臺中市政府警察局違法查詢個資及洩密防貪指引手冊

臺中市政府警察局 編印
中華民國 112 年 10 月

慎用個資 避免觸法

警察為維護治安、交通和為民服務，擁有使用資料庫職權，並得查詢違反法（令）或相關民眾之個人資料，以確定當事人身分，釐清事實並作後續偵查、違序、交通裁罰或為民服務處理。少數警察同仁非因公查詢相關資料庫，已經違反相關規定，或因承辦業務故意洩漏機密訊息，尤有甚者將民眾個資販售、轉讓、通知或PO文公開，觸犯貪污、洩密或違反個資等罪嫌，因而遭到司法追訴和行政懲處，不僅戕害民眾對警察信任度，也必需付出免職、降級和處分等慘痛代價，得不償失。

為提升同仁正當使用資料意識，避免發生不當查詢資料庫，擅自使用個資衍生貪污、洩密等重大違法（紀）情事，本局特別蒐集警察機關曾經發生之違法查詢、洩密之個案，並參照相關法令規定，編撰防貪指引手冊，提供同仁參考，並請同仁「慎用個資 避免觸法」。

局長 李文尊

目 錄


一、前言

一、前言

員警於偵辦或查察案件時，需查詢民眾個資或其它相關隱私資料，惟近年民眾對於個人資料保護意識抬頭，更要求執法機關於查詢民眾個資及隱私資料時要有明確法律依據；然而，員警如非因公務私自查詢民眾個資時，相關查詢紀錄均可被事後追溯，該不當查詢行為可能遭受行政及刑事上之不利處罰。為確保同仁對於相關公務機密保護法規之了解，本局爰製作此一防貪指引手冊，內容包括警察機關公務機密維護相關法規、廉政相關法令簡介、案例研析等，並搜集相關司法判決。期望藉由本防貪指引手冊，使同仁對於法規有更加具體且正確之瞭解，避免誤觸法令，且於執行勤務時亦能有所依循。

二、警察機關公務機密維護相關法規

警察機關公務機密維護實施規定

中華民國 105 年 02 月 04 日修正

一、內政部警政署（以下簡稱本署）為確實維護警察機關公務機密，特訂定本規定。

二、警察機關為落實執行公務機密維護工作，其政風業務單位應辦理下列事項：

（一）推動訂定或修正公務機密維護規定。

（二）會同相關業務單位宣導公務機密維護法令及作法。

（三）推動資訊保密措施及查處洩密案件。

未設政風室者，由保防單位會同相關業務單位辦理。

三、警察機關應結合業務特性及主客觀環境，配合實際發生案例，以生動、活潑、柔性及自然方式，透過各項集會、專題演講、訓練講習及傳播媒介，辦理公務機密維護宣導，增進所屬保密觀念，其宣導內容如下：

（一）公務機密維護相關法規。

（二）公務機密維護專業知識及實務作法。

（三）公務機密維護現存缺失檢討及策進作為。

（四）洩密或違反保密規定相關案例、檢討研析及補救措施。

四、警察機關檔案管理及業務主管單位，應依國家機密保護法、國家機密保護法施行細則、文書處理手冊及其他相關法規，針對機密文書及設備採取必要之管制措施，並依下列規定辦理：

（一）機密文書應存放於具有安全防護功能之箱櫃，並裝置密鎖。存放場所或區域，得禁止或限制人員、物品進出，或為其他必要之管制措施。

（二）機密文書應定期清查，並依法辦理機密等級之變更或註銷事宜。

（三）廢棄文書及內建有記憶體晶片或硬碟機之報廢設備，應指派專人監督、澈底銷毀。

五、警察機關事務管理單位應會同政風業務單位，檢查機關內部之

通信設備、辦公廳舍、會議室及其他重要機密設施；發現可疑或異常，應保持現場完整，報告機關首長核可後，洽請相關單位派員處理。

六、警察機關配有保密裝備者，密碼作業單位應依政府機關密碼統合辦法及密碼作業規定，加強注意保密措施及辦理下列事項：

（一）審慎遴派密碼作業人員，並切實辦理平時考核，發現可疑或異常情事，足以影響業務之安全時，應迅速簽報機關首長，妥適處理，並知會政風業務單位。

（二）密碼作業場所應設置消防及安全防護設備，非授權人員不得進入。

（三）保密裝備、密體及保密作業相關文件辦理架裝、汰換、交接及銷毀，政風業務單位應切實監督其作業情形。

七、警察機關應加強資訊使用管理及建立資訊安全稽核制度，防止公務機密外洩，經稽核發現異常者，應即清查其原因及具體事證，妥適處理。

政風業務單位應針對前揭執行情形定期辦理檢查。

八、警察機關政風業務單位，應會同業務權責單位實施公務機密維護檢查，並依下列規定辦理：

（一）針對機關特性，綜合分析公務機密維護狀況。

（二）根據狀況研判，研擬檢查計畫，簽報機關首長核定後實施。

（三）檢查結果之優劣事實、改善意見或具體建議，簽報機關首長核閱後，移請缺失單位檢討改進，並綜整執行成效，每半年陳報本署備查。

（四）每半年應實施一次以上之定期檢查。但為機關業務需要或因應實際狀況，得隨時辦理不定期檢查。

九、警察機關發現洩密或違反保密規定案件時，應依下列規定辦理：

（一）屬於本警察機關者：

1.應即密報機關首長，並將查處情形密陳本署審辦。

2.於查處結果確定後，將行政懲處或移送法辦情形，進行專案檢討，並將相關檢討報告及策進作為，於十五日內密陳本署

備查；本署派員查處時亦同。

3.前目之檢討報告及策進作為，列為本署年度政風查處及預防工作考核之公務機密維護專報成績。

（二）非屬本警察機關者：應通報該管警察機關處理並副陳本署。

（三）非屬警察機關者：應通報該管機關政風機構處理及副知法務部廉政署，並應注意相關保密規定。

（四）各級人員發現承辦或保管之機密資料已洩漏或遺失，或有洩漏或遺失之虞者，應報告單位主管，迅作處理，並通報政風業務單位。

（五）政風業務單位應協調業務主管單位，在不影響偵辦原則下，研採必要之補救措施，使損害減至最低程度，並個案研析洩密或違反保密規定之原因及管道，以資防範。

（六）各級人員洩密或違反保密規定者，視情節追究相關責任及其主官或主管之考核監督責任。

前項違反保密規定，指違反業務主管單位訂定之保密作為，尚未達洩密之程度者。

十、警察機關得視主管業務性質及實際需要，訂定公務機密維護要點，陳報本署核定後實施。

警察機關資通安全實施規定

中華民國 112 年 05 月 31 日修正

一、內政部警政署（以下簡稱本署）為促進各警察機關訂定資通安全政策，建立資通安全管理制度，採行適當必要之資通安全措施，確保資訊蒐集、處理、利用、儲存及傳輸之安全，特訂定本規定。

二、本規定所稱資通安全政策，指為達成以下資通安全目標所訂定之資通安全管理作業規定、措施、標準、規範及行為原則：

（一）建立資通安全管理制度，訂定重要資訊資產及關鍵性業務之防災對策及災變復原計畫，確保機關可持續運作。

（二）確保資訊資產包括硬體、資訊、軟體、公共設施及人員等之安全，避免不當使用、洩漏、竄改或破壞等情事。

（三）防止洩漏機密資料，建立資通安全，人人有責之觀念，進行資通安全必要訓練，提高資通安全意識。

三、警察機關資通安全維護，應依據個人資料保護法、國家機密保護法、政府資訊公開法、資通安全管理法及其子法、行政院及所屬各機關資訊安全管理規範、行政院及所屬各機關資訊安全管理要點等相關法令，衡酌機關業務需求，參考本規定訂定資通安全政策，研訂資通系統之安全等級，並以書面、電子或其他方式通知所屬員工及有關機關（構）。

