慈濟大學
個人資料檔案安全維護計畫

中華民國105年11月29日

目　次

壹、製作依據

一、計畫書制定之法律依據

(一)個人資料保護法 104 年 12 月 30 日總統公告修正版本。

(二)個人資料保護法施行細則，法務部於 105 年 3 月 15 日公告施行版。

二、制定參考

(一)教育部私立專科以上學校及私立學術研究機構個人資料檔案安全維護實施辦法。

(二)慈濟大學個人資料保護推動委員會設置要點。

(三)慈濟大學個人資料安全維護辦法

貳、個人資料保護管理政策

一、制定依據

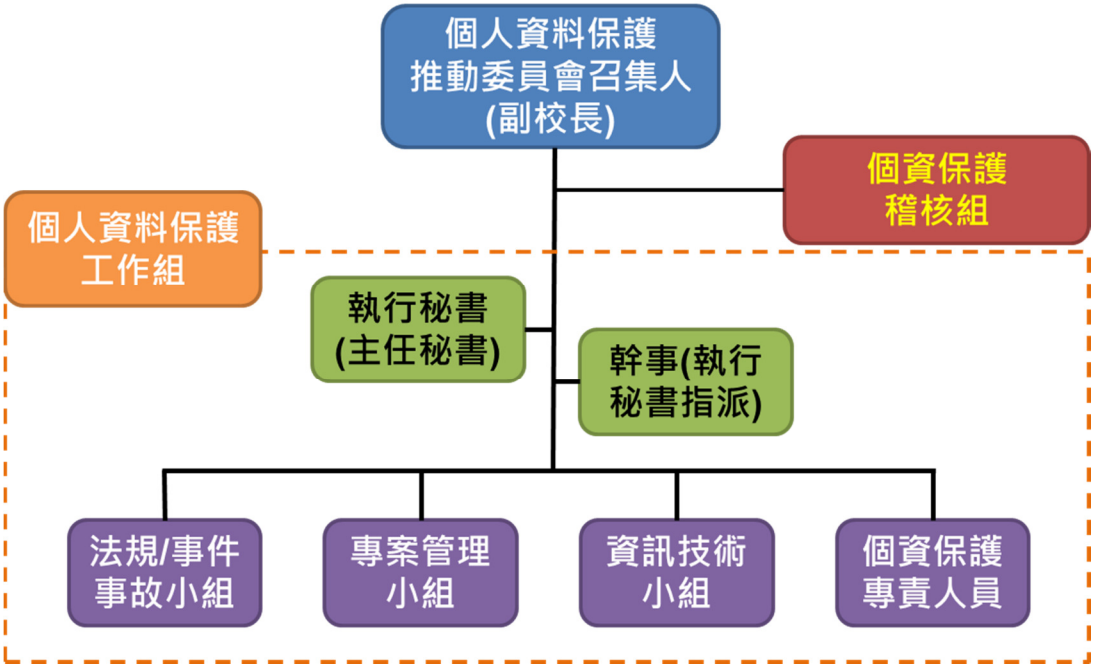
慈濟大學（以下簡稱本校）依個人資料保護法、個人資料保護法施行細則及本校個人資料保護之相關規定，制訂本個人資料保護管理政策(以下簡稱本政策)。

二、個人資料保護推動委員會

本校設立個人資料保護推動委員會(以下簡稱本會)，由校長指派副校長一人擔任召集人，負責督導、召集及主持會議，並由教務長、學生事務長、總務長、研發長、各學院院長、主任秘書、圖書館館長、電子計算機中心主任、人事室主任、會計主任為當然委員，另由校長指定具專業背景之委員一至三人，以及學生會代表二人共同組成，本會委員任期一年，連聘得連任。

主任秘書擔任本會執行秘書兼本校個資保護聯絡窗口。

三、組織架構



各組及角色職責如下：

(一)召集人

1.任命執行秘書及個資保護稽核組組長。

2.提供充分人力及資源確保本會之運作。

3.負責核准本校個資保護管理政策

4.負責核准相關個資管理程序及辦法。

5.確認個人資料管理制度內部稽核結果及改善結果，視必要委任個資保護稽核組組長進行結果確認。

(二)執行秘書

1.於本會設執行秘書一名，負責協助處理本會事務，即個人資料管理作業。

2.管理個人資料檔案安全維護計畫之執行與運作。

3.於委員會議中向召集人報告個人資料檔案安全維護計畫之運作情形，並於委員會議後將個人資料檔案安全維護計畫之運作情形審查會議紀錄陳請召集人核閱

4.規劃個人資料檔案安全維護計畫之執行計畫。

5.審查、更新個人資料管理政策及製作及核可內部規則、表單。

(三)個資保護稽核組

1.負責本校個人資料安全維護計畫之內部稽核作業。

2.規劃稽核計畫、時程及任命執行稽核人員。

3.規劃並負責稽核之教育訓練及稽核作業之執行。

4.向召集人報告稽核結果。

(四)幹事

1.由執行秘書指派個資保護工作組成員之一擔任。

2.協助執行秘書進行本會相關事務及個人資料檔案安全維護計畫之執行與運作。

(五)法規/事件事故小組

1.定期進行個資保護暨資通安全適用法規一覽表更新。

2.協助專案管理小組及資訊技術小組進行案件處理。

3.提供各單位個資保護專責人員法律諮詢。

4.研議並主導個資外洩事件之通報、應變及處理相關作業。

(六)專案管理小組

1.規劃教育訓練計畫及負責執行相關作業

2.追蹤當事人權利行使、申訴諮詢之處理情形。

3.統籌辦理個人資料盤點及風險管理作業，並訓練相關專責人員進行盤點及風險管理之作業。

4.制定個人資料風險管理之相關規範，並進行風險之管制。

5.彙整各單位之風險評估作業結果呈報執行秘書，於年度委員會議時由執行秘書向召集人進行報告。

(七)資訊技術小組

1.依據個資法施行細則第 12 條負責有關相關資訊技術相關之適當安全維護措施。

2.各項資訊諮詢、資訊支援之協助窗口。

(八)各單位個資保護專責人員(同個人資料保護業務聯絡人)

1.負責於各單位推行本個人資料檔案安全維護計畫並管理單位內之個人資料。

2.確認所屬單位內部個人資料檔案安全維護計畫之運作情形及紀錄。

3.擔任單位內當事人權利之窗口，並將結果回報給專案管理小組。

4.協同處理個資外洩之通報、應變及處理作業程序。

參、組織成員說明

個人資料保護推動委員會及各組成員之名單請詳見附件一。

一、政策之制訂與管理

(一)政策之制定

本校之政策制定經本會審議，陳請校長核定後，公布實施。

(二)政策之執行

本政策公布實施後，所有本校與個人資料保護相關之作業，均應遵循本政策。

本政策之執行由個資保護工作組進行規劃，並由各單位個資保護專責人員協助政策之推行。

個資保護稽核組應定期進行對於政策遵循的查核，以確保政策之執行成效。

(三)政策修改與調整

本會應於每年或於個人資料保護法相關法規、主管機關規定有重大變化後審視及修訂本政策，以確保本政策之適用性。

二、政策內容

為確保本校對於個人資料管理作業符合個人資料保護法之規定，並確保當事人隱私及相關權益，訂定此個人資料保護管理政策，本校所有人員於執行與個人資料相關之業務時均應遵循此政策。

(一)本校將遵守個人資料保護法相關法令及本校所訂定之其他有關法令規範。。

(二)本校將訂定個人資料保護管理相關之規範、作業準則以落實執行個人資料保護管理，並透過定期檢查、內部稽核或檢視之方式，持續改善之。

(三)本校於建置個人資料保護管理制度後，將公告全體人員周知以落實執行運作。

(四)本校於告知事項中將明示以下內容：本校將於利用目的範圍內，蒐集、處理及利用當事人所提供之個人資料，並於不逾越當事人提供個人資料之利用目的必要範圍內為處理、利用行為，亦將採取適切之個人資料保護措施。

(五)為維護當事人所提供之個人資料為正確且最新之狀態，將採取適切措施預防個人資料的被竊取、洩漏、竄改等侵害。並提升本校資訊安全相關措施以保護所蒐集、處理以及利用之個人資料，同時持續改善內部所建置之個人資料管理制度。於確認發生個資外洩事故時，將迅速採取緊急應變措施作為，並將事實通知當事人。

(六)本校於當事人提出有關其提供個人資料之查閱、複製、更正、刪除等之申請時，將依個資保護法之相關規定確實、迅速回應之。

(七)本校個人資料之保存應符合法律及本校業務需求之期間，並確保個資的保存達到法定要求之最小期限。

肆、適用法規盤點程序

一、執行目的

個人資料保護法及相關配套法令因社會變遷及實際實行狀況將陸續進行修訂或增補，各目的事業主管機關或政府單位亦將陸續針對個人資料保護法提出規範或指引做法，本校為確保所有執行之作業均能遵循法令規範及確保當事人個人資料之權益，特訂定此程序。

二、執行人員

由法規/事件事故小組進行法規之蒐集及彙整清冊。

三、法規盤點

本校應於個人資料保護法及其他相關法律規定後，應以適當方式要求所有人員確實遵守。

四、檢視修訂法令及其他規範

法規/事件事故小組為維持個人資料保護法及其他相關法令規範為最新之狀態，應定期檢視或於法律修訂公告後進行法規之更新狀況檢查。於本校校務行政作業項目、範圍有新增變動時，亦必須重新檢視法規盤點清冊之內容。

五、調查法令及其他規範

各單位之個資保護專責人員應針對其單位內之業務與個人資料保護相關法令及規範進行調查，並將調查結果彙整交予法規/事件事故小組。

六、登載法令及其他規範

法規/事件事故小組於執行秘書/召集人裁示後，應將結果更新於「個資保護暨資通安全適用法規一覽表」中並提供於本校各單位知悉，格式如附件二。

七、公告周知

各單位個資保護專責人員於收到個人資料保護法及其他規範內容後，應向該單位人員宣導及公告周知。

伍、個人資料作業管理程序

一、個人資料蒐集管理

(一)個人資料新蒐集前應檢查蒐集合法性並由各業務承辦人員填具「新個資蒐集前查檢表」經各單位個資保護專責人員核准後，呈報單位權責主管及委員會，並於一個月內更新個人資料盤點表。

(二)本校各單位個資保護專責人員應進行蒐集作業之監督，確保所有蒐集的作業均符合「新個資蒐集前查檢表」之蒐集方式及符合個人資料保護法之規定。

(三)「新個資蒐集前查檢表」使用之表單如附件三。

二、個人資料處理及利用管理

(一)間接蒐集個人資料前應特別注意其資料來源之合法性，本校不得處理或利用未確認合法性來源之個人資料。

(二)本校各單位個資保護專責人員應確認所處理之資料均符合「新個資蒐集前查檢表」中的資料項目，如果蒐集內容有超出或差異的部分，應向權責主管及執行秘書反應，並於改善後進行處理作業。

