

公務員廉政倫理規範

公務員廉政倫理規範案例

壹、案情概述

00 區公所農業課公務員楊步棋，渠係負責審核農用許可相關之業務。100 年 2 月 10 日晚上與國小同學李巧巧到知名餐廳用餐，巧遇承包該公所路樹修剪廠商李爾郁，雙方互打招呼後，逕自回座用餐。當日楊員與同學消費額共計 1,100 元，孰料結帳時發現廠商李爾郁已代為結帳並先行離去，致公務員楊員不及拒絕收受。翌日，楊員至公所上班後，即立刻報告其區長，並知會公所政風室，完成登錄，並於 2 月 12 日將 1,100 元歸還廠商李爾郁。

貳、研析

本案中公務員楊步棋因對公務員廉政倫理規範之規定極為瞭解並恪遵該規範，於發現廠商代為結帳後，即立刻報告其長官，並知會該所政風室，完成拒收餽贈登錄，故能免責，茲分述如下：

一、按公務員廉政倫理規範第七點規定公務員不得參加與其職務有利害關係者之飲宴應酬，第二點第二項又規定，與其職務有利害關係：指個人、法人、團體或其他單位與本機關（構）或其所屬機關（構）間，具有下列情形之一者：1. 業務往來、指揮監督或費用補（獎）助等關係。2. 正在尋求、進行或已訂立承攬、買賣或其他契約關係。3. 其他因本機關（構）業務之決定、執行或不執行，將遭受有利或不利之影響。本案路樹修剪廠商李爾郁，因與公所已訂立路樹修剪承攬之業務關係，應為前揭規定之關係人，蓋公務員楊步棋對於廠商李爾郁代為結帳不得接受。

二、又本規範第七點但書規定，1. 因公務禮儀確有必要參加。2. 因民俗節慶公開舉辦之活動且邀請一般人參加。3. 屬長官對屬員之獎勵、慰勞。4. 因訂婚、結婚、生育、喬遷、就職、陞遷異動、退休、辭職、離職等所舉辦之活動，而未超過正常社交禮俗標準，則不在此限，亦即例外可以參加飲宴。而本案公務員楊步棋係與國小同學李巧巧一起用餐，並非參加上開情形之飲宴，並不適用例外規定，故應予拒絕，並簽報其長官及知會政風機構。

三、小結：本案中公務員楊步棋因飲宴而受廠商代為付款，雖非事前接受邀請飲宴應酬，惟廠商李爾郁為公務員廉政倫理規範第七點規定之不得參加飲宴應酬之職務有利害關係人，且確有為楊步棋飲宴付款事實，因此基於維護公務廉潔自持形象，對於不及退還之帳款，應於事件發生之日起三日內，簽報其長官及知會政風機構，並將代付金額退回，才得以免責。

參、結語

公務員對於廠商之邀宴，無論是否與其執行業務有關，皆應謹守分際，予以拒絕，避免產生不必要的麻煩；遇有邀宴，應即報告長官，知會政風，以維護公務員清廉自持形象。

廉政宣導

案例-戒護人員協助受刑人傳遞訊息貪瀆案

壹、前言

矯正機關乃刑罰執行的場所，監所的廉潔度攸關囚情的安定與教化的成效；矯正人員若存私心謀私利、不守法紀，除戕害矯正風氣，並危及司法公平正義的實踐。監獄的高牆雖可限制受刑人的人身自由，但藉由不肖人員的媒介，以代為傳遞訊息的方式，仍能操控或進行監外的不法行為，持續危害社會的安全與安定；因此，如何發掘與防範上開情事，實值得重視與探討的課題。

