公務機密維護　錦囊 第 1 號

~「人民保母洩漏個資侵害隱私」

前言

警察機關為執行各項勤、業務及辨別轄區戶口之良莠，並達到偵查與預防犯罪之目的，必要時須大量蒐集、運用民眾個人資料，加以分析、研判，建立了龐大基本資料庫。此外，投機分子、不肖徵信業者、犯罪集團亦處心積慮利用各種管道，如透過關說、行賄利誘或非法入侵電腦、資料庫等手段獲取民眾個人資料。是以，警察機關如何保護民眾個人資料免於遭受到有心人士竄改，抑或盜取而損及民眾權益，為當前不可忽視的重要課題。

案例摘要

- ○○縣警察局○○所警員陳○○友人 A、B 因有民事糾紛，A 遂請陳員代為查詢 B 的刑案資料，以提供雙方談判時參考。陳員明知刑案資料查詢必須依規定辦理，屬警察局應管制作業，用來查詢犯罪偵防或特定任務所需刑案資料，不得任意洩漏給其他人或單位。惟陳員仍將 B 的「刑案資料作業個別查詢報表」列印，並交付友人 A，觸犯洩漏國防以外秘密罪。陳員經臺北地方法院以洩漏國防以外應秘密之文書罪嫌，處有期徒刑肆個月。

- ○○地檢署偵辦○○鄉前鄉長林○○貪瀆案，經調查人員監聽該案相關人王○○時，發現某警察局○○分局○

○所警員謝○○，涉嫌於 96 年 10 月間為友人吳○○所請託，以電腦查詢自小客車籍資料，並將該車籍資料及車主姓名提供予吳姓友人，涉有洩漏國防以外秘密之罪嫌，全案謝員坦承不諱，經高雄地方法院檢察署裁定予以緩起訴在案。

- 某警察局○○分局○○所警員陳○○接獲友人○○○之電話，以想跟朋友做生意為理由，請託陳員查詢一輛自小客車的車主資料。事後友人向車主謊稱發生車禍，請其出面處理，實為查明實際開車為何人，車輛實際使用人知悉後心生不滿，循線提出檢舉。全案雖經高雄地方法院檢察署偵查終結，認車籍資料並非陳員提供，予以不起訴處分，然陳員確有查詢該筆車籍資料，查詢時亦未於電腦資料查詢紀錄簿登記，縱未將資料提供他人，仍依違反相關作業規定，核定申誡二次處分。

問題分析

- 利用電腦查詢車籍、戶役政或其他個人刑案資料時，未依規定登記電腦資料查詢紀錄簿，或列印資料後，未於電腦資料查詢紀錄簿簽收。
- 單位主管未依規定每日、逐筆審核電腦查詢紀錄簿之查詢狀況，並逐筆核章。
- 各使用單位對查詢電腦資料（刑案查詢系統）之查詢紀錄未定期下載供單位主管審核。

策進作為

- 賡續加強公務機密維護宣導：民眾個人資料外洩的主因

大部分皆屬人為因素，因此欲降低資料外洩的機率，最主要還是要從培養個人之保密觀念著手。警察機關應以現行法令規定、洩密違規（法）案例，以及可能導致洩密管道與因素，利用各種集會時機向員警宣教，務使每一位員警均能瞭解相關保密法令規定，與涉及洩密或違反保密規定者，須承擔之法律責任（行政責任、民事責任、刑事責任或國家賠償），以養成警察人員時時保密、處處保密之良好習慣。

- 強化單位主官考核監督責任：各單位主官（管）身負督導重任及業務成敗之責，對於該管業務及所屬員警狀況最能深入掌握，倘能落實業務督導及人員考核，自然能收防範於未然的效果。尤其，應針對作業或生活違常、交往複雜、財務狀況不良、收支顯不相當、經濟狀況來源可疑或時遭檢舉反映操守風評不佳人員，則應加強平時輔導考核作為，並適採必要之防處作為，以防範洩密情事發生。
- 落實資訊安全稽核檢查作為：為使保密工作能更臻完善，除了事前的教育宣導預防工作要做好外，適時對所屬機關（單位）的保密工作執行情況，辦理督導考核亦是重要的一環，務期透過稽核、檢查過程中發掘優、缺點，對於執行良好者，從優獎勵，對於執行不利者，則依照相關規定懲處，以落實保密執行工作。
- 嚴格審核使用者代號及密碼：警察機關為偵查與預防犯罪需要，必須使用內政部警政署資訊系統蒐集民眾個人資料。而欲進入各該作業系統查詢民眾個人資料時，須先申請使用者代號、密碼，經過單位主官（管）及相關

單位審核後，承辦人才可以各業務主管單位配賦的密碼登入系統查詢。因此，若單位主官（管）對員警於使用者代號、密碼申請時，能謹慎審核申請表所申請的項目是否與其職務有關並考慮申請者的品德操守，確保權限申請後均能使用於公務。