四、各警察機關應實施資訊資產安全分級管理措施，其規定如下：

（一）訂定資通安全等級分類基準，建立資訊資產目錄，包括資訊資產項目、保管者及安全等級分類等。

（二）資訊及系統之輸出資料，標示適當安全等級及保護措施，以利使用者遵循。

（三）各資訊作業單位自行設計之紀錄表件，應按機密等級訂定保存期限，妥為保管，備供查考。

（四）應指定機關副主官以上人員或相當人員，負責推動、協調及督導資通安全業務。

五、資通安全管理業務分工如下：

（一）資訊單位：負責資通安全政策、計畫及訓練，以及技術規範之研議、評估、建置、運作、維護及業務督考等事項。

（二）各系統業務單位：負責主管電腦系統資料之安全需求研議、使用管理維護及訂定資料保密安全措施。

（三）政風業務單位：負責洩密或違反保密規定案件之調查、處理及資通安全稽核事宜，並會同相關單位辦理。

（四）督察單位：負責政風業務單位分工外之違法及違紀案件查處。

（五）使用單位：負責追蹤及管制電腦資料處理過程，防止資料外洩。

六、資訊系統應具備下列之安全保護功能：

（一）帳號密碼保護。

（二）系統使用權限及管理。

（三）電腦病毒及惡意程式防制。

（四）軟體程式保護。

（五）資料庫保護。

七、帳號密碼保護之安全管制規定如下：

（一）系統使用者應妥善保存其帳號密碼，不得供他人使用，並嚴禁多人使用同一帳號密碼，以明責任。

（二）系統使用者因業務調整、調職、停職或離職時，管理者應立即依規定辦理異動事宜。

（三）系統使用者至少每三個月應定期更換密碼，其長度以英文及數字至少八位組成，發覺有洩漏之虞時，應立即更換。

八、系統使用權限及管理之安全管制規定如下：

（一）應用系統應依業務需要建立使用者權限，避免非業務人員操作、使用或破壞。

（二）使用者因業務調整、調職、停職或離職時，管理者應立即辦理系統使用權限異動事宜。

（三）透過網路分享資料檔案時，必須設定使用權限。

（四）使用權限管理應定期更新並作成書面紀錄，妥適保管備查。

九、電腦病毒及惡意程式防制之安全管制規定如下：

（一）應在電腦、個人電腦、行動設備及伺服器安裝防毒軟體，定期掃描電腦系統及資料儲存媒體，並定期更新病毒碼、掃描引擎及修補系統漏洞。

（二）使用儲存媒體、外接式硬碟或隨身碟，應先執行病毒掃描。

（三）使用解毒軟體應先充分瞭解電腦病毒特性及確定解毒軟體功能。

（四）應建立防制電腦病毒及惡意程式攻擊及回復作業之處理程序。

（五）發現病毒感染或惡意程式時，由資訊承辦人負責記錄追蹤及處理。

（六）使用Virustotal等雲端防毒網站掃描病毒或惡意程式時，上傳資料應以編碼後的HASH作為檢測值，不得直接傳送原始檔案上網掃描，避免資料外洩。

十、軟體程式保護之安全管制規定如下：

（一）各單位自行開發之應用系統，應建立版本控管機制，非經單位主管授權不得任意修改。

（二）安裝及修改後之應用系統，其原始碼及相關文件，應責由專人保管，並複製三份分別儲存。

（三）軟體程式之儲存應由系統人員規劃及配置，並建立權限控管機制。

（四）應用系統開發或維護時，不得提供正式資料測試。

（五）資訊作業人員於修改程式或資料媒體內容時，必須經過各該主管核 可後實施。

（六）與非機關人員討論應用系統時，應簽訂保密協定。

（七）應用系統應訂定故障復原程序，以能迅速處理故障，恢復正常使用。

（八）不得將機關之應用系統複製至機關以外之設備。
（九）開發、測試及正式作業環境應作區隔。
（十）應注意避免軟體常見漏洞（如 OWASP TOP 10）及實作必要控制措施。
（十一）應執行軟體程式源碼及弱點掃描等安全檢測，修正應用系統漏洞。

十一、資料庫保護之安全管制規定如下：
（一）資料建置後，應定期執行資料及系統軟體備份。
（二）備份資料應異地儲存，並定期測試回復程序。
（三）備份資料儲存場所安全維護措施，應比照實體及環境場所辦理。

十二、網路之安全管制規定如下：
（一）對外開放資通系統主機，應架設於網路防火牆之非軍事區網（DMZ），並以防火牆與機關內部網路區隔，提高機關網路安全性。
（二）對外開放之資通系統主機，非必要不得開放遠端登入功能。
（三）對外開放之資通系統涉及機關或民眾資料檔案時，應以加密方式處理。
（四）具機密性及敏感性資料或文件，不得存放於對外開放之資訊系統中。
（五）網路管理者應隨時注意警示訊息，檢測連線狀況及安全防護措施，維護網路正常運作。
（六）各機關開放與非公務機關連線作業需求時，應做安全評估，訂定資通安全管理計畫，報經本署核准後實施。
（七）提供內部人員使用之網路服務，與開放有關人員從遠端登入內部網路系統之網路服務，應嚴格執行身分辨識作業，進行安全控管。
（八）對公務機關之連線，均須透過機關網路，未經機關核准，不得擅自建置有線或無線連線設備，以免造成安全漏洞；

有個別需求時，應與機關網路隔離，並另建置防火牆。

（九）非機關配置之電腦設備不得介接於各機關之網路；確有業務需求時，應提出申請，經機關首長核可後方可連線，作業結束後，原申請人應主動通知管理者撤銷其帳號及工作站網址。

（十）處理或存放機關重要機密業務資料之個人電腦應作實體線路隔離。

（十一）網路對外提供之連線服務，應以提供最低限度需求為原則，不對外提供服務之通訊埠應關閉。

（十二）網路管理員不得閱覽、增加、刪除及修改員工之私人資料。但發現可疑網路安全情事時，得報請主管同意後處理。

十三、網站之安全管制規定如下：

（一）網頁維護人員應每天檢查所屬業務之網頁，有無遭入侵、受攻擊或無法運作等異常情形，發現異常時，應即時通報資訊作業單位。

（二）網站首頁須具備即時自動復原機制。

（三）網頁應作備份管理，異動網頁須經單位主管核可後實施。

（四）網站資料應實施資料安全等級評估，機密性、敏感性及未經當事人同意之個人隱私資料不得上網公布。

（五）網站管理者應定期檢核相關日誌檔，遇有異常時，應立即採取有效因應措施。

十四、電子郵件安全管制規定如下：

（一）郵件伺服器禁止提供轉信功能。

（二）屬於「密」等級以上之公文及資料，不得以電子郵件傳送。但有電子郵件傳送之必要時，得經單位主管核准後以加密處理傳送。

（三）禁止以遠程終端機模擬形式來開啟電子郵件。

（四）使用者停（離）職後應立即刪除其郵件帳號。

（五）使用者如長期未收信以致影響郵件伺服器正常運作時，基於業務需要得移除該帳號。

（六）應設置郵件掃瞄過濾功能，以防範垃圾郵件與電腦病毒。

十五、個人使用者之管理規定如下：

（一）不得任意取得他人之登入帳號或密碼。

（二）不得以任何儀器、設備或軟體工具，竊聽網路上之通訊。

（三）不得於網路上取用未經授權之網路資源或檔案。

（四）不得將非法檔案建置於機關網路，或於網路上散播色情文字、圖片、影像或聲音等不法或不當資訊。

（五）不得以任何手段蓄意干擾或妨害網路系統之正常運作。

（六）不得於機關電腦逕行安裝未具合法版權或非公務用之軟體。

（七）非因公務不得瀏覽賭博或色情等網站。

（八）個人帳號及密碼應妥為保管，不得借予他人使用或張貼於電腦設備等場所。

（九）違反網路安全情事時，應限制或撤銷其網路資源存取權利。

（十）使用者離開電腦時，應鎖定使用環境，每日下班前，使用者應確實將主機、螢幕、印表機及印表機伺服器登出系統並關機。

十六、本署警政資訊系統資料查詢及更新之安全管制規定如下：

（一）於法定職掌必要範圍內，使用本署警政資訊系統查詢時，應確實登輸實際查詢人相關資料，查詢完畢時，務必結束連線登出系統。各機關應於每月下載前月之轄區內查詢紀錄電子檔，自行管考運用，並將相關稽核工作做成書面紀錄備查。

（二）本署警政資訊系統之電腦主機，應自動記錄全部帳號查詢及更新資料之時間、種類、內容及結果，並保留五年，以資查考。各機關下載之查詢紀錄電子檔，應指定專責人員保管，同時保存五年。