(三)在個人資料處理及利用過程如發現處理不合於個人資料保護法蒐集要件所取得之個人資料，或不合於特定目的之處理作業，應立即停止該資料之處理及利用，並呈報權責主管及執行秘書且須提出對於該資料的刪除及後續矯正作業。

(四)個人資料新利用作業前，包含本校因校務行政作業需要(校內校務行政作業需求、受主管機關委託、契約及國家法律)，需使用本校既有保管及持有之個人資料，利用前應檢查利用之合法性並由各業務承辦人員填具「個人資料利用前申請書」之表單如附件四，申請書經各單位個資保護專責人員核准後，陳報權責主管及執行秘書審查。

(五)本校各業務單位及權責主管應對個人資料利用的行為超出範圍時，應予以糾正，並提出矯正計畫避免事件再次發生。

(六)個人資料之保管人或使用人調離職務時,應將所保管個人資料(檔案/紙本)交付權責主管或指定之交接人員，並副知執行秘書備查。

(七)個人資料於處理及利用過程中應注意確保其正確性及完整性。

三、個人資料保存管理

(一)各單位個資保護專責人員應負責查詢相關法律對於資料保存最小年限及最長年限之要求。

(二)個人資料及蒐集相關告知及同意證據之紙本及電子資料，如無其他法令限制，應至少保存五年；電子形式軌跡資料(含應用系統及資料庫之軌跡資料、網路設備之異常軌跡資料等)，如無其他法令限制，應至少保存十年，以確保相關證據於個資法損害賠償請求權時效內均能完整提出。

(三)與告知事項之蒐集目的有合理的關聯，並在特定目的消失後主動或依當事人請求進行刪除。

四、特種個人資料之蒐集、處理、利用限制

本校有關病歷、醫療、基因、性生活、健康檢查、犯罪前科等特種個人資料，非有法令規定，不得蒐集。

如需蒐集特種個人資料，各單位業務承辦人員應於經權責主管核准後向專案管理小組提出，由執行秘書核決後，依本文件伍、**個人資料作業管理程序**之規範進行。

五、個人資料封裝及傳遞

(一)個人資料實體形式封裝應由各單位承辦人員封裝於傳遞信封內，外觀上不得標示其他足以顯示個人資料內容之註記。

(二)個人資料於傳遞前應填寫簽收紀錄，並記錄相關傳遞細節以供日後查閱。

(三)個人資料實體形式之傳遞，應依規定進行密件處理。

(四)個人資料之電子形式傳遞，應加密後傳送。

六、個人資料銷毀管理

(一)為防範個資文件外流及配合政府環保資源再生政策，個人資料若有超過保存期限，不予保留而須進行銷毀時，應由業務承辦人員填寫「銷毀申請單」，經權責主管核准後，進行銷毀。

(二)送至本校以外銷毀之實體形式資料，須派專人參與運送並全程監督銷毀過程，留存相關紀錄並附於「銷毀申請單」以供備查。

(三)「銷毀申請單」應由專案管理小組統一保管並永久保存。

(四)「銷毀申請單」請詳附件十二。

七、個人資料委外蒐集、處理、利用管理

(一)本校如需委由委外單位進行蒐集、處理、利用作業，應於委外事項進行前與該受委託單位進行委外作業的簽約。

(二)本校應依個人資料保護法相關規定對於個人資料委外作業進行監督。

(三)本校應要求受委託單位，定期或於需要時針對提供受委託之個人資料業務執行報告，並將報告呈報權責主管及副知執行秘書。

(四)本校應定期或於需要時針對受委託單位進行稽核，以確保所有的個人資料委託處理之作業均符合本校之要求。

(五)委外作業結束，本校各業務單位應監督受委託單位返還或銷毀本校已交付之個人資料，以確保個人資料之委外作業安全。

詳細之作業流程依本文件**陸、個人資料委外管理程序**之規範進行。

八、個人資料事故通報

本校人員發現個人資料疑似洩露、遺失或遭竄改等異常現象，應立即通報單位個資保護專責人員及法規/事件事故小組。

陸、個人資料委外管理程序

依據個資法施行細則第 8 條,本校於執行委外作業時應依本程序進行確認,並於委外過程中善盡監督之責任，委外作業應包括以下事項:

一、確認項目

(一)確認受委託者知悉蒐集、處理或利用個人資料之範圍、類別、特定目的及其期間。

1.委外業務承辦人員應以合約條款或書面確認方式，確認受委託者知悉本校委託蒐集、處理或利用之個人資料

(1)範圍：本次委託作業中包含蒐集、處理、或利用那些個人資料項目。(如:姓名、電話、地址、身分證字號等)

(2)類別：本次委託作業中包含蒐集、處理、或利用那些個人資料類別。(參考個資法法定類別列表)

(3)特定目的：本次委託作業中蒐集的特定目的，或於委託處理、利用時告知本校原蒐集個資的特定目的。(用於規範受託單位於蒐集、處理、利用個人資料時不超出特定目的)

(4)期間：委託蒐集、處理、利用個資的期間。(此期間可能小於整體委託契約之契約有效期間)

2.本校所涉及個人資料蒐集、處理、利用之委外作業，如需簽訂合約時，均須經由個資保護工作組確認其合約項目是否符合本委外管理程序要求，並經執行秘書確認後始得進行該委外作業。

(二)應填具相關表單

1.本校委外業務承辦人員，在交付個人資料時，應填具「個人資料交付表」(附件十三)並經全責主管審核後，始得提供。

2.受委託單位，於接收個人資料時，應填具「個人資料接收表」(附

件十四)，並填寫收受人。

二、確認受委託者就第十二條第二項應採取之必要措施

委外業務承辦人員應於受委託者接觸本校個人資料或開始進行個人資料蒐集前，確認該受委託者已採取適當安全之必要措施:

(一)於合約中載明要求受委託者應依據個資法施行細則第 12 條第 2 項進行適當之安全維護措施，以及下列項目：

1.本校對於受委託者之適當安全維護措施具體要求或條件。

2.適當安全維護措施定期檢核的頻率及方式(方式可能為要求受委託者定期繳交報表)。

3.如無法通過本校對於受委託者的適當安全維護檢核，本校有權解除委外合約，受委託者並應賠償本校因此產生之損失。

4.如需要,本校得進行受委託者之稽核作業或委由第三方進行稽核,以確保受委託者已進行適當安全維護措施，受委託者不得拒絕，並應支付稽核作業所需之費用。

(二)於受委託者開始進行作業前確認已實施適當安全維護措施之證明，建議該證明為(選擇其中一項即可)

1.各項要求之受委託者已執行之證據（程序書、執行紀錄等)。

2.第三方公正單位出具之證明。(如:ISO 27001、BS10012 證照等)

3.本校進行受委託者稽核之結果。

4.其他足資證明之文件。

以上之證明，應於受委託者開始進行作業前，由委外作業承辦人員蒐集並留存紀錄，該證據並應經過專案管理小組進行確認，必要時得請求電算中心行技術性確認。

(三)委外合約中應載明定期檢查適當安全維護措施之頻率及方式，並依其方式定期檢查並留下紀錄，合約中並應載明，無法通過本校檢核該適當安全維護措施者，本校可依規定立即終止或解除該委外合約。

(四)如受委託者未能通過本校對於適當安全維護措施之檢核，應

1.於合約簽訂前，應暫緩該合約之簽訂。

2.於合約簽訂後，委外作業開始執行前，應暫停該作業之啟動，並要求受委託者提出改善的時程及方式，如無法達成，應依合約條款逕行解約。

3.於合約簽訂後，委外業務執行中，應要求受委託者暫停該作業之執行，要求受委託者提出改善作業及矯正預防計畫，並依據合約條款進行相關作業因暫停而遲延之賠償。

(五)外部稽核作業

如需要進行外部稽核以確認受委託者已進行適當安全維護措施，本校應注意

1.應由個資保護稽核組組成稽核小組，人員得包括

(1)本校各單位個資保護專責人員

(2)本校法律顧問人員

(3)本校資訊技術人員或外部技術人員

2.應建立稽核計畫,稽核查檢表設定內部對於通過稽核之標準條件，並於稽核前通知受委託者以確保受委託者做好受稽核準備。

3.於稽核時應紀錄稽核發現之不符合項目，並做成稽核紀錄，該紀錄並應經過受委託者之負責人簽署確認。

4.如發現不符合事項，應要求受委託者提出矯正預防措施，並提出改善計畫及時程，必要時，得再次到現場進行稽核。

5.所有受委託者之矯正預防措施、改善計畫應取得個資保護稽核組之確認後結案。

三、規範複委託者，其約定之受託者

本校禁止受委託者進行再轉包給複委託對象，但如為分包之複委託情形時，應事先取得委外作業承辦單位個資保護專責人員、權責主管及專案管理小組確認。並執行以下項目

(一)於合約載明本委託案件不得再轉包，如需分包時，需取得本校之事前書面同意，同意該複委託對象。

(二)應要求受複委託者，執行同於本校要求受委託者之所有條件，並要求受委託者協助本校對於該複委託對象所需之衍生監督義務，並支付其衍生之費用。

四、違反通知

確認受委託者或其受僱人違反個資法、其他個人資料保護法律，或其法規命令時，應向本校通知之事項及採行之補救措施。

根據個人資料保護法第 12 條，本校於發生個資事故時須於查明後通知當事人，如受委託者或其受僱人違反個資法或相關法令，或本校之委託合約時，應規範受委託者向本校通知及採行補救措施包括:

(一)應於委外合約中載明

1.受委託者及其所有與本校委外業務相關人員均應接受個人資料保護法及相關法令之訓練，以及了解本校委外業務之要求。業務承辦人應定期確認所有受委託者人員狀態，以確保所有人員均知悉法令及本校委外合約之規定或需求。

2.要求受委託者訂定於違反個資法法令及本校委外合約時之處理程序，該程序必須包括：

(1)受委託者處理專責人員指派。

(2)應於事故發生後 24 小時內通知本校業務承辦人員。

(3)預擬補救措施之執行方式、資源及人力。

(4)於事故處理完畢前，定期通知事故處理進度的頻率及方式。

3.如受委託者發生個人資料違法或違反本校合約條款之事故，本校得於事故處理完畢後即終止合約，未完成部份，另覓廠商完成。如受委託者無能力或因受委託者之故未能進行補救措施者，本校得將委託其他單位進行該補救措施，受委託者並應支付該衍生之費用。