本署叮嚀

公務員能否遵守保密義務，攸關國家安全利益之維護、政策推動之順遂與民眾權益保障，因此每一個公務機關內之成員，皆應將維護公務機密資訊視為最重要之工作。各警察機關為積極推動各項勤、業務，落實為民服務，擁有查詢民眾個人資料之諸多資訊作業系統權限，更應嚴守保密規定，不可輕忽公務機密維護之重要性。此外，受理民眾檢舉案件及偵辦刑案過程中，亦應注意相關檢舉人身分保護作為及「偵查不公開」原則，以免因過失或疏誤而侵害民眾權益，造成嚴重之不良後果。

是以，如何善用電腦資訊作業系統資料，以提升行政之效能，同時保護民眾個人資料不致外洩，實有賴每一位公部門服務人員共同努力，並持續透過宣導與教育加強保密觀念，使其養成專業的保密素養與習慣，防制違反保密規定或洩密情事發生，俾使公務機密維護作為更臻完善。

本署謹提供以下措施作為參考：

- 加強資訊機密維護宣導及教育訓練。
- 落實辦理資訊機密稽核。
- 協助機關取得資安管理認證。
- 推動使用紀錄管理。
- 建立異常徵候指標。

- 強化主管考核監督責任。
- 辦理資安評估考核。
- 查調權限定期檢討。
- 落實職務定期輪調制度。
- 妥善資訊設備報廢管理

結語

政府為達成其施政目標，必須廣泛蒐集與運用各項個人資料，例如：稅務機關擁有納稅義務人的財產、所得、納稅資料；地政機關擁有不動產所有權及相關權利的歸屬資料；醫療機構擁有病患就診資料；榮民服務機構擁有榮民個人檔案資料；警察機關因執行公務，經戶役政查詢系統、車駕籍查詢系統等查詢民眾身分資料、全戶資料及車輛所有人資料等，上述資料攸關個人隱私及權益，如因保管或處理不當，除極易肇致觸法外，將引發民眾的恐慌與抱怨，並造成對政府機關的不信任。

電腦科技發展日新月異，網路資訊安全的風險不斷增加，惟爲避免過度方便使用資訊，反造成民眾個資或公務機密洩密之可能，除落實定期稽核制度及不定期抽核工作外，應機先針對公務機密業務可能發生缺失，追蹤並研擬各項興利防弊措施或建言，以減少資訊系統遭非法使用或洩密等不法事件之發生，提升為民服務的效率，確保民眾個人資料安全，展現行政革新ｅ化政府應有之作為，以造福民眾。

公務機密維護　錦囊 第 2 號

~「機敏會議資訊保密之道」

前言

政府機關為推動政策及執行業務，常透過會議方式，以凝聚共識並形成決策。由於會議內容往往涉及政策之擬定及執行之協調，部分會議因攸關國家安全及利益或依法令規定而有保密之必要。若將具有機密性或敏感性的會議資訊(簡稱：機敏會議資訊)公開或提供，輕則易招致外界關切，有礙機關決策之作成與執行，重則危害國家安全及人民權益，不可不慎。然而，從報章媒體上仍不免看到部分政府機關同仁因作業疏忽或為一己之私，而將機敏會議資訊提供或洩漏予他人，顯示會議資訊保密之觀念仍有待加強。

由於會議機敏資料常以電腦繕打、儲存及使用網際網路傳遞，任一環節都可能遭有心人士刺探、蒐集，若相關人員未能提高警覺，極易因疏忽而洩漏相關資訊，加上事後追查不易，致使機敏會議資訊外洩時有所聞。是以，政府機關如何妥善保管機敏會議資訊避免外洩，應予正視並妥適因應。

案例摘要

- 某機關召開「○○經營地區劃分及調整」工作會議，該案雖尚未定案且未對外公布，卻傳聞業者已有資料，機

關高階主管甚至接獲業者來電表達不滿。為瞭解有無洩漏機敏會議資訊情事，政風單位訪談會議出（列）席及相關人員，發現會議資料並未以機敏資料處理，在會議前係以電子郵件傳送至承辦人及主管，知悉者眾，致資料是否外洩及由何者所為均難論斷。為避免發生類似情事，政風單位衡酌機關業務狀況及可行做法，建議保密興革事項及辦理保密宣導。提供該機關辦理類似機敏會議，除於會議簽到表及資料上註記保密警語外，主席亦於會議中提醒與會人員，會議資料及內容不得任意發表或提供外界，有效減少洩密事件發生。

問題分析

- 參與會議之機關同仁或外聘委員可能因未建立機敏會議資訊維護的正確保密觀念，而擅將相關訊息提供予外界。
- 機敏會議資料未註記密等或保密警語，以致相關文書處理流程未提高警覺，致生洩密情事。
- 機敏會議之決議、決定事項須發布新聞者，未依發言人制度，由發言人統一對外發言。
- 重要機敏會議資料之檔案未使用隔離電腦處理，易遭致駭客入侵盜取。
- 機敏會議資料未予管制分發及會後收回，致他人有機會探悉、取得。
- 辦理機敏會議之文書簽擬稿、繕印時之廢件（紙），或誤繕誤印之廢紙及複寫紙等，未即時銷毀。

