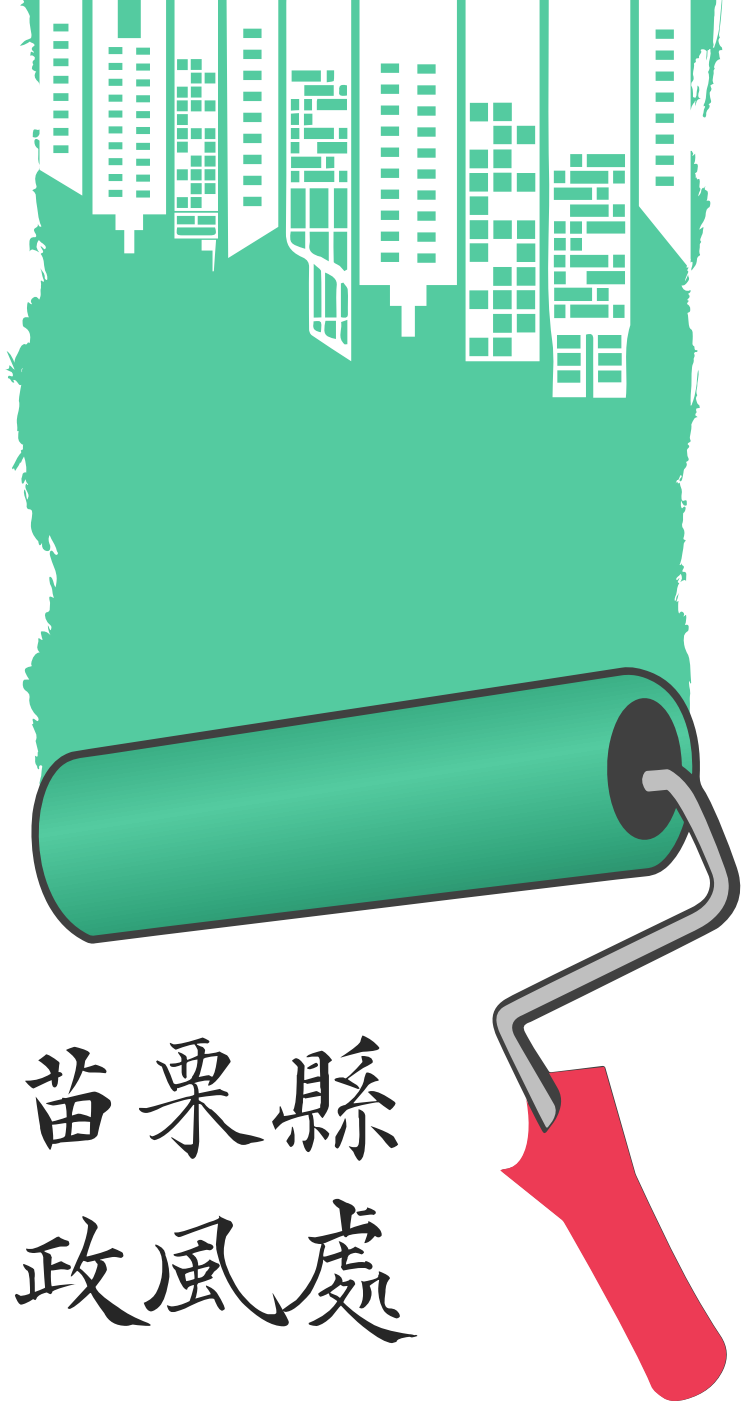
苗栗縣政府111年
政風處2月宣導

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、IG、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，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。



苗栗縣
政風處

01 案例摘要

02 問題分析

03 法律觀點

04 改善及策進作為

05 結語

案例摘要

案例1

甲係某機關收發人員，其不知道司法單位向該機關調閱某採購案件卷宗之公文屬應保密事項，竟將該公文電子檔傳送至該機關之公務Line群組，而觸犯刑法第132條第1項之公務員交付關於中華民國國防以外應秘密之文書罪，案經地方檢察署檢察官處以緩起訴處分。

解析:

機關同仁缺乏對於機關機密文書保密之觀念，並忽視對於新型設備、軟體之洩密評估風險及預警，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。