貳、案情概要

一、犯罪事實

受刑人邱○○為竊車集團首謀，99年8月10日因案遭警方緝獲，於次日解送入監服刑，99年8月18日宜蘭監獄政風室於複聽邱犯之接見談話內容，發現其在監期間疑有透過監所人員為其傳遞訊息，持續操控竊車集團在外從事不法行為。經政風室主動深入清查結果，發現該監戒護科管理員簡○○及科員林○○等2人，疑涉為邱犯傳遞訊息予竊車集團共犯朱○○等情，其並指示以「賓士」及「國瑞」廠牌自用小客車，無償贈予簡員使用；另免費為林員修理、更換自用小客車引擎等涉有貪瀆不法罪嫌。上情於99年12月21日函送法務部調查局宜蘭縣調查站查辦，案經宜蘭地檢察署於101年8月20日偵結起訴處分在案。

二、涉犯法條、起訴或判決理由

(一) 管理員簡○○部分

簡○○明知矯正人員「不得接受收容人或其家屬之招待或餽贈」及「不得為收容人傳遞訊息、金錢或其他違禁品」等規定，竟利用管理、戒護邱○○之機會，基於違背職務行為而收受賄賂之犯意，多次為邱○○傳遞訊息，並收受不法對價，係觸犯貪污治罪條例第4條第1項第5款之對於違背職務行為收受賄賂罪嫌，爰依刑事訴訟法第251條第1項提起公訴，求處有期徒刑15年。

(二) 科員林○○部分

林○○明知邱○○為其修理完成後之小客車車體及引擎並非原車所有，係來路不明之贓物，竟仍基於收受贓物及行使變造準私文書之犯意而予收受，並自95年起，持續駕駛上開車輛而行使之，已觸犯刑法第349條第1項之收受贓物罪嫌及同法第216條、第210條、第220條之行使偽造準私文書罪嫌，爰依刑事訴訟法第251條第1項提起公訴，求處有期徒刑2年。

參、弊案發生原因分析

一、弊端態樣

監所為「人管理人」之特殊行政機關，人治色彩濃厚，性質封閉，入監執行收容人或亟思與外界聯繫，或為尋求較佳處遇，或為炫耀身分等心態，而有央託家屬親友運用各種方式請託關說，以不正利益誘惑、疏通管理人員，遇價值觀偏頗及存有僥倖心態管理人員，極易衍生風紀問題、貪瀆弊端。

二、內部控制死角

矯正機關戒護人員與收容人間，存在直接與特別的權力關係，不正當的互動行為具有高度隱匿性與保守性，非實體性的違規行為（如：傳遞訊息、違禁物品）不易被察覺，又弊端事件之發生瞬間即逝，犯罪證據難以及時、具體的掌控。

三、原因分析

本案邱犯為竊車集團首腦，前在宜蘭縣經營○○汽車修理廠，曾於91年5月間因案入監服刑，因地緣關係而結識簡、林兩位戒護人員。在通緝期間，邱犯仍從事竊取汽車及變造汽車引擎號碼等不法行為，99年8月11日突遭警逮捕，不及處理後續銷贓事宜，故於入監7日後即請該監簡員及林員代為傳遞訊息予竊車集團共犯朱○○等人。

消費者保護宣導

購車分期付款需知

(一)問題之發生：

冬梅是社會新鮮人，訂購一輛時尚的小型進口汽車，但是存款有限，因此買車同時，透過車行業務員介紹，與銀行辦理貸款手續；約定貸款新台幣（下同）五十萬元，等交車後，銀行始撥款給車商，冬梅再分期清償。為擔保清償借款，冬梅應銀行人員要求，簽發一紙面額五十萬元的本票，交給銀行。

冬梅訂購的那款汽車因故遲遲未進口，但銀行卻通知冬梅須分期清償本息，令冬梅極為訝異，因貸款時雙方明明約定交車後，才撥款給車商，為何銀行竟提前撥款？冬梅因此拒絕清償本息，數月後接到法院通知，銀行提出冬梅簽發的本票，起訴請求伊一次給付五十萬元及利息。

