國立高雄師範大學

車輛通行證線上申請系統及資訊安全 Q&A

➢ 為何需上傳「行車執照與駕駛執照」?

本校有鑑於和平校區汽車停車位嚴重不足,須依實際與校區工作者之教職員工生需求為核發車證要件,依本校「車輛行駛暨停放校區管理辦法」第七條:申請通行車證應檢附下列文件:

一、汽車通行證:

1.教職員工識別證或學生證或兼任教師、社團指導教師之聘書或校長核定之文件等影本。

2.申請人之汽車駕駛執照及行車執照(應登記為本人或其配偶、直系親屬或配偶之父母、親兄弟姊妹所有)之影本。如行車執照記載之車主與申請者不同時,另需檢附可資證明其與車主關係之文件影本,如申請人之身分證影本。

3.行車執照之車主非本人或其配偶、直系親屬或配偶之父母者、**親兄弟姊妹所有**,僅能辦理限燕巢校區使用之通行車證。

4.在職進修碩、博士班學生如有機關或公司配屬其專用之汽車,可切結辦理汽車通行證。

二、機車通行證:

教職員工識別證或學生證或兼任教師、社團指導教師之聘書或校長核定之文件等影本及本人機車駕駛執照等之影本。

三、單車通行證:

教職員工識別證或學生證或兼任教師、社團指導教師之聘書或校長核定之文件等影本。

廠商申請前項通行車證時,應檢具業務相關單位簽認之申請書、本人駕駛執照及行車執照等文件影本。

上揭條文規定如此嚴謹，亦係經過本校車輛管理委員會修訂通過經行政會議審議通過公告實施，為保障本校教職員工生停車權益而規定。因本校位處市區精華地，停車位一位難求，常有利用各方管道借證停車情事與流弊，造成校內停車位短缺，因此車管會為保障本校師生停車權益，在申請時須初步審核，預防有借證停車情事，敬請同仁為共同維護本身權益，能協助與支持車管會辦理。

➢ 改為線上系統為力求行政程序精簡。

為便於教職員工生申請車證之前置行政作業，改為線上系統後以減少各單位等候辦證時間大為縮短流程，尤其日間部與進修學院之學生更為便利。

➢ 可以由系、所或單位統一申請嗎?

目前業已開放可由單位申請統一窗口為單位同仁辦理線上申請，惟所需檢附之行照駕照等相關文件仍須交由窗口協助掃瞄上傳。

以往所需檢附資料「行車執照、駕駛執照」影本，目前改為線上登錄，只要不換車可持續使用，下一年度辦理時只需申請續辦即刻核發車證，已達簡化之程序。

如能覺不方便可直接至本校兩校區總務處事務組臨櫃逕行辦理，開學後亦開放集體申請車證(和平校區：行政大樓 3 樓開標室、燕巢校區：行政大樓 3 樓開標室)。

➢ 有關上傳相關證件，個資保護事宜之疑慮?

經本校「圖書資訊處」詳細說明如下，請卓參：

一、 為確實落實資訊系統之安全管理，需要導入風險管理，本校已導入 ISMS (Information Security Management System)資訊技術規範。(細部說明如下『第一點說明』)

二、 且本校為強化資安稽核，並因應教育部來文強力要求，目前已按規劃完成相關資料、程序處理，預計於 105 年底進行校外稽核，以取得資訊安全認證。(細部說明如下『第二點說明』)

三、 為加速實體網路安全，本校和平骨幹網路防火牆試機測試，完成連線教育

部網路攻擊行為資料庫。(細部說明如下『第三點說明』)

第一點說明：

所謂風險是指一個事件對資訊安全目標所造成的衝擊或影響程度。資訊系統面對的風險非常多，包含系統受駭客攻擊，資料被竊取，網路無法連線、機房空調故障，以至系統不穩定，無法提供正常服務等。本校導入並落實 ISMS 稽核，當中針對資訊安全的三要素進行:

