

保障個人資料私隱 使用社交媒體及 即時通訊软件的指引



“ 社交媒體及即時通訊軟件在香港已獲廣泛使用。然而，使用社交媒體及即時通訊軟件會為用戶的個人資料私隱帶來不容忽視的風險。香港個人資料私隱專員公署的《使用社交媒體及即時通訊软件的指引》旨在指出這些風險，並提供減低風險的實用建議。 ”

社交媒體、即時通訊軟件及其服務

社交媒體及即時通訊軟件涵蓋多種網上平台和服務，這些平台和服務的設立目的是供大家互相溝通，以及製作和分享內容。本指引統稱兩者為「社交媒體」。

雖然大部份社交媒體平台都不收取任何費用，但不等於有關服務是「免費」，皆因用戶資料一般都會被收集和分享。用戶在平台進行活動（例如閱讀帖文或對帖文按讚）或使用其服務（例如發送和接收訊息）時，這些資料通常都會被收集作個性分析之用。這類用戶活動所產生的大量資料經採集後（有時甚至在用戶不知情下被採集），會被社交媒體平台用於廣告活動或再分享而從中圖利。

與使用社交媒體及即時通訊軟件 相關的個人資料私隱風險

● 私隱受損

- 若用戶在社交媒體過度分享資訊，便會在不知不覺間透露比預期中更多的個人資料。
- 幾乎所有在社交媒體分享的事情都會留下永久的數碼足跡，並且難以從網絡世界中移除。
- 發送至個別用戶的即時訊息，即使已被加密，仍可由接收者轉發或廣泛地分享予身份不明的第三者。

● 個人資料被濫用

- 使用「社交媒體帳號登入」功能 (Social log-in) (即利用社交媒體帳號登入第三方的流動應用程式或網頁) 或會令社交媒體可進行跨平台追蹤用戶的活動。
- 公開予大眾的資料, 可被第三方透過「數據擷取」(data scraping) 的自動化程序收集及整合。
- 過度披露的個人資料或會被濫用於身份盜用、網絡欺凌或「起底」行為。

● 虛假帳戶及身份

- 騙徒或會透過虛假的網上身份誘騙用戶提供個人資料或親密照片以用作詐騙、其他犯罪活動或不當行為。

給社交媒體及即時通訊軟件用戶的實用建議

以下的建議有助社交媒體用戶減低因使用社交媒體而引起的個人資料私隱風險。由於不同的社交媒體平台各有不同的設計和功能, 以下僅列出部份建議, 但並非所有建議都適用於全部社交媒體平台之上。

問題 1: 在註冊新的社交媒體帳戶時有甚麼需要注意?

- 答**
- 每個社交媒體平台都有各自的私隱政策及常規。閱讀私隱政策以了解社交媒體平台如何處理及分享用戶的個人資料。此舉有助用戶了解有關社交媒體平台是否符合自身要求, 並作出明智的決定。
 - 例如, 應確認社交媒體平台會否將用戶的個人資料分享予第三方、所分享的資料種類和分享的目的。
 - 使用即時通訊軟件前, 檢查軟件有否提供端對端加密, 以及在使用前檢查是否已開啟有關功能。
 - 減少在登記使用時所提供的個人資料。如非必要, 切勿提供敏感個人資料。例如, 不應隨便提供詳細地址和完整的出生日期。
 - 如須提供電郵地址, 應開設一個社交媒體帳戶專用的電郵帳戶。
 - 設定高強度、獨特的密碼, 以保障帳戶。如社交媒體平台有提供多重身份認證, 應採用有關功能。多重身份認證是指社交媒體平台在用戶登入帳戶時, 透過另一途徑 (例如用戶的流動電話) 發送確認訊息或認證碼。