五、本校如對受委託者有保留指示者，監督保留指示之事項

(一)應於委外合約中要求

1.明確載明本校對於受委託者之保留指示事項。

2.要求受委託者定期回報本校要求保留指示之事項辦理狀況。

3.要求受委託者以書面方式或其他本校事前同意方式取得本校對於保留指示事項之同意，並留存相關紀錄。

(二)留存相關受委託者請求指示及本校指示紀錄。

(三)定期或不定期對於受保留指示事項辦理狀況進行抽檢或稽核。

六、委託關係終止或解除

委託關係終止或解除時，個人資料載體之返還，及受託者履行委託契約以儲存方式而持有之個人資料之刪除。

本校委外作業承辦人員應進行：

(一)於合約中載明

1.受委託者應維持接受本校個人資料之個人資料交付清冊，內容應包括，

(1)個人資料的內容說明，個人資料項目、範圍及數量。

(2)使用之載體及交付之方式。

(3)日期、時間。

(4)本校交付人員及受委託者之收受人。

(5)相關交付及接受之證明(例如簽名、簽收單據等)。

(6)受委託者對於該交付資料的後續處理方式說明(包括複製、儲存、轉換等作業及可能產生之資料軌跡)

2.受委託者應定期清查並更新該資料清冊，確保其內容為最新，並定期交付給本校委外業務承辦人員。

3.於合約終止或到期前一個月，應依據個人資料交付清冊訂定個人資料刪除之計畫，並取得本校委外作業承辦人員之同意。

4.於合約終止或到期時交付個人資料刪除之清冊，其中包括，

(1)原接收清冊之編號、範圍、項目及數量。

(2)受委託者儲存的方式及數量清查結果。

(3)受委託者進行的刪除方式及其刪除結果。

5.要求受委託者於刪除後提供由該組織簽署之切結書，切結受委託者未留存本校交付之個人資料以及載明違反切結事項所應承擔之賠償責任，並經由本校同意該切結內容。

6.如受委託者因合理之理由而無法刪除或需保留本校所交付之個人資料，應向本校委外作業承辦人提具申請及未刪除個資清冊、保留時間及方式，於取得本校核准後留存及進行後續合約解約、終止作業。

七、監督之方式

(一)委外業務承辦人應於合約簽署前，確認以下監督方式

1.監督定期查核的頻率。

2.監督的方式，以下為建議的監督方式

(1)要求受委託者於每月(或其他頻率)繳交服務報告書內容時，交付個人資料安全維護狀況說明文件，其中包括本程序內之各項要求內容及異常或例外狀況說明。

(2)由本校人員定期進行文件、遠端或現場查核方式進行監督作業並留存紀錄。

3.監督之紀錄

委外業務承辦人員應定義監督記錄的方式、內容要項及其保存方式。

(1)監督之管理

A.應定義執行監督之人員及其角色、權責。

B.監督人員於發現不符合事項後之處理方式。

柒、申訴及當事人權利行使管理程序

一、申訴及當事人權利請求作業流程說明

(一)當事人對本校個資之申訴作業

1.申訴受理及作業流程說明

(1)受理申訴申請管道

A.當事人透過書面投書至本單位或本校郵寄信箱。

B.當事人透過 E-mail 至本校信箱。

C.當事人透過主管機關或其他單位進行申訴(函轉)。

(2)要求當事人進行表格填寫

A.請當事人上網下載申訴表單。

B.現場領取申訴表單。

(3)受理作業

專案管理小組受理該申訴申請單後，應進行紀錄管制，並視需求函覆申訴人或函轉單位。

(4)查明主辦業務單位

由專案管理小組判斷該案件之主辦業務單位，並將申訴案件移送該主辦業務單位，由主辦業務單位進行處理。

(5)主辦業務單位進行申訴案件處理作業

A.主辦業務單位或委員會應組成調查/稽核小組，其人員得包括

a.本校法律專業或法律顧問人員。

b.單位個資保護專責人員。

c.視調查/稽核所需，得會同電信、資訊、法律專業人員加入調查/稽核小組。

B.進行調查作業

a.調查/稽核小組於進行調查時需取得召集人/執行秘書之同意，進入檢查，並得命相關人員為必要之說明、配合措施或提供相關證明資料。

b.調查/稽核時，對於可為證據之個人資料或其檔案，得扣留或複製之。對於應扣留或複製之物，得要求其所有人、持有人或保管人提出或交付。

c.調查/稽核小組之人員，因檢查而知悉他人資料者，負保密義務。

C.調查結果及處分

a.相關作業單位如有違反個資法規定之情事者，調查/稽核小組應呈報執行秘書/委員會得進行下列處分：

- 要求該單位立即停止蒐集、處理或利用個人資料。
- 要求刪除經處理之個人資料檔案。
- 要求銷毀違法蒐集之個人資料。

b.調查/稽核小組進行處分時，應於防制違反個資法規定情事之必要範圍內，採取對該主辦業務單位損害最少之方法為之。

D.調查報告及申訴結果

a.調查/稽核小組應進行相關調查報告之產出。

b.調查/稽核小組應進行相關處分之決定。

c.回覆

E.申訴結果回覆

由專案管理小組於主辦單位進行申訴處理作業回覆後函覆申訴人，並副知委員會。

(二)本校個資作業當事人權利請求作業流程

1.權利請求申請

專案管理小組及各單位之個資保護專責人員負責個人權利請求申請，本校人員接受到相關請求，由各單位個資保護專責人員確認後，進行相關權利申請之受理作業

2.回應請求申請

各單位個資保護專責人員於收受個人資料當事人行使權利申請作業後，依個人資料保護法之要求，迅速回應當事人之申請。

3.當事人權利

依個資法第 3 條之規定，當事人就以下事項，可向本校行使其權利:

(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

4.當事人請求行使查詢或請求閱覽時，若有下列情形之一者，本校

可拒絕當事人行使權利之申請：

(1)妨害國家安全、外交及軍事機密、整體經濟利益或其他國家重大利益

(2)妨害公務機關執行法定職務

(3)妨害本校或第三人之重大利益

5.當事人權利行使之程序

(1)以各單位個資保護專責人員為當事人權利行使之負責窗口。

(2)當事人行使個資法第 3 條之權利時，應由當事人本人填寫「個人資料權利行使申請書」及出示身份證明文件向本校提出申請，若委託法定代理人代為申請時，除檢具申請書外，尚須提出委託之授權書。

6.當事人權利行使時時應檢具之文件

(1)對本校行使當事人權利時應檢具下列文件

A.當事人本人提出申請者

a.個人資料權利行使申請書

b.當事人須出示其身分證、健保卡、護照、駕照、居留證或其他足資證明身分之證件以供查驗。

B.受託之法定代理人提出申請

a.受託人須出示其身分證、健保卡、護照、駕照、居留證或其他足資證明身分之證件以供查驗。

b.當事人權利行使申請書以及授權書，授權書必須經當事人親筆簽名。

(2)當事人查詢資料應檢具真實文件並據實填寫相關資料,如有虛偽不實者，本校得拒絕其查詢。

7.當事人權利行使之回覆

各單位個資保護專責人員經審核確認當事人或其法定代理人符合上述資格規定之要件後，應就本校所保存之現有個人資料進行查詢，並以書面將當事人權利行使之結果回覆當事人，並由各單位個資保護專責人員自行保存之。

8.處理期間

(1)本校受理當事人行使查詢、閱覽、製給複製本之申請後，應於十五日內處理；必要時得延長十五日，並應將其原因以書面通知客戶；如駁回當事人之申請時並附駁回之原因。

(2)本校受理當事人行使更正補充、刪除、停止處理利用申請後，應於受理日起三十日內回覆結果，必要時，得予延長，延長之期間不得逾三十日，並應將其原因以書面通知請求人；如駁回當事人之申請時並附駁回之原因。

9.成本費用

對於查詢、閱覽、製給複製本個人資料之申請，本校得酌收成本費用。相關收費標準如本校未有訂定者，將參照政府資訊公開法之政府資訊重製或複製收費標準計算之。

10.個人資料權利行使申請書，詳見附件五

捌、個人資料之風險評估及管理機制

一、個人資料盤點作業

(一)個人資料分類分級

本校之個人資料依照其屬性、種類、數量、格式及保存方式進行分級

1.屬性

(1)特種個資：個資法第 6 條所規範之個資包括：病歷、醫療、基因、性生活、健康檢查及犯罪前科之個人資料。此類個資為特種個資，本校僅於以下狀況始得蒐集，且蒐集時必須依據個資法規定實施適當安全維護措施：

A.法律明文規定。

B.公務機關執行法定職務或非公務機關履行法定義務必要範圍內，且事前或事後有適當安全維護措施。

C.當事人自行公開或其他已合法公開之個人資料。

D.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，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。

E.為協助公務機關執行法定職務或非公務機關履行法定義務必要範圍內，且事前或事後有適當安全維護措施。

F.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。

(2)一般個人資料：依據個資法第 2 條所規定，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。

2.種類

依據本校之個人資料特性，將本校之個人資料種類區分為

(1)學生個資：因本校業務蒐集、處理、利用之學生個人資料，包括特種或一般個資。

(2)廠商個資：因與本校有業務(採購、承包....)往來或承接本校委外業務而交付之廠商員工或個人之聯絡資訊，此類個資可能為本校直接向當事人蒐集或廠商間接交付之各類資料，包括個人聯絡資訊、個人財務資訊等等。

(3)教職員資訊：包括本校人事單位依法蒐集之正式員工、約聘僱人員等之教職員資訊，其中包含學校各單位不同方式聘用之人事資料包括卓越計畫、國科會計畫等。

(4)其他個資：無法歸類於前三種個人資料之種類。

3.數量

依據本校之作業特性將個人資料之數量進行分級

(1)大量個資：個人資料數量 10,001 筆以上。

(2)中量個資：個人資料數量介於 1,001 筆-10,000 筆。

(3)小量個資：個人資料數量 1,000 筆以上。

4.蒐集個人資料範圍(欄位)

依據本校之作業特性將蒐集個人資料範圍(欄位)進行分級

資料衝擊	資料欄位

低衝擊欄位	1. 僅單一個人資料欄位 (如：姓名、學號等) 或 2. 與學校產生的資料(學號、員編、分機、職稱等等)相連 或 3. 從公開資訊取得 4. 若遭洩露不會對當事人造成衝擊
中衝擊欄位	1. 兩種以上個人資料欄位組合(如：姓名及電話) 或 2. 若遭洩露可能會對當事人造成衝擊
高衝擊欄位	1. 個人詳細學籍資料 或 2. 高敏感個人資料(如：身份證字號、護照號碼、銀行帳號、完整個人資料、敏感性的協商內容、宗教或信仰) 或 3. 特種個人資料(病歷、醫療、基因、性生活、健康檢查、犯罪前科) 或 4. 資料外洩將造成個人身心受到危害、社會地位受到損害、或衍生財物損失，對當事人造成嚴重衝擊

