亞東學校財團法人亞東科技大學停車場個人資料檔案安全維護計畫
(草案)

一、訂定依據

依據交通部於 104 年 9 月 24 日以交路字第 10450122941 號令訂定發布之「停車場經營業個人資料檔案安全維護計畫及處理辦法」規定辦理。

二、管理人員及資源

（一）管理人員：

1. 配置人數：1 人。
2. 職責：負責規劃、訂定、修正與執行計畫或業務終止後個人資料處理方法等相關事項，並定期向亞東學校財團法人亞東科技大學（以下簡稱本校）主管或負責人提出報告。本計畫經檢視有修正必要時，應於修正後 6 個月內送地方主管機關備查。

（二）個人資料保護管理政策：遵循個人資料保護法關於蒐集、處理及利用個人資料之規定，並確實維護與管理所保有個人資料檔案安全防止個人資料被竊取、竄改、毀損、滅失或洩漏。

三、個人資料之範圍

（一）特定目的：本校以月租方式出租停車格位，並依「路外停車場租用定型化契約應記載或不得記載事項」與停車位租用人所簽訂之契約。

（二）個人資料：本計畫所稱自然人之個人資料，係指停車位租用人姓名、出生年月日、國民身分證統一編號、聯絡方式（住址、電話、電子郵件）、車號及其他得以直接或間接方式識別該個人之資料。

四、風險評估及管理機制

（一）風險評估

1. 經由本校電腦下載或外部網路入侵而外洩。
2. 經由接觸書面契約書類而外洩。
3. 員工及第三人竊取、毀損或洩漏。

（二）管理機制

1. 藉由使用者代碼、識別密碼設定及文件妥適保管。
2. 定期進行網路資訊安全維護及控管。

3. 電磁資料視實際需要以加密方式傳輸。
4. 加強對員工之管制及設備之強化管理。

五、個人資料蒐集、處理及利用管理措施

（一）直接向當事人蒐集個人資料時，應明確告知以下事項：

1. 本校名稱。
2. 蒐集目的或其他特定目的。
3. 個人資料之類別。
4. 個人資料利用之期間、地區、對象及方式。
5. 當事人得請求閱覽、製給複製本、補充或更正、停止蒐集、處理、利用或刪除其個人資料。
6. 當事人得自由選擇提供個人資料時，不提供將對其權益之影響。

（二）所蒐集非由當事人提供之個人資料，應於處理或利用前向當事人告知個人資料來源及前項應告知之事項。

（三）本校得為辦理第二點第一款停車場租用契約之特定目的進行個人資料蒐集、處理、利用，於租用期限屆滿時應主動刪除或銷毀。

（四）當發現蒐集之個人資料不正確時，適時更正或補充；因可歸責於本校之事由，未為更正或補充之個人資料，並應於更正或補充後，通知曾提供利用之對象；個人資料正確性有爭議者，應主動或依當事人之請求停止處理或利用。

（五）利用個人資料為行銷時，當事人表示拒絕行銷後，應立即停止利用其個人資料行銷，並週知所屬人員。

（六）停車位租用人表示拒絕行銷或請求閱覽、製給複製本、補充或更正、停止蒐集、處理、利用或刪除其個人資料時，連絡窗口為：林甄怡 ；電話為：02-77388000 分機 1518。並將聯絡窗口及電話等資料，揭示於本校營業處所或網頁。

（七）負責保管及處理個人資料檔案之員工，其職務有異動時，應將所保管之儲存媒體及有關資料檔案移交，以利管理。

（八）本校員工如因其工作執掌相關而須輸出、輸入個人資料時，均須鍵入其個人之使用者代碼及識別密碼，同時在使用範圍及使用權限內為之，其中識別密碼並應保密，不得洩漏或與他人共用。

（九）由指定之管理員工定期清查所保有之個人資料是否符合蒐集特定目的，

若有非屬特定目的必要範圍之資料，或特定目的消失、期限屆滿而無保存必要者，即予刪除、銷毀或其他適當處置。

（十）本校如有委託他人（或他公司）蒐集、處理或利用個人資料時，當對受託者為適當之監督並與其明確約定相關監督事項。

（十一）所蒐集之個人資料如需作特定目的外利用，必須先行檢視是否符合規定。

（十二）本校因故終止業務時，原保有之個人資料，即依規定不再使用，並採銷毀方式處理。

（十三）停車場租用契約屆滿或終止，本校將主動刪除或銷毀個人資料。

六、事故之預防、通報及應變機制

（一）預防：

1. 本校員工如因其工作職掌而須輸出、輸入個人資料時，均須鍵入其個人之使用者代碼及識別密碼，同時在使用範圍及使用權限內為之。
2. 本校對內或對外從事個人資料傳輸時，加強管控避免外洩。
3. 加強員工教育宣導，並嚴加管制。