（三）請求查詢及提供資料，應符合個人資料保護法及機密檔案

管理辦法等相關法令規定。

（四）警察機關請求整批方式查詢資料或非警察機關請求查詢資料時，均應備文，並經該資料業務單位簽陳同意後辦理，其權責單位律定如下：

1.中央機關及其所屬機關或機構申請查閱電腦處理之民眾個人資料，由本署受理提供。

2.直轄市、縣（市）政府申請查閱電腦處理之民眾個人資料，由各該地區之警察局受理。

3.刑案資料由刑事警察局或各縣市警察局刑事單位負責受理提供；其餘資料除法令另有規定外，應由業務單位依個人資料保護法規定，簽會資訊單位陳請主官核定後提供。

（五）除系統業務單位訂有特別規定、員警執行公務當場表明身分或發生斷網、停電等情事外，禁止跨機關或單位代查資料。遇有辦案需要且出於情況急迫時，僅限於同一單位查詢，並應報告單位主管同意，嚴格執行身分辨識程序，將委託查詢員警及事由等資料，確實載明資訊系統或工作紀錄簿，以利日後稽核。

（六）資料應維護正確，發現資料錯誤時，應依相關規定，檢附正確資料，送相關單位辦理更正。

十七、資料輸出之安全管制規定如下：

（一）由本署警政資訊系統查得之各項系統資料，非經單位主管同意，不得擅自複製或外洩。

（二）報表提供遞送，其屬於密等級以上資料者，應以密件公文處理。

（三）輸出產生之廢紙應一律銷毀，不得留作他用。

十八、電腦維修作業之管理規定如下：

（一）電腦主機之維修，以設置現地實施，且不危及設備安全及資料之完整性為原則。

（二）對於委外廠商或參與維修人員，應限制其工作地點，並由

系統或有關人員直接監督或配合作業。

（三）有關記憶媒體組件更換及報廢，必須經由系統人員鑑定，並清除記憶內容後始得為之。

（四）委外廠商或參與維修人員檢驗或測試時，不得使用正式資料。測試資料及產生之紀錄必須攜出時，應經系統人員及其主管同意。

（五）非經核准嚴禁私接具有儲存裝置或對外連線功能設備及擅自加裝硬體配備或更改電腦系統環境之設定。

（六）電腦設備報廢前，應將所有儲存裝置資料移除。

十九、實體及環境場所之管理規定如下：

（一）電腦機房，未經核可，不得對外開放參觀及攝影或錄影。

（二）主要電腦設備，應置放於電腦機房，並設置門禁管制，未經許可，不得擅自進入及非法攜出資料、設備。

（三）視需要派值日人員值勤，加強場地及設施安全管制，未派駐值日人員時，應採必要之安全措施。

（四）危險或易燃物品及器具不得攜入機房，並定期檢查及評估發生火災、煙、水、灰塵、震動、電力供應及電磁幅射等風險之可能性，並採取必要之因應措施。

（五）電腦專用之電源插座，未經評估，不得使用於電腦以外之設備，避免造成跳電當機，影響電腦正常作業。

（六）不得攜帶筆記型電腦、行動儲存裝置、平板、手機、照相機或攝影機等裝置進入電腦機房。

二十、行動裝置之安全管制如下：

（一）行動裝置僅可安裝來自可信任來源之軟體，注意軟體權限，定期更新修補程式及安裝資安防護軟體。

（二）不得於行動裝置中留存重要資料，重要資料使用後應即刪除，另設定遠端定位及資料刪除功能，行動裝置報廢時，應清除所有資料。

（三）避免連結公開無線Wi-Fi網路傳輸隱私性高或機敏資料，

並確保使用之網路系統為可信任之網路。

（四）藍芽功能、GPS定位功能及NFC未使用時，應將其關閉。

（五）當行動裝置重新啟動、閒置或按下待機鈕後相當時間內未使用時，應設定自動進入畫面上鎖模式。

（六）不得破解行動裝置之安全措施。

（七）避免透過行動裝置上之即時通訊軟體（如：Line、WhatsApp、WeChat等），討論重要資訊或交換檔案，並不得加入來歷不明之聯絡人，避免遭受社交工程詐騙之風險。

二十一、各機關應定期辦理資通安全教育訓練及宣導，建立人員資通安全認知。

二十二、資通安全緊急應變處理程序規定如下：

（一）發生資通安全事件時，應依行政院國家資通安全會報之國家資通安全通報應變作業綱要，進行通報應變處理，以解決危機事件。

（二）資通安全事件發生時，應將發生事件之事實、可能影響之範圍、採取之應變措施等事項，依限填具資通安全事件通報單，透過上網、電話、傳真或電子郵件等方式，登錄於國家資通安全通報應變網站，並於完成處理後結案通報；於三日內將處理情形陳報本署。

二十三、各機關應訂定業務永續運作計畫，評估各種人為及天然災害對業務運作之影響，並訂定緊急應變與回復作業程序及相關人員之權責，定期演練及調整更新計畫。

二十四、各機關資訊單位每年依當年度本署函頒資訊業務督考計畫及警察人員獎懲標準辦理獎懲；本署當年度未函頒相關計畫，由各機關視需求辦理所屬資訊業務督考工作者，得於督考結束時，自行辦理業務獎勵，其規定如下：

（一）承辦人嘉獎一次，總額度嘉獎二次。

（二）得就所屬評核前三分之一單位辦理行政獎勵，承辦人嘉獎

一次，總額度嘉獎三次。

本署辦理本規定業務人員，承辦人每半年嘉獎二次，協辦人員嘉獎一次一人次，業務單位主管嘉獎一次。

有下列情形之一者，依規定辦理懲處：

（一）因個人明顯疏失違反本規定，應依情節輕重，核予申誡二次以下懲處併暫停使用資訊設備及網路資源。

（二）非因公務擅自查詢警政資訊系統資料經查屬實，尚未達洩密，視情節輕重核予記過一次以下懲處。

（三）非因公務擅自查詢警政資訊系統資料，因而發生洩密或資訊系統遭受破壞，未經起訴或不起訴，視情節輕重，核予記過二次以下懲處。

（四）查詢警政資訊系統資料，因而發生洩密或資訊系統遭受破壞，經起訴或緩起訴，除依各該法令查究處理外，並依警察人員獎懲標準相關規定視情節輕重議處。

二十五、各機關與委外廠商簽訂合約時，應明定委外廠商必須遵守之保密安全事項，並監督其資通安全維護事項；其違反合約情事時，應依相關法令追究責任。

警政日誌管理系統作業規定

中華民國 110 年 07 月 30 日修正

一、內政部警政署（以下簡稱本署）為強化員警正確使用警政資訊系統查詢資料作業，推動警政日誌管理系統（以下簡稱本系統），督促機關及所屬人員確實依法行政，防止濫用或侵害個人資料隱私，確保民眾個人資料安全，維護警察整體形象，特訂定本規定。

二、本系統提供之功能如下：

（一）各警察機關資訊、政風及各警政資訊系統（以下簡稱各系統）業務單位線上調閱員警查詢日誌。

（二）員警線上調閱個人查詢日誌。

三、本系統提供日誌內容如下：

（一）作業時間。

（二）單位。

（三）使用者。

（四）IP。

（五）作業種類。

（六）查詢條件。

（七）實際查詢者。

（八）實際查詢單位。

（九）用途。

四、本系統使用及權限管理之層級區分如下：

（一）第一層級：本署資訊室、政風室及各系統業務單位。

（二）第二層級：警察局、署屬各警察機關（構）、學校（以下簡稱專業警察機關）之資訊單位、政風單位及各系統業務單位。

（三）第三層級：警察分局、專業警察機關相當層級之資訊單位及各系統業務單位。

（四）第四層級：分駐（派出）所、隊及專業警察機關相當層級

之單位。

（五）第五層級：各系統使用者及單位主管。

五、第一層級使用及權限管理之分工如下：

（一）本署資訊室：

1.負責系統維運、使用權限管理、資料庫維護、系統監控等整體管理及教育訓練工作。

2.負責本署政風室、各系統業務單位與各警察機關資訊單位使用權限管理及配賦，並設定本署各系統業務單位可調閱系統範圍。

3.提供本署政風、督察單位、各級法院及檢察署來文調閱跨轄之日誌紀錄。

4.定期針對異常查詢稽核、不定期抽查稽核。

（二）本署政風室及各系統業務單位：

1.運用本系統之業務稽核調閱功能，進行即時稽核。

2.每月應定期針對統計分析表異常之查詢數量、時間及對象進行稽核，有明顯不當情形時，應責成第二層級單位進一步查處深入稽核。

3.各系統業務單位，應指定專責人員辦理業管系統稽核工作，專責人員得由各系統具權限配賦人員或單位主管指定人員擔任。

六、第二層級使用及權限管理之分工如下：

（一）資訊單位：

1.應指派專人負責所屬單位使用權限管理及配賦。

2.運用本系統之業務稽核調閱、統計分析及主動稽核功能，落實執行各系統日誌紀錄稽核。

3.依各級法院及檢察署來文調閱所轄範圍之日誌紀錄。

4.每月應定期抽檢五分之一以上單位（含所屬機關），且查核量須達單位查詢紀錄總數之百分之二。稽核結果應簽陳機關首長核准並及提報機關相關會議檢討，各項稽核紀錄並應保存一年備檢。