5.格式

本校之個人資料可歸類為以下格式，但注意部分個人資料於處理過程中包含多種個資格式。

(1)書面/紙本格式：包括一般書表、單據、手寫稿...等。

(2)電子文件格式/檔案格式：包括網頁、email、電子公文、Office 軟體之檔案、PDF 檔案、備份檔案或暫存檔、郵件附件等。

(3)資料庫格式：存放於資料庫主機內之資料。
(資料庫之備份檔案屬於檔案格式)。

6.保存方式

依據個人資料的存放及保存方式，本校個人資料之保存方式可分為：

保存方式	書面/紙本	電子文件/檔案 (郵件、公文、WORD、EXCEL)	資料庫
高安全保存	1. 上鎖 且 專人保管鑰匙	1.已依據職責區分存取權限且無法進行變更 或 2. 個資檔案文件已加上密碼保護，密碼長度六碼以上	1. 僅有系統管理者可存取
中安全保存	1. 具基本防護遮蔽或 2. 集中存放 或 3. 專人管理	1. 使用者皆有獨立帳號密碼 或 2. 個資檔案文件已加上密碼保護，但密碼未達六碼 或 3. 具存取控制	1. 獨立帳號密碼 且已區分權限
低安全保存	1. 未有管理	1. 具敏感性個資檔案文件未加上密碼保護 或 2. 未有任何存取管制措施 或 3. 共用帳號	1. 未有任何存取措施或 2. 共用帳號

二、風險評估作業

(一)由各單位個資保護專責人員於個資盤點作業後進行風險評估作業。

(二)風險評估作業，依據本章第一點之分類方式進行對於個人資料檔案之風險評估作業。

1.風險分級表

衝擊性 保存方式	低(1)	中(3)	高(5)
高安全保存(1)	低風險(1)	低風險(3)	低風險(5)
中安全保存(3)	低風險(3)	中風險(9)	高風險(15)
低安全保存(5)	低風險(5)	高風險(15)	高風險(25)

風險評估作業評估結果為高風險者，應提出風險處理計畫/辦法，風險評估結果為中度風險者，應視可改善的方式提出改善建議。低風險者，可以免為進行改善或風險處理計畫。

三、資料外部傳遞之合法性及安全性

針對有將個人資料往外部單位(如主管機關、進行傳遞之作業，需進行合法性及安全性之評估，評估原則如下：

傳遞安全性	**評估原則**
高安全傳遞	1. 依據個資法第 8 條或第 9 條於告知函中之敘明相關利用對象及方式（包含外部單位及其再利用之對象)後，並已做好如下之傳送安全措施： a. 實體個資檔案傳送時有彌封後透過專人傳遞，並可確認已確實送達對象（如掛號、快遞）或 b. 電子個資檔案若有含中、高衝擊之個資欄位需加上密碼後再行傳遞，密碼另行提供；若僅含低衝擊各資欄位則可直接傳遞不需加上密碼。 2. 或 未有外部傳送。
中安全傳遞	依據個資法第 8 條或第 9 條於告知函中之敘明相關利用對象及方式（包含外部單位及其再利用之對象)後，但未執行安全措施或措施不完善，如： 1. 實體個資檔案傳送時有彌封後傳遞，未確認已送達該對象 或 2. 有含中、高衝擊之個資欄位的電子個資檔案，已加密碼後再行傳遞，密碼於同封郵件中提供
低安全傳遞	1. 未依據個資法第 8 條或第 9 條進行告知 或 2. 告知事項不完整

四、風險管理作業

由前段風險評估作業所評定之個人資料風險，應包括以下作業：

(一)風險評估作業執行

1.執行負責：各單位個資保護專責人員負責彙整該單位所有風險評估作業結果。

2.彙整作業：由專案管理小組進行相關風險評估及風險處理計畫之彙整。

3.整體核定：由執行秘書進行計畫之審查後向召集人報告並核定。

(二)風險改善及處理

1.風險評估作業評估結果為高風險者,應提出風險處理計畫/辦法，並由單位權責主管進行核准該風險處理計畫能將該資產之風險有效控制至低或中度風險。

2.風險評估結果為中度風險者，應視可改善的方式提出改善建議。由各單位之個資保護專責人員進行評估。

3.低風險者，可以免為進行改善或風險處理計畫。

4.各單位之風險評估結果應交由專案管理小組進行全校之風險評估，並由召集人或執行秘書進行全局之風險管理作業之核定，確保所有個人資料檔案風險均有改善措施或處理計畫。

(三)風險可接受等級：本校之風險可接受等級為中風險。

(四)風險處理計畫，其中應包括風險處理計畫說明，執行人員，預計完成日期及所需資源，處理後的風險預估值，所有高風險值應控制之中或低風險。

(五)風險改善管控作業，應由單位主管核准相關計畫後，由專案管理小

組人員進行後續控管作業，確保所有改善及風險處理計畫均已依原計畫有效完成控制個人資料之風險。

(六)與資訊安全管理系統之整合

個資風險中如為資安風險之考量，因本校已實施資訊安全管理系統，應轉交由資訊安全管理系統之資訊安全保護管理小組針對該資產或系統進行相關風險管控。

(七)整體風險評估結果與風險處理計畫應於風險評估作業完成後，由執行秘書向召集人進行報告。

(八)風險管理表單：風險評估處理計畫(如附件七)。

玖、事故之預防、通報及應變機制

由於本校已建置資訊安全管理系統(ISMS 系統)，於資安或個資事故發生時，將先行判定是否為與資訊系統資訊安全無關之事件，例如人員誤用、洩漏個資等，如果屬於與資訊系統相關之個資/資安事件，將由本校之資訊安全事故處理流程進行流程。

一、判定方式

發現事件之人員應儘速將事件內容依據 ISMS 資訊安全管理系統之通報流程通報資訊安全執行秘書及個人資料保護推動委員會之執行秘書，依 ISMS 資安事故程序進行判定後決定是否為資安事件，如判定結果為

(一)資訊安全事故：交由本校資訊技術小組依據 ISMS 之異常事件處理作業說明書進行處理，並於事故處理完畢後呈報執行秘書。

(二)非與資訊系統相關之個資事故：依據本章之事故應變機制進行應變。

二、個人資料事故處理流程(非與資訊系統相關)

(一)疑似期：與此階段查證引起個人資料事件之原因並做成相關報告。

1.本校各業務單位應由個資保護專責人員查證引起個人資料事件之原因並做成相關報告，呈報權責主管及副知執行秘書。

2.若為資訊系統面之事件由本校之資訊安全管理系統資安事故流程辦理。

(二)處理黃金期

1.本校各業務單位分析案由提交權責主管及執行秘書，並呈報召集人。

2.由法規/事件事故小組蒐集相關證據並與本校秘書室及本校法律

顧問討論可能之法律責任。

3.由法規/事件事故小組及發生事故單位個資保護專責人員就事故之範圍擬定事故通知之當事人及相關單位。

4.如事故涉及跨一個單位以上時，應由法規/事件事故小組為單一聯絡窗口，整合各單位之個資保護專責人員進行後續之事故處理及通知當事人。

5.由本會召集本校相關單位及本校法律顧問與當事人召開事故協調會避免事件擴大。

(三)事故擴大期

1.由本校個人資料保護推動委員會及本校法律顧問組成事故說明小組向外說明，其對外發言部分得由召集人指定，並應同時要求本校相關同仁不得自行針對此事故進行發言。

2.由本校法規/事件事故小組、秘書室及本校法律顧問共同擬定訴訟策略。

(四)司法訴訟

由法規/事件事故小組、秘書室及本校法律顧問共同擬定訴訟策略、進行訴訟或尋求事故和解之可能性。

三、個人資料事故通報管理

本校個人資料事故通報流程，

(一)內部通報流程

本校所有人員發現疑似資安或個資事故現象，應立即通報各單位之個資保護專責人員。

(二)外部通報流程

當事人如果透過申訴管道向法規/事件事故小組通報相關疑似資安或個資事故，法規/事件事故小組於判定為疑似事故時應立即通知該單位個資保護專責人員。

(三)事故之紀錄與處理

各單位個資保護專責人員接收到相關通報，應記錄事故通報內容，並依本章之事故處理程序進行處理。

四、個人資料之事故懲處管理

委員會查明相關人員疏失之責任歸屬後，視情節之輕重為適當之處理。

壹拾、資料安全管理及人員管理

本校之資料安全管理措施要求共分為四大類安全措施，全校各單位個資保護專責人員應進行該單位內之資料安全管理措施之推行，並視需求回報執行秘書執行狀況及資源需求。

一、資料安全防護措施

(一)蒐集作業安全防護措施

1.紙本蒐集方式：以紙本方式進行個人資料之蒐集，應進行以下之防護措施

(1)紙本之個人資料蒐集，應進行實體存取之防護(例如鎖於檔案櫃內)

A.一般等級：僅含系級、姓名、學號之資料，不須特別標示。

B.敏感等級：內含特種個資或高風險資料、含身分證之敏感性資料，僅限授權人員存取使用。

C.機密等級：完整的個人資料檔案及學籍檔案。

(2)敏感等級請用黃色卷宗保存；機密等級請用紅色卷宗並存放於上鎖檔案櫃內保存。

(3)須依據法規盤點及個資盤點結果之保存年限要求進行保存。

2.媒體蒐集方式：透過媒體(CD/DVD/TAPE/行動碟等)接收個人資料檔案需進行以下防護

(1)如收送媒體時，應建立清單進行數量管制。

(2)媒體應明確標示媒體內儲存之內容。

(3)媒體應進行實體存取之防護。

(4)媒體資料輸入資訊系統後，應視其需求進行保存，如不須保存該媒體，應進行必要之清除。

3.網站蒐集方式：透過本校網站進行個人資料之蒐集時，應進行以下防護措施

(1)確保輸入之網頁具有 SSL (Secured Socket Layer)等安全措施(或其他對等之安全措施)，確保該蒐集作業簿在傳輸過程遭未授權存取或擷取。

(2)網頁所產出之資料檔案應注意其安全防護，該資料檔案不應置放公共可存取之目錄。

(3)網頁程式或網站系統所保存之暫存檔(Server Log, Server Cache檔)應定期刪除或確認存放於伺服器內避免遭受未授權之存取。

(二)處理作業安全防護措施

1.處理設備之實體安全

請參考本文件壹拾壹、設備安全管理。

2.處理設備之邏輯安全及網路安全

請參考本文件壹拾壹、設備安全管理。

3.資料儲存設備之安全

請參考本文件壹拾壹、設備安全管理。

4.資料正確性檢查

(1)應用系統或網站系統，應於蒐集個人資料後，進行對於資料正確性的檢查，例如查核筆數、設定資料正確檢查碼(Parity Check)等方式進行正確性檢查。

(2)重要個人資料之輸入作業，應於輸入作業完成後，進行資料正確性之複核作業。

(3)資料於傳輸或接受後，應進行資料正確性之檢查，確保傳輸/接受前後之資料正確性。

5.刪除作業(依據當事人權利要求)

