

公務員廉政倫理規範宣導

案例：戒護人員、役男夾帶違禁物品入監不法案

(一)事實概述

99年8月間，○○監獄政風室受理匿名檢舉指稱「有役男夾帶茶葉予收容人」情事，初步調查發現役男陳○○有夾帶違禁品進入戒護區，透過合作社服務員轉交其他場舍服務員，再交付予特定收容人，並索討「走路工」等情，進一步策動並陪同陳男向臺灣雲林地方法院檢察署自首。

案經承辦檢察官深入查察及政風聯繫中心協助下，進行近2年蒐證，於101年6月查獲該監管理員黃○○，林○○、替代役役男蔡○○、陳○○、吳○○、鄭○○等4人，於98年至100年12月間，明知違反監獄行刑法等相關法規，多次私自夾帶香菸、茶葉、色情書刊等違禁物品進入該監戒護區交付、圖利收容人丁○○新臺幣（下同）3萬元、吳○○5萬2千元、楊○○9千元、賴○○5千2百元、陳○○5百元等情。

(二)違反規範條款

1、管理員部分

- (1)管理員黃○○涉犯貪污治罪條例第6條第1項第4款對於主管或監督之事務，明知違背法律及法律授權之法規命令，直接圖私人不法利益，案經雲林地方法院判處應執行有期徒刑2年，褫奪公權2年，緩刑5年，並應於判決確定之日起1年內，向公庫

支付新臺幣拾萬元。

- (2)管理員林○○擔任警備隊長職務，負責替代役役男生活管理工作，餘查無具體不法事證，檢察官處以不起訴處分。

2、替代役役男部分

役男蔡○○等 4 人以涉犯貪污治罪條例第 6 條第 1 項第 5 款對於非主管或監督事務，明知違背法律及法律授權之法規命令，直接圖私人不法利益，因而獲得利益之圖利罪嫌起訴。案經雲林地方法院判決定讞，吳○○判處有期徒刑 2 年，褫奪公權 2 年，緩刑 5 年，所得財物新臺幣參仟元沒收，鄭○○判處有期徒刑 2 年，褫奪公權 2 年，緩刑 2 年。

(三)懲處(戒)情形

○○監獄核予管理員黃○○記大過一次及林○○記過一次等處分；替代役役男陳○○記過二次、並處禁足 2 天及停止散步假 3 次等處分。

(四)案例分析

1、矯正機關弊端黑數

收容人或其家屬，為使收容人於矯正機關內獲得照顧、較佳的處遇，或與外界聯繫，甚或為炫耀成分，以請託關說疏通、飲宴餽贈、行賄等違規、違法手段利誘矯正人員，遂其目的。反之，矯正人員利用執行職務之機會，不守分際違法亂紀，與收容人及其親友過從甚密，謀取不當利益，破壞機關風紀。

2、服務員管理鬆散

本案管理員黃○○於擔任搬運隊、陶藝班主管竟夾帶違禁物品予服務員，接受服務員親友飲宴；替代役役男蔡○○等人為服務員傳遞訊息、夾帶違禁物品，更委託服務員傳遞違禁物品送至其他場舍予特定收容人，顯示服務員管理鬆散，內部控制尚有策進。

3、安全檢查未能落實

本案管理員及替代役男夾帶違禁物品進入戒護區長達2年，交付予服務員及傳遞予特定收容人使用，足見未能落實進出人員、物品之檢查；對於具有「交通」機能小單位（如：搬運隊、合作社等）服務員的檢查及抽查工作，尚有策進空間。部分場舍收容人持有、使用不明來源衣物、香菸、安眠藥、清潔用品等異常情狀，亦可藉由加強定期檢查、不定時抽查與擴大安全檢查等措施，機先發掘查辦，以杜絕違禁物品流入監內、防制貪瀆違法事件。