5.依各機關業務分工，設定各系統業務單位可調閱系統範圍。

（二）政風單位及各系統業務單位：

1.運用本系統之業務稽核調閱功能，進行即時稽核。

2.各系統業務單位，應指定專責人員辦理業管系統稽核工作，專責人員得由各系統具權限配賦人員或單位主管指定人員擔任。

七、第三層級使用及權限管理之分工如下：

（一）資訊單位：

1.應指派專人負責所屬單位使用權限管理及配賦。

2.運用本系統之業務稽核調閱、統計分析及主動稽核功能，落實執行各系統日誌紀錄稽核。

3.每月應定期抽檢所屬五分之一以上單位，且查核量須達單位查詢紀錄總數之百分之二。稽核結果應簽陳機關主官核准及提報相關會議檢討，各項稽核紀錄並應保存一年備檢。

4.依各機關業務分工，設定各業務單位可調閱系統範圍。

（二）各系統業務單位：

1.應指定專責人員辦理業管系統稽核工作，專責人員得由各系統具權限配賦人員或單位主管指定人員擔任。

2.運用本系統之業務稽核調閱功能，進行即時稽核。

八、第四層級使用及權責之如下：

（一）由單位主管負責運用本系統之業務稽核調閱功能，進行即時稽核。

（二）每月應定期稽核所屬人員查詢日誌，員警人數二十人以下者，應稽核至少一人；二十一人以上未滿四十人者，應稽核至少二人，依此類推，有明顯不當情形時，應陳報分局進行複查，並深入稽核。

九、第五層級各系統使用者，得運用個人調閱功能查詢其本人日誌紀錄；單位主管得依實際需求申請主管稽核權限查詢所屬單位人員查詢日誌紀錄。

十、本系統使用權限申請方式如下：

（一）本署以外之各警察機關資訊單位專責人員職務異動時，應至本署警政知識聯網／電子化表單填寫權限申請表，向上一層級資訊單位辦理權限異動；各警察機關送本署之申請表應經各機關一層主管核准。

（二）各警察機關政風單位、各系統業務單位專責人員及單位主管，應至本署警政知識聯網／電子化表單填寫權限申請表，向同層級資訊單位申請權限。

（三）各系統使用者查詢個人日誌使用權限由本署資訊室設定自動配賦，個人無須申請。

十一、本系統之日誌內容不得擅自複製或外洩，並應遵守個人資料保護法、警察職權行使法或其他相關法規等規定。

十二、各系統另有稽核規定，且稽核頻率及內容較本規定嚴謹者，得免執行本規定稽核事項。

十三、本署資訊室得定期或不定期稽核各警察機關執行情形，各警察機關並應配合提供相關資料；本署發現異常查詢情形時，得請各警察機關調閱相關查詢紀錄，進行調查。

十四、本署發現各警察機關有下列情形之一者，應將其列為特定機關，並加強稽核其警政日誌稽核工作執行情形：

（一）發生洩密案件。

（二）發生洩漏個資案件。

（三）發生資安事件或通報案件。

（四）發生社會重大負面矚目案件。

（五）發生濫查公務機密案件。

（六）未落實辦理警政日誌稽核工作或日誌查詢量異常等不當情事。

十五、本署對特定機關實施不定時稽核作法如下：

（一）書面稽核：特定機關於本署發函通知後一個月內（遇假日順延之）應將前半年度辦理情形，連同相關佐證資料電子檔陳報本署。

（二）實地機動稽核：針對發生較多案件之特定機關或經書面稽核發現執行情形不佳之特定機關，本署資訊室及政風室得組成特定機關日誌稽核小組，實施實地機動稽核。

前項第一款無正當理由未於期限內陳報資料者，業務主管申誡二次，承辦人員記過一次。

十六、執行警政資訊系統日誌稽核及管理工作，有下列出力或不力情形，視其具體情節，依警察人員獎懲標準規定辦理獎懲：

（一）本署資訊室辦理本系統維運、資料庫維護、系統監控及管理等工作，未發生疏失者，各承辦人員於嘉獎總數三次以下核實敘獎。

（二）各警察機關資訊單位承辦人員辦理權限核發及管理業務，未發生疏失者，各承辦人員於嘉獎總數二次以下核實敘獎。

（三）辦理各警察機關跨轄查詢及他單位行文配合日誌調閱比對工作，每半年提供資料累計達二千筆以上者，嘉獎一次；達四千筆以上者，嘉獎二次。上半年累計件數未達敘獎基準者，其件數得併入下半年計算，惟不得跨年計算。

（四）同時符合第一款至第三款規定者，擇一從優辦理敘獎。

（五）本署資訊室執行特定機關加強警政資訊系統日誌稽核工作人員，於嘉獎四次範圍內辦理獎勵；政風室人員於嘉獎二次範圍內辦理獎勵。辦理不力人員，視情節輕重，分別議處。

（六）為落實平時稽查，加強建立層級化個資安全維護措施，各機關因善用本系統成功防阻、阻止系統濫用或資安事件發生，經查證有具體事實者，個案辦理獎勵。

（七）未依本規定方式作業者，資訊業務主管及資訊業務承辦人員，各申誡二次。

（八）對於上級機關交查其機關內發生之洩密案件，未盡調查或處理之責，或事後未盡防護之責者，資訊業務主管及資訊業務承辦人員，各申誡一次。

警用行動電腦使用管理要點

中華民國 111 年 01 月 18 日修正

一、內政部警政署（以下簡稱本署）為律定各級警察機關警用行動電腦之使用及管理權責，確保人民資訊隱私權及維護機關資訊安全，特訂定本要點。

二、本要點所稱警用行動電腦，包括手持行動電腦、警用行動載具、智慧型手機、平板電腦及路邊臨檢箱等設備。

三、警用行動電腦使用之安全管制，應依下列規定辦理：

（一）各設備使用單位（以下簡稱使用單位）應律定專責保管人，負責該單位之設備保管、註冊、資料更新及使用人員管理，並依警政日誌管理系統作業規定辦理稽核及管理等工作。

（二）使用單位之專責保管人或使用人員有異動時，應辦理人員權限異動，並應填寫權限申請表，權限申請資料應保留五年備查。

（三）未經本署同意，不得擅自拆裝硬體配備、安裝軟體、或任意變更系統環境設定。

（四）不得擅自連結非警察機關之電腦設備及網路系統。

四、警用行動電腦之使用管制，應依下列規定辦理：

（一）設備及設備內之各項警政資訊應用系統查詢使用，應限於警察機關所屬人員執行勤務或維護治安之目的，不得做目的以外之運用。

（二）應建立帳號或密碼等身分鑑別機制，使用者應善盡保管個人鑑別資訊的責任，並依相關規定使用，以明責任。

（三）警用行動載具及智慧型手機不得使用他人帳號或密碼之情事，使用者於使用完畢後，應登出系統。

（四）警用行動電腦應每日進行資料更新，逾七十二小時未更新者，設備將予以鎖定。即時車牌辨識系統及路邊臨檢箱，應於每次出勤前進行資料更新。

（五）執勤領用及退勤繳還警用行動電腦時，均應於員警出入及領用槍彈、無線電、行動電腦登記簿記錄。

（六）執勤領用警用行動電腦，應持領機證（領機證式樣如附表）向保管或值班人員領取，保管或值班人員應清點及管理領取情形，並彙齊保管領機證列入交接管理；退勤應立即繳還警用行動電腦及取回領機證。