冬梅向法院答辯：訂立貸款契約時，前後不到十五分鐘，銀行人員所提示的定型化契約條款共有數十條，文字密密麻麻，她都沒有看就簽名蓋章。契約書中所記載銀行可隨時撥款給車商，與當時口頭約定不符，因此該條款不構成契約的內容，另依消保法第十五條規定，該條款與雙方磋商條款抵觸，應屬無效，伊可拒絕還款。法官傳訊車商業務員及銀行人員後，認定冬梅的答辯屬實，因此判決冬梅勝訴。

(二)法律之規定：

依消費者保護法第十一條之一規定，業者（本件為銀行）與消費者（冬梅）訂立定型化契約（即貸款契約）前，應有三十日以內的合理期間，供消費者審閱全部條款內容。銀行違反上開規定時，該條款不構成契約的內容，但是消費者可以主張該條款仍構成契約的內容（例如條款內容對冬梅有利時，冬梅可主張該條約定有效）。

(三)因應之道：

消費者對於業者所提供的定型化契約，可以要求事先審閱，關於審閱期間，行政院消費者保護委員會所訂各種契約範本分別訂為三天至七天不等，可供參考。

反毒宣導

少年悔染 K 毒：媽媽為籌錢過勞死

「我因為拉 K，一度沉淪！」台東 1 名 17 歲少年阿銘，因結識損友，染上吸食非他命惡習，進出警局成家常便飯，讓家人頭痛不已：直到母親因他過勞而死，才痛下決心戒掉毒癮，半年多的時間，終於讓他找到自己，重新點亮青春。

國中三年級就輟學的阿銘，為了生活獨自在外工作，認識了一群輟學青少年。下班後，大家就騎車到處閒晃，喝酒、抽菸，也接觸要命的毒品：阿銘從此跌入深淵，迷失了自己。

「K 他命、大麻、安非他命都吸食過。」阿明說，一開始覺得沒什麼，很酷！很新鮮。從一個月吸幾次，到幾天吸一次，最後天天必須吸一次，否則整個人焦慮，脾氣也很暴躁，最後變成班也不想上，整天想著要買毒來吸。

阿明說：「想吸毒，就必須花錢買毒。」他沒工作，沒收入買 3、4 千的毒品，只能回家向母親伸手要錢，母親不給就大吵大鬧，為了籌錢買毒品，他和朋友到處偷東西，常常進出派出所，讓親友們不願和他接觸。

阿銘表示，母親為了供錢給他，日夜操勞不停地工作，最後罹患癌症過世，才讓他徹底覺悟；他毅然決然借調吸食安非他命習慣，遠離狐群狗黨。雖然剛開始很痛苦，但一想到母親，就給了她戒毒的動力，整整花了半年多的時間，才真正恢復健康的身體，也重返職場，半工半讀。

安全維護宣導

未到期門號退租免違約金？小心老梗詐騙手法

門號沒在用，協助取消免付違約金？邇來發生詐騙集團以此說法，要求被害人先墊成本費用，事後再行退費為由行騙，利用宅配公司之代收服務降低出面取款曝光之風險。

家住彰化劉先生因與經銷商在有糾紛情形下辦理 2 支手機門號，因而前往電信公司申訴，並在保留 2 支手機門號情形下達成和解，之後接到自稱該電信公司的門號處理部門楊主任的電話，指稱接獲太多經銷商不當行為誘騙消費者辦理門號，所以總公司要求強制解除劉先生這 2 個門號，不過因劉先生之前收到 2 支手機贈品，應以現金 5,600 元付清，請陳先生將錢放入信封袋寄送，陳先生依指示辦理。之後楊經理要求陳先生支付 16,000 元違約金，並稱收到後會門號解約並退回之前款項共 21,600 元。數日後楊經理又來電，指稱同事多開 1 張 21,600 元的支票，要劉先生再寄 21,600 元，之後一併退還 43,200 元。之後又來電要陳先生再支付 11,200 元，之後一併退還 54,400 元。數日後接到自稱該電信公司財務部陳經理來電，指稱 54,400 元財物異常，要求陳先生與楊經理各支付 4 成的保證金，陳先生此時才驚覺可能遭騙，經與電信公司朋友聯絡，才確認遭到詐騙，總計被騙 54,400 元。