個人資料保護法所規範之刪除，應使個人資料於個人資料檔案中消失，因此，資料的刪除作業應確保下述事項：

(1)該資料於個人資料檔案中消失，包括備份之資料。

(2)以去識別化進行刪除時，應注意該資料不應於去識別後得以其他方式重新組建其具識別性之欄位。

(3)刪除作業應確保於暫存檔案、原始紙本、原始資料檔案或媒體之資料也同時被刪除。

(三)資料利用作業安全防護措施

1.資料利用之安全防護控管

資料之利用除須依本文件利用管理程序進行申請外，並應於核准該利用時檢核其利用過程之安全性。

2.資料傳輸至其他單位之控管

(1)紙本傳輸

A.如必須應指派人員親自交付。

B.透過公文傳遞者，應視情形進行密件標示處理。

C.需透過郵遞業者傳遞紙本時，應以掛號方式寄出，並應進行該紙本資料密封作業。

(2)電子傳輸

A.應避免以未有安全防護之電子傳輸方式進行個人資料之傳輸。

B.以電子傳輸個人資料，至少應以 Winzip 等壓縮軟體進行密碼保護，並以分開的傳遞方式遞送該密碼。

C.視需求得以加密(Encryption)方式進行資料加密，以確保檔案之機密性。

D.傳輸前，應確認接收端之收件人、位置、主機等資訊，確保不在傳輸過程中遭攔截或竊取。

E.大量資料電子傳輸或經常性資料電子傳輸應進行申請，由召集人/執行秘書確認其安全性後始得進行。

二、資料存取安全措施

執行個人資料處理之資訊系統或資料庫，其存取控制應包括：

(一)帳號唯一性原則

1.所有帳號應為唯一性，如非必須，不得多人共用帳號。

2.帳號共用應事先經過單位權責主管之同意，並於適當安全配套(如增加其可歸責性措施)後使得進行。

3.嚴禁帳號之借用，以避免破壞帳號使用之可歸責性。

(二)帳號核發、變更及刪除方式

1.本校人員、委外廠商或外部人員帳號之核發流程請依循本校內控制度辦理或資訊安全管理制度之「○○○」文件辦理。

2.委外廠商或外部人員之帳號申請應記錄使用人員及使用期間。

3.帳號之啟用及通行碼(password)發放，應有安全防護，以避免遭他人未授權使用。

4.帳號之變更應經過事先之申請審核，並留存相關紀錄。

5.帳號於人員離職或變更職務後應進行刪除或停用，如需保留一定的期限，應填寫「資訊需求申請單」，經權責主管之核准。

(三)帳號通行碼(password)原則

1.處理個人資料之資訊系統其通行碼應至少為八碼。

2.處理個人資料之資訊系統其通行碼應至少每 180 天更換一次。

3.帳號通行碼複雜度應有一定之複雜度(如：英數混合)。

(四)軌跡資料保存

1.申請及變更資料

(1)所有個人資料蒐集、處理、利用之申請作業與變更作業應留存適當之軌跡資料。

(2)帳號之申請作業紀錄(電子紀錄及紙本紀錄)應至少保留 3 年。

(3)使用者(當事人)申請之存取帳號作業紀錄，如無其他法律規定保留期限，應至少保留 3 年。

2.存取紀錄

(1)個人資料之存取紀錄，應留存其存取紀錄，重要個資檔案或個人資料主檔資料庫之存取紀錄，應至少保留三年。

(2)電腦資料發生錯誤且無法經由應用系統鍵入更正時，應填寫「資訊需求申請單」，陳單位主管核准後，送交予電算中心執行更正。電算中心相關系統負責人將更正步驟內容及時間記載

於「資訊需求申請單」後保存備查。

(3)其他機關索取資料時應有正式公文，確定其依法蒐集、處理、利用是否符合法定職務，各承辦單位應依據「個人資料保護法」及相關規定予以審查，並經召集人/執行秘書核准後始可提供資料。

(五)定期審查存取權限

有關個人資料之資訊系統或資料庫系統存取權限，應至少每年進行一次存取權限之審查。

三、資料存放安全措施

(一)紙本資料

1.紙本資料應進行實體存取之安全管控，大量紙本保存時應注意該紙本事後檢索、取回之可能性及作業方式，以因應當事人進行刪除之請求。

2.紙本之存放應注意防潮及防火，避免意外毀損紙本個資。

3.紙本存放之倉庫，應注意其安全性，如與其他物品共置於一室內，應透過監視防護措施，或其他安全管制制度(例如人員陪同)進行其存取控制防護。

(二)電子資料(存放於電腦或伺服器)

1.存放於個人電腦者

(1)電子(檔案、資料庫等)型態之個資存放於個人電腦，應注意該電腦至少應裝設防毒軟體並定期更新病毒碼，嚴禁使用 P2P 等高風險軟體。

(2)電子型態之個人資料存放於個人電腦，應確保僅存放最少之需

求資料，以避免過多資料存放之風險。

(3)個資保護稽核組應於稽核時進行個人電腦之檢核，確保個人電腦未存放非業務需求之個人資料檔案。

(4)經常性存放個資於個人電腦者，應事先進行申請，由該單位主管及該資料業管單位進行審核，並確保該電腦有足夠安全防護。

(5)個人資料存放於個人電腦者，如必要時應進行資料之加密，以降低資料遭竊取、遺失之風險。

2.存放於電腦伺服器者

(1)檔案伺服器等應嚴禁以未有存取控制之方式進行檔案共享。

(2)檔案伺服器之存取權限應視需求開放，並應定期檢視其存取權限之設定。

(3)檔案伺服器之管理者權限應控制其必要數量，避免過多的管理者權限可存取非業務相關之資料檔案。

(4)存放於檔案伺服器中之檔案，應視需求定期進行檢視，確保其存放之安全防護需求。

(5)視需求高重要或大量個人資料存放之檔案應進行加密作業，以避免個資洩漏、遺失之風險。

(6)檔案伺服器應留存相關存取紀錄，並由管理人員定期檢視是否有異常之存取行為。

(三)資料儲存媒體

可移除式媒體(含行動硬碟、USB、CD、DVD 等)未經核准不應使用可移除式媒體進行個人資料之複製或備份。

四、資料備份安全措施

(一)備份作業之規劃

1.訂定備份政策

應訂定備份政策進行個人資料檔案之備份作業。

2.訂定備份計畫或清單

備份管理人員或系統管理人員應依據備份政策進行該資訊系統或檔案之備份作業，並產出備份計畫或清單，透過人工或工具進行備份並留存紀錄。

3.評估及訂定備份的安全防護需求

對於備份後的備份檔案應視其存放之媒體種類、存放之位置、系統、既有之安全防護評估並擬定備份檔案之安全防護需求，並依據該需求進行防護措施的實施，並將結果紀錄於備份計畫或清單表格內。

4.評估及訂定備份的測試需求

針對備份計畫或清單內之備份結果，應評估該備份資料之重要性及其還原需求之頻率、可能性進行評估後產出備份測試之需求。

(二)備份作業執行及記錄

於備份計畫或清冊內記錄下述事項：

1.記錄備份之執行狀況

2.記錄備份之儲存位置及保護措施

3.記錄備份之目的、使用方式

(三)備份作業之監督及測試作業

1.定期審查備份作業之正確性

2.定期執行備份資料之盤點作業

盤點備份資料須注意備份檔案可能存放在以下媒體

(1)TAPE

(2)CD

(3)DVD

(4)存放於媒體或虛擬主機(Virtualized Server) 上(Ghost、Image 檔案)

(5)伺服器、儲存設備內之檔案

A.檔案伺服器內

B.NAS SAN 網路儲存設備內

C.遠端主機、遠端儲存設備、網路儲存設備等

D.可移除式媒體上

a.可移除式硬碟

b.USB 儲存設備

E.資料庫主機之 Mirror 主機、Redundant 主機、Syndication (backup or DB transaction log backup)、備份資料庫主機等

3.備份媒體之測試

(1)依據測試需求擬定測試計畫

(2)於測試執行後將測試結果記錄於備份計畫或清冊內

五、人員聘僱管理

(一)人員任用

1.正式教職員、約聘僱人員及其他計畫或臨時人員依照本校人事管理相關之規定辦理。

2.本校新進人員於報到時，需簽署保密切結書。保密切結書涵蓋包括到職期間與離職後，均應負保密之責任，任何因未遵守本校個人資料安全維護計畫導致之個資或資訊安全意外事件將依相關規定懲處。

3.本校資訊業務委外服務之廠商或人員，應於簽訂契約時同時簽署保密協議(或於合約中包含個人資料保護之相關條款)，遵守本校個人資料保護管理制度。

4.帳號及電子郵件之使用申請，均應確實依人員之任離職及工作執掌變動情形填列帳號申請單，以利進行帳號管制。

5.本校同仁離職時，須依照人事室規定填寫離職單並於人事系統中註記，始完成離職程序。

6.應用系統使用者如因職務異動而成為非授權使用者時，相關單位應主動通知電算中心管理人員及各業管單位管理人，同步異動該使用者帳號及操作權限。

(二)人員職務異動或離職

1.本校同仁離職或職務異動時，應進行資產之移交，以防止人為舞弊或個人資料及資訊資產損失之風險。

2.本校同仁離職或職務異動時，應依照規定變更或註銷其相關系統之使用權限。

六、機密維護責任

(一)本校同仁應遵守「個人資料保護法」等相關規定，以及本校之個人資料檔案全維護計畫，於辦理與個人資料及資訊安全之相關業務時，因業務所獲知之機密資訊，非經權責主管授權不得對外透露。

(二)為確保本校個人資料及資訊安全，若與往來廠商簽訂合約，應依據陸、個人資料委外管理程序章節之規範訂定合適之合約內容；廠商人員應遵守合約及本規定有關個人資料及資訊安全之規範，並簽訂「合約廠保密切結書」，對於執行業務所獲知之資訊，非經本校授權同意前不得對外透露。

七、人員資訊作業注意事項

(一)應遵守本校所有個人資料及資訊安全之相關規定。

(二)所有本校同仁(含新進教職員、約聘雇人員)均應接受個人資料及資訊安全之訓練課程。

(三)不得自行安裝非法軟體於個人電腦。

(四)不得以任何手段蓄意干擾或妨害網路系統的正常運作。

(五)禁止利用本校網路資源從事個人網站營利及不法情事。

(六)不宜隨意開啟來路不明的電子郵件，以免啟動惡意執行檔或惡意連結。

(七)帳號密碼必須定期更換，且不得洩露予他人。

(八)禁止冒用他人的帳號及密碼登入電腦操作系統。

(九)未經授權人員不得進入電腦機房。

(十)所有個人電腦含筆記型電腦在經過 15 分鐘的閒置後，必須啟動設有密碼的螢幕保護程式。

(十一)屬於機密等級需控管之資料，離開座位時勿停留在螢幕畫面，敏感及機密文件不得留置於桌面。

(十二)下班時應關閉個人電腦與螢幕電源。

(十三)禁止使用違反智慧財產權相關的資訊資產。

壹拾壹、設備安全管理

個資法要求對於個人資料處理設備進行安全的管控，本校對於設備安全管理之程序分為

一、個資處理設備清查

進行對於本校內部個資處理設備之清查作業，透過清查進行對於設備的識別，確保所有與個人資料蒐集、處理、利用作業相關之設備均於此過程中被清查出，以便後續進一步的評估設備所需要的安全要求。