策進作為

- 訂定機敏會議資訊保密措施：

  為落實保密機制並明示保密責任，各機關應依業務需要研訂機敏會議資訊保密措施，內容建議如下：

  一、重要機敏會議資訊應使用隔離電腦處理，避免使用於連結網際網路之電腦設備。

  二、機敏會議資訊相關檔案及紙本均應加註密等或「機敏資料」之浮水印文字，並予編號分發。

  三、召開機敏會議時，於會議開始前，主席或主辦單位應提示與會人員知悉，並於簽到表上註記「本會議因具機敏性質，與會人員應行保密。」等宣示文字。

  四、會議使用管制分發之機敏資料，均應於會議後按編號收回，與會人員如因公務需要留用，應經主席核准並簽收。

  五、禁止透過網際網路(如電子郵件)傳送機敏會議資訊，若因公務需要透過網際網路傳送者，應刪除涉密內容，該部分資料則另採書面發送並經簽收程序。

  六、機敏會議應以秘密方式舉行，並選擇單純或有隔音設備之場所以防止竊聽，同時禁止非相關人員任意進出。

  七、訂定重大專案機密維護措施，研判作業流程可能發生洩密之事項、防範措施、執行分工等，由有關業務單位按執行分工落實執行。

  八、在職期間所經手或保存之機敏資訊，於退休離職或職務異動時，應列入移交或依規定銷毀。

- 加強公務機密維護宣導：

由於機敏會議資訊外洩多屬人為因素，其中又以機關同仁輕忽導致疏失者居多，因此欲降低機敏資料外洩機率，要從培養機關同仁保密素養著手。各機關應將現行法令規定、內部行政規則及保密措施、洩密案例以及可能導致洩密管道等，利用集會或機關內部資訊網路等方式加強宣導，務使機關同仁均能瞭解有關保密規定、法律責任及公務機密維護作為，以養成同仁落實機敏會議資訊保密之習慣。

- 指定專人統合對外發言工作，落實發言人制度。
- 落實機關資訊安全稽核：

  為機先發掘資安漏洞，同時檢視機關同仁實際執行保密情形，各機關應定期、不定期或遇有重大洩密案件時，執行資安稽核或保密檢查，除改善缺失漏洞並提高防火牆功能以防駭客入侵外，同時藉此對執行良好者從優獎勵，對執行不力者依規定懲處，以導正機關同仁建立機密資訊維護的正確認知。
- 機敏會議資訊列入保密檢查：

  因機敏會議資料多屬公文之附件，故亦為機密文書之範圍。準此，是否以機密文書之方式辦理收發、傳遞、歸檔、清查、機密等級變更(註銷)及銷毀等程序，應一併列入公務機密維護檢查項目。除藉以強化保密措施是否確實及督促同仁提高警覺外，並可事先發掘可能洩密管道，防範機敏會議資訊遭刺探而洩漏。

本署叮嚀

公務員有保守秘密之義務，然會議資訊應否保密，取

決於內容有無涉及機密或敏感資訊，而在相關法令規定繁瑣以及執行保密措施徒增作業的情況下，可能導致公務員刻意輕忽未能落實相關保密措施，致造成機敏會議資訊保密工作之隱憂。

機敏會議資訊外洩所造成的損害，雖因個案不同而有不同程度之影響，然不容置疑，機先預防絕對比事後懲處更為重要，平時未加強保密宣導、檢查，終將使相關人員受到洩密、刑事及民事責任之追究。是以，如何藉由研訂保密措施、保密作為宣導、資訊安全稽核及公務機密檢查等方式，將正確觀念落實在機關同仁日常工作中，不僅可確保機敏會議資訊不致外洩，亦能保護機關同仁避免遭受相關責任之追究。

結語

為保障人民知的權利，藉以協助人民公平利用政府依職權所作成或取得之資訊，進而增進民眾對公共事務之瞭解、信賴及監督，政府資訊自以公開為原則。然涉及國家安全及利益、政策擬定、公務執行及個人隱私等，部分機敏會議資訊的確不宜任意公開，如一旦洩漏，將造成政府機關決策及執行困擾，損及機關或民眾權益等負面效應，甚至影響國家安全及利益，也會損害人民對政府機關之信賴。

因此，公務員應深刻體認機敏會議資訊維護的重要性，提高保密警覺，以維護機敏資訊的安全。

公務機密維護　錦囊 第 3 號

~「駐外機構資訊保密之道」

前言

駐外機構為我國外交打拼的最前線，其工作環節容易受到敵對勢力的刺探、蒐集，且隨著資訊科技日新月異，網路上的駭客攻擊手法也不斷翻新，部分駐外機構屢遭網路駭客惡意攻擊，蒐集公務機密資料或侵擾其行政運作，網路安全與資安管理面臨嚴峻的挑戰。若相關人員未能提高警覺，極易因疏忽而洩漏相關資訊，加上事後追查不易，致使機敏資料外洩時有所聞。