警方呼籲，如有取消門號之需求，務必至電信公司之營運據點申辦，勿聽信「無須付違約金」等藉口，而透過不明人士代辦。

你，「防毒」了嗎？

網際網路，這個起源於冷戰時期，美國「星戰計畫」的產物。已經超越它原先所設定的標的，進一步地改變了人類的生活、社會與產業結構，讓我們從原本的工業社會，蛻變成現在的資訊社會。

但是在我們享受網路便利性的同時，是不是也忽略了這其中潛藏的危機呢！除了「病毒」、「木馬」、「蠕蟲」可能已潛藏在我們所不知的角落蠢蠢欲動外，在過於便捷、快速的資訊流通過程中，我們又能對情資的傳遞有多少把關？我們所持有的個人或工作上的種種情資，是否也會在不知不覺間輕易外流呢？面對這些問題，大多數人只能選擇從三種方向來加以防範。

首先就是防毒軟體，防毒軟體所背負的任務，是隨時監控電腦程式的舉動，並掃描是否含有病毒等惡意程式存在。防毒軟體對即時監控的技術不盡相同，有的防毒軟體會利用部分空間，使正在運行的程式特徵與病毒資料庫比對，以判斷是否為惡意程式。另一些防毒軟體會類比系統或使用者所允許的動作，使受測程式執行內部程式碼的要求，再根據程式的動作判斷是否為惡意程式。

而在掃描方面，防毒軟體也涉及：掃描壓縮檔、程式竄改防護、修復技術。使其可以對壓縮和封裝的檔案進行掃描，並避免惡意程式藉由刪除防毒程式而躲過偵測，並對惡意程式損壞的檔案進行還原。另外，現有的防毒軟體多半還具備沙盒防護技術（註：沙盒〈Sandbox〉是一種虛擬系統，在這之中的所有更動都不會對作業系統造成任何損失，因此被電腦技術人員廣泛使用，更是一個觀察電腦病毒的重要環境。）能對一些無法判斷意圖的程式，提供一個虛擬的環境進行測試。

其次就是防火牆，防火牆的功能是檢查每一筆欲通過的資訊以及封包，是否符合事先設定的安全標準，如是則放行通過，反之則阻擋在外；此在阻絕木馬及駭客上，具有不可抹滅的功效。其中最簡單、最常見，也最早被實用的，就是封包過濾式防火牆。其最大優點就是速度快、容易建置且成本較低。但由於其作用層次較低，僅在 OSI 架構中的前三層進行作用，所以無法對經過的資料有較高層的稽核能力，而產生安全上的漏洞，在實用上必須加上其他的防火牆機制，以建立更嚴密的安全管控。

另外，還有應用層閘道式防火牆，它是採用與前述之封包過濾式防火牆截然不同的觀點來處理網路的安全問題。它是利用一些針對性的程式：閘道、代理器（Proxy），做為網路程式應用的中介，隔絕內部與外部網路的直接連結，改以存儲轉發的方式運作。由於此類防火牆是作用在 OSI 架構的最高層，所以能了解過往所有資料的通訊協定，並加上特定的安全功能，而目的地伺服器也無法得知原始資料的發送位置，使內部網路得以隱藏。在安全上應用層閘道式防火牆是各類型防火牆中最優良的，但是對使用者來說，它不完全具有通透性，有些應用程式可能會莫名其妙地被阻擋在外，而且它常會修改原有程式的處理程序，使某些特殊的應用程式無法完全施展。

由於這些缺失，因此又有電路層閘道式防火牆的研發，它是介於封包過濾器以及應用層閘道器之間的防火牆型式。此類防火牆最大的特點在於：它會在客戶端與目的地伺服器之間，建立一個點對點的虛擬線路，並允許多重的客戶端與多重伺服器溝通。但是，不一定可以隨處找到可用的客戶端；執行時往往必須先修改客戶端的電腦組態，使客戶端知道伺服器的存在，因此在執行上往往會遇到一些阻力。

