「公務機密維護宣導」

公務即時 LINE，洩密也能賴？

★【焦點話題】

拜科技進步所賜，即時通訊軟體(例如 skype 及 Line 等)越來越夯，這個工 具不僅在一般企業組織或社群中受到歡迎，也成為政府機關提升公務聯繫效 率的新幫手。在提升公務聯繫效率的同時，即時通訊軟體的潛在風險也引發 討論。例如，某公務人員曾將首長批示意見透過 Line 對外傳送，造成消息 不當曝光；又例如因某公務群組遭駭客入侵，促使機關自我檢討公務聯繫作 業，甚至自此嚴禁「機密公文」以即時通訊方式傳遞。面對公務聯繫效率及資訊安全保護的兩難，曾有議員質疑通訊軟體存有潛在 風險，部分政府單位早已禁用通訊軟體。更深度的問題是，與一般公文不同， 即時通訊所傳送的訊息無須依法進行存檔及列管，也無從追查，未來恐成了 洩密和弊案的溫床。【資料來源：聯合報 104/4/18】

★【重點摘要】

1. 公務人員線上進行公務討論聯繫時，應注意資訊安全與通訊內容之機密性。
2. 公務人員利用行動裝置從事公務討論時，應進行資料備份與加密防護，並注意該裝置遺失或廢棄之資料處理。

★【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 36 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。

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

★【管理 Tips】

在本案中，組織在導入或使用行動式設備時，應訂定相關政

策規範，其中應 包括：可在行動設備中使用的工作項目、資料儲存方式、行動設備需具備的 保護設施、資料傳送要點，及資料銷毀的程序等。此外，組織應採取相關配 套措施以管控風險，並透過教育訓練、宣導或公告注意事項等方式，讓員工 明瞭設備使用範圍、限制及相關安全規則；必要時，對於違反使用規範之員 工應有相當內部懲處措施，以兼顧行動辦公需求並同時落實對於機敏資訊的保護。

另一方面，針對就行動式設備的資料，組織應定期執行備份作業；如有包含 機敏性資料，尤其應考量機敏性資料加密的方式，以避免機敏性資料被其他 未經授權的人員取得。此外，組織應明確告知員工，如授權的行動設備遺失 時，務必要進行內部通報，以防止損害擴大。對於使用的行動設備，如有報 廢或汰換之需求，應先將原有資料備份到新的裝置，而後刪除原有資料或破 壞原有行動設備，以避免資訊安全事件的發生。

*資料來源：行政院國家通安全會報技術服務中心