4、強化預防機制

落實戒護區淨化管理工作，強化服務員管理與內控查察作為，以防杜弊端並確保囚情安定，並加強矯正人員及替代役役男廉政教育訓練，達預防貪瀆違法之目標。

廉政宣導

詐領差旅費

(一) 行政院農業委員會水土保持局南投分局治理課技工 詐領差旅費案（臺灣南投地方法院 104 年度訴字第 41 號刑事判決參照）

- 1、偵審情形：第一審判決有罪。
- 2、弊端類型：利用職務上機會詐取差旅費。
- 3、弊端手法：
 - (1) 假借出差事由，從事非關公務之活動。
 - (2) 填載不實之出差旅費報告單及經費請領核銷清冊，詐領差旅費。
- 4、違反法條：貪污治罪條例第 5 條第 1 項第 2 款之罪。
- 5、案情概述：

甲擔任行政院農業委員會水土保持局(下稱水保局)南投分局技工，負責工程督導業務，為依法令服務於國家所屬機關而具有法定權限之公務員。

甲於 102 年 11 月至 103 年 2 月間，利用機關指派其辦理工程會勘及內部稽查等職務上機會，預先於電腦差勤系統填載出差事項並將員工差假單送請核准，其後或因實際上並未出差、或雖出差但先行離開，而利用差假等機會逕自處理私務。且詎其意圖為自己不法之所有，竟未據實修改電腦差勤員工差假單之出差申請，反登入電腦出差旅費報支系統，列印原申核之出差假單及與實際出差事實不符之出差旅費報告表，並製作各項經費請領核銷清冊後，逐層報由不知情單

位主管、主辦人事人員、主計人員審核，使渠等均陷於錯誤，誤認其有依原核准之出差假單實際至出差地點執行公務，並依報請之數額由主計室人員辦理核銷，致使水保局主計人員不疑有詐，陷於錯誤而如數核發，甲因而詐得出差旅費合計新臺幣（以下同）1萬982元。

案經臺灣南投地方法院檢察署檢察官簽分及法務部廉政署移送臺灣南投地方法院檢察署檢察官偵查起訴。

臺灣南投地方法院於104年7月20日判決甲違反貪污治罪條例第5條第1項第2款利用職務上機會詐取財物罪，依犯罪時間各判處有期徒刑1年9月至11月不等，定應執行有期徒刑2年，緩刑4年，並應向公庫支付5萬元，褫奪公權2年，所得財物發還水保局南投分局。

消費者保護宣導

消費警訊－購買中古車之消費資訊

消費者想買一部中古汽車，卻常常擔心會不會買貴了？會不會買到一輛不堪使用、要經常修理的問題中古車？因此，在購買中古車前，有那些管道及資訊可以協助消費者瞭解中古車的實際狀況？行政院消費者保護委員會（下稱行政院消保會）表示，消費者可以從「定型化契約」及「電子公路監理網」知道車輛的相關資訊：

一、「定型化契約」：

中古車買賣，出賣人負有提供車輛相關資訊之義務。行政院消保會為減少中古車買賣所衍生的消費糾紛，委員會通過「中古車買賣定型化契約範本(修正草案)」，暨其應記載及不得記載事項(草案)，要求出賣人在買賣契約中必須充分揭露：如車輛的廠牌、

年份、領照日、領牌日、引擎、配備、里程數、交易次數、車輛原使用情形，以及車輛是否為泡水車、是否發生重大事故、是否知悉車輛曾因交通事故致人於死、或車內曾發生自殺、他殺、或意外事故死亡等影響車況重大事項之相關資訊。

有關「中古汽車買賣定型化契約範本（修正草案）暨其應記載及不得記載事項（草案）」新聞稿可上該會網站查詢。

二、「電子公路監理網」：

購買中古車，除在簽訂契約時可要求出賣人依定型化契約範本提供車況資訊外，消費者也可以進入交通部公路總局「電子公路監理網」查詢相關資訊：

（一）車主可以在「電子公路監理網」以自然人憑證申請，即可免費查詢之資訊：

1. 如交通違規（件數）、燃料費繳納情形（欠費期數）、定期檢驗（下次定檢日期）、動保（動產擔保）申請進度等。
2. 另行政院消保會協調交通部自今年8月1日起新增因交通事故致車輛嚴重損壞之「事故車」項目。

（二）消費者也可以在「電子公路監理加值網」輸入車號或車主的身份證字號等，每次付費2元即可查得相關資訊：如汽車行車執照所列資訊（如廠牌、顏色、出廠年月、發照日期、換補照日期、定檢日期等）、牌照狀態、車種、動保次數及日期、吊扣日期、違規、欠稅費、發牌原因，及禁止異動次數。