任何一個能夠上網的裝置或電腦，都很容易被網路上的惡意活動影響，因此，駐外機構人員應嚴格遵守相關資訊安全規定，以降低資通安全威脅，提高電腦資訊使用風險承受能力，並妥善使用公務電腦，避免機敏資料外洩，以確保國家安全及利益，實為駐外機構資訊機密維護的重要課題。

案例摘要

- 駐○○代表處○○組所屬電腦於 101 年 2 月 1 日非上班時間，發生大量資訊封包傳送至外部特定電腦情事，經查係該組乙類雇員林○○使用之外網電腦及實體隔離電腦。據瞭解林員以更新電腦病毒碼為由，私自將內網連接外網電腦，傳送大量資訊封包至外部特定電腦，有洩

密之虞。林員所使用之 2 臺電腦硬碟，經查共計 26 件機敏資料外洩，違反資訊安全規定情節嚴重。案經○○委員會召開專案小組會議，決議將林員解聘。

問題分析

- 系統遭入侵：未經授權之使用人（駭客）入侵資訊系統進行攻擊、竊取或竄改資料等非法破壞情事。例如，「社交工程」(Social engineering)郵件設計愈來愈精巧可信，不知情的收儲，一旦開啟郵件附件，或點擊郵件內的惡意網站連結，任何一個動作都會讓電腦感染病毒。
- 未落實資訊安全規定：
  - 隔離電腦未落實隔絕於網際網路之外，專用於公務作業。
  - 個人電腦之使用者識別碼及密碼，未妥善保存或交付他人使用，及未定期更換。
  - 機敏資料存放在對外開放的資訊系統中。
  - 隔離電腦未以人工更新防毒程式病毒碼。
  - 非經權責主管核准，個人電腦擅自下載軟體或變更硬體規格。
  - 遇有資安異常事件發生，未即時向資訊單位反映處理。
- 維護措施不足：
  - 可攜式設備或媒體（如筆記型電腦、行動硬碟、隨身碟等）應妥為保管，非因公務需要並經主管核准，不得攜出辦公處所，攜回時應進行掃毒或系統還原。

- 對於電腦發生異常情事，未有警示系統，俾及時採取有效的防範措施。
- 重要機敏檔案之備份媒體，未嚴密管制或由專人管制。

稽核功能不彰：未依機關資訊安全環境，實施資訊稽核，致未能即時發現缺失。

使用人違規使用：經授權之使用人明知違規而使用，致系統資料外洩等情事。

策進作為

網路流量監控、分析及管制：

為防範系統遭駭客入侵，防火牆建置後，網管人員應隨時對資訊網路進行流量監控、分析及管制，俾利及時因應處理。

加強教育宣導：

辦理駐外人員資訊安全教育訓練，建立正確的資安共識，以避免發生違規使用電腦及公務資訊之情事，其宣導重點如下：

- 隔離電腦應隔絕網際網路並專用於公務作業，禁止私接；上網電腦連接網際網路並專用於上網瀏覽資訊或收發一般電子郵件。兩者不得混用，並於電腦設備明顯處張貼區別用途之識別標籤。
- 隔離電腦變更用途為上網電腦或上網電腦變更用途為隔離電腦時，須先將電腦硬碟格式化、重新安裝作業系統。
- 資料之加解密須在隔離電腦進行。

- 嚴禁安裝使用 P2P 點對點分享軟體。
- 禁止下載安裝或使用未經授權來路不明之軟體。
- 避免開啟來路不明的電子郵件及檔案，以避免駭客病毒入侵。
- 上網電腦禁止瀏覽非法或機關所限制之網站。
- 電腦應避免 24 小時開機，不使用時即關機或離線。
- 機密性或敏感性資料須以主管機關認可之加密機制加密後儲存於光碟、磁片、外接式硬碟等可攜性媒體或隔離電腦硬碟中，並予以妥善保存。
- 禁止使用上網電腦處理機密性或敏感性公務。

落實機關資訊安全稽核：

為機先發掘資安漏洞，同時檢視駐外機構人員實際執行保密情形，各駐外館處應定期、不定期或遇有重大洩密案件之虞時，執行資安稽核或保密檢查，除改善缺失漏洞並提高防火牆功能以防駭客入侵外，同時據以檢討策進，以建立同仁機密資訊維護的正確認知。

本署叮嚀

駐外機構人員對資訊保密工作應存有「時時保密」、「處處保密」及「維護機密安全是個人的專業責任」之觀念，尤以當前資訊設備精進，傳遞資訊的速度極快，洩密者或竊密者只要利用資訊設備，即可將所竊取之資訊即時傳遞，進而影響國家安全及利益。因此，對於資訊異常狀況，應保持高度警覺，以避免非相關人員接觸或使用資訊設施或資料，增加洩密之機會，為有效維護資訊安全，應妥採下列作為：