- 機密性：是指採用適當的安全機制保護資料和資源以避免暴露於無權限人員或程式之下，而危害到資訊安全目標。換言之，機密性是為維護資料在傳輸、儲存、與處理狀態時，不被非授權人員之存取、使用、或竄改。許多攻擊型態都是以破壞資訊的機密性為主，例如：網路抓取封包、偷取密碼檔案、利用監視軟體、網路掃描等，都是破壞機密性的攻擊行為。
- 完整性：是指確保維持資料原來的狀態，只允許有權限的使用者可以修改資料內容。在資料內部與外部均需維持資料的一致性，例如，傳輸資料時，在傳輸中的資料與接收、儲存的資料，均需要保持一致而且是可以確認的。
- 可用性：是為了確保資訊與系統能夠持續營運、正常使用，當合法使用者要求使用資訊系統時，例如，電子郵件、應用系統等，使用者均可以在適當的時間內獲得回應，並獲得所需服務。可用性需要與前述的機密性與完整性配合一起考慮，以符合既定的資訊安全目標。

第二點說明：

本校為強化資安稽核，並因應教育部來文強力要求，目前已按規劃完成相關資料、程序處理，預計於 105 年底進行校外稽核，以取得資訊安全認證。

(一) 建立資安通報機制，即時處理相關資安事件。

(二) ISMS 教育訓練課程。

(三) 資安內部稽核、管審會議及驗證稽核。

(四) 本處以既有資訊安全管理規範 ISO27001:2005 為基礎框架，並參考 2013 新版規範及教育部規範修訂原有文件、持續辦理有關業務。預計於 105 年底取得 ISO27001:2013 之資訊安全認證。

第三點說明：

為加速實體網路安全，和平骨幹網路防火牆試機測試，完成連線教育部網路攻擊行為資料庫。實體校園防火牆試機建置，完成連線教育部網路攻擊行為資料庫，並建置本校資安檢測實體沙箱環境，在不影響主骨幹資訊服務運作下，對未知的網路攻擊進行預測、導流、檢測及防治。

對於人員上之疑慮：

(一)個資保護相關法律規範(細部說明如下『第一點說明』)

(二)本校導入個資稽核(細部說明如下『第二點說明』)

(三)本校圖資處資訊系統相關同仁須簽署個資保密協定，若有違反相關規定，將加重刑責，保密協定內容如下『第三點說明』)。

第一點說明：

公務員違反個資法刑責個人資料保護法修法之後，加重了罰責。違反個資法，不僅要面對民事損害賠償，還有刑事責任與行政處罰，簡單的說，不只要賠錢，還可能被抓去關。而且，負責人（代表人、管理人）更要負起實質的監督責任，非公務機關若因違法而被處以罰鍰，負責人亦會被課以相同額度的罰鍰，可不能卸責；除非，負責人能證明已善盡防止的義務。在民事損害賠償部分，個資法對於不易或不能證明實際損害額時，規定每人每一事件可求償 5 百元以上 2 萬元以下，而同一事件的最高賠償總額為 2 億元以下。但是若可證明實際損害金額每人超過 2 萬元、總額超過 2 億元，則以實際的損害額賠償。

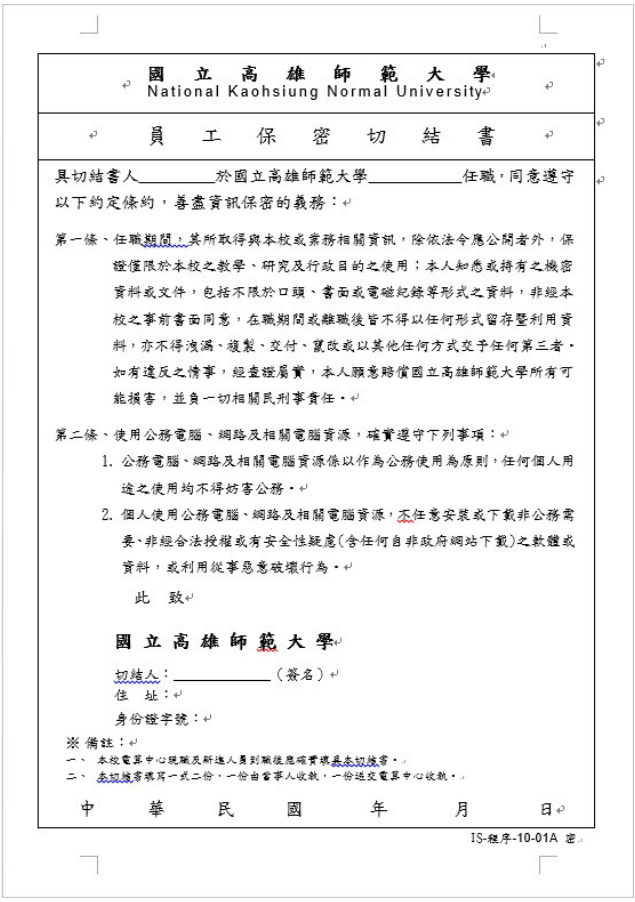
在刑事責任方面，違法最高可處 2 年以下有期徒刑、拘役或科或併科新臺幣 20 萬元以下罰金，對於意圖營利而犯罪者，特別加重罰責，最高可處 5 年以下有期徒刑，得併科新臺幣 100 萬元以下罰金。