問題 2：用戶應如何管理私隱設定？

- 答** • 檢視帳戶的預設私隱設定並作出適當的調整。例如，用戶應限制以下資訊的公開程度：
- (1) 個人經歷，例如學歷和工作履歷；
 - (2) 個人聯繫，例如家庭成員和朋友；
 - (3) 聯絡資料，例如電話號碼、電郵地址和住址；及
 - (4) 社交媒體平台的帖文。
- 在即時通訊軟件上，用戶的個人頭像和狀態應設定為只向通訊錄上的聯絡人公開，而非向所有用戶公開。
 - 在剛開立社交媒體帳戶時應採用最「私隱友善」的設定，然後在用戶認為合適時才逐步放寬。
 - 在私隱設定中，選擇被其他用戶在其相片或帖文作出標註時，先發出提示。
 - 在給予以下權限前，用戶應三思：
 - (1) 容許社交媒體平台利用臉容識別技術從相片中識別；
 - (2) 容許社交媒體平台利用電子裝置的定位功能，作實體追蹤，或公開用戶的位置訊息；
 - (3) 容許社交媒體平台追蹤自己在其他應用程式及網站的活動；
 - (4) 容許其他用戶在其相片或帖文中「標註」或「提及」自己；
 - (5) 容許其他用戶利用自己的電郵地址或電話號碼作出搜索；及
 - (6) 容許第三方應用程式查閱自己的社交媒體個人檔案。
 - 定期檢視私隱設定，以確保有關私隱設定不會因社交媒體平台的軟件更新而遭修改。
 - 如欲了解如何更改私隱設定，請參閱本文末的「更改私隱設定指南」。

問題 3：當私隱政策有所更改時應如何處理？

- 答** • 認真審視新的私隱政策，並在同意有關更改前評估所涉及的個人資料私隱風險。切勿在未清楚了解新的私隱政策下點選「同意」。
- 檢查有關更改是否涉及所收集的個人資料的種類、收集的目的以及與第三方分享方面的改動。
 - 對一些使用「黑暗模式」設計的社交媒體平台時刻保持警惕，以免被誘導而分享了比預期多的資料。這類「黑暗模式」通常包括利用彈窗訊息、視覺效果、不顯眼的另類選擇或使用令人混淆的語言等等。

問題 4：用戶在社交媒體張貼或發送資訊時應留意甚麼？

- 答** · 在社交媒體分享或發送任何資訊前應三思。在按下滑鼠按鈕的一刻，資料即成為永久的數碼足跡。
- 避免透過即時通訊軟件發送敏感資料，皆因即使訊息只發送至個別用戶，仍可以被轉發或廣泛地分享至身份不明的第三者。
 - 考慮所分享的資訊的公開程度（例如只限朋友還是向所有用戶公開）。
 - 分享位置資料時要謹慎，尤其是住址、工作地點及顯示慣常出行路線的資訊。
 - 如無需使用電子裝置內的定位功能時，應考慮關閉有關功能，以減少社交媒體平台及其他應用程式收集位置資料。
 - 在自己的相片標註其他人或在社交媒體平台分享他人的個人資料時應謹慎。標註他人或會使社交媒體平台於日後能識別他們的臉容，平台亦可能將他們的臉容影像加入其生物辨識資料庫。
 - 良好和尊重別人的做法，是在未肯定當事人是否同意前不要分享人家的個人資料。

問題 5：用戶在社交媒體平台玩遊戲時應注意甚麼？

- 答** · 在社交媒體平台安裝來自第三方的應用程式（例如遊戲或性格測驗）時應時刻保持警惕。
- 檢查第三方應用程式欲查閱及收集哪些資料，以及有關查閱及收集是否有需要。
 - 定期檢視已安裝的第三方應用程式，以及移除不再需要的應用程式。以上事項一般可透過社交媒體平台的「私隱設定」處理。

問題 6：用戶應如何保障自己的個人資料安全和防範網上騙案？

- 答** · 避免與現實生活中不認識的人連繫。其他用戶在社交媒體的名字或描述可以是虛構的。
- 提防有人透過主動提供好處和獎品、以慈善活動為名，發送超連結等形式，要求「登入」或提供個人資料，這些很可能是網上騙案。
 - 切勿向任何不認識的人發送個人資料，或點擊可疑連結。

- 避免使用「社交媒體帳號登入」功能（即以社交媒體帳戶登入第三方應用程式或網站）。用戶可以透過社交媒體平台的「私隱設定」中斷已連結至自己社交媒體帳戶的第三方應用程式及網站（即終止「社交登入」）。
- 如用戶使用非個人電子裝置（例如咖啡店的共用電子裝置）登入社交媒體帳戶，切勿允許瀏覽器記住密碼，並緊記在使用後登出。
- 如社交媒體平台發出警示，表示有人嘗試登入帳戶但未能成功，或透過陌生的電子裝置登入帳戶，用戶應檢查帳戶狀況或更改密碼。
- 如用戶使用手機應用程式登入社交媒體，應及時更新有關應用程式至最新版本，以保障資料安全。