行政院消保會提醒消費者，車況資訊將影響中古車的價值及行車安全，消費者可以上網瞭解車輛資訊，以為購車之參考，讓自己買到便宜又安全的代步車。

反毒宣導

免費毒趴 中學生被臉書勾癮

臉書竟成了揪團吸毒的新聯絡工具！恆春警方查獲一販毒集團，專門針對校園青少年販賣毒品，經同步在卅多處進行搜索、拘提，

共逮捕廿三名嫌犯，其中有八名國、高中生。家長趕到警局時痛哭失聲，有的小孩一付不在意的樣子，其中一名國三生，小五時就吸毒，讓員警訝異不已。

恆春警方是在去年九月監聽時，發現有毒販將毒品銷往校園，前天開始出擊抓人，兩天行動共逮捕主嫌黃家偉（廿五歲），及徐偉凱、潘秋震等廿三名毒蟲、毒販，其中有八名國高中生，這些學生有的是恆春在地生，有的則是在外地念書，寒假返鄉過年。還有一名在墾丁某夜店工作的變性人。

警方調查，黃嫌因染毒入不敷出，便利用涉世未深的青少年，先免費提供K他命或金錢，吸收成為下游，待成癮後便販毒牟利。黃嫌多利用學生聚會唱K TV時，建議他們可以買毒品吸食來HIGH一下，學生則利用臉書的留言板，呼朋引伴，學長姊拉學弟妹、同學拉同學，相招作伙來吸毒，從去年開始，共辦了四場毒趴。因為學生的經濟能力不充裕，只好大家集資，參加者每人繳交六百到一千元，租借民宿開「轟趴」，作為購買毒品的費用。

現今科技日新月異，網際網路發達，線上遊戲及網路臉書常為民眾之休閒娛樂活動，建請機關同仁及一般民眾多加留心家中年青學子使用網路之情況，俾利防範網路交友不慎，以促成大錯。

機關安全維護宣導

詐騙犯罪手法

（摘錄自內政部警政署刑事警察局及165反詐騙網站）

（一） 網路博弈下注遇詐騙，資金有去無回！

新北市李先生（30歲，工程師）在網路聊天室認識一名在香港工作的許姓女網友，兩人透過網路即時通聯繫相談甚歡，兩週後許女介紹他一個專營網路運動博弈的「鑫辰運動網（<http://www.sports699.com>）」，指稱該公司負責操盤者係其親戚，可暗中幫忙讓他們贏錢，慫恿他加入會員，一起進行外國球賽博弈的

投資下注。

李男依照許女指示上網申請帳號及登錄會員，之後接獲一名自稱該網站客服人員陳姓男子的來電，要求他繳納 40 萬元的會員開戶費，經與許女討論後，雙方議定各自分擔及匯款 20 萬元，以完成開戶手續。後來許女打電話給他，說要增額投資才能賺得比較快，遊說他加碼下注，由於李男手頭並不寬裕，最後僅匯款增額 10 萬元。歹徒透過網站偽造賽事結果，對李男謊稱下注賭球贏得 2000 多萬元，並以稅金及擔保金等名義，要求李男匯款 30 萬 6000 元以結算領取獎金。李男向銀行辦理小額貸款後，聽信操作陸續分匯 3 筆金額至對方指定帳戶。嗣後詐騙集團又以繳交臺灣所得稅要扣 2% 稅金為由，欲再次進行詐騙，李男察覺對方有意找藉口推延，心生懷疑撥打 165 專線查詢，才驚覺被騙。

類似詐騙被害案件已有 2 件，均先以假交友取得信任後，再輔以假投資（鑫辰運動網博弈）誘使被害人受騙，刑事局提醒民眾應提高警覺。另歹徒經常利用網路無遠弗屆且難以查證的特性，在網路聊天室物色詐騙被害對象，一旦有人上勾，即哭窮裝可憐借錢、佯稱遭黑道控制賣淫須贖身、利誘參與高報酬投資或邀約進行投機取巧中獎操作，以遂行詐騙。警方呼籲，網路交友危險多，攀談中遇網友請求金援或邀約金錢交易，務必查證對方身分真偽及其說詞或撥打 165 專線諮詢，以免被騙。

