PCPD
HK
PCPD.org.hk

Guidance Note

香港個人資料私隱專員公署
Office of the Privacy Commissioner
for Personal Data, Hong Kong

Guidance on Protecting Personal Data Privacy in the Use of Social Media and Instant Messaging Apps

About this Guidance

Social media and instant messaging apps are widely used by people in Hong Kong. However, the use of social media and instant messaging apps carries inherent yet non-negligible risks to users' privacy in relation to personal data. This Guidance aims to highlight those risks and provide practical advice that will help to mitigate the risks.

Social Media, Instant Messaging Apps and Their Services

Social media and instant messaging apps encompass a variety of online platforms and services set up for a large number of people to communicate as well as create and share contents. They are collectively referred to as "social media" in this Guidance.

Even though most social media platforms do not charge any fee, the services are not entirely "free" in that users' data are generally collected and shared. Users' participation in the platforms (such as viewing and liking posts) and use of the services (such as sending and receiving messages) are often profiled. Such user activities generate a massive amount of data which is then harvested – sometimes without the users' knowledge – and monetised via advertising or further sharing.

Risks to Personal Data Privacy Relating to the Use of Social Media and Instant Messaging Apps

- **Loss of privacy**
  - Users who over-share information on social media could unwittingly reveal more personal data than they anticipate.
  - Almost everything shared on social media leaves a perpetual digital footprint that is difficult to eradicate from the online world.
  - Instant messages sent privately to a single recipient, even if encrypted, can be forwarded or shared widely by the recipient with unknown third parties.

- **Misuse of personal data**
  - The use of "social log-in" (using a social media account to sign into third-party apps or websites) may enable cross-platform tracking by the social media platform.
  - Publicly visible information can be collected and aggregated by third parties using an automated process known as "data scraping".
  - Excessive sharing of personal data may provide the materials for identity thefts, cyberbullying or doxxing.
- **Fake accounts and identities**
  - Fake online identities may seek to induce users to disclose personal data or intimate photos in order to perpetrate frauds, other crimes or misconducts.

Practical Advice to Users of Social Media and Instant Messaging Apps

We outline below some advice to assist you, as a user of social media, in minimising the risks to personal data privacy arising from the use of social media. Given the variety in the designs and functions of different social media platforms, this is not an exhaustive list of advice, and not all recommendations are applicable to all social media platforms.

Q1: What should I watch out when signing up for a new social media account?

A:

- Privacy policies and practices vary among different social media platforms. Read the privacy policy to understand the manner in which the social media platform handles and shares your personal data. This would enable you to make an informed decision as to whether the particular social media platform meets your requirements.
- For example, you should ascertain whether the social media platform will share users' personal data with third parties, what kinds of data will be shared, and for what purposes.
- For instant messaging apps, check whether an end-to-end encryption function is provided by the apps, and check that the function is switched on before use.
- Limit the amount of personal data to be handed over for registration. Sensitive personal data should not be submitted unless it is necessary. For example, full address and full date of birth should not be handed over casually.
- If an email address is required, set up a dedicated email account solely for the use of the social media account.

- Set a unique and strong password to secure your account. Use multi-factor authentication if it is available. Multi-factor authentication may involve the sending of a verification message or code by the social media platform to you via a separate channel, such as your mobile phone, upon log-in.

Q2: How do I handle privacy settings?

A:

- Examine the default privacy settings and amend them as appropriate. For example, you should limit the extent to which the following information is publicly visible:

  (a) your personal history, such as education and employment histories;
  (b) your personal connections, such as family members and friends;
  (c) your contact details, such as telephone number, email address and residential address; and
  (d) your posts on the social media platform.

- For instant messaging apps, restrict your profile photo and status to be visible only to people who are on your contact list, and not to everyone.

- Adopt the most privacy-friendly settings when you first create your social media account, and relax them gradually as and when you feel comfortable to do so.