問題 7：當出現問題時應如何處理？

- 答**
- 如用戶在不情願下被標註於社交媒體的相片或帖文中，可透過社交媒體平台提供的方法移除標註。例如，在帖文的快顯功能表中通常有一選項，用來「取消標註」或「移除」標註。如情況許可，可要求分享相片或資訊的用戶刪除有關帖文。
 - 如用戶發現有自己的私人、敏感或不當的資訊在未取得同意下分享到社交媒體上，可以要求該社交媒體平台移除有關資訊。在帖文的快顯功能表中通常有一選項，讓用戶向社交媒體平台「報告」不當內容。
 - 如用戶在使用即時通訊軟件時不慎發送訊息至錯誤的用戶，應立即向「所有接收者」「撤回」或「刪除」有關訊息。
 - 如有需要可封鎖某些社交媒體用戶或解除與某些用戶的「朋友關係」。視乎用戶所選用的社交媒體平台，有關功能可在「私隱設定」或有關用戶的個人檔案頁面中找到。
 - 如遇到敲詐勒索或人身安全受到威脅，應記錄相關的勒索或威脅的證據（例如擷取有關訊息的螢幕截圖），並向執法機構報案。
 - 如用戶發現使用的社交媒體平台發生資料外洩事故，即使不肯定有關事故是否影響帳戶，應該立即更改密碼。
 - 如用戶察覺個人資料被惡意公開，可致電香港個人資料私隱專員公署專為「起底」行為而設的查詢和投訴熱線（電話：+ 852 3423 6666）。

問題 8：怎樣才可減少留下數碼足跡？

- 答** · 定期檢視過往的社交媒體帖文，找出並刪除不再想分享的資料。
- 終止不再使用的社交媒體帳戶。有關功能一般可以依從「私隱設定」中的「終止」、「刪除」或「停用」帳戶的步驟做到。只刪除存放在社交媒體平台的資料，並不能夠提供足夠的保障。
 - 在終止社交媒體帳戶前，用戶可要求下載自己的資料複本（例如相片、訊息及帖文）以作個人記錄。

問題 9：用戶應如何協助子女安全地使用社交媒體？

- 答** · 分享兒童的相片及資訊時要非常謹慎。兒童通常不了解披露個人資料所帶來的風險或不能識別網上騙案。
- 為子女開設帳戶時，可行的話，應考慮開啟「家長管控」(parental control) 功能，並讓子女知道「家長管控」功能經已啟動。一般而言，「家長管控」包括封鎖某些網站內容、限制更改私隱設定，以及禁止在應用程式進行購物等功能。此舉能減少子女可能面對的風險。
 - 為子女就使用社交媒體給予指導，例如：
 - (1) 教導子女有關使用社交媒體的風險，包括留下的永久數碼足跡的風險；
 - (2) 檢查子女的社交媒體帳戶的私隱設定；
 - (3) 提醒子女不應隨便在社交媒體上披露個人資料，例如全名、地址、電話號碼或學校名稱；及
 - (4) 教導子女尊重他人的私隱和不應隨便在社交媒體上分享他人的個人資料，例如相片和地址。

更改私隱設定指南

下面就如何在手機操作系統或手機應用程式內更改私隱設定提供指南。

請留意，手機操作系統（例如 Android 和蘋果 iOS）及個別流動應用程式均會不時更新。因此，更改私隱設定的確切步驟以及可供選擇的私隱設定亦有機會隨之而改變。

Android

以下設定步驟參照 Android 11 版本。

1. 位置

- 第一步：在手機上開啟「設定」
- 第二步：選擇「私隱」
- 第三步：選擇「權限管理員」
- 第四步：選擇「位置」後，會看到一列有權查閱用戶地理位置的應用程式
- 第五步：可點選當中的任何一個應用程式，並在系統提供的選項中，選擇是否以及何時容許該應用程式查閱用戶的地理位置