在以上這些技術性介紹之後，可發現所有的技術都是不完美的，沒有一種防毒軟體、防火牆能讓你安裝之後就一勞永逸，不再受任何資安危機所困擾。

防毒軟體的病毒掃描率，無論如何都會受限於病毒資料庫的大小；而封包過濾器由於問世較久，早有不少駭客開發出能繞過封包過濾的入侵方式；又電路層閘道器在虛擬線路建立之後，其他應用程式也能經由同一虛擬線路進入防火牆內，產生安全上的漏洞；至於安全性最高的應用層閘道器，其代理器也不是隨時可供使用，每當有新的通訊協定、TCP/IP 服務出現，就必須重新發展新的閘道過濾器，對於尚未發展出代理程式的網路服務也不支援。因此，最後也是最重要的防護機制，就是使用者的習慣。

使用者的習慣和上述那些技術性的東西不同，是一種較為抽象的概念。首先要注意的是，防護措施不能省，就算世上沒有完美的防護技術，防毒軟體、防火牆也是有比沒有好。

在此分享一段過去的親身經歷。很久以前，當我還是大一新生時，有一段時間，宿舍的網路忽然異常地慢；之後宿舍就多出一條新規定：未裝防毒軟體的電腦不准上網。此規定一出，網路問題很快就迎刃而解。之後才得知，當時由於宿舍內有許多人的電腦未裝防毒軟體，導致惡意程式恣意橫行，嚴重拖慢了網路速度。所以，不裝防毒軟體不但害己，而且害人。

另外，在密碼的設置上，也不可過於簡單，切忌使用某種單純的數字組合或一個英文單字作為密碼。美國 CIA 就曾經以所謂的「字典破解法」破解 150 萬組以上的密碼。

此外，就是避免不明程式、資訊進入自己的電腦，除了最基本的不要任意下載不明程式、檔案外，電子郵件也必須經過確認、掃毒之後再開啟；至於新買的儲存裝置使用前也必須先行格式化，以確保安全。過去曾有某知名廠牌在大陸製造的硬碟，出廠前就全被預先植入木馬程式的案例；也曾有某知名 P2P 下載軟體，在啟動後會使整個電腦的檔案都處於可供外界任意下載的危險狀況。因此，良好的使用習慣是重要的，而且任何細節都不可疏漏，只有時時注意資安危機出現可能性，才能將資安危機的發生率降到最低。

公務機密維護（保防）宣導

員警未依規定使用公務電腦案

壹、案情概述

一、黃○○係○○縣警察局○○分局警員，101 年 4 月 7 日未依規定使用公務電腦查詢戶役政資料連結作業及查詢國民身分證資料，未依規定登載使用事由達 18 筆，遭該局資訊室查獲，核予申誡一次處分。

二、王○○係○○縣警察局○○分局警員，101 年 4 月 7 日未依規定使用公務電腦查詢戶役政資料連結作業及查詢民眾陳○○國民身分證資料，未依規定於戶役政查詢登記簿登記，遭該局資訊室查獲，核予申誡一次處分。

三、鄭○○係○○縣警察局○○分局警員，101 年 8 月 21 日未依規定使用公務電腦查詢戶役政資料連結作業及查詢民眾影像檔資料國民身分證資料，未依規定於任務為成後將電子檔刪除，遭該局資訊室查獲，核予申誡一次處分。

貳、經驗教訓

一、缺失檢討

(一) 黃員、王員、鄭員使用公務電腦查詢完畢未依規定登載顯係對公務機密之維護缺乏警覺。

(二) 王員查詢民眾陳○○國民身分證資料，未依規於戶役政查詢任務完成後將電子檔刪除，恐致洽公民眾有機可乘，公務電腦遭不當使用，亦有洩密之虞。

(三) 探究其洩密肇因，不外乎以下幾點：1、漠視保密作業規範。2、個人法紀觀念淡薄。3、資訊安全常識不足。4、資安管控機制失調。5、個人品行習性不佳。6、保密安全警覺鈍化。7、心存僥倖貪圖便利。8、掃毒軟體未保常新。9、資訊保密紀律鬆散。10、監督機制日久玩忽。