- Select the privacy setting that enables you to be alerted when you are tagged by other users in their photos or posts.

- Think twice before granting the following permissions:

  (a) permission to the social media platform for using facial recognition to recognise you in photos;
  (b) permission to the social media platform for using the location function of your device to track you physically, or to make your location publicly visible;
  (c) permission to the social media platform to track your activities across different apps and websites;
  (d) permission to other users to "tag" or "mention" you in their photos or posts;
  (e) permission to other users to look you up by using your email address or telephone number; and
  (f) permission for third-party apps to access your social media profile.

- Regularly review the privacy settings to ensure that software updates by the social media platform have not altered them.

For **Step-by-Step Guide on Adjusting Privacy Settings,**
please refer to Annex (P. 8-11).

Q3: What should I do when there is a change in privacy policy?

A:

- Examine the new privacy policy carefully and assess the personal data privacy risks before you agree to the change. Do not click "agree" without a clear understanding of the new privacy policy.
- Check whether the change involves any changes in the types of personal data which would be collected, the purpose(s) of collection and the sharing of data with third parties.
- Be vigilant about the design features of some platforms which may seek to nudge you into sharing more data than you wish. Sometimes referred to as "dark patterns", these design features may include the use of pop-up messages, visual effects, inconspicuous alternatives or confusing language, etc.

Q4: What should I watch out when posting or sending information on social media?

A:

- Think twice before you share or send any information on social media – with a click, data becomes perpetual digital footprint.
- Avoid sending sensitive information on instant messaging apps because messages sent to even a single person can be forwarded or shared widely with unknown third parties.
- Consider how widely your information is being shared, e.g. *friends only* or *everyone*.
- Be cautious about sharing your location data, especially your home address, workplace and information that reveals your habitual routes of travel.
- Consider switching off the location function of your device when it is not needed, to minimise the collection of your location data by the social media platform and other apps.
- Be cautious about tagging other people in your photos or sharing their personal data on social media platforms. By tagging them, the social media platforms may recognise their faces in future, and may enroll their facial images in a biometric database.
- As a good practice and as a matter of respect, do not share other people's personal data unless you are confident that you have their permission.

Q5: What should I watch out when playing games on social media?

A:

- Always be cautious about installing third party apps on social media platforms, such as games or personality tests.
- Check how much of your data the third-party apps wish to access and collect, and whether the access and collection are necessary.
- Regularly review the third-party apps that you have installed, and remove those that are no longer needed. This can usually be done under "privacy settings" of the social media platforms.

Q6: How do I safeguard the security of my personal data and guard against online scams?

A:

- Refrain from connecting with people whom you do not know in real life. The names or descriptions of other social media users may be fictitious.
- Beware of online scams that come in the form of unsolicited benefits, prizes, charities or hyperlinks that request you to "log-in" or provide personal data.
- Do not send personal data to anyone whom you do not know, or click on suspicious links.
- Refrain from using "social log-in", i.e. signing into third-party apps or websites by using a social media account. You may disconnect third-party apps and websites already connected to your social media account (i.e. terminate "social log-in") under "privacy settings" of the social media platforms.
- If you use non-personal devices, such as a device in a cafe, to access social media, do not allow the browser to remember your password. Remember to log out after use.
- Check the status of your account or change your password if your social media platform alerts you about a failed attempt to log into your account, or about a log-in conducted on a new device unknown to you.
- If you use mobile apps to access social media, update the apps to the latest version to maintain data security.

Q7: What should I do when things go wrong?

A:

- If you are tagged in photos or posts on social media against your will, follow the available options to get the tag removed. For example, there is usually an option to "untag" or "remove" yourself from social media posts in the quick menu of the posts. If possible, request the person who shared your photos or information to delete those posts.

- If you discover private, sensitive or inappropriate information about you is shared on social media without your consent, you can request the social media platform to take it down. There is usually an option to "report" improper contents to the social media platforms in the quick menu of the social media posts.