2. 通訊錄（電話簿）

第一步：在手機上開啟「設定」

第二步：選擇「私隱」

第三步：選擇「權限管理員」

第四步：選擇「通訊錄」後，會看到一列有權查閱用戶通訊錄的應用程式

第五步：可點選當中任何一個應用程式，並在系統提供的選項中，選擇是否以及何時容許該應用程式查閱用戶的通訊錄

3. 儲存裝置

第一步：在手機上開啟「設定」

第二步：選擇「私隱」

第三步：選擇「權限管理員」

第四步：選擇「儲存裝置」後，會看到一列有權查閱儲存在用戶手機內的相片、媒體檔案及其他檔案的應用程式

第五步：可點選當中任何一個應用程式，並在系統提供的選項中，選擇是否容許該應用程式查閱用戶手機內的檔案（包括相片）

蘋果 iOS

以下設定步驟參照 iOS 14.4.1 版本。

1. 定位服務

第一步：在手機上開啟「設定」

第二步：選擇「私隱」

第三步：選擇「定位服務」後，會看到一列有權查閱用戶地理位置的應用程式

第四步：可點選當中任何一個應用程式，並在系統提供的選項中，選擇是否以及何時容許該應用程式查閱用戶的地理位置

2. 網絡追蹤

第一步：在手機上開啟「設定」

第二步：選擇「私隱」

第三步：選擇「追蹤」

第四步：可選擇是否允許手機上的應用程式向用戶索取權限，以追蹤在其他應用程式和網站中的活動

3. 通訊錄（電話簿）

第一步：在手機上開啟「設定」

第二步：選擇「私隱」

第三步：選擇「通訊錄」後，會看到一列有權查閱用戶通訊錄的應用程式

第四步：可選擇是否容許那些應用程式查閱用戶的通訊錄

4. 相片

第一步：在手機上開啟「設定」

第二步：選擇「私隱」

第三步：選擇「相片」後，會看到一列有權查閱用戶相片的應用程式

第四步：可點選當中任何一個應用程式，並在系統提供的選項中，選擇是否容許該應用程式查閱用戶全部或部分相片

於應用程式內更改私隱設定

部份私隱設定是相關社交媒體平台特有的。這些設定只能於社交媒體平台上更改。以下重點介紹一些適用於 Facebook、Instagram 和 Twitter 並且有較大私隱影響的設定。

設定	Facebook	Instagram	Twitter
更改個人檔案（例如學歷、聯絡資料）的公開程度	<ol style="list-style-type: none"> 1 前往「設定和私隱」 2 選擇「設定」 3 選擇「私隱設定」 4 選擇「管理個人檔案」以作出更改 	<ol style="list-style-type: none"> 1 前往「設定」 2 選擇「私隱設定」 3 選擇「不公開帳戶」以作出更改 	<ol style="list-style-type: none"> 1 前往「設定和隱私」 2 選擇「隱私和安全」 3 選擇「保護你的推文」以作出更改
更改應用程式利用臉容識別技術從相片中識別用戶的權限	<ol style="list-style-type: none"> 1 前往「設定和私隱」 2 選擇「設定」 3 選擇「臉部辨識」以作出更改 	不適用	不適用
更改應用程式在其他應用程式及網站追蹤用戶的活動權限	<ol style="list-style-type: none"> 1 前往「設定和私隱」 2 選擇「設定」 3 選擇「Facebook 站外動態」以作出更改 	不適用	<ol style="list-style-type: none"> 1 前往「設定和隱私」 2 選擇「隱私和安全」 3 選擇「個人化與資料」以作出更改
更改其他用戶在其相片中作出「標註」的權限	<ol style="list-style-type: none"> 1 前往「設定和私隱」 2 選擇「設定」 3 選擇「個人檔案和標籤」以作出更改 	<ol style="list-style-type: none"> 1 前往「設定」 2 選擇「私隱設定」 3 選擇「標籤」以作出更改 	<ol style="list-style-type: none"> 1 前往「設定和隱私」 2 選擇「隱私和安全」 3 選擇「相片標記」以作出更改

如欲了解更多有關個人資料私隱的資料，可聯絡香港個人資料私隱專員公署。

熱線電話：+852 2827 2827

傳真：+852 2877 7026

地址：香港灣仔皇后大道東 248 號大新金融中心 13 樓 1303 室

電郵：communications@pcpd.org.hk

網址：www.pcpd.org.hk



掃二維碼
下載本指引電子版