（七）警用行動電腦領機證為一人一證，個人應妥善保管，髒污破損應檢具原證向資訊單位換取新證，資訊單位並應列冊管控領機證配發情形。

（八）人員調離機關應向資訊單位繳回領機證，資訊單位應立即或批次辦理銷毀工作。

（九）警用行動電腦僅限公務使用，勤餘領用辦理公務時應填具申請表單，經單位主管核准後依第五款及第六款規定辦理。

（十）未經單位主管同意，不得將設備借予他單位使用。

（十一）不得私自更換SIM卡，或將公務SIM卡置於私人設備中。

（十二）使用單位及資訊單位應設警用行動電腦報修管制簿，列冊管制設備報修期程；設備故障時，使用單位應於發現後三日內通報資訊單位處理。

五、警用行動電腦內之資料，應予保護，並切遵下列保護措施：

（一）警用行動電腦內之資料列為一般公務機密。

（二）應依規定查詢、作業，不得非法複製或洩漏。

（三）承商於使用單位實施維修時，使用單位應指定專人全程陪同。

（四）承商將警用行動電腦攜回維修時，使用單位專責保管人及資訊承辦人員，應告知承商善盡資料保護之責。

六、使用單位對警用行動電腦應予列冊管理；專責保管人應定期養護，使設備保持正常狀態。

七、各警察機關（含分局）對配置警用行動電腦之使用維護，應確實考核執行成效，檢查有關紀錄，每月定期依警政日誌管理系

統作業規定執行稽核及督導工作，並作成書面紀錄備查。

八、各警察機關執行本要點工作相關人員，有下列出力情形，視其具體情節，依警察人員獎懲標準規定辦理獎勵：

（一）主動發現缺失，並提出改進建議，經本署評估可行，並依建議事項改善完竣者，於記功一次以下覈實敘獎。

（二）各單位辦理本要點相關工作未發生疏失，每半年資訊業務主管嘉獎一次、資訊承辦人（一人次）嘉獎二次獎勵。

（三）依規定能妥適養護及管理設備，且半年內未有任何缺失者，核予專責保管人嘉獎一次獎勵。

前項人員有下列情形之一者，視其具體情節，依警察人員獎懲標準，核予申誡處分：

（一）未依規定更新資料，致令設備鎖定，半年累計達三次。

（二）設備故障逾三日未通報資訊單位。

（三）服勤攜出使用或退勤繳回，未於登記簿登錄或置放領機證，半年累計達三次。

（四）使用他人登錄碼、帳號或密碼登入系統。

（五）擅自拆裝硬體配備、安裝軟體、或任意變更系統環境設定。

（六）警用行動電腦擅自與非警察機關設備及網路系統連接。

（七）擅自將設備借予非警察機關所屬人員使用。

（八）擅自更換警用行動電腦SIM卡。

（九）遺失警用行動電腦。

（十）勤畢未依規定繳回或非因公務攜出。

九、遺失或惡意破壞警用行動電腦設備者，應負賠償責任。

十、各單位自行開發之行動電腦並得比照本要點規定使用管理。

臺中市政府警察局公務機密維護作業規定

中華民國 105 年 05 月 31 日

一、目的

為維護本局暨所屬分局、（大）隊公務機密安全，嚴防洩密情事發生，特依警政署函頒「警察機關公務機密維護實施規定」訂定本作業規定。

二、權責

（一）各級主官（管）應負責督導及執行機關（單位）公務機密維護工作。

（二）政風室及各分局、（大）隊兼辦政風業務之督察人員承機關首長之命，負責策訂本機關（單位）公務機密維護工作，並配合相關單位推動執行。

三、作法

（一）一般機密維護

1、文書機密維護

（1）機密文書處理流程，應採取保密措施，以防洩密情事發生。其管制原則如下：

A.專責處理：本局各單位及所屬機關應指定專責人員處理機密文書。

B.減少層次：盡量減少處理過程之層次或參與人員。

C.限制分發：分發限於必須獲得或知悉機密資料人員，並加強編號紀錄。

D.妥慎傳送：應視機密等級、傳遞地區，依規定妥慎傳送。機密以上文件必須指派專人親自送達。如使用電腦設備處理機密文書，資訊系統帳號及密碼，應建立安全控管機制，相關電子憑證亦同。

E.安全保管：機密文書之保存與管理，應設置保密櫃或機密文書保存室存放，並由檔管人員依規定妥慎管理。借調文書檔案不得有塗改、損壞、短少及逾期歸還檔案等情事，其情節重大者，簽報議處。

F.澈底銷毀：廢棄之機密稿件或文書，應指派專人監督並會同政風人員澈底銷毀。

（2）為防制無關人員接近或獲取機密文書，應落實櫃臺作業及防護責任區巡查，嚴禁非洽公人士及閒雜人員出入辦公處所。檔管單位並應針對納入檔管之一般公務機密文書，每年定期清查，其須變更機密等級或解密者，應按規定辦理變更或解密手續。