（一）人員管理及資訊保密教育訓練；

針對駐外機構人員之品德操守，主管應負起考核責任，瞭解屬員生活作息、交友、家庭、財務等有無異常狀況，適時輔導。調（派）任工作前，應施以保密安全教育，使其了解個人保密安全責任，熟悉有關安全要求與方法，對未依規定者，應適時調整職務，並在決定或提出建議之時，採取隔離措施。

（二）厲行稽核管制措施：

為有效稽核駐外機構電腦作業情形，發現潛存危險因子，資訊單位應對所屬電腦系統實施定期與不定期方式抽檢，並嚴格針對駐外人員於電腦作業時之磁碟暨檔案管理情形、密碼設定、實體隔離、電子郵件實施全面性檢查，確保資訊安全。

（三）緝密資料處理儲存：

電腦資料處理應設定安全防護措施，建立預警功能。在電腦資訊系統未採取任何安全存取控制及保密措施前，任何機敏資料，禁止存放於硬碟。

結語

駐外機構資訊機密維護工作，是否落實，攸關國家安全及利益，為確保資訊機密的安全，除了必要的資訊安全機制外，最重要的還是需要使用者的保密素養，因為資訊的掌握者、運用者都是「人」，唯有「人」對於資訊安全與保密工作能夠做好，才是維護資訊機密的根本之道；再者，唯有使用者都具備健全的觀念與知識，體認資訊機密安全的重要性，資訊安全政策才能落實。

公務機密維護　錦囊 第 4 號

~「烏龍露個資・洩密又挨告」

前言

政府機關受理民眾陳情請願，常可能因此取得民眾陳情書及相關個人資料，雖陳情請願屬於公開訴求，惟仍應依人民陳情相關法令為後續處理，如需運用陳情資料亦須符合個人資料保護法規定，避免產生未經同意或與原目的不符之公開、洩漏情事，造成當事人損害，衍生政府機關國賠責任，實不可不慎。

案例說明

小李和鄰近住戶組成土地重劃自救會向某地政機關陳情，拒絕徵收所有土地進行其他開發，除於該機關網路信箱陳情外，一行人浩浩蕩蕩到該機關門前進行陳情請願，並遞交載有相關自救會成員身分資料之陳情書，經該機關派代表受理後離開，嗣後卻發現該自救會成員陳情書中的個人資料，竟成了該機關於重大重劃案件評估說明會之附錄資料，且該機關為求便利，又以網站留言板回覆陳情人，亦未適當遮掩相關個人資料，造成該自救會成員的身分證字號、電話、地址等個人資料全部公開在網站上可供人點閱、下載，該自救會立即電洽該機關抗議其作法失當，且違反相關規定，揚言告到底，並要求國賠。

問題分析

本案為洩漏民眾自救會陳情書及附件之個人資料，該自救會附件資料主要用於反對土地徵收之陳情附件，並未同意其他使用或公開於網站中，又雖係公開陳情，惟主管業務機關受理後，應將陳情書及相關附件，回歸機關受理檢舉陳情案件保密相關規定，交由負責辦理之承辦人員，再將資料密封後交由收發人員登錄，且登錄之內容不得顯示檢舉(陳情人)姓名或身分辨識資料，另於公文簽辦過程除應以密件簽核，且須用密件答覆處理結果，而非將該案以一般案件處理，衡酌本案因受理民眾陳情書與相關個人資料，應屬公務機密範疇，該機關於網路留言板答覆，亦未適當隱去陳情人之個人資料，實有未妥，已衍生洩密問題。

另依據個人資料保護法第 16 條規定，公務機關如對個人資料之有特定目的外之利用，應符合相關要件方得為之，例如有法律明文規定、為維護國家安全或增進公共利益、有利於當事人權益或經當事人書面同意等。而該機關於重大案件評估報告書中，未經同意，擅將隨附於陳情書中之個人資料作為該案附錄，顯與上述要件不符，又依據同法第 28 條規定，公務機關違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。因此，該機關後續尚須面對相關國賠問題。

綜觀受理本案機關之處理作為，應係對於陳情案件與個人資料之相關規定與要件判斷有誤，致生洩漏情事，確有違失檢討空間。

改善及策進作為

◎本案肇因機關同仁對於民眾公開陳情請願性質未正確

之研判，且就相關個人資料管理及運用不慎所致，機關應積極檢討下列措施，以避免類似情事發生:

一、重新審視受理陳情案件相關規定，並確實檢討相關規範是否完備、受理程序是否妥適，以使機關承辦人員知所依循，避免衍生洩密情事。

二、藉由本案顯現陳情案件處理過程易生洩密，因此，應積極建立各項陳情案件判斷歸屬流程，檢討各環節之弱點與錯誤頻率，落實風險管理，降低誤判機率，提升機關維護效能。

三、全面檢核類似案件屬性判斷是否合宜，相關處理過程是否符合規定，避免重蹈相同問題。

四、妥訂陳情案件相關個人資料檔案管理機制：如針對機關因陳情案件蒐集個人資料所應制訂機關內部管理規範，規範個人資料之蒐集者、蒐集方式（直接或間接）、告知當事人、蒐集界面及儲存位置、法定保存年限及自定保存年限等事項，並落實檢核陳情案件個資蒐集、處理及利用過程，當事人隱私權保護之需求，俾能確實監督管理狀況。