（二） 網路賣家請注意！奈及利亞跨國假扮買家詐騙

玩遊戲玩到一半，突然跳出通知中獎訊息？請小心是詐騙陷阱。1 月剛結束就有 2 位網路賣家出面報案，表示自己遇到了國外買家以「買兒子的生日禮物」為由，要求被害人將商品寄到奈及利亞，並且偽造銀行通知以提高可信度。

台中林同學（78 年次）於網路上拍賣價值新臺幣 1 萬 2,000 元

的平板電腦，一位自稱 Mrs. Lorna 的買家用英文在賣場上表示有購買意願，並留下電子郵件和即時通帳號希望進一步聯繫。林同學透過即時通瞭解對方人在韓國，想購買拍賣商品作為兒子的生日禮物，但兒子人在奈及利亞，因次必須代為寄送商品到奈及利亞，並且務必包裝精美，而買家願意支付運送費用。Lorna 還告訴林同學於隔日起床後即可檢查郵件信箱裡的銀行匯款通知，再請林同學儘速寄出商品，並且將寄送單據影本回傳至銀行的電子郵件信箱。林同學隔日的確收到來自 Woori Bank 的郵件通知，於是林同學即依照指示處理，但對方銀行和買家卻於數日後又同時表示，由於有匯款金額下限，請林同學透過西聯匯款美金 500 元給買家，銀行始能放款。林同學至此發現有異，上網查詢後始知遭到詐騙。

根據統計 100 年 5 月起至 101 年 1 月為止，共有 7 位被害人遭遇類似詐騙手法，並出面完成報案程序，損失金額從 6,000 元至 3 萬元不等，寄送地址均為奈及利亞境內，下訂商品則以 3C 產品及高級手錶為主，除騙取商品外，歹徒另會以外匯金額限制為由，要求被害人補足差額。警方呼籲網路賣家應注意上述特徵，以免掉入陷阱，而奈及利亞詐騙盛行，手法五花八門，請網路族群多加利用 165 反詐騙網站吸收新知，以加強自身保護知能。遇任何與詐騙相關問題，歡迎撥打 165 反詐騙諮詢專線查證。

公務機密維護宣導

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。

您的密碼夠不夠安全？

在資訊發達的今日，人們的日常生活跟資訊的關係也越來越密切，我們每天所要使用的密碼也越來越多，多到我們可能都記不住。以前可能只要用簡單的幾個數字就可以應付，但因密碼被破解的案例越來越多，很多系統已要求使用者採用複雜度高的密碼，以確保安全。

但是，即使系統要求如此嚴謹，仍然常發生密碼被破解的危安事件。報載：閩南語天后江蕙的 gmail 信箱不止一次遭到不明人士企圖登入，顯見駭客的非法入侵行為，至今仍是常常發生。

小潘看到這則新聞，直覺密碼不是都由自己設定的嗎？怎麼會被人家知道？這個疑問放在心裡多日，趁著與司馬特老師下午茶的機會提出。司馬特老師表示：一般人以為系統設定密碼就萬無一失，實際上這是太樂觀的想法；Intel 公司做過實驗，一組由數字及字母組成的 6 字元密碼，在短短的 1.18 分鐘就可以被破解。

小潘聽完立即問道：如果把密碼設長一點，是不是比較安全？司

馬特老師接著回應：美國科技網站 Ars Technica 曾經做過實驗，發現就算密碼以加密的雜湊形式呈現，駭客利用暴力攻擊法，仍可在 1 小時內破解超過 1 萬筆的密碼。那麼要怎麼樣才能設出一組較為安全的密碼呢？Microsoft 建議使用者，在建立密碼時，應該注意它的強度，也就是讓它不容易被猜到或是被破解，最好是電腦的所有使用者帳戶都使用強式密碼。強式密碼在設定時，要注意以下幾件事：密碼的長度至少要有 8 個字元，且不能包含使用者名稱、真實姓名或公司名稱，也不能包含完整的單字，與先前用過的密碼也要完全不同。除了強式密碼外，Microsoft 也建議可以用強式複雜密碼，它除了跟前述強式密碼一樣的條件外，密碼的長度要在 20 到 30 個字元之間，而且最好不包含文學或音樂作品中的常見詞句，以及字典中的詞句。