2、電腦、資訊機密維護

（1）資訊單位應加強資訊安全控管機制，並建使用者紀錄檔（LogFile），以防止公務機密資訊（尤其個人料）之外洩。

（2）個人電腦通行密碼定期變更，應確實保密，嚴禁借予他人使用。

（3）各單位人員處理電腦資料應遵守「個人資料保護法」相關規定。其職務異動或（休）職，權限並應即時調整或取消。

3、其他機密維護

基於業務性質需要，對於前來參觀、訪問、洽公之來賓，得訂定必要之管制規定。

（二）專案機密維護

1、業務主管單位，應針對重大施政及其他易滋洩密事項，會同政風室策訂專案機密維護計畫，預先研擬嚴密之保密措施，以杜絕洩密。

2、專案機密維護之範圍

（1）查核金額以上採購案件之招標過程。

（2）舉辦各種考試及機會均等公平競爭之措施。

（3）重要人事調動、人事考績或甄選受評人員達三十人以上者。

（4）各種重要機密會議之召開。

（5）機關辦理採購或人事案件經檢舉有洩密跡象者。

（6）其他須保密之重大施政措施。四、公務機密維護檢查

由本局政風室會同業務主管單位實施公務機密維護檢查：

（一）狀況研判：

1、處理公務機密之員工保密警覺程度。

2、機關之主客觀環境及其各項保密設備。

3、曾發生洩密單位近期之改進措施。

（二）就下列事項實施實地稽核：

1、文書機密。

2、公務機密宣導。

3、密碼使用管理情形。

4、保密裝備管理情形。

5、資訊安全管理。

6、檔案室管理。

7、辦公處所安全管理。

8、檢舉及陳情人資料保密。

9、洩密或違反保密規定案件查處及通報情形。

（三）公務機密維護檢查結果，就優劣缺失及改進措施提出書面意見，並通報缺失單位確實檢討改進。

（四）除每年度定期辦理公務機密維護之檢查外，另視實際需要得實施不定期檢查。

五、洩密案件處理

遇有洩密案件發生，除逐級陳報外，並應即知會本局政風室，會同研擬適當補救措施，使洩密損害減至最低程度，並個案分析洩密原因及管道，以防範再發生。

六、獎懲

執行公務機密維護成效卓著者，由本局政風室簽報獎勵；推行不力致發生洩密情事者，依有關規定處理。

三、廉政相關法令簡介

三、廉政相關法令簡介

刑法、貪污治罪條例與個人資料保護法罪責說明		
名稱	相關規範	說明
不違背職務受賄罪	**刑法第121條**，處7年以下有期徒刑，得併科70萬元以下罰金。 **貪污治罪條例第5條第1項第3款**，處7年以上有期徒刑，得併科新臺幣6,000萬元以下罰金。	無論係「職務上之行為」或「違背職務之行為」，只要有「要求」、「期約」或「收受」其一行為，且所要求、期約或收受之不正利益與該行為**有「對價關係」**，即觸犯本罪。 因而為違背職務之行為，加重處罰。
違背職務受賄罪	**刑法第122條**，處3年以上10年以下有期徒刑，得併科200萬元以下罰金。因而為違背職務之行為，處無期徒刑或5年以上有期徒刑，得併科400萬元以下罰金。 **貪污治罪條例第4條第1項第5款**，無期徒刑或10年以上有期徒刑，得併科新台幣1億元以下罰金。	
圖利罪	**刑法第131條**，對於主管或監督事務圖利，處1年以上7年以下有期徒刑，得併科100萬元以下罰金。 **貪污治罪條例第6條第1項第4、5款**，對於主管或監督事務，或非主管或監督事務圖利，處5年以上有期徒刑，得併科新臺幣3,000萬元以下罰金。	只要主觀上「明知違背法令」，而使自己或他人獲得不法利益，不以**「對價關係」**存在為要，即成立本罪。
公務員登載不實罪	**刑法第213條**，處1年以上7年以下有期徒刑。	如於公務系統中不實輸入相關資訊，並登載於系統中，足以生損害於公眾或他人者，即成立本罪。
公務員假借職務上之機會違法蒐集個人資料罪	**個人資料保護第41條**，處5年以下有期徒刑，得併科新臺幣一百萬元以下罰金。 **個人資料保護第44條**，犯本章之罪者，加重其刑至二分之一。	如意圖為自己或第三人不法之利益或損害他人之利益，違法本法之相關規定，將因公務員身分加重其刑。

四、案例研析

四、案例研析

案例一、洩漏臨檢消息予色情業者

甲為○○市政府○○分局○○派出所所長，明知A經營之○○時尚生活館為違法色情行業，竟因與A私下交好，將該所編排臨檢消息以電話方式透漏予A，俾利A事先準備，避免其妨害風化犯行遭查獲，以此方式包庇A所涉上開妨害風化犯行未為警查獲，而得以順利經營上開色情按摩店。

案經法院判決，甲犯公務員包庇他人圖利容留猥褻罪，處有期徒刑1年1月；又犯對主管事務圖利罪，處有期徒刑2年9月，褫奪公權3年。應執行有期徒刑3年2月，褫奪公權3年。

風險評估

第一線同仁常因久任其職，因業務機會或績效需要，與地方人士形成緊密聯繫關係，易因此私下透漏因職務身分知悉之中應秘密之消息，而誤蹈法網。

防治措施

一、落實風紀清查

鑒於色情場所、職業性賭場常為員警風紀誘因來源，且部分案件更有員警涉嫌參與賭博或包庇之情事，嚴重影響警譽。為端正警察風紀，應針對檢舉事證明確之色情場所、職業性賭場等不法行業進行探訪查緝，落實風紀清查。

二、預防性職務調整機制

警察勤務涉及干預及取締作為，易成為不法業者極力拉攏之對象，長期久任，恐因利益誘惑，衍生弊端，爰應確依警察人員陞遷辦法及相關規定執行職務遷調或業務輪調，透過預防性職務調整機制，避免員警有機會與不法業務掛鉤，減少因長期久任而產生之人情壓力或利益誘惑，藉以杜絕貪瀆不法問題。

參酌自臺灣高等法院
111 年度重上更一字第 8 號刑事判決

案例二、洩漏公務機密予詐騙集團

甲為○○市政府警察局○○分局○○派出所警員，透過友人結識詐騙集團成員A，俟因A之請託，甲明知其所查詢之刑案資料非屬公務所需，且A所大量查詢者，顯非自己持用之銀行帳戶，竟意圖為第三人不法之利益，基於洩漏國防以外應秘密之消息，在其任職之辦公處所，利用職務權限於公務機關電腦開啟內政部警政署警政知識聯網網頁，並進入165反詐騙系統平台，非法輸入身分證號或銀行帳號等條件，再將查得之警示帳戶通報日期、報案機關、165受理案號及受騙金額等應秘密之消息，以傳送文字或翻拍165反詐騙系統平台查詢畫面截圖之方式，多次洩漏予A，使A得以及時掌握所使用之人頭帳戶有無遭通報列為警示帳戶之重要資訊，進而得以順利將被害人匯入之詐騙所得迅速轉帳或及時更換使用其他人頭帳戶，致生損害內政部警政署對警政知識聯網系統管理之正確性。

案經地檢署認本案甲涉犯洩漏國防以外應秘密之文書有洩密之情事，故予以起訴。

• 風險評估 •

甲明知友人所欲大量查詢之資料，非屬友人所有之隱私資料，仍意圖為第三人不法利益，將他人之隱私資料洩漏予友人為非法使用，嚴重缺乏公務機密保密意識。

防治措施

一、定期稽核員警利用公務系統查詢民眾個資之相關紀錄

實務上員警偵辦案件時，常會利用公務系統查詢民眾個資，惟為避免有不法或不當之利用情形，機關主官（管）應定期稽核員警相關之查詢紀錄，避免有違失情形發生。

二、強化法紀宣導

對於因案使用公務系統查詢民眾個資之同仁，定期進行保密宣導，使其瞭解公務機密保密範圍，對於法令規定要保密事項，應謹守公器使用之分際，避免過失洩密。

案例三、無故洩漏個資予友人

甲為○○市政府警察局○分局○派出所警員，於臉書社團結識A女，利用服勤期間領取警用小電腦之機會，查得A女之身分證字號、戶籍地、住家市內電話號碼及國民身分證照片影像，致損害A女之隱私權及個人資料保護之利益，嗣後再以手機照相功能翻攝A女之國民身分證照片影像，並將之截圖以通訊軟體LINE傳送予A女，並向A女自承查詢其身分證字號等個資，A女始知悉上情並向○分局告發。

案經地檢署偵查終結，核甲所為涉犯個人資料保護法第44條、第41條公務員假借職務上機會非法蒐集個人資料罪，經檢察官為緩起訴處分，期間為1年，並自緩起訴處分確定之日起3個月內，向公庫支付新臺幣6萬元。

風險評估

警察人員係依法令服務於國家所屬機關而具有法定職務權限之公務員，具有登入內政部警政署警用 行動電腦「M-POLICE」查詢資料之權限，惟因職務查詢便利而致降低洩密敏感度，又資訊科技日新月異，流通快速，具備不可回復特性，易因一時輕忽而造成嚴重後果。

防治措施

一、提升警務人員個資保密意識

警察機關洩漏個資事件時有所聞，警務人員為防止危害及預防與偵查犯罪，得依警察職權行使法規定蒐集與利用個人資料，惟應加強宣導警職法第17條「應於法令職掌之必要範圍內為之，並須與蒐集之特定目的相符」規定，以免假借職務不當洩漏或提供他人為不合目的性使用，傳遞警察不當作為將對個人隱私之保護造成極大威脅的觀念，強化警務人員自我約束。

二、強化主管考監責任

員警勤餘生活狀況及交往情形，往往容易成為考核工作之死角，各單位主管對於員警日常生活及家庭狀況應確實掌握，以有效杜絕違法犯紀之外在因素。

案例四、洩漏個資予徵信業者

○○市政府警察局○○分局小隊長甲受退休同事A請託，利用職務上之機會，於辦公室內使用公務電腦輸入警政知識聯網帳號，輸入不實之查詢事由，因而查得民眾個人資料，並將上開不實之查詢事由之電磁紀錄，登載在警政知識聯網系統電腦資料查詢系統中，再透過當面告知、通訊軟體或翻拍等方式提供予A，再由A提供予徵信業者，足生損害於前揭被查詢者及內政部警政署對警政知識聯網系統管理之正確性。

案經法院判決，甲涉犯個人資料保護法及刑法洩漏國防以外之秘密等罪，判處共同犯公務員登載不實罪，共120罪，各處有期徒刑1年2月，應執行有期徒刑2年。緩刑5年。

• 風險評估 •

有心人士基於私人利益恩怨等動機，無所不用其極編造各種理由請託員警查詢民眾個資，因警政資訊系統具備戶役政、車籍、刑案紀錄等資料庫，是最直接且最有用之資料獲得來源，而員警因受人情請託、缺乏資安警覺性、資訊法令常識不足、資安內控機制疏漏或為牟取不當利益等因素，違規查詢並洩漏民眾個資，衍生違法洩密情事，除造 成民眾權益損害，更嚴重破壞政府公信力及警察形象。