- If you have inadvertently sent a message on an instant messaging app, you may "unsend" or "delete" the message "for everyone" immediately.

- Block or "unfriend" other social media users if necessary. Depending on which social media platforms you are using, this may be done under "privacy settings" or on the profile page of the users whom you wish to block.

- If you encounter extortion for money or threats to personal safety, record evidence of the demand or threat (such as by taking a screenshot of the messages), and report to law enforcement agencies.

- If you discover that your social media platform has suffered a data breach, you should change your password immediately even if it is unclear whether the breach impacts your account.

- If you think that your personal data has been maliciously disclosed, you can report it to the Office of the Privacy Commissioner for Personal Data, Hong Kong, via a hotline (Tel: 3423 6666) dedicated to receiving enquiries and complaints about doxxing behaviour.

Q8: What do I need to do to minimise my digital footprints?

A:

- Regularly scan through your past social media posts to identify and delete anything that you are no longer comfortable about sharing.

- Terminate the account if you no longer wish to use a particular social media platform. This is generally done by following the steps for "termination", "deletion" or "deactivation" of account under "privacy settings". Mere deletion of data on the social media platforms may not be sufficient.

- Prior to termination of a social media account, you may request to download a copy of your information (such as photos, messages and posts) for your own record.

Q9: How do I help my children stay safe on social media?

A:

- Be very cautious when sharing photos and other information about children. Children usually are not able to identify the risks of giving away too much personal data online or spot online scams.

- If you are setting up accounts for your children, consider switching on "parental control" if that is available, and make it known to your children that "parental control" is activated. Generally, "parental control" consists of features like blocking some web contents, restricting changes to privacy settings, and preventing in-app purchases. This will reduce the risks to which your children may be exposed.

- Provide guidance to your children about the use of social media. This may include, for example:

  (a) teaching your children about the risks of using social media, including the risks of leaving perpetual digital footprints;
  (b) checking the privacy settings of the social media accounts for your children;
  (c) explaining to your children that they should not disclose personal data, such as full names, addresses, phone numbers or school names, on social media arbitrarily; and
  (d) teaching your children to respect other people's privacy and not to share other people's personal data, such as photos and addresses, arbitrarily.

Annex

Step-by-Step Guide on Adjusting Privacy Settings

This Annex outlines the steps you can follow in order to change the privacy settings via the operating systems of your mobile phones or by directly adjusting the settings in mobile apps.

You may wish to note that operating systems (such as Android and Apple iOS) and individual mobile apps are updated from time to time. The precise steps for adjusting privacy settings and the privacy settings available may change consequently.

For Android

The settings below are based on Android version 11.

(1) Location

Step 1: On your mobile phone, go to '**Settings**'

Step 2: Select '**Privacy**'

Step 3: Select '**Permission Manager**'

Step 4: Select '**Location**'
You will now see a list of apps that have permission to **access your physical location**

Step 5: Select an app, and you will be given options to change the permission as to whether and when the app can access your physical location

(2) Contact list (phone book)

Step 1: On your mobile phone, go to '**Settings**'

Step 2: Select '**Privacy**'

Step 3: Select '**Permission Manager**'

Step 4: Select '**Contacts**'
You will see a list of apps that have permission to **access your contact list**

Step 5: Select an app, and you will be given options to change the permission as to whether and when the app can access your contact list

(3) Photos and media files

Step 1:	On your mobile phone, go to '**Settings**'
Step 2:	Select '**Privacy**'
Step 3:	Select '**Permission Manager**'
Step 4:	Select '**Files and media**' You will see a list of apps that have permission to **access the photos, media files and other files stored on your mobile phone**
Step 5:	Select an app, and you will be given options to change the permission for the app to access the files (including photos) in your mobile phone

For iOS (Apple)