（二）通報及應變：

1. 發現個人資料遭竊取、竄改、毀損、滅失或洩漏即向地方主管機關及本校主管或負責人通報，並立即查明發生原因及責任歸屬，及依實際狀況採取必要措施。
2. 對於個人資料遭竊取之停車位租用人，應以適當方式通知使其知悉及本校個人資料外洩事實、已採取之處理措施、客服電話窗口等資訊。
3. 針對事故發生原因研議改進措施。

七、資料安全管理、員工管理及設備安全管理

（一）資料安全管理

1. 電腦存取個人資料之管控：

（1）於電腦設置識別密碼、保護程式密碼及相關安全措施。

（2）本校員工如因其工作職掌相關而須輸出、輸入個人資料時，均須鍵入其個人之使用者代碼及識別密碼，同時在使用範圍及使用權限內為之，其中識別密碼並應保密，不得洩漏或與他人共用。

（3）個人資料檔案使用完畢應即退出，不得任其停留於電腦顯示畫面上。

（4）定期進行電腦系統防毒、掃毒之必要措施。

（5）重要個人資料（如國民身分證統一編號等）應另加設管控密碼，非經陳報本校主管核可，並取得密碼者，不得存取。

2. 紙本資料之保管：

（1）對於契約書件應存放於公文櫃內並上鎖，員工非經本校主管或負責人或業務主管同意不得任意複製或影印。

（2）對於記載個人資料之紙本丟棄時，應先以碎紙設備進行處理。

（二）員工管理

1. 本校依業務需求，得適度設定所屬員工（例如主管、非主管員工）不同之權限，以控管其個人資料之情形。
2. 本校之員工每學期應變更識別密碼1次，並於變更識別密碼後始可繼續使用電腦。
3. 本校員工應妥善保管個人資料之儲存媒介物，執行業務時依個人資料保護法規定蒐集、處理及利用個人資料。
4. 本校與員工所簽訂之相關勞務契約列入保密條款及相關之違約罰則，以確保其遵守對於個人資料內容之保密義務（含契約終止後）。
5. 對於新進員工應特別給予指導，務使其明瞭個人資料保護相關法令規定、責任範圍及應遵守之相關管理措施。

（三）設備安全管理

1. 建置個人資料之有關電腦設備，資料保有單位應定期保養維護，於保養維護或更新設備時，並應注意資料之備份及相關安全措施。
2. 建置個人資料之個人電腦，不得直接作為公眾查詢之前端工具，非有必要不得任意移動電腦設備，並適度建置空調、消防、防鼠除蟲等保護設備或技術。
3. 本校應指派專人管理儲存個人資料之相關電磁紀錄物或相關媒體資料，非經單位主管同意並作成紀錄不得攜帶外出或拷貝複製。
4. 本校對於停車位租用人之個人資料檔案應定期(例如：每個月)備份。
5. 電腦、自動化機器或其他存放媒介物需報廢汰換或轉作其他用途時，本校主管或負責人或業務主管應檢視該設備所儲存之個人資料是否確實刪除。

八、資料安全稽核機制

（一）本校定期(每年至少 1 次)辦理個人資料檔案安全維護稽核，查察本校是否落實本計畫規範事項，針對查察結果不符合事項及潛在不符合之風險，應規劃改善措施，並確保相關措施之執行。執行改善與預防措施時，應依下項事項辦理：

1. 確認不符合事項之內容及發生原因。
2. 提出改善及預防措施方案。
3. 紀錄查察情形及結果。

（二）前項查察情形及結果應載入稽核報告中，由本校主管或負責人簽名確認。

九、使用記錄、軌跡資料及證據保存

本校建置個人資料之電腦，其個人資料使用查詢紀錄，每年需將該紀錄檔備份並設定密碼，另亦將儲存該紀錄之儲存媒介物保存於適當處所以供備查至少五年。

十、個人資料安全維護之整體持續改善

（一）本校將隨時依據計畫執行狀況，注意相關技術發展及法令修正等事項，檢討本計畫是否合宜，並予必要之修正。

（二）針對個資安全稽核結果不符合法令之虞者，規劃改善與預防措施。

十一、業務終止後（含契約屆滿或終止）之個人資料處理方法

本校結束營業後，所保有之個人資料不得繼續使用，紙本資料以碎紙機絞碎銷毀，儲存於本校系統及電腦硬碟資料逕行刪除，並留存相關紀錄（標註有日期並揭露地點之照片或錄影影片）至少五年。

十二、核定與發布

本計畫經總務會議審議通過後，陳請校長核定後發布實施，修正時亦同。