香 港 童 軍 總 會
政策通告
電話：2957 6433　傳真：2302 1001　電郵：it@scout.org.hk

2023 年 10 月 1 日
第 02/2023 號通告
[政策]

資訊科技保安

本通告取代 2019 年 12 月 15 日發出之政策通告第 03/2019 號。

2. 香港童軍總會（下稱「本會」）非常重視資訊科技保安及個人資料私隱保障，各童軍單位及成員在使用資訊系統、電腦及行動裝置時，均有責任保障本會電子資料的安全，以防止任何遺失、外洩和誤用的情況。

3. 本通告列出本會對資訊科技保安的原則及基本要求，各童軍單位及成員在處理本會電子資料時，必須注意和貫徹遵守，以確保有關資料得到適當的管理及在安全的情況下使用。

資訊科技保安核心原則

4. 在處理、傳送和儲存童軍單位或與其相關的電子資料時，須按以下原則確保資料的機密性、完整性和可用性：

- 機密性：按「需要知道」原則設定用戶及使用者的存取權限，確保有關資料只可在獲授權的情況下存取。
- 完整性：確保資料的準確性、一致性及可靠性，以免未經授權下受到更改。
- 可用性：確保資訊系統、電腦及行動裝置能夠全面及正常運作，讓獲授權人士可即時可靠地取用所需的資料。

個人資料私隱

5. 在本會活動和日常運作中處理電子個人資料時，須遵守本會個人資料私隱政策。詳情請參照政策通告第 11/2018 號《香港童軍總會個人資料私隱政策聲明》。

電子資料保安級別

6. 本會電子資料分類為以下四個資訊保安級別，以便採取相應的資訊科技保安措施：

保安級別	分類原則	例子
公開	適用於可開放給公眾查閱的資料。披露此類資料不會對本會／童軍單位造成任何風險。	童軍的一般資訊；本會網站公開的政策、指引、通告和統計資料
內部	適用於本會特定成員內部參閱的資料，以及與合作夥伴分享的非敏感運作資料。披露此類資料可能會產生一般程度的不良影響，但不會對本會／童軍單位造成嚴重損害。	訓練資訊、成員手冊、內部政策及運作程序
限閱	適用於特定授權人員才可存取的敏感資料。未經授權披露、修改或銷毀此類資料可能會給成員帶來不便，對本會／童軍單位的運作產生不良影響，以至一定程度的經濟損失或本會／童軍單位聲譽的損害。	成員的個人資料及童軍記錄（如：出生日期／電話號碼／地址／訓練記錄）；招標文件及記錄

保安級別	分類原則	例子
機密	適用於性質非常敏感且受嚴格限制的資料。這類資料對本會／童軍單位的運作極為重要，遺失、損壞或未經授權的披露可能會對本會／童軍單位的聲譽和運作造成重大不利影響，並會給資料當事人（即屬相關個人資料的當事人本人）帶來不便、威脅或損失。	成員的敏感個人資料（如：香港出生證明書／香港身份證號碼）；本會／童軍單位的敏感管理資料

7. 本會各系統／資訊負責人有責任將轄下電子資料分類為適當的資訊保安級別，並以「需要知道」原則授予合適人士相應的存取權限。一般而言，如資訊屬「內部」、「限閱」或「機密」級別，系統／資訊負責人必須在有關資料的適當位置上清楚列明其資訊保安級別，以提示各使用者採取相應的資訊科技保安措施。

使用者責任

8. 童軍單位及成員不時使用電腦、資訊系統、互聯網、電郵、社交媒體、即時通訊軟件、雲端儲存等處理和分享他們的資料。他們必須透過以下各項確保身處的環境並無保安風險，並致力保護資料（包括但不限於個人資料）的安全及私隱性：

(a) 確保妥善的保安及私隱設定。
(b) 只按「需要知道」原則與可信任及獲授權的人士分享個人及／或敏感資料。
(c) 保持警惕，防範可疑／未經請求的電子訊息及欺詐。
(d) 透過如電話等其他方式驗證可疑／未經請求的電子訊息的發送者身分。
(e) 在做出任何回應或採取任何行動之前，確定電子訊息、附件、超連結或二維碼的真實性、可信度和安全性。
(f) 向負責的童軍單位或資訊科技支援團隊報告可疑活動和事件。
(g) 尋求專業協助處理重要資料遭受竊取或騙取的情況，以減低損失及妥善執行補救工作。

9. 使用者亦應時刻保持資訊科技保安習慣和警覺性，並留意最新的保安資訊，以履行責任。本通告附件列舉常用電子資訊系統「應做」及「不應做」的資訊科技保安要點，各童軍單位及成員均應細閱和遵守。

查詢及支援

10. 如欲進一步了解本通告的內容，請按下列電郵地址查詢：

地域／署及屬會	電郵地址
港島地域	it_enquiry@hkirscout.org.hk
九龍地域	kritadmin@krscout.org
東九龍地域	it@hkscout-ekr.org
新界地域	ntrscout.it@gmail.com
新界東地域	it.nterscout.official@gmail.com
署及屬會	it@scout.org.hk