行政處罰亦加重罰則，最高可處新臺幣 5 萬元以上 50 萬元以下罰鍰，並可限期改善，若未改善可繼續處罰。此外，個資法對公務機關加重責任。由於公務機關掌管大量的國民個人資料，因而必須以更嚴格的標準看待。公務機關為無過失損害賠償責任，只要違法就必須負損害賠償，由國家賠償；此外，公務人員經手大量人民的個人資料，若假借職務上的權力、機會或方法之便，故意違法，應處以更嚴厲的處罰，加重刑責至二分之一，因而意圖犯法的公務人員，最高可處以 7 年 6 個月的有期徒刑。

第二點說明：

應教育部來文強力要求，已協商秘書室，展開個資保護稽核準備工作，預計年底前進行，106 年完成。依據 ISO29100:2011、BS10012:2009 及教育部「教育體系資通安全暨個人資料管理規範」等相關個資法規，由秘書室主辦、本處協辦建置本校個人資料保護管理系統(PIMS)及相關程序、表單。

第三點說明：



國立高雄師範大學
National Kaohsiung Normal University

員工保密切結書

具切結書人_____於國立高雄師範大學_____任職，同意遵守以下約定條約，善盡資訊保密的義務：

第一條、任職期間，其所取得與本校或業務相關資訊，除依法令應公開者外，保證僅限於本校之教學、研究及行政目的之使用；本人知悉或持有之機密資料或文件，包括不限於口頭、書面或電磁紀錄等形式之資料，非經本校之事前書面同意，在職期間或離職後皆不得以任何形式留存暨利用資料，亦不得洩漏、複製、交付、竄改或以其他任何方式交予任何第三者，如有違反之情事，經查證屬實，本人願意賠償國立高雄師範大學所有可能損害，並負一切相關民刑事責任。

第二條、使用公務電腦、網路及相關電腦資源，確實遵守下列事項：

1. 公務電腦、網路及相關電腦資源係以作為公務使用為原則，任何個人用途之使用均不得妨害公務。
2. 個人使用公務電腦、網路及相關電腦資源，不任意安裝或下載非公務需要、非經合法授權或有安全性疑慮(含任何自非政府網站下載)之軟體或資料，或利用從事惡意破壞行為。

此　致

國立高雄師範大學

切結人：_____（簽名）
住　址：
身份證字號：

※備註：
一、本校電算中心現職及新進人員到職後應確實填具本切結書。
二、本切結書填寫一式二份，一份由當事人收執，一份送交電算中心收執。

中　華　民　國　　年　　月　　日

IS-程序-10-01A 密

➢ 新規劃之車證線上系通將與本校兩校區車輛出入管制系統提升與介藉接與監視錄影系統之改善。

本校預訂於 105 年 9 月，將完成兩校區出入口網路攝影機(IP Camera/IPCam)架設，另搭配「車牌辨識系統」將校區已辦「車證」，及取得「臨時通行證」之來賓車輛出入只要出示本校核發之「QR Code」手機、或書面圖檔，即可快速進入校區，已達校區車輛出入作有效管制，與管理作業申請程序精簡。