本署叮嚀事項

民主法治時代，政府職責係為民服務，而人民為爭取權益或表達訴求，得依法透過陳情請願等合法管道向政府機關表達訴求，政府機關因而取得大量個人資料，應有良好的管理或保護措施，避免未合法運用，造成民眾權益受損，或保護不善產生如駭客入侵等洩漏風險。因此各級機關管理該等資料，除就涉及公務機密部分應依密等文件程

序進行保管外，另需參照個人資料保護法儘速落實相關維護工作，俾提升使該等資料於機關內部運用與保管安全性，本署就該案提出下列叮嚀，以資參酌：

一、積極檢討訂定機關主管機密範圍項目，俾利公務機密與個人資料確實依據其個別管理模式妥為執行。

二、嚴密機關組織分層審核措施，協助同仁處理相關案件，確符個案處理程序，避免衍生洩密疑慮。

三、重新檢視個人資料保護法施行後，機關各項作業程序與有關之行政規則，是否有相悖或未盡之處，以符實際，並減少疏失。

四、加強公務機密與個人資料保護法之法治教育：綜觀洩密多肇因公務員對於案件與法令認知未盡周詳，因此，透過現行法令規定、洩密違規（法）案例，以及可能導致洩密管道與因素，積極提升個人之保密法治觀念，方能落實宣導效益。

結語

公務機關就各項涉含個人資料之公務文件，因應個人資料保護法施行，應更為審慎，尤以面對各項法令產生見解上之歧異時，應以專業並合乎法治精神，對於當事人有利之方向做決策，除避免衍生後續洩密疑慮外，並有助於提升民眾對於政府之信賴。本案因機關同仁受理民眾陳情請願案件取得他人個人資料，又於處理方式與後續運用，未符合公務機密與個人資料保護法之規定，導致陳情人權益受損，實應深入檢討，避免類似案件再發生，以保護民眾權益，維護機關廉政效能。

公務機密維護錦囊　第 5 號

~「勞工申訴身分保密須謹慎」

前言

勞動檢查機構職司勞動檢查業務，除依據勞動檢查法、勞工安全衛生法等相關勞動法規執行檢查職務，另依據勞動基準法規定受理勞工申訴案件。惟因申訴者多為現職員工，申訴人身分一旦外洩致雇主知悉，將可能使申訴勞工陷於遭受解僱、調職或減薪等不利處分之困境，是以，對於受理勞工申訴案件處理程序，若未確實嚴守保密規定或因疏忽而有不慎洩漏申訴人身分情形，除打擊勞工公益舉發行為外，亦極易斲喪機關公信力，並將對申訴勞工造成相當大之損害，爰如何妥善保護申訴人身分免於外洩及確實嚴守保密規定，為不可忽視之重要課題。

案例摘要

某甲為勞動檢查機構檢查員，其係初任公職剛滿一年的菜鳥，在一次受理民眾檢舉渠任職之「○○大廈管理維護公司」（下稱○○公司）違反勞動條件，並要求身分保密之申訴案件中，某甲為查明○○公司有無違反勞動基準法等相關情事，至申訴人任職之○○公司實施檢查，並向雇主調閱含申訴人在內之員工名冊。惟在案件處理上，某甲疏未注意○○公司員工總數及調閱人數

間之抽樣比例（該公司員工總計 7 名，某甲僅調閱 2 名員工之資料），且調閱之員工資料均係在同棟大樓任職管理員之人員，致雇主得縮小臆測申訴人之範圍。

檢查員某甲翌日接獲雇主來電訛稱其知悉何人為申訴人，並表示該員同意撤回申訴案。某甲聽聞即欲聯繫申訴人確認其真意，然因受理時未詳加確認申訴人聯絡電話，致無法立即聯繫到申訴人，隨即某甲竟選擇直接傳真申訴撤案單至○○公司。此舉讓雇主直接接獲該撤案單，並持單要求其懷疑為申訴人之員工撤案，且公開質疑申訴人對公司之忠誠度，致申訴人在公司承受莫大壓力，進而心生強烈的離職念頭，造成十分嚴重的傷害。

問題分析

一、 受理案件未詳加確認申訴人聯絡電話

本案檢查員受理申訴案件，對於申訴人所留可供聯絡之電話、地址等資料，未詳加確認，致電話號碼辨識錯誤，無法與申訴人聯繫確認案件相關程序。

二、 檢查抽樣方式洩漏申訴人身分

本案檢查員調閱員工（含申訴人）資料未注意公司總人數及調閱人數間之抽樣比例，抽樣比例過低；另所調閱之人員均在同一棟大樓任職管理員。從抽樣比例及空間關聯上，極易遭雇主臆測出申訴人身分。