防治措施

一、落實職務任期及遷調規定

針對易滋弊端之業務，除以機動督導方式追究執行不力人員之責任外，另應注意同仁避免人情包袱或業者趁虛而入之情事，如有違法或違紀顧慮者，應即提報列管，以防衍生風紀問題，必要時即時調整職務，調離敏感性或易滋弊端職務。

二、加強教育訓練，內化保密意識

甲身為單位之中堅幹部，理應知曉查詢個人資料之權限及不當洩漏之法律責任，卻未深思熟慮，僅憑一己之私而觸法，足見屢續強化員警保密觀念及積極加強所屬員警保密意識，建立正確觀念防杜個人資料外洩及個人資料保護之觀念。

參酌自臺灣臺北地方法院
111 年度訴字第 336 號刑事判決

案例五、洩漏偵查資訊予通緝犯

甲為○○市政府警察局○分局○分駐所巡佐兼副所長，明知司法警察單位偵辦刑事案件進行跟監之方式及使用之交通工具，係屬中華民國國防以外應秘密之消息，竟為持續獲取情資，多次將其線民A遭地檢署及地院通緝乙事告知A，嗣受A之託，登入警政知識聯網車籍資訊系統查詢停放在A租屋處附近之車輛是否為警方使用之車輛，查詢後得知上開車輛為○○市政府警察局使用之偵防車輛後，再以通訊軟體LINE告知A此等訊息，使A提高警覺，躲至他處，以致○○市政府警察局當日因無法掌握A之確切住居所，而查緝未果。

案經法院判決，甲洩漏關於中華民國國防以外應秘密之消息罪，處有期徒刑1年2月，緩刑4年，並應於判決確定之日起6月內向公庫支付新臺幣10萬元。

• 風險評估 •

警察人員為遂行法律賦予之任務，自掌有機密之資訊，甲顯未落實公務機密保密義務相關規定，將職務上掌有應秘密之資訊加以洩漏，致使公務機密外洩，嚴重影響查緝毒品任務。

防治措施

一、加強考核深入發掘輔導

各單位主管利用平日各項督導與考核，發掘風紀問題，深入了解、蒐集風紀實況，結合勤務督導、幹部考核與風紀查察，全盤掌握風紀狀況，對違紀傾向人員或搶報績效者優先列管、輔導，各項考核勿流於虛應形式，應秉持不護短之決心，機先防範。

二、加強勾稽查核及建立異常徵候指標

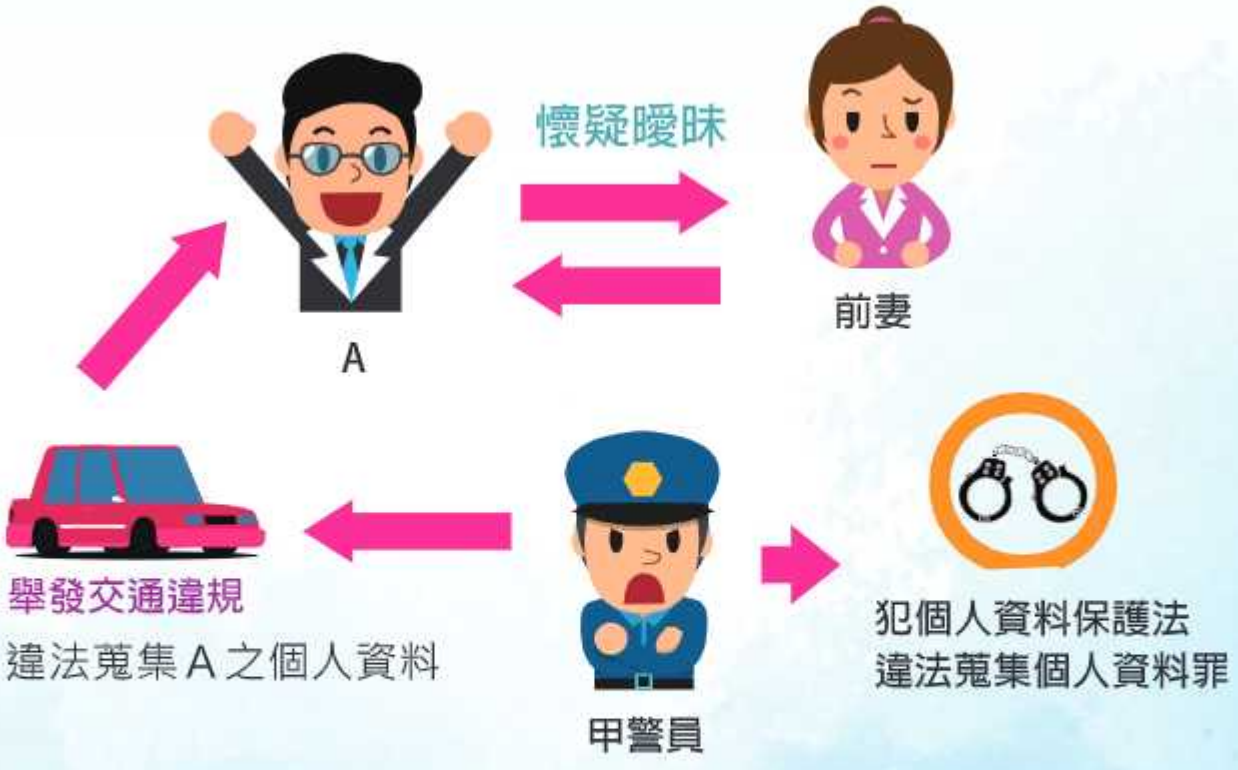
針對系統產出之查詢紀錄資料(LOG 檔)，逐筆勾稽使用者之「勤務分配表」、「出入登記簿」、「工作登記簿」等紀錄，同時針對查詢條件異常、高查詢量帳號、單位查詢量排名、高風險違紀對象等異常狀況，建立異常徵候指標，以提升稽核成效。

參酌自臺灣高等法院臺南分院
111年度上訴字第 830 號判決

案例六、因好奇不當查詢個資

甲為○○縣警察局○○隊警員，因懷疑A與其前妻曖昧，明知A並未交通違規，仍使用○○隊公務電腦，非於執行法定職務必要範圍，亦未經A同意，以公務帳號登入警政署知識聯網公路電子閘門系統，勾選查詢用途為「舉發交通違規」，查詢A所使用，其父B所有之自小客車車牌號碼共2次，而登載不實事項之電磁紀錄準文書於該公路電子閘門系統，足生損害於A及○○縣警察局管理公務查詢業務之正確性。後又意圖損害A之利益，非於執行法定職務必要範圍，亦未經A同意，使用警用電腦M-POLICE行動載具，接續輸入、檢索A所使用之自小客車車牌號碼，及A之身分證號碼，而違法蒐集A之個人資料，足生損害於A。

案經法院判決，甲犯個人資料保護法第41條之違法蒐集個人資料罪，共2罪，各處有期徒刑6月。又犯公務員假借職務上之機會，犯個人資料保護法第41條之違法蒐集個人資料罪，處有期徒刑4月。應執行有期徒刑10月，緩刑2年。



• 風險評估 •

甲非因公查詢A車籍、個資等情，雖無涉洩密情事，惟其以舉發交通違規之不實事項，利用職權為目的性以外之查詢及登載不實電磁紀錄之行為，致生損害於警察機關對警政知識聯網管理之正確性，足見甲欠缺法規知識及無視紀律。

防治措施

一、落實業務督導及人員考核

主動針對異常查詢數量、時間及對象，深入勾稽比對，並應強化自主管理檢查，嚴禁不當查調，機先防處，有效遏止同仁僥倖心理。

二、加強教育訓練，內化法紀意識

持續加強同仁公務機密暨資訊安全維護觀念，針對現行法令規定、案例及可能導致洩密管道與因素，落實利用各項集（機）會加強宣導，使同仁均能瞭解相關法令規定，與違反規定所須承擔法律責任，降低員警因故意或過失違規查詢民眾個資及洩密之情事發生。

