萬能科技大學

個人資料保護管理政策

機密等級：一般

文件編號：PIMS-A-001

版　　次：2.3

發行日期：113 年 12 月 31 日

修　訂　紀　錄				
版次	修訂日期	修訂頁次	修訂者	修訂內容摘要
1.0	103 年 3 月 4 日	-	個資保護推動委員會	初版
2.0	108 年 9 月 11 日	1~4	資訊安全暨個人資料保護推動委員會	修訂目標、壹、肆、伍、陸、柒
2.1	112 年 12 月 5 日	4	資訊安全暨個人資料保護推動委員會	修訂柒
2.2	113 年 10 月 15 日	4	資訊安全暨個人資料保護推動委員會	修訂陸
2.3	113 年 12 月 31 日	1	資訊安全暨個人資料保護推動委員會	修訂壹

目錄

壹、 個人資料之蒐集、處理與利用 1

貳、 個人資料之國際傳遞 1

參、 個人資料之調閱與異動 2

肆、 個人資料之例外應用 2

伍、 個人資料之保護 3

陸、 利害關係人之參與及期許 3

柒、 個人資料保護管理政策之修正權 4

個人資料保護管理政策					
文件編號	PIMS-A-001	機密等級	一般	版次	2.3

萬能科技大學（以下簡稱本校）係以從事教學與研究為目的之機構，為符合我國個人資料保護法之要求與展現本校對個人資料保護之決心，建立個人資料管理制度以符合「個人資料保護法」（以下簡稱個資法）之法規及其它有關法令規範要求，特訂定個人資料保護管理政策（以下簡稱本政策）為最高指導原則以進行個人資料的蒐集、處理及利用。個人資料保護管理目標如下：

一、遵守「個人資料保護法」、「個人資料保護法施行細則」與「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計畫實施辦法」之要求，並採取適切之個人資料保護措施以保護個人資料蒐集、處理、利用、儲存、傳輸、銷毀之過程。

二、訂定個人資料保護管理相關規範及作業準則，並透過定期檢查、稽核或檢視等方式持續改善之，以落實執行個人資料保護管理，期使本校業務相關個人資料之安全，免於因外在威脅，或內部人員不當之管理與使用，遭致竊取、竄改、毀損、滅失、或洩漏等風險。

三、提升對個人資料之保護與管理能力，降低營運風險，並創造可信賴之個人資料保護及隱私環境。

壹、個人資料之蒐集、處理與利用

一、本校因營運所需在遵循我國個資法等法令規範下，於利用目的範圍內，蒐集當事人所提供之個人資料，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，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及利用之行為。

二、如需為特定目的以外之蒐集、處理及利用時，將依據個資法第十九、二十條之規定辦理；倘有需取得當事人同意之必要者，本校應依法取得當事人同意。

三、提升本校相關安全防護措施以保護所蒐集、處理以及利用之個人資料。

貳、個人資料之國際傳遞

本校取得之個人資料，如有進行國際傳遞之必要時，應遵守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，

並於確實有必要且在適當充分保護的狀況下辦理，又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，以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。

參、個人資料之調閱與異動

一、當本校接獲當事人提出有關其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、請求刪除等事項。

二、本校將盡力維護當事人提供之個人資料為正確與最新之狀態，並預防個人資料被竊取、洩漏、竄改等侵害。

肆、個人資料之例外應用

一、本校對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，應符合個資法第二十條及相關法令規定，並以正式公文查詢外，本校不得對第三人揭露：

(一)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者。

(二)其他政府機關因執行公權力並有正當理由所需者。

(三)與公眾生命安全有關之機關（構）為緊急救助所需者。

二、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：

(一) 法律明文規定。

(二) 為增進公共利益。

(三) 為免除當事人之生命、身體、自由或財產上之危險。

(四) 為防止他人權益之重大危害。

(五) 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。

(六) 有利於當事人權益。

(七) 經當事人同意。

伍、個人資料之保護

一、成立個人資料保護組織，明確定義相關人員之責任與義務。

二、建立與實施本校個人資料管理制度(以下簡稱 PIMS)，以確認本政策之施行；全體員工及委外廠商均應遵循本校 PIMS 之規範與要求，並定期審查 PIMS 之運作。

三、為防止個人資料被竊取、竄改、毀損、滅失或洩漏，本校設置資訊安全暨個資保護推動委員會，統籌各項個資保護作業原則規劃事宜。

四、個人資料檔案應建立管理制度，分級分類管理，並針對業務流程與接觸人員建立安全管理規範。

五、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，防止未授權的非法存取，維護個人資料之隱私性，應建立安全保護機制，並定期查核。

六、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。

七、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，且有效維護處理紀錄。

八、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「個人資料保護緊急應變處理作業說明書」通報程序辦理。

九、本校係以嚴謹之措施與政策保護當事人(包含未成年)之個人資料，包括本校之所有接觸到個人資料的教職員工生，均受有個資法及隱私權保護之教育訓練。倘有洩露個資之情事者，將將視情節輕重追究其民事及刑事責任或依本校之相關規定進行懲處。

十、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。

陸、利害關係人之參與及期許

一、本校個人資料保護及管理決議事項應納入個人資料保護推動委員會報告，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

及其他與本決議相關人士等)，如有任何回饋事項，將列入下次推動委員會議之討論議題。

二、為確保本校矯正措施之有效運作，應落實管理審查機制，本校每年至少舉行一次推動委員會議，並確實討論下列議題：

(一) 過往管理審查之議案的處理狀態

(二) 資通訊安全或個資管理要求的變更，如上級機關要求、最高行政管理會議決議事項

(三) 管理目標與指標量測結果

(四) 內外部稽核結果

(五) 資安/個資事故與不符合項目之矯正情形

(六) 風險評鑑結果及風險處理計畫執行進度

(七) 持續改善之機會

柒、個人資料保護管理政策之修正權

本政策每年定期或因環境變遷或法令修正等事由，得予以適當修訂，經本校資訊安全暨個人資料保護推動委員會通過，陳 校長核定後公告實施，修正時亦同。