三、 未向申訴人確認真意即逕自傳真至遭申訴單位

本案檢查員遭雇主訛詐，誤認申訴人有將申訴案撤案

之意思，因無法聯絡上申訴人確認真意，逕自傳真申訴案撤案單至遭申訴之事業單位，導致雇主得持該撤案單據以要求其懷疑為申訴人之員工撤案。

四、檢查員未具保密觀念，輕率誤信雇主說詞

本案檢查員為初任公職剛滿一年之員工，因資淺無經驗，尚無堅強之監督分際界線及保密觀念，對於事業單位雇主單方表示知悉何人為申訴人並告以該人有撤案之意思，輕率誤信，未循正式管道通知申訴人，逕將撤案單傳真至事業單位。

改善及策進作為

一、詳加確認申訴人之聯絡資料

受理申訴案件，對於申訴人所留可供聯絡之電話、地址等資料，應詳加確認，俾將來公（文）務往返聯絡無誤。

二、檢查抽樣方式應避免申訴人身分曝光

執行檢查有關受檢場所抽調員工資料人數應具有廣泛性及不特定性，避免因取樣比例過低及時間、空間關聯因素，而使受檢查之雇主易於臆測出申訴人身分，間接造成申訴人身分之曝光。

三、撤案程序應憑申訴人之真實意思辦理

申訴案撤案程序應由申訴人主動向勞動檢查機構提出，並由該案承辦檢查員直接對口聯絡，由承辦檢查員確認申訴人之真實意思並提供撤案單憑辦，不得透過申訴人以外之第三人，以確保撤案表示之真實性。

四、強化檢查員辦案技巧並落實員工保密觀念

持續教育檢查員辦理申訴案之執法技巧，加強宣導深化檢查員行政程序作為及公務保密觀念，將公務機密教育列為新進檢查員之訓練課程，杜絕任何可能洩漏申訴人身分之管道及避免滋生洩密爭議之方式。

叮嚀事項

勞動檢查機構因業務屬性特殊，執行各項勞動檢查業務時往往會持有民眾個資及事業單位資料，如檢查紀錄登載受檢人個資、調閱事業單位勞工保險資料、出差勤紀錄等，對於公務機密維護之重要性更不可輕忽。此外，受理民眾申訴陳情案件，於處理程序及執法技巧上更應注意相關檢舉人身分保護作為，以免因過失或疏忽而侵害民眾權益，造成嚴重之不良後果。

為使公務機密維護作為更臻完善，俾防杜違反保密規定或洩密情事發生，可加強下列作為：

一、定期檢視機關處理保密業務作業流程，就受理申訴法制程序以及實際作業，如受理申訴表格之填寫、處理過程進行勾稽，並彙整缺失情形研析。

二、持續辦理教育相關保密業務之執法技巧，加強宣導深化公務人員行政程序作為及公務保密觀念，使其養成專業的保密素養與習慣，並保持高度警覺。

三、加強保密督導檢查，對檢查所發掘之保密缺失，應儘速採取改進措施，並列為追蹤複查，澈底杜絕保密漏洞。

結語

政府機關除提供公共福利服務外，尚有維持社會秩序、增進公共利益之職能，尤其在負有稽查、檢查等公權力性質的機關，面對民眾舉發或申訴違反法令之情形，除依法查辦外，對於舉發人或申訴人之身分，尤須注意保護其身分，切勿使其身分曝光。若過程中因故意或過失洩漏舉發人或申訴人身分，除公務員個人將負擔刑事責任外，將嚴重打擊民眾對於違背公益行為舉發之信賴，更斲喪政府機關之公信力。

保密是公務員之法定義務，保護申訴人身分更是掌有公權力機關責無旁貸的責任。是以，公務機密維護作為之完善，實賴每一位公部門服務人員之努力，持續透過宣導與教育加強保密的觀念，使其於平時行政作業時即養成良好的保密習慣與警覺，有效防杜違反保密規定或洩密不法情事發生，俾提升公務機關為民服務品質。

公務機密維護　錦囊 第 6 號
~「LINE 不當轉傳致洩密」

前言

隨著智慧型手持裝置日益普及，資通網絡升級與即時通訊軟體大行其道，資訊運用除了更加便利外，更伴隨著令人擔憂之資安事件及機密外洩等問題。熱門通訊軟體中，不論是 LINE、Facebook Messenger、WeChat 等，其通訊安全性都備受質疑，甚有媒體報導警政署表示即時通訊應用軟體有其便利性，但都是民間研發的商業軟體，政府機關不能管控，難防洩密。加以邇來媒體報導使用該等軟體諸多被駭、詐騙、洩密及誤傳事件，讓其安全性備受爭議。此等資訊安全情事屢見不鮮，值得機關加以防範與管制。

案例摘要

- 刑事局某外勤隊日前與多個縣市警方共同偵辦一起詐騙集團犯罪案，行動前所有專案成員都在智慧型手機上開立一個 LINE 的群組，用 LINE 傳送嫌犯照片、即時資訊、並下達攻堅指令。惟至現場攻堅時，發現空無一人，原來嫌疑犯等人早已獲知消息，提早一步逃離。經調查發現，該次搜索行動採用時下流行的 LINE 傳送訊息，因使用群組發送，群組中某些負責情報蒐集成員在轉傳訊息時「手滑誤觸」其他友人頭像，致搜索行動訊息被轉傳，輾轉流連最後傳到詐騙集團手