參酌自臺灣雲林地方法院
111年度簡字第260號刑事判決

案例七、因疏失遭被詢問人將公文翻拍

甲為○○市警察局○○分局警員，為偵辦案件約詢A女至○○分局製作筆錄，A女依約到場，甲向A女說明案情後，A女要求檢視證據資料，甲遂將該案偵查卷宗交付給A女檢視，致A女知悉本案公文，並趁甲未察時，將本案公文及LINE對話影像資料翻拍上傳至LINE群組，甲疑涉有過失洩漏國防以外之機密罪。

案經地檢署認本案遭翻拍之公文內並無相關檢舉人資料，難認甲之行為有洩密之情事，故予以不起訴處分，然而甲對密件公文保管不當，致遭翻拍外傳，仍有疏失，經所屬機關核予行政處分。

• 風險評估 •

於警詢時因警力不足，僅由1人製作筆錄，雖事前告知A女不得翻拍，惟登打筆錄時因忙碌疏未注意，致A女趁機以手機拍攝公文並上傳通訊軟體LINE群組。

防治措施

一、張貼明顯標語，使規範深植人心

於機關駐地張貼明顯標語提醒民眾嚴禁攝影錄音，製作詢問筆錄前亦事先向民眾再多加強調，使相關規範深植人心。

二、取消電腦雙螢幕模式，嚴守保密義務

取消進行詢問筆錄時電腦採雙螢幕模式，改採製作完成後列印紙本予嫌疑人檢視，避免詢問過程遭側錄或偷拍。

案例八、洩漏查緝行動予犯罪友人

甲為○○市警察局偵查隊小隊長，於警局實施查緝賭博專案行動時，明知專案期程為其因職務上所得知之應秘密消息，惟仍以LINE通訊軟體像涉嫌經營網路博奕之友人A男洩漏相關專案行動之情資及時程。

案經地檢署認本案甲涉犯洩漏國防以外應秘密之文書有洩密之情事，故予以起訴，目前刻正於法院審理中，且甲並遭所屬單位予以停職處分。

• 風險評估 •

甲藉由職務上之機會得知應秘密之查緝賭博專案行動，卻趁機向經營網路博弈之友人A洩漏相關行動之資訊，足生損害公務執行之順利進展，並促使犯嫌逍遙法外，甲顯然缺乏保密意識。

防治措施

一、案件管控及審核機制

對於員警偵辦案件過程，從起案到移送，均要求承辦單位全程掌握管控，以避免有洩密情事發生。

二、落實考核機制，實施久任輪調

應依照每位員警之公務辦理情形考核優劣，並做出評估調整，使每位員警都能適才適所任用，對於久任員警並應時時職期輪調，避免員警有與地方勾結之情事發生，如確有發生嚴重違紀情事，應將不適任員警斷然淘汰，以端正警紀。

案例九、開標前洩漏採購訊息

甲為○○市警察局警務正，於辦理○○勞務採購案時，負責製作招標文件、履約管理及驗收等業務，並知悉友人乙經營之公司有意願參與該標案，甲明知依政府採購法第34條第2項規定，機關辦理招標，不得於開標前洩漏底價、領標、投標廠商之名稱與家數及其他足以造成限制競爭或不公平競爭之相關資料，竟以電話告知乙該標案之預算金額，造成廠商間之不公平競爭。

案經法院判決，甲犯公務員洩漏國防以外秘密罪，處有期徒刑2月。緩刑2年，並應自判決確定之日起6個月內項檢察官指定之公庫支付新臺幣5萬元。

• 風險評估 •

甲辦理採購相關業務，應遵守保密義務，卻利用職務上之機會洩漏應保密之事項，造成廠商間之不公平競爭，顯然欠缺恪遵法紀之觀念。

防治措施

一、內部積極宣導，避免誤蹈法網

警員於辦理採購業務時，可能因不熟法令或心存僥倖而洩漏採購應秘密之事項於他人，造成廠商間有限制競爭或不公平競爭之情事發生，應對承辦員警積極宣導並加強法治觀念，避免損害警譽。

二、案件追蹤管考，留意辦理情形

應針對各員警所承辦之採購案件定期追蹤管考，並留意相關辦理情形，使主官（管）能隨時掌握進度，提升公務效率並避免違失情形發生。

參酌自臺灣桃園地方法院
111年度矚重字第4號刑事判決

案例十、洩漏檢舉人資訊

A男向○○院電子信箱反映，渠曾向○○署電子信箱反映○○案，惟○○市警察局偵查隊承辦員警甲約談A男之朋友B女時，將A男之個人資料及檢舉內容洩漏給B女知悉，涉有洩漏國防以外秘密罪之情事。

案經地檢署認本案所洩漏之秘密內容均為B女所知悉之事項，尚未造成重大危害，故予以不起訴處分，然而甲洩露檢舉內容致遭民眾非議，仍有疏失，經所屬機關核予行政處分。

• 風險評估 •

甲偵辦案件時，誤認相關應秘密事項縱為受詢問人所知悉，即可將涉及個人隱私之資訊告知被詢問人，造成被詢問人獲知更多原先所不知之資訊，處事欠妥。

防治措施

一、指派幹部指導，灌輸法紀觀念

針對新進、甫畢業（結訓）之員警，要求各單位主管於偵辦刑案時指派幹部或資深員警予以指（督）導，深植各項法紀教育，灌輸正確價值觀念，避免因法紀意識缺乏而誤蹈法網。

二、宣達法律規定，加強案例宣導

加強宣達案件偵查過程，應恪遵刑事訴訟法、偵查犯罪手冊及行政程序法及相關檢舉人保密規定，同時要求各單位主管利用各項集（機）會場合，綿密宣導「公務機密及洩露個資」等相關規定及案例，以強化員警法治觀念，務使每位員警均能瞭解相關保密法令規定。

案例十一、因疏失將偵查行動洩漏予當事人

甲為○○市警察局○○分局督察組擔任組長，於知悉該分局內同仁A違法查詢165反詐騙系統並洩密予他人後，遂製作A任內所查詢資料之「查詢清冊」，未注意A之犯行已非單純行政違失，而將該「查詢清冊」交付A供答辯，使A得以事先知悉偵查機關所掌握之偵查秘密，並得以充分答辯；另甲不慎將「檢察官要查扣A手機之消息」透漏予A，使A事前得以知悉檢察官之偵查活動及計畫，足生妨害於A刑事洩密案件之司法偵查結果。

案經地檢署認本案甲涉犯洩漏國防以外應秘密之文書罪，惟因一時不察致罹刑章，遂核予緩起訴處分，緩起訴期間1年。

• 風險評估 •

甲因長期久任警政督察系統，未熟悉相關刑事偵查流程相關法令，未細究行政調查與刑事偵查性質區分，致誤罹刑章。

防治措施

一、透過舉辦講習，提升專業知能

各單位主管利用平日各項督導與考核，發掘風紀問題，深入了解、蒐集風紀實況，結合勤務督導、幹部考核與風紀查察，全盤掌握風紀狀況，對違紀傾向人員或搶報績效者優先列管、輔導，各項考核勿流於虛應形式，應秉持不護短之決心，機先防範。

二、適時業務輪調，熟悉各項業務

針對系統產出之查詢紀錄資料(LOG 檔)，逐筆勾稽使用者之「勤務分配表」、「出入登記簿」、「工作登記簿」等紀錄，同時針對查詢條件異常、高查詢量帳號、單位查詢量排名、高風險違紀對象等異常狀況，建立異常徵候指標，以提升稽核成效。

五、結論

五、結論

本防貪指引手冊蒐集警察機關公務機密維護之相關法規，期望員警於承辦案件時能有所依循。本防貪指引手冊並參酌法院判決及地檢署相關書類，撰寫為11個案例故事，說明正確之員警保密義務，及未依規保密可能面臨之處罰，希能使員警更加有所警惕。

公務機密維護是警察承辦案件重要任務之一，亦會影響民眾對警察之信賴程度，員警更應依法行政，嚴守公務機密保護之準則，並維護警譽，確保公共利益。

MEMO

MEMO

MEMO

違法查詢個資及洩密
廉政防貪指引

發行機關：臺中市政府警察局
總 策 劃：臺中市政府政風處
編輯小組：侯建廷、陳志忠、張台貴、黃信曉、王振宇
陳金龍、陳映慈、姜佑霖

發行日期：中華民國112年10月

廉能臺中
透明城市