
29	是否擬定預防措施，避免先前查檢不符合事項再發生？					
30	受任人與委任人是否於契約終止前，每年至少一次審視矯正預防落實度與後續改善？					

廠商 公司章		負責人 簽章	

以下欄位由東華大學委任單位填寫

檢查項目	
檢查結果	檢查結果 □符合 □不符本校要求 不符內容：

檢查日期		委任單位 二級主管核章	
檢查人核章		委任單位 一級主管核章	

LICxxx 1031125

【附件三】

國立東華大學圖書資訊中心

非法影印教課書之學生輔導機制標準作業處理流程

核定	
日 期	
審核	
日 期	
擬辦	
日 期	

編號：SOP-LIC-6-17

版本：1.00

中華民國　103　年　12　月　　日訂定

國立東華大學
非法影印教課書之學生輔導機制標準作業處理流程
(SOP- LIC-6-17)

一、目的

為保護智慧財產權，落實學生非法影印教科書之學生輔導機制，特訂定此作業處理流程。

二、依據

本校學生獎懲辦法。

三、範圍

本校學生。

四、作業流程說明

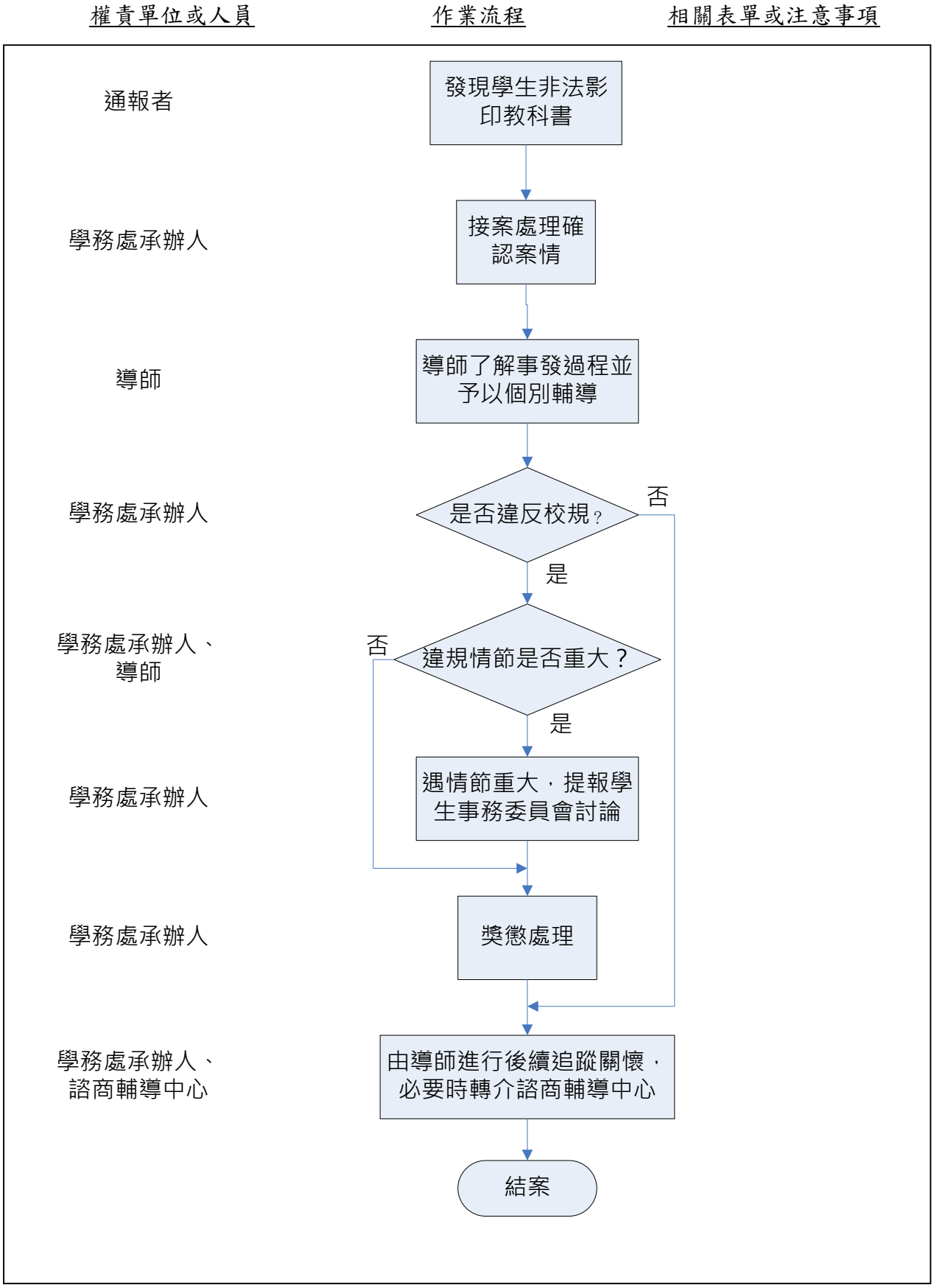
（一） 經發現學生非法影印教科書事件，轉送學務處受理事件通報。

（二） 學務處轉介班級導師、輔導教官了解事發過程並予以個別輔導，並依校規進行懲處。

（三） 遇情節重大或累犯，提報學生事務委員會議討論。

（四） 提報【保護智慧財產權宣導及執行工作小組會議】報告。

五、作業流程圖



非法影印教課書之學生輔導機制標準作業處理流程圖