二、策進作為及建議

(一) 各機關應建立管制民眾進入辦公處所辦法，以強化安全防護，並應禁止洽公民眾使用公務電腦及可攜式儲存媒體，俾防止有心人士藉出入之便刺密。

(二) 各機關應經常辦理資訊安全稽核及資安講習，持續宣導資訊安全之重要，務使公務人員遵守保密規定，確保公務機密安全。

(三) 機關內部的電腦須有層層嚴密的防護措施，有專業資訊技術人員的監控防護。

(四) 家中的私人電腦防護能力通常較為薄弱，很容易遭駭客入侵或感染病毒、木馬等惡意程式，造成資料的外洩，因此涉及公務機密之文件不得攜帶回住家使用或作業，以維護保防工作的落實。

(五) 目前在電腦網路的運用上，要完全避免病毒或駭客的襲擊是不容易的，所以我們必須要有正確的觀念與應對措施，才能在安全的前提下，享用電腦和網路帶來的便捷。以下的作為應是電腦使用者的基本安全素養：

1、使用正版軟體：盜版軟體除了侵害智慧財產權、運用上不如正版軟體來得穩定外，也常挾帶惡意程式，導致電腦中毒或被入侵，資料被竊取或遭篡改，甚至成為惡意郵件的散播者。

2、重要資料加密：為避免重要資料外流，最基本的功夫就是將重要檔案加密，並且設定為隱藏檔案，置於特定的目錄夾內，以降低被人搜尋發現的機會。

3、不公務家辦：若將公事帶出辦公室不僅會增加洩密之風險，且

因家中電腦在安全機制上往往不如辦公室，又可能多人使用該電腦，甚至早已被植入木馬，所以公務家辦經常成為資料外流的主因。

4、避免開啟不明網站或不明郵件：許多不明網站之網頁或不明郵件經常暗藏或被寫入惡意程式，同時藉由驚聳誘人的標題或連結，吸引他人點閱，藉以散播惡意程式或竊取帳號密碼等，造成當事人的財產損失、資料被竊。

5、定時更新病毒碼與掃毒：惡意程式翻新與變化的速度非常快，所以我們最基本的防護必須定時更新掃毒引擎與病毒碼，時常進行掃毒以降低電腦被駭的風險。

參、相關法規

- 一、該單位資訊設備管理使用作業要點第 17 點：「個人電腦由同仁專屬使用，非經同意不得任意開啟使用，亦不得供本局以外人員使用。」
- 二、刑法第 132 條：「公務員洩漏或交付關於中華民國國防以外應秘密之文書、圖畫、消息或物品者，處三年以下有期徒刑。」

筆記型電腦資料安全管理

* 案例情境

美國交通部位於邁阿密總監察長辦公室的一台筆記型電腦，被歹徒破壞公務車門鎖後由車上偷走，該筆記型電腦中含有 13 萬筆佛羅里達州居民的個人資料。

這些個人資料包括姓名、住址、生日及社會安全號碼等，雖然這台筆記型電腦需要密碼才能登入，但那些個人資料皆未加密。該辦公室只能思考如何設法保障這些資料的安全。

* 防範措施：

由於筆記型電腦具有便於攜帶的特性，已成為現今行動辦公室最方便的工具，然而容易攜帶的便利特性，卻也致使歹徒可以輕易偷竊走電腦。所以近來國內外因筆記型電腦遺失或遭竊，造成機密資料外洩的案例屢見不鮮。

以下提供幾點保護筆記型電腦內資料的小撇步供參考：

1. 使用防護鎖或移動感應器來降低筆記型電腦失竊機率。
2. 電腦開機設定保護密碼。
3. 重要資料使用加密措施，防止未經授權存取。
4. 定時備份重要資料於其它儲存媒體中，並予以妥善保存。