中，導致整個搜索行動提前曝光，致該不法集團成員先行逃匿，功敗垂成。

問題分析

- 機關缺乏對於新型設備、軟體之洩密評估風險及預警，LINE、Facebook Messenger、WeChat 等即時通訊軟體帳號被盜、洩密、誤傳訊息之新聞時有所聞，機關未建立相關預警機制。
- 未停用 LINE 等即時通訊軟體利用行動電話號碼自動加入陌生人為好友的功能，亦未定期刪除或封鎖 LINE 等即時通訊通訊錄之陌生人。
- 機關對智慧型手持裝置防制洩密之宣導不足，機關同仁對於智慧型手持裝置洩密方式不甚清楚。
- 貪圖傳訊快速便利，忽略即時通訊軟體無法加密或刪除所發訊息，低估該等軟體洩密風險。
- 公、私務器材物品混用不分，智慧型手持裝置通訊錄之聯絡人亦公私不分。

改善及策進作為

- 落實資訊安全稽核檢查作為：

  為使資訊安全保密工作更臻完善，除了加強教育宣導之預防工作外，定期或不定期對所屬機關（單位）同仁之資訊安全保密工作執行情況，辦理督導考核亦是重要的一環；務期透過稽核、檢查過程中發掘優、缺點，對於執行良好者，從優獎勵，對於執行不利者，則依照相關規定懲處，以落實資訊安全保密執行工作

，並提高機關同仁對於落實資訊安全之警覺性。

- 定期清查或檢測智慧型行動裝置防駭防毒效能：

  智慧型行動裝置之功能已趨近於電腦，由於其攜帶方便之特性，使用者對於 LINE、Facebook Messenger、WeChat 等通訊軟體使用頻率及依賴性增加，遭受資安威脅之機率亦更高，故對於智慧型行動裝置應比照電腦定期辦理資訊稽核，並加裝及定時更新防毒防駭軟體，以及審慎維護管理 LINE 等通訊軟體之帳號，避免機密資料外洩或遭受惡意程式攻擊的危機。

- 確實落實公務機密宣導事宜，深植資訊安全觀念：

  目前智慧型行動裝置使用率極高，但是使用者對於智慧型行動裝置潛在之資安危機普遍缺乏警覺，尤其以 LINE 等即時通訊軟體傳送公務訊息或資料時，如能提供同仁瞭解智慧型行動裝置可能存在之資安漏洞，方能明瞭弱點進行強化與修補。是以，各機關得彙整相關公務機密法令規定、洩密違規案例，以及可能導致洩密管道與因素，並結合機關各項會議及活動，有計畫有系統的利用各種時機向同仁宣導，使每一同仁均能瞭解相關法令規定，以培養時時保密、處處保密之良好習性，提高同仁保密警覺，藉以降低洩密風險。

- 使用安全性更高之即時通訊軟體：

  LINE、Facebook Messenger、WeChat 等通訊軟體屬於國外公司研發之軟體，其電腦主機與管理權限皆不屬我國管轄，且上述軟體使用人數破億，商機極為龐大已成為駭客覬覦的目標，洩密風險日益升高。若機關

有即時通訊需求，建議使用安全性更高，使用者較少之即時通訊軟體，如我國工業技術研究院研發的開發之揪科（Juiker）APP 作為替代，惟在未轉換更安全之相關軟體前，建議各機關妥善維護管理 LINE 帳號。

- 以公務用或私用之用途區隔智慧型手持裝置：

使用公務用智慧型行動裝置，應避免私人用途及連結不明網站或下載不明之程式或軟體；傳送訊息時，應再三確認收件者對象及內容是否正確，避免誤傳，內容涉及隱私、機敏資料，應盡量避免使用即時通訊軟體傳送。

- 其他注意事項

公用智慧型手持裝置（含新型警用 M-Police 裝置）不可任意破解，如 iPhone 或 iOS 裝置不可提權越獄（Jailbreak）、Andriod 系統不可取得最高權限（Root）、刷機。

結語

公務機密維護方案已進入 E 化轉換時期，方能提升維護策略，且須由多方面著手，方能立見其效。然公用智慧型手持裝置已成為公務機關相關提升工作效率必要設備，而是否有良好管理介面輔助，並能對同仁同步專業資訊訓練，以提供正確使用方式，且研討其可能發生洩密及違失態樣，俾免資料外露與洩密疑慮，均為研析核心。

是以，如何善用公用智慧型手持裝置，以提升行政

之效能，同時保護公務機密與個人資料不致外洩，實有賴公務同仁的努力，並持續透過宣導與教育加強保密觀念，使其養成專業的保密素養與習慣，防制違反保密規定或洩密情事發生，俾使公務機密維護作為更臻完善，確實保護民眾與機關權益。