

個人資料保護管理政策					
文件編號	Takming-PIMS-A-001	機密等級	一般	版次	1.0

德明財經科技大學

個人資料保護管理政策

機密等級：一般

文件編號：Takming-PIMS-A-001

版 次：V 1.0

初版日期：110.04.26

個人資料保護管理政策					
文件編號	Takming-PIMS-A-001	機密等級	一般	版次	1.0

1. 目的

德明財經科技大學(以下簡稱本校)為落實個人資料之保護及管理並符合「個人資料保護法」之要求，保障當事人之權利，降低個人資料檔案受侵害之可能性及衝擊，特訂定本校個人資料保護管理政策（以下簡稱「本政策」）。

2. 適用範圍

本校內含有與個人資料相關的業務流程及個人資料檔案(包括備份資料)。

3. 名詞定義

3.1. 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。

3.2. 個資檔案

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、整理之個資之集合。

3.3. 蒐集

指以任何方式取得之個人資料。

3.4. 處理

指為建立或利用個人資料檔案所為資料之記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結或內部傳送。

3.5. 利用

指將蒐集之個人資料為處理以外之使用。

3.6. 國際傳輸

指將個資作跨國（境）之處理或利用。

3.7. 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。

3.8. 非公務機關

指公務機關以外之自然人、法人或其他團體。

3.9. 當事人

指個人資料之本人。

3.10. 個人：

指現生存之自然人。

4. 權責

設置本校「智慧財產權暨個人資料保護委員會」，負責政策之核定及監督、個人資料保護事件審查及危機處理。

5. 要求事項

個人資料保護管理政策					
文件編號	Takming-PIMS-A-001	機密等級	一般	版次	1.0

5.1. 個人資料之蒐集與處理

本校因營運所需取得或蒐集之包括但不限於個人之姓名、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、職業等個人資料，應遵循我國個人資料保護法（以下簡稱個資法）等法令，不過度且符合目的、相關且適當並公平與合法地從事個人資料之蒐集與處理。

5.2. 個人資料之利用及國際傳遞

5.2.1 本校於利用個人資料時，除需依個資法之特定目的必要範圍內為之外，如需為特定目的以外之利用時，將依據個資法第十六條之規定辦理；倘有需取得用戶之書面同意之必要者，本校應依法取得用戶之書面同意。

5.2.2 本校所蒐集、處理之個人資料，應遵循我國個資法及本政策之規範，且個人資料之使用為本校營運或業務所需，方可為本校承辦同仁利用。

5.2.3 本校取得之個人資料，如有進行國際傳遞之必要者，定謹遵不違反國家重大利益、不以迂迴方法向第三國傳遞或利用個人資料規避個資法之規定等原則辦理；倘國際條約或協定有特別規定、或資料接受國對於個人資料之保護未有完善之法令致有損害當事人權益之虞者，本校將不進行國際傳遞，以維護個人資料之安全。

5.3. 個人資料之調閱與異動

當本校接獲個人資料調閱或異動之需求時，應依個資法及本校所訂之程序，於合法範圍內進行當事人之個人資料查詢或請求閱覽、請求製給複製本、請求補充或更正、請求停止蒐集、處理、利用、請求刪除。

5.4. 個人資料之例外應用

5.4.1 本校因業務上所擁有之個人資料負有保密義務，除當事人之要求查閱或有下列情形外，應符合個資法第十六條及相關法令規定，並以正式公文查詢外，本校不得對第三人揭露：

5.4.1.1 司法機關、監察機關或警政機關因偵查犯罪或調查證據所需。

5.4.1.2 其他政府機關因執行公權力並有正當理由所需者。

5.4.1.3 與公眾生命安全有關之機關（構）為緊急救助所需者。

5.4.2 本校對個人資料之利用，除個資法第六條第一項所規定資料外，應於蒐集之特定目的必要範圍內為之。但有下列情形之一者，得為特定目的外之利用：

個人資料保護管理政策					
文件編號	Takming-PIMS-A-001	機密等級	一般	版次	1.0

5.4.2.1 法律明文規定。

5.4.2.2 為增進公共利益。

5.4.2.3 為免除當事人之生命、身體、自由或財產上之危險。

5.4.2.4 為防止他人權益之重大危害。

5.4.2.5 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。

5.4.2.6 經當事人書面同意。

5.5. 個人資料之保護

5.5.1 為防止個人資料被竊取、竄改、毀損、滅失或洩漏，本校設置個資保護執行小組，統籌各項個資保護作業原則規劃事宜，由電算中心主任擔任召集人，並依相關法令規定辦理個人資料檔案及個人資料清冊安全維護及更新事項。

5.5.2 個人資料檔案應建立管理制度，分級分類管理，並針對接觸人員建立安全管理規範。

5.5.3 為確保所有個人資料安全，應強化個人資料檔案資訊系統之存取安全，防止非法授權存取，維護個人資料之隱私性，應建立安全保護機制，並定期查核。

5.5.4 個人資料檔案儲存於個人電腦者，應於該電腦設置可辨識身分之登入通行碼，並視業務及重要性，考量其他輔助安全措施。

5.5.5 個人資料輸入、輸出、存取、更新、銷毀或分享等處理行為，應釐定使用範圍及調閱或存取權限。

5.5.6 本校各單位如遇有個人資料檔案發生遭人惡意破壞、毀損或作業不慎等安全事件，應進行緊急因應措施，並依本校通報程序辦理。

5.5.7 本校以嚴密之措施、政策保護當事人之個人資料，本校之所有教職員工生，倘有洩露個資之情事者，將依法追究其民事、刑事及行政責任。

5.5.8 本校之委外廠商或合作廠商與本校業務合作時，均應簽訂保密契約，使其充分瞭解個人資料保護之重要性及洩露個資之法律責任。倘有違反保密義務之情事者，將依法追究其民事及刑事責任。

5.6. 利害關係人之參與及期許

5.6.1 本校個人資料保護及管理決議事項應納入「智慧財產權暨個人資料保護委員會」報告，涉及重大決議之會議紀錄應提報主管機關（教育部）及利害關係人（如企業雇主、畢業校友、學生家長、本校教職員工生及其他與本校相關人士等），如有任何

個人資料保護管理政策					
文件編號	Takming-PIMS-A-001	機密等級	一般	版次	1.0

回饋事項，將列入下次「智慧財產權暨個人資料保護委員會」會議之討論議題。

6. 修訂

為確保個資保護管理矯正預防措施之有效運作，應落實管理審查機制，或因時勢變遷或法令修正等事由，本校每年至少舉行一次「智慧財產權暨個人資料保護委員會」會議予以適當評估或修訂。

7. 施行

本政策須經「智慧財產權暨個人資料保護委員會」審核，核定後公告實施，修正時亦同。