The settings below are based on iOS 14.4.1

(1) Location Services

Step 1:	On your mobile phone, go to '**Settings**'
Step 2:	Select '**Privacy**'
Step 3:	Select '**Location Services**' You will now see a list of apps that have permission to **access your physical location**
Step 4:	Select an app, and you will be given options to change the permission as to whether, when and how precise the app can access your physical location

(2) Online tracking

Step 1:	On your mobile phone, go to '**Settings**'
Step 2:	Select '**Privacy**'
Step 3:	Select '**Tracking**'
Step 4:	You will be given options to change the permission as to whether to allow apps on your mobile phone to request to **track your activities across other apps and websites**

(3) Contact list (phone book)

Step 1: On your mobile phone, go to ‘**Settings**’

Step 2: Select ‘**Privacy**’

Step 3: Select ‘**Contacts**’

You will see a list of apps that have permission to **access your contact list**

Step 4: You will be given options to change the permission as to whether the app can access your contact list

(4) Photos

Step 1: On your mobile phone, go to ‘**Settings**’

Step 2: Select ‘**Privacy**’

Step 3: Select ‘**Photos**’

You will see a list of apps that have permission to **access to your photos**

Step 4: Select an app, and you will be given options to change the permission as to whether and to what extent the app can access your photos

In-apps Privacy Settings

Some of the privacy settings are specific to the social media platforms concerned. These settings can only be adjusted on the social media platforms. Below highlights some of the major privacy settings in Facebook, Instagram and Twitter which have greater privacy implications.

Settings	Facebook	Instagram	Twitter
To adjust the **public visibility of your profile information** (such as education, contact details)	1. Go to '**Settings and Privacy**' 2. Select '**Settings**' 3. Select '**Privacy Settings**' 4. Select '**Manage your profile**' to make changes	1. Go to '**Settings**' 2. Select '**Privacy**' 3. Select '**Private Account**' to make changes	1. Go to '**Settings and privacy**' 2. Select '**Privacy and safety**' 3. Select '**Protect your Tweets**'
To adjust the permission granted to the app to use **facial recognition technology** to recognise you in photos	1. Go to '**Settings and Privacy**' 2. Select '**Settings**' 3. Select '**Face Recognition**' to make changes	Not applicable	Not applicable
To adjust the right granted to the app to **track your activities** across different apps and websites	1. Go to '**Settings and Privacy**' 2. Select '**Settings**' 3. Select '**Off-Facebook Activity**' to make changes	Not applicable	1. Go to '**Settings and privacy**' 2. Select '**Privacy and safety**' 3. Select '**Personalization and data**' to make changes
To adjust the permission granted to other users to "**tag**" you in their photos	1. Go to '**Settings and Privacy**' 2. Select '**Settings**' 3. Select '**Profile and Tagging**' to make changes	1. Go to '**Settings**' 2. Select '**Privacy**' 3. Select '**Account Privacy**' 4. Select '**Tag**' to make changes	1. Go to '**Settings and privacy**' 2. Select '**Privacy and safety**' 3. Select '**Photo tagging**' to make changes

PCPD website

PCPD.org.hk

香港個人資料私隱專員公署
Office of the Privacy Commissioner
for Personal Data, Hong Kong

Download
this publication

Enquiry Hotline	**:**	**(852) 2827 2827**
Fax	**:**	**(852) 2877 7026**
Address	**:**	**Room 1303,13/F, Dah Sing Financial Centre, 248 Queen's Road East, Wanchai, Hong Kong**
Email	**:**	**communications@pcpd.org.hk**

Copyright

Disclaimer

The information and suggestions provided in this publication are for general reference only. They do not serve as an exhaustive guide to the application of the law and do not constitute legal or other professional advice. The Privacy Commissioner makes no express or implied warranties of accuracy or fitness for a particular purpose or use with respect to the information and suggestions set out in this publication. The information and suggestions provided will not affect the functions and powers conferred upon the Privacy Commissioner under the Personal Date (Privacy) Ordinance.

First published in April 2021