案例2

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。

法律觀點

隨著網路及行動應用的蓬勃發展，越來越多民眾喜歡使用即時通訊軟體聊天、甚至會將他作為討論或交辦工作的工具。針對利用即時通訊軟體處理公務的作法，目前已有政府單位訂定技術性或細節性規範加以因應。整體來看，這些規範大抵可分為「軟體安裝與設定」、「群組管理」及「資訊傳遞」三個部分。針對「軟體安裝與設定」，使用即時通訊軟體進行公務討論時，應先進行密碼設定及管理，並就裝置進行相關安全環境設定，這部分其實與一般電腦安全並無二致。針對「群組管理」，先依據公務需求不同成立各類群組，再依此設定分組原則及成員資格，而後由群組管理者 (組長) 本於管理權限進行群組加入或退出之審核；在此模式下，如果不具有加入群組資格，即無法進入該群組而有後續接觸公務資訊的機會，藉以降低公務資訊外流的風險。至於「資訊傳遞」則為資安風險控管之關鍵點，在做法上，公務資訊如涉及機密性、資訊安全及隱私事項，一律不得以即時通訊軟體傳輸，原則上就不可能會有透過即時通訊軟體傳輸或外洩的機會。其次，針對非屬機敏性之公務資訊，如果涉及公文檔案傳遞，另應同時注意符合公文公開作業原則等規定。

法律觀點

此外，為俾利公務資訊的後續使用、舉證、追蹤等，公務人員對於重要資料，應注意備份存放；針對重要資料，例如含有大量個人資料檔案，應以密碼或加密措施保護。而為避免公務資訊在無意間外洩，在丟棄任何儲存資訊之電子媒介時 (例如，光碟片及隨身碟等)，應先將儲存資訊刪除，並徹底消磁或銷毀至無法解讀的程度。並且，在任何公開之新聞群組、論壇、社群網站或公布欄中，應特別注意不可透漏任何公務機密相關之細節。公務人員如有違反上開規定，將依政府機關人事相關規章面臨行政懲處。如涉及重要之公務機密外洩事件，不論出於故意或過失，可能構成刑法洩漏公務秘密罪，最重可處以三年有期徒刑。如洩漏者屬國家機密時，更可依國家機密保護法規定，處一年以上七年以下有期徒刑。在提升公務聯繫效率的同時，對於潛在的資安風險必須格外謹慎，以免因一時的無心之失，反而為自己增添無謂的牢獄之災。

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。

改善及策進作為

使用安全性更高之即時通訊軟體：

LINE、Facebook Messenger、IG、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。

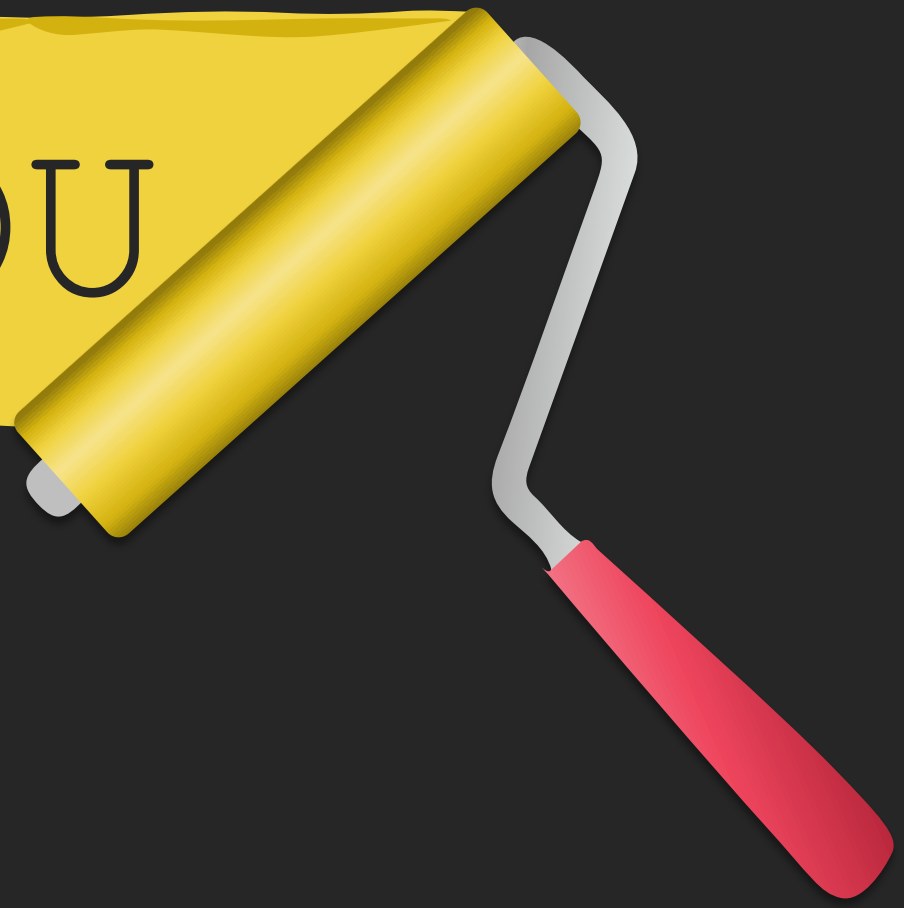
以公務用或私用之用途區隔智慧型手持裝置：

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。

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，俾免資料外漏與洩密疑慮，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。

THANK YOU



廉政專線：

037-356639

苗栗縣政府

政風處關心您❤