(一)個人資料輸入處理設備

1.辦公輸入設備：掃描器、傳真機、影印機等用來處理紙本資料個資蒐集設備。

2.個人資料輸入管道:包括網站設備等可能用來接收或處理蒐集個人資料之設備。

(二)個人資料處理設備

1.個人電腦設備：包括人員使用之個人電腦設備、筆記型電腦、手持式電腦設備等資料處理設備。

2.檔案伺服器：儲存檔案的公共檔案主機，包括各類、各種技術形式的檔案集中儲存設備。

3.資料庫主機設備：主要以資料庫形式(包括各種不同資料庫，例如SQL Server, My SQL, Access Database, LDAP …)存放個人資料的設備。

4.通訊設備：例如傳真機，答錄機，影印機等通訊設備，因目前科技進步，該等設備內均有設置儲存裝置(例如硬碟機)，以加速或增加該設備的功能，因而可能因為當事人傳真進本校或本校人員影印相關含個人資料之紙本而在該等設備中留存部分個人資料

（此類設備維護廠商通常可以檢視或存取該儲存裝置）。

5.其他資料處理設備：例如各式側錄主機(例如 email 側錄設備，網路訊息側錄設備)，各類 Log 紀錄蒐集及分析設備。

6.資料儲存設備

(1)備份空間、伺服器(包括異機備份、SAN 或 NAS 網路儲存設備)。

(2)備份媒體、磁帶、光碟(CD, DVD)等之儲存設備。

二、設備安全需求

對於處理個人資料設備於清查後應進行該設備安全需求控管作業，包括以下：

(一)設備實體安全防護措施

評估設備需要適當的實體安全控管，例如

1.應有實體存取預防措施：例如上鎖、加上密碼控管、專人看管、或其他實體保護。

2.如設備數量較多，應進行數量的盤點及控管，確保該等設備無遭竊之可能。

(二)設備邏輯及網路安全防護措施

如果設備可以接上網路、通訊網路等邏輯(非實體)通路時，應注意對於此類網路安全的需求

1.設備之網路安全措施

應有適當的網路安全措施，例如進行適度的網路區隔，進行相關的 NAT (Network Address Translation) 以確保 IP 位置不被外

部人員所知悉，安裝防火牆設備或設定連線端條件(固定 IP、 回撥、特殊路由等)。

2.資料傳輸安全防護措施

此類設備在傳輸資料時,應進行額外的資料保護,例如傳輸加密、安全通道、VPN 等強化傳輸安全之防護措施。

(三)資料安全防護措施

如果設備具備存放或短暫存放資料的能力,應針對此類設備進行資料安全的防護包括

1.資料機密性的保護需求：資料應進行機密性的保護，例如加密機制、設置存取控制、通行碼管制、進行資料遮罩等。

2.該等設備應於送修、維修前移除資料或以其他方式控制不被維護廠商未授權存取。

3.該設備應進行資料完整性的保護，例如避免震動、電流不穩、資料傳輸後複核等保護。

4.資料可用性的保護：規劃該等設備進行備份，不斷電保護及其他確保資料可用性之防護。

(四)設備存取權限之管制措施

如果設備可以讓多人進行存取,應進行存取權限的控管保護,包括

1.帳號申請作業需求，應具備帳號申請作業，確保開放該設備存取之過程經過相關人員核准。

2.帳號存取權限安全措施：例如帳號長度控管，通行碼更換頻率，通行碼複雜度及通行碼的交付安全保護。

3.帳號審查作業：應進行定期的帳號權限審查，以確保該設備之存

取權限開放均為正確。

4.其他防止未授權存取的安全保護：例如進行 OTP (One Time Password), 雙因認證等強化存取控制的作法，螢幕保護控制、Session Time Out 等對於存取控管的安全防護。

三、可攜式儲存媒體管理

對於處理個人資料設備於清查後應進行該設備安全需求控管作業，包括以下：

(一)原則性規定

1.行動資訊媒體未經權責單位同意不得任意存取本校資料。

2.若為業務需要，使用者應充份向業務承辦人告知行動資訊媒體之使用用途，並填寫「行動資訊媒體使用申請單」，在獲得審核通過後方可使用；若逾越原內容，使用者應負起全部責任。

3.機房內使用行動資訊媒體，應避免散播病毒或被植入惡意程式碼，確保本校電腦機房資料之機密性、完整性與可用性，降低對機房資訊安全的影響。

4.業務承辦人應評估或檢查對方所使用之行動資訊媒體的安全性，確定本校相關設備已具備適當之防護能力；業務承辦人必須確認行動資訊媒體已經完成掃毒或安全檢查，方可作業。

5.將機密資料存放於行動資訊媒體時，應採取適當保護措施(壓縮檔案後設定密碼)，避免遺失時洩漏資訊。

6.行動資訊媒體使用完畢後，應立即清空敏感與機密資訊。

7.可攜式電腦及終端管理端電腦(Console)，應安裝防毒軟體並啟動

連線時即時主動更新，保持病毒碼為最新狀態，以具備自我保護之能力。

8.行動資訊媒體遺失時應通報權責主管，並評估資料遺失是否具有機密性，權責主管依情節之重大程度決定是否向上陳報。

四、應用程式漏洞及修補程式管理

(一)作業系統及各應用程式應定期更新（例如安裝新的版本）

1.作業系統及應用程式更新時，應評估其對應用系統是否造成負面的影響，或是產生安全問題。

2.如有重大系統漏洞或重要更新,得選擇以手動方式進行更新作業,以確保即時性之防護

(二)作業系統及應用程式更新之評估應考量的要項如下：

1.評估應用系統的安全控制措施及查驗系統之完整性，以確保其未受作業系統變更之影響。

2.作業系統變更的評估及測試結果，如須進行必要的資源調整，應提出資源分配及調整計畫。

3.伺服器主機之作業系統更新應即時通知相關人員，以便在作業系統變更前，相關人員可以進行適當及充分的評估作業。

壹拾貳、認知宣導及教育訓練

一、訓練需求評估

(一)執行人員

本校之個人資料安全教育訓練由專案管理小組執行。

(二)執行時間

於每下半學年度產出次學年度之教育訓練計畫，並由召集人審核後，由專案管理小組執行。

(三)評估內容

評估內容依參考

1.法規變化

2.上級主管機關提出之教育訓練需求

3.人員個資保護知識需求

4.配合資安教育訓練

二、訓練計畫

專案管理小組於每下半學年度產出次學年度之教育訓練計畫，並由召集人審核後，由專案管理小組執行。

三、訓練執行

由專案管理小組委由本校內部人員或聘請外部講師進行訓練。

四、訓練結果維持

職員工教育訓練成果報告表應予以留存，並於每年委員會議中提出成效報告。

五、成效評估與計畫修正

於每年之成效報告後，應提出隔年之教育訓練計畫之修正，如有重大差異或成效缺失，應提出矯正預防計畫，確保教育訓練之成效管理。

壹拾參、資料安全稽核機制

一、個資保護稽核組

本校之個人資料安全稽核由個資保護稽核組進行。

二、稽核管理

(一)本校之個人資料保護管理內部稽核工作之執行者不限於本校個資保護執行個資保護稽核組之人員，可以委由外部具備專業資格之人士進行，但不論由內部或外部人士執行，稽核人員必須具備獨立性及客觀性，內部稽核人員不能稽核本身之工作。

(二)稽核工作必須對稽核過程所查核事項的事實加以記錄，以顯示其稽核軌跡作為稽核發現之佐證。

(三)稽核所發現之缺失及觀察事項與建議，應由稽核人員及被稽核單位就是否屬實取得一致之見解，被稽核單位應對稽核所見加以檢討並尋求改善，稽核結果及改善行動執行情況應交付本校委員會。

三、稽核準則

(一)個人資料保護法

(二)個人資料保護法施行細則。

(三)主管機關對於個資保護管理相關作業規定。

(四)本校個人資料保護管理規定及各單位作業內容。

四、稽核計劃

(一)個資保護稽核組於每學年結束前須完成下學年度的個人資料保護管理稽核計畫。

(二)稽核人員必須於預定執行時間一個月前就該次稽核編定其執行計

畫，稽核計畫之制定須考慮過去稽核之結果決定稽核範圍及查核重點。稽核人員應於評估本校作業週期及風險後， 擬定包含稽核目的、稽核項目、稽核對象、實施期程、稽核方法、作業程序、稽核重點及稽核結果等之稽核計畫，依照所排訂之稽核項目，訂定作業程序及稽核重點，稽核時並得依情況適時調整。

(三)稽核計畫經個資保護稽核組審議通過，並應經召集人核定實施，修正時，亦同。

(四)稽核人員應與受稽單位主管事前溝通，確定稽核時間及相關協調工作。並應於稽核前 7 日，通知受稽核單位。

五、稽核範圍

(一)個人資料保護告知事項及同意內容 (個資法第 8 條及第 9 條要求)

(二)個人資料盤點作業與個人資料範圍界定作業(施行細則第 8 條第 2 項第 2 款規定)

(三)個資法規盤點作業(本文件第肆章要求)

(四)風險評估與風險管理作業(施行細則第 8 條第 2 項第 3 款規定)

(五)個人資料事故之預防、通報及應變作業。(施行細則第 8 條第 2 項第 4 款規定)

(六)個人資料蒐集、處理、利用行為之檢查(施行細則第 8 條第 2 項第 5 款要求)

(七)資料安全維護作業檢查(施行細則第 8 條第 2 項第 6 款規定)

(八)認知宣導及教育訓練作業檢查(施行細則第 8 條第 2 項第 7 款規定)

(九)設備安全維護 (施行細則第 8 條第 2 項第 8 款規定)

(十)個人資料保護持續改善作業(施行細則第 8 條第 2 項第 11 款規定)

(十一)使用紀錄、軌跡資料及證據保存作業檢查(施行細則第 8 條第 2 項第 10 款規定)

(十二)當事人行使權利所執行之各項檢查。(個資法第 3 條及第 10、11、13 條要求)

六、稽核頻率

(一)本校個人資料保護管理每年執行一次定期稽核，對於特殊事項之稽核，本校委員會得指派人員進行特別追蹤稽核。

七、稽核方法

(一)稽核採抽樣方式進行，一般單一查核項目之抽樣不得少於 5 件，對於特別查核項目之抽樣數可由稽核人員指定。

八、稽核紀錄與報告

(一)稽核工作必須保留工作底稿(如附件九)，工作底稿可為電子檔或書面手寫，但須清楚顯示每一查核項目之查核準則、訪談對象、所檢視紀錄及所進行之抽樣及該項查核之結果。