小潘聽完司馬特老師的說明，隨即想到曾在網路看到單因素認證及雙因素認證，一直弄不懂是什麼意思，便把這個問題也順便提出。

司馬特老師接著說明，大部分的入口網站採用單因素認證，當使用者需要取得資源或登入系統時，網站會提示用戶輸入帳號和密碼。系統採用加密方式，將帳號和密碼傳送到伺服器端進行比對，其中帳號用來辨識使用者的身分，密碼就是所謂的單因素認證；如電子郵件、線上遊戲等系統的登入機制都屬於這種單因素認證。雙因素認證則是結合使用者所知道的「內容」與所擁有的「物品」兩種因素，作為身分識別之用，當使用者通過此兩種因素認證時，就能登入應用程式或網站；其中使用者所知道的「內容」，包括密碼和身分證號碼等，而所擁有的「物品」則是指動態密碼卡、IC 卡、磁卡等。日常生活中最常見的雙因素認證，即是銀行或郵局的自動提款機，使用者到提款機前，必須先插入提款卡，此即為使用者所擁有的物品，再輸入個人所設定的密碼，此即使用者所知道的內容，兩項認證都要同時通過，才能存取帳戶的款項。

隨著網路的發達，個資外洩所造成的盜刷事件也層出不窮，但是

民眾透過網路銀行、行動銀行進行繳費、轉帳的頻率也越來越多，而且已成為習慣，為了避免個人資料因為使用網路服務而外洩，於是銀行業者推出網路銀行簡訊動態密碼確認機制，作為線上交易時的安全機制。簡訊動態密碼的服務，是當客戶透過網路銀行或行動銀行進行特定交易時，系統就會自動發送一封內含6位數交易驗證碼的簡訊到客戶所登記的手機號碼中，客戶必須在交易過程中，輸入該組6位數交易驗證碼，才能完成交易驗證。這樣的防護機制是為了確保該筆交易是由客戶本人進行而非遭他人盜用，以確保客戶的交易安全性。

小潘聽了司馬特老師的一番說明，對於密碼的安全有了進一步的認識。最後，司馬特老師還是語重心長地做了結論：由於資訊科技的進步，各種維護資訊安全的技術不斷被研發出來，但是維護密碼的安全至少要做到兩點：不同的網路系統要有不同複雜度的密碼、不要在所有系統上使用同一組密碼。

從日常網路使用行為談資通安全

社交工程是近年常見的駭客攻擊手法，人性因素是資安防護中最弱也是最難控制的一環。

電子郵件測試就是利用人性的弱點，發送一些能吸引人點閱的郵件標題，讓人因好奇心而點開電子郵件或附件，隱藏在裡面的惡意程式就會自動安裝在電腦裡，造成電腦裡的個人資料被竊取，或是鍵盤被側錄導致輸入的帳戶資訊外洩，這種利用人性弱點的手法稱為是「社交工程」。社交工程是近幾年來常見的駭客攻擊手法，因為人性的因素是資安防護中最弱也最難控制的一環，資訊系統的防護可以藉由安裝防毒軟體、架設防火牆等來防堵外界的入侵，但是人性的防火牆不管再堅固都有可能因為一時的不查而受騙，所以社交工程可說是利用人性的好奇心或是容易受騙上當來破解人性的防火牆。

常聽到跟社交工程有關的還有像是收到朋友的信，主旨可能是「我的出遊照」、「我的小孩照片」等，點選進去後是「.zip」的檔案，解壓縮後可能的附檔名為「.exe、.com、.bat、.scr、.pif、.lnk」的檔案，這些都是常見的惡意程式執行檔；此外像是直接隱藏在圖片中的惡意程式，當收到這些含有惡意程式的圖片，不需解除壓縮，只要誤點圖片就會感染病毒，造成重大的損失。

其實日常生活中，我們常會收到朋友傳送的檔案或是 email 郵件，但由於傳送或寄件者是認識的人，大家往往都會直接點選開啟，為了確保安全，我們應先確認傳送者是否為朋友本人，及傳送的內容是否含有惡意程式，才能避免不必要的損失。