11. 若遇資訊科技保安事故需要特別支援，亦可直接與總會資訊科技署聯絡（電話：2957 6433，電郵：it@scout.org.hk）。

助理香港總監（資訊科技及支援）
岑 偉 建

常用電子資訊系統「應做」及「不應做」的資訊保安要點

A. 使用電腦及行動裝置

應做	不應做
(i) 安裝和妥善設定防毒軟件，定期更新病毒定義檔案，安排定時進行自動掃描。	(i) 不應直接使用從其他人士獲取的檔案，需經防毒軟件掃描檢查後方可開啟使用。
(ii) 定時更新作業系統及程式，以堵塞保安漏洞。	(ii) 不可使用來歷不明或未獲正式授權的程式。
(iii) 使用個人防火牆以控制網絡通訊，減低被黑客入侵或攻擊的風險。	(iii) 不應以管理員帳戶進行日常工作，避免惡意軟件能以管理員權限自行安裝。
(iv) 個人帳戶應設定登入密碼或其他身分認證方式，以防止他人以你的個人帳戶使用有關設備。	(iv) 不應在無人看管時保持登入狀態。不論離開多久，在離開前，應啟動屏幕鎖、登出或關機。
(v) 如需在單位電腦處理敏感資料，單位應按需要設立個別成員個人帳戶以供使用。成員亦應在使用後把有關檔案徹底刪除（包括清理電腦內「資源回收筒」）。	(v) 不應使用公用電腦或單位電腦的公用帳戶處理敏感資料。
(vi) 如使用便攜式儲存裝置，應小心保管以避免遺失，並使用加密程式[1]及密碼保護資料，以確保只有獲授權人士才可存取資料。	(vi) 不應在公眾地方隨便放置而沒有妥善看管任何行動裝置，以防他人輕易盜取。
(vii) 定期進行備份，尤其是在重大系統或軟件安裝／更新，或進行機件維修前亦應進行備份，以備遭受病毒／黑客攻擊或硬件失效時，可以利用備份進行復原，以減少資料損失。	(vii) 不應將未移除儲存裝置的電腦或行動裝置直接送往維修或棄置，以免被盜取當中資料。如需把儲存裝置送往維修或棄置，事前應採用安全及永久性的方法把所有儲存的資料徹底刪除[2]。

B. 管理資訊系統帳戶及密碼

應做	不應做
(i) 請使用最少由八個數字、字母及符號組成的複雜密碼，或按照網站提示的密碼複雜性來設定密碼。	(i) 不應以生日日期、用戶名稱、電話號碼、常用字等設定密碼。
(ii) 如系統許可，應使用雙重認證（two-factor authentication），加強保安。	(ii) 不應向別人透露個人帳戶和密碼，亦不應共用系統帳戶。
(iii) 應定期更改密碼，並妥善保存。	(iii) 不應在不同系統使用同一密碼。

[1] 加密程式包括 Windows 平台的 BitLocker、MAC 平台的 FileVault 等。

[2] 例如採取硬盤適用的 DBAN (www.dban.org)或檔案適用的 FileShredder (www.fileshredder.org)

C. 使用互聯網及設立網站／社交媒體帳戶

應做	不應做
(i) 當瀏覽含敏感資料的網站或登入任何處理童軍事務的系統（例如成員系統、電郵、社交網站等）時，應確保採用加密通訊保護（即網址前端為“https”）。 (ii) 設立單位網站時亦應採用加密通訊保護，令使用者瀏覽時更為安心。 (iii) 當網站要求用戶提供個人資料時應小心留意，以保障個人資料私隱。 (iv) 單位專用無線網絡（Wi-Fi）應設有密碼（例如 WPA2），以保護資料傳輸安全。如需開放無線網絡給非單位成員使用，應另設公用無線網絡及確保和單位專用無線網絡分隔。	(i) 不應保留過時單位／活動之網站／社交媒體帳戶。 (ii) 不應把網站管理員帳戶給予第三者。如需把有關資料給予服務供應商等人士處理網站問題，應在開始處理前及完成後更改密碼。 (iii) 不應在公用及行動裝置儲存任何敏感資料（例如網上帳戶登入資料及密碼）。 (iv) 不應造訪可疑網站或下載來歷不明的軟件及檔案。

D. 使用雲端儲存、電郵及即時通訊軟件[3]

應做	不應做
(i) 當使用雲端儲存保留及分享敏感資料，應只授權予特定使用者（例如以電郵地址授權），而非只需獲取連結便可檢視／編輯。 (ii) 使用電郵或即時通訊軟件發放訊息時（特別是涉及敏感資料），應採用「需要知道」原則。 (iii) 在活動完結後，應及早刪除在雲端儲存、電郵帳戶及即時通訊軟件內相關的活動的敏感資料（例如參加者的聯絡電話、電郵地址等）。	(i) 不應隨意以電郵或即時通訊軟件傳送敏感資料，如需傳送，應以檔案形式和加密處理[4]，並使用其他渠道通知收件者解密密碼。 (ii) 不應隨意回應可能包含惡意附件、超連結或二維碼的可疑／未經請求的電子訊息。如有懷疑，應先向發送者查核。 (iii) 不應在未獲個別人士的明確同意下，披露其電話號碼或電郵地址等個人資料[5]。

[3] 即時通訊軟件例子：WhatsApp / LINE / WeChat / Telegram / Facebook Messenger

[4] 例如採用 Microsoft Office 的密碼加密或 7-ZIP 的 AES256 密碼加密

[5] 採用電郵內的 bcc 傳送、WhatsApp 的訊息廣播功能等可避免不必要的個人資料披露。