(二)對於不符合事項必須填具稽核報告單，進行改善。

(三)稽核人員須於稽核結束兩週內提交稽核報告，報告須包括各項建議、觀察事項及不符合事項之彙整及統計、對於整體個人資料保護管理之有效性及適切性之評估以及就稽核過程之有效性之自我檢討與評估。

(四)稽核人員依據稽核工作底稿及審定「內部稽核觀察、建議及回覆紀

錄表」撰寫「稽核報告」，稽核報告經個資保護稽核組召集人覆核，應送交本校委員會審查。

九、稽核改善與追蹤

依照本校內部稽核實施細則第 6 條及第 7 條之規定進行稽核改善與追蹤，方式如下：

(一)稽核人員依受稽核單位所提出之預定完成改善期限進行追蹤查核。

(二)稽核人員依據稽核追蹤工作底稿撰寫「追蹤報告」。

(三)受稽核單位之改善事項未於改善期限完成或未執行改善者，稽核人員應於「追蹤報告」中明確記載。

(四)「追蹤報告」應經個資保護稽核組覆核，轉受稽核單位會簽後，陳送召集人核閱，並將副本交付校長查閱。

(五)改善事項未於改善期限完成或未執行改善追蹤事項者，個資保護稽核組應將相關書面資料，副知本會，列入年度考核該單位考績之參考，並列入下次稽核重點。

(六)與經費有關之事項，提報至校務會議，做為下學年度預算之參考。

(七)稽核時所發現之不符合事項，應於年度稽核報告中據實揭露，並檢附工作底稿及相關資料，作成稽核報告，定期追蹤至改善為止。稽核報告、工作底稿及相關資料，應至少保存五年。

壹拾肆、個人資料安全維護之整體持續改善

一、程序目的

本校個人資料保護須依循管理系統之 PDCA 循環，除本校於計畫階段進行訂定個資政策、個資保護管理規定及要求人員遵循政策及本規定外，本程序將建立持續改善之方式以確保本校對於個資管理的有效性。

二、檢查

本校透過稽核機制及通報機制進行相關個資遵循的檢查作業包括

(一)例行性的個人資料保護稽核作業。

(二)設置各單位個資保護專責人員，針對個人資料保護進行例行性的檢查作業

(三)個人資料保護推動委員會

透過管理審查作業，由召集人每年進行至少召開一次對於個人資料保護作業整體成效審查，參加成員包括委員會成員及各單位個資保護專責人員，確保所有之個人資料檔案安全維護計畫執行結果均符合本校之需求。審查項目得包括

1.專案管理小組

(1)個人資料保護認知及教育訓練次年度規劃

(2)本年度個人資料保護教育訓練之成效

(3)個人資料保護申訴事件及處理結果

(4)當事人權利申請狀況及處理結果

(5)個人資料風險評估結果

(6)風險管理結果報告

2.資訊技術小組

(1)該年度的個人資料相關事故統計及處理情形

3.個資保護稽核組

(1)提供內部稽核報告。

(2)矯正預防措施

4.各單位個資保護專責人員

針對該單位個人資料保護管理作業情形進行報告。

三、持續改善

(一)於各項檢查後之發現結果，該發生單位之個資保護專責人員應該針對該發現點提出矯正措施包括

1.發現原因，事件發生或異常發生的原因。

2.矯正計畫：針對原因提出解決方案。

3.計畫預計完成日期：矯正措施所需之完成時間預估。

4.計畫執行人員：指派之矯正措施執行人員。

5.需求資源：完成計畫所需之資源，包括人員、預算或相關資源之需求。

(二)矯正計畫之審查

各單位提出之矯正措施，應由該單位權責主管進行核准後監控執行到完成，後將相關執行結果送交執行秘書簽核後結案存查。矯正措施單之格式如附件十一。

附件一、個人資料保護推動委員會名單

個人資料保護推動委員會	
委員	姓名
召集人	
執行秘書	
幹事	

個資保護工作組	
組別	召集人
個資保護稽核組	
法規/事件事故小組	
專案管理小組	
資訊技術小組	
個資保護專責人員	

附件二、個資保護暨資通安全適用法規一覽表

編號	主管機關	法規名稱	最新公告日期	版本	個資相關條文	備註

附件三、新個資蒐集前查檢表(範本)

慈濟大學 新個資蒐集前查檢表			
申　　請　　人		申 請 日 期	
業　務　名　稱			
內　容　摘　要			
蒐　集　類　別			
特　定　目　的			
法源依據及法律要求說明(例如：最小保存時間)	(請注意確認為法律規定，行政命令)，如有公文請列為附件 法律名稱：　　條文: 公文名稱：		
蒐　集　格　式	☐ 紙本 ☐ 電子檔案 ☐ 資料庫		
保　存　時　間			
保　存　方　式	☐ 紙本 ☐ 電子檔案 ☐ 資料庫		
預計利用方式(期間、地區、方式)			
蒐　集　方　式	☐ 直接蒐集 ☐ 間接蒐集 ☐ 委外蒐集		
如為間接蒐集	間接蒐集資料來源:_____ 來源分類: ☐合法公開資料庫☐公開可取得來源☐其他_____ 間接蒐集資料來源合法性檢查:_____		
第十九條蒐集處理合法要件	☐法律明文規定 ☐與當事人有契約或類似契約之關係 ☐當事人自行公開或其他已合法公開之個人資料 ☐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 ☐採用書面同意, 書面說明:_____ _____, 該書面預計保存方式:_____ ☐與公共利益有關 ☐個人資料取自於一般可得之來源		

其他項目檢查	內　　容	是否符合
告知函撰寫		
委外合約監督條款擬定		
會　　簽　　意　　見		
法規/事件事故小組(可提供法律意見同仁或小組)		
核　　准		

申　　請　　人		日　　期	
單位主管核准		日　　期	
個資保護專責人員		日　　期	
專案管理小組		日　　期	
執行秘書/幹事		日　　期	

附件四、個人資料利用前申請書

慈濟大學 個資利用前申請書			
申　請　人		申請日期	
將利用之個資說明（說明利用的標的及簡述利用之狀況）			
現有個資蒐集、處理、利用狀況說明			
☐ 直接蒐集資料 ☐ 間接蒐集資料：取得來源說明 _____ 告知義務：☐ 已依個資法第 8 條或第 9 條進行告知 ☐ 依法免告知_____ 目前資料保存方式、存放地點:_____ 目前資料管理單位及管理人員: ☐ 同申請單位☐_____			
原蒐集取得同意之方式	☐ 法律規定 _____ ☐ 書面同意 _____ ☐ 其他方式 _____		
個人資料檔案說明			
個人資料檔案名稱			
範圍			
檢附文件			
預計利用方式說明			
利用之方式說明（方式、對象、地區、期間）交付方法、安全措施	方式: 期間: 地區： 對象:		
與原蒐集目的檢查	是否與原告知之利用方式、對象、期間、地區相符或與原蒐集目的相符 ☐是 ☐否 ☐保留意見_____		
是否合於原蒐集之特定目的	☐是 ☐否 ☐保留意見_____		

利用方式(傳遞方式)是否合乎適當安全維護之說明	(例如：原有資料傳遞方式如電子郵件、光碟等之保護措施)		
會　　簽　　意　　見			
法規/事件事故小組(可提供法律意見同仁或小組)			□是□否□不適用
核　　准			
申　　請　　人		日　　期	
單位主管核准		日　　期	
個資保護專責人員		日　　期	
專案管理小組		日　　期	
執行秘書/幹事		日　　期	

附件五、個人資料權利行使申請書

<table>
<tr><td colspan="5">慈濟大學　個人資料權利行使申請書</td></tr>
<tr><td>申　請　人</td><td colspan="2"></td><td>申請日期</td><td></td></tr>
<tr><td>申請事項</td><td colspan="4">□查詢　□閱覽　□複製本　□更正　□補充　□停止蒐集
□停止處理　□停止利用　□刪除</td></tr>
<tr><td>檢附文件</td><td colspan="4"></td></tr>
<tr><td colspan="5">申請事由:
本人_____之需求
向 貴校申請個人資料之 □查詢 □閱覽 □複製本 □更正 □補充 □停止蒐集
□停止處理 □停止利用 □刪除 之作業。
擬請 貴校協助處理作業。</td></tr>
<tr><td>查　　詢</td><td colspan="4">(請填寫需求例如範圍、期間....)</td></tr>
<tr><td>閱　　覽</td><td colspan="4">(請填寫需求例如範圍、期間....)</td></tr>
<tr><td>複　製　本</td><td colspan="4">(請填寫需求例如範圍、期間、需求份數等....)</td></tr>
<tr><td>更　　正</td><td colspan="4">(請填寫需求例如範圍、資料欄位....)</td></tr>
<tr><td>補　　充</td><td colspan="4">(請填寫需求例如範圍、資料欄位....)</td></tr>
<tr><td>停止蒐集、
處理、利用</td><td colspan="4">(請填寫需求例如範圍、資料欄位....)</td></tr>
<tr><td>刪　　除</td><td colspan="4">(請填寫需求例如範圍、資料欄位....)</td></tr>
<tr><td colspan="5">申請人權益影響說明(申請停止蒐集、處理、利用及刪除者)
1. 申請停止蒐集、處理、利用者，由於本校無法進行前述之個人資料作業動作，因而部分之系統功能或當事人權益將因停止前述動作而有影響，其影響之結果申請人願意自行承擔。
2. 申請刪除作業者，申請人了解資料一經刪除後無法復原，因為刪除個人資料後造成之申請人權益損失將自行承擔，並不再提出恢復資料之要求。
□申請人詳閱並同意上述權益影響說明:</td></tr>
<tr><td>申請人簽名</td><td colspan="2"></td><td>日期</td><td>年　　月　　日</td></tr>
</table>

<table>
<tr><td>受 理 單 位
審 查 意 見</td><td colspan="3">☐ 接受(符合本校申請條件)

☐ 拒絕(不符合本校申請條件)

☐ 酌收資料處理費(查詢/閱覽/製給複製本)：　　元</td></tr>
<tr><td>受理單位人員</td><td></td><td>日期</td><td>年　　月　　日</td></tr>
<tr><td>受理單位主管</td><td></td><td>日期</td><td>年　　月　　日</td></tr>
<tr><td>專案管理小組</td><td></td><td>日期</td><td>年　　月　　日</td></tr>
</table>

附件六、個人資料盤點表

慈大盤點表.xlsx

附件七、風險處理計畫

現況說明	風險改善措施	權責單位	預計改善時間 與處理方式	風險評估彙整表對照

附件八、職員工教育訓練成果報告表

教育訓練計畫　　製表日期 年 月 日 執行教育訓練負責人(　　)		
教育訓練名稱		
教育訓練目的		
教育對象		
執行教育訓練人(講師)	總計　　名	
使用資料		
預定執行日期		場所
例) 第 1 次　年 月 日		
第 2 次　年 月 日		
教育訓練內容		
<反應上次教育訓練內容>		
<教育訓練內容>		
確認教育訓練效果方法	例)問卷調查、隨堂測驗 等	
教育訓練負責人 核決	年　月　日　印	
執行教育訓練紀錄 製表日期　年　月　日　製表人(　　)		
<執行教育訓練內容>		
<應出席學員人數/出席學員人數說明>		
<本次教育訓練結果應反映於下次教育訓練事項>		
教育訓練結果處理	□ 不須處理 □ 需要追蹤教育訓練 □其他	
處理內容		
教育訓練負責人 審核	年　月　日　印	
個資保護管理代表　核決	年　月　日　印	

附件九、稽核查檢表暨工作底稿

序號	領域	評估細項	符合	未符合	不適用	說明
1	組織	學校是否已指派單位內負責個人資料管理的人員?				
2	組織	學校是否已組成個人資料保護組織或工作小組，同時可清楚說明維護本校內部個人資料之管理作業權責?				
3	組織	承上題，上述要求是否已有文件化，載明成立個人資料保護管理組織及角色，並配置相當資源?				
4	組織	單位是否指派個資保護專責人員進行個人資料檔之管理及維護?				
5	組織	學校是否已清楚了解組織內部有關個人資料之蒐集 、處理 、利用之範圍?				
6	組織	學校是否已辨識單位個資保護措施與個人資料保護法之適法性是否一致?				
7	組織	學校是否訂定經管理階層核准之宣告客戶、教職員生個人資料如何與何時被蒐集、利用、以及保護之個人資料管理政策?				
8	告知	學校直接蒐集個人資料是否已取得當事人書面、電話、傳真或電子方式同意?(法令授權免通知者除外)				
9	告知	學校法依法向當事人直接蒐集個資時，是否明確說明蒐集個人資料的機關名稱、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/不提供之影響?				
10	告知	學校是否提供清楚與明顯的說明有關個人資料的安全維護方式?				

序號	領域	評估細項	符合	未符合	不適用	說明
11	告知	學校是否提供清楚與明顯的說明有關當事人如何查詢或存取其個人資料?				
12	告知	學校是否提供清楚與明顯的說明有關當事人如何更正或刪除其個人資料?				
13	告知	學校內間接蒐集之個人資料是否已規劃告知當事人?				
14	告知	學校是否設計提供當事人申訴程序與管道?				
15	蒐集處理利用	學校是否有盤點機關內所有的個人資料,並建立清冊以利管理?				
16	蒐集處理利用	學校內是否針對各項個人資料之蒐集、處理、利用及銷毀建立資料流程以掌握資料流向及管理方式?				
17	蒐集處理利用	學校進行個人資料蒐集時是否遵循所屬主管機關的法規或公約(例如教等)?				
18	蒐集處理利用	學校內是否識別間接蒐集之個人資料之適法性及特定目的之合理性?				
19	蒐集處理利用	學校是否針對特種個資(醫療、基因、性生活、檢康檢查、犯罪前科)進行蒐集、利用及處理?				
20	蒐集處理利用	學校若有蒐集特種資料是否取得法令依據?				
21	蒐集處理利用	學校若有蒐集特種資料是否清楚了解機關內有關特種資料之用途?				

序號	領域	評估細項	符合	未符合	不適用	說明
22	蒐集處理利用	學校若有蒐集特種資料,是否有適當之安全維護計畫?				
23	蒐集處理利用	學校之個人資料管理是否有建立必要之使用紀錄、軌跡資料(Log Files) 及證據之保存措施?				
24	蒐集處理利用	學校內是否有針對個人資料分級進行風險評鑑?				
25	蒐集處理利用	學校內是否有針對個人資料不同等級處理進行安控措施(含備份檔案及軌跡檔案)				
26	蒐集處理利用	學校之是否執行資料安全管理?				
27	蒐集處理利用	學校之是否執行人員安全管理?				
28	蒐集處理利用	學校之是否執行設備安全管理?				
29	蒐集處理利用	學校之是否有針對個人資料顯示進行適當的去識別化?				
30	蒐集處理利用	學校與其他單位個人資料交換是否已識別個人資料之適法性及特定目的利用之合理性?				
31	蒐集處理利用	學校與其他單位個人資料交換是否已採取適當保護措施?				
32	蒐集處理利用	對於個資(紙本及數位資料)之存取及利用是否保有完整的紀錄、軌跡資料?				

序號	領域	評估細項	符合	未符合	不適用	說明
33	蒐集處理利用	學校是否已針對受委託處理個資案件之單位,於契約上訂有個資保護法令及機關內部個資相關規定要求?				
34	蒐集處理利用	學校是否已針對受委託單位,於契約上訂有明確監督要求?並執行監督?				
35	蒐集處理利用	學校是否有將資料傳送於境外,該境外地區是否有個資保護法令(規範),且已取得中央目的主管機關同意?				
36	蒐集處理利用	學校是否以逕行有效的個人資料保護全面性(含新人)人員宣導及教育訓練?				
37	訓練	學校是否針對負責管理及維護個人資料檔案之個資保護專責人員進行有效的專業教育訓練?				
38	程序	學校是否已建立個人資料內管理程序或規則,以確保單位內個人資料蒐集、處理、利用刪除及傳輸符合特定目的的要求?				
39	程序	學校是否有設計當事人查詢、變更、刪除資料之程序?				
40	程序	學校是否有設計當發生個人資料被竊取、洩漏、竄改或其他受害者事件之主動通知程序?				
41	程序	學校是否有設計風險評估及管理程序?				
42	程序	學校是否有設計個資事故通報及應變處理程序?				
43	程序	學校是否有設計內部稽核程序?				
44	程序	學校是否有設計當個人資料蒐集目的消失或屆滿之資料刪除程序?				

序號	領域	評估細項	符合	未符合	不適用	說明
45	程序	是否訂有個人資料檔案維護計畫及業務終止後個人資料處理方法等相關事項之辦法				
46	程序	是否訂有個人資料檔案維護計畫?				
47	程序	是否訂有業務終止後個人資料處理方法?				
48	PDCA	學校對於個資之蒐集、處理與利用之流程,是否進行內部稽核?				
49	PDCA	學校是否定期檢視個資政策及個資保護執行結果?				
50	PDCA	學校是否有實施個人資料安全維護之整體持續改善計畫?				

稽核人員：_____

附件十、稽核報告書

00 年度 內部稽核報告書

報告日期:_____

報告人(個資保護稽核組召集人)_____

稽核範圍	
稽核日期	
稽核地點	
稽核人員	
受稽人員	
陪檢人員	
稽核項目	
稽核結果：	
總結建議：	

受稽核/人員	陪檢人員	稽核人員
個資保護稽核組召集人		
召集人		

附件十一、矯正措施單

矯正措施單

編號				年月日	
矯正措施 執行單位		措施負責人 (單位負責人)		提出糾正不符合人	

矯正計畫	「不符合內容」(記載為內部稽核報告書<糾正事項。要求改善指示事項>、機關外部糾正等)			
	「原因」(記載糾正事項發生的根本原因)			
	提出計畫日期:		核決計畫日期:	
	提出計畫人: (單位負責人)		計畫核決人: (個人資料保護管理負責人)	
	預定執行矯正措施完畢日期:		是否需要確認矯正措施:□ 是 □ 否	
矯正措施執行結果	【執行矯正措施 內容】			
	執行完畢日期:		核決日期:	
	提出計畫人: (單位負責人)		計畫核決人: (個人資料保護管理負責人)	
審核	【確認矯正措施效果及有效性】			
	執行日期:		核決日期:	
	報告人:		召集人	

附件十二、銷毀申請單

紀錄銷毀申請單

表單編號：(紀錄保管人員於存檔時編號)

申　請　單　位		
申　請　人　員		
申　請　日　期	年　　月　　日	
表　單　編　號		
銷　毀　資　訊	起訖流水號 _____~_____ 起迄日期 _____~_____ 數量 _____	
銷　毀　方　式		
委外銷毀陪同人員	(委外銷毀始需填寫此欄位)	
委　外　銷　毀　廠　商	(委外銷毀始需填寫此欄位)	
銷　毀　日　期	年　　月　　日	
紀錄保管人員	委　外　銷　毀　陪　同　人　員	單　位　主　管
	(委外銷毀始需簽核此欄位)	

註：若委外執行銷毀，紀錄保管人員應確認相關陪同紀錄已附於此表單，始得存檔。

附件十三、個人資料交付表

慈濟大學
個人資料交付表

註：將個人資料檔案傳送至委外單位時皆需填寫本表單。

委外承辦單位填寫

委外承辦單位			申請日期	
委外承辦人			簽章 (主管核章)	
契約(計畫)名稱				
委外單位				
交付原因				
個人資料內容	範圍			
	類別			
	數量			
附件				
使用行為		☐蒐集作業 ☐處理作業 ☐利用作業		
使用目的				
使用期間				
結束後處理方式				

交付單位填寫

交付單位			交付日期	
交付方式		☐紙本 ☐電子檔 ☐其他：		
預計處理方式				
安全保護機制技術細節		☐紙本密件處理 ☐電子檔加密處理 ☐其他：＿＿＿＿＿＿＿＿		
接收人員姓名				
交付人員			權責主管	

附件十四、個人資料接收表

慈濟大學
個人資料接收表

註：將個人資料檔案傳送至委外單位時，由委外單位填寫本表單。

合約名稱		
編號(流水號)		
單位名稱		
涉及個資行為		☐蒐集　☐處理　☐利用
使用目的		
慈濟大學交付人		
接收日期及時間		
接收方式		☐紙本　☐光碟　☐電子檔　☐其他_____
個人資料內容	範圍	
	類別	
	數量	
後續處理方式		
委託案結束後之預計處理方式		
安全防護機制		

收受人：

附件十五、行動資訊媒體使用申請單

慈濟大學

行動資訊媒體使用申請單

<table>
<tr><td>申　請　單　位</td><td colspan="2"></td><td>申　請　日　期</td><td></td></tr>
<tr><td>申　　請　　人</td><td colspan="2"></td><td>申 請 人 電 話</td><td></td></tr>
<tr><td>承　　辦　　人</td><td colspan="4"></td></tr>
<tr><td>行 動 資 訊 媒 體
名稱/規格/數量</td><td colspan="4">行動資訊儲存媒體設備項目：
□隨身碟
□筆記型電腦
□其他_____
規格：
數量：</td></tr>
<tr><td colspan="5">申請原因：</td></tr>
<tr><td rowspan="2">資 訊 技 術 小 組
審　　核</td><td colspan="4">□ 同意　□不同意
說明：

□ 是　□否　完成掃毒或安全檢查</td></tr>
<tr><td>系統管
理員</td><td></td><td>二級
主管</td><td></td></tr>
<tr><td>備　　註</td><td colspan="4"></td></tr>
</table>