PROTECTING ONLINE PRIVACY

BE SMART ON SOCIAL NETWORKS

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

When you register for social networks

- Read the privacy policy to find out how the social network will handle your personal data.

- Avoid providing excessive personal data. When you create a new account, consider the genuine need to provide each piece of personal data and whether supply of the data is obligatory. *(e.g. why should you provide your day and month of birth when it only wants to impose an age limit on users?)*

- If you want to prevent others from collating information about you from different social networks, consider creating different account names on different networks and registering them with different email addresses. People may easily track you down if you register using the same personal data across multiple sites.
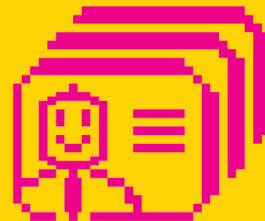
Privacy setting

- Make sure you understand how the social network's data sharing works before posting your data.

- Find out how your personal data will be shared on the social networks. In particular, find out how you may create different groups of friends so that you can limit the posted information that each group can see.

- Some sites often change their privacy settings. Keep checking the privacy setting pages to see what kinds of personal data are being shared and how.

- Do not accept people you do not know, or are unsure of, as your friends.

- Some social networks offer third-party applications to users. These applications have different privacy settings and will access different types of personal data from your profile, and pass the data to third parties. Make sure you understand the implications before accepting any such application.

Your personal data will go public

- Once disclosed online, your personal data may be copied or kept permanently, and you will no longer have control over who can read it. Do you want any information you may regret later to be available online forever for all to read?

- You may not want everyone to read your postings. Think what may happen if someone (e.g. for youngsters, potential employers or university admission offices) in the future reads things you post today.

- Picture tells a thousand words – they may be embarrassing or contain information you do not intend to share (e.g. company logo in the background or uniform that identifies where you work/study, even name tags or tickets that may give your name away).

- Treat others the way you would like to be treated. You should seek permission from others before posting their pictures or identifying them in your posting (think about the long term impact on children who cannot give an informed consent now).

- Even if you only leave fragmented information about yourself in each site, collectively you may have left a lot of information about you. Others may find ways to collate all those information about you without your knowledge.

- Social networks are not entirely virtual. If you leave too much information of yourself or your friends (such as your whereabouts), people could trace you in the physical world.

- You may think that you are sharing your comments only to a group of close friends but bear in mind the possibility that they may copy and redistribute your comment to other open social networks without you knowing, thus causing embarrassment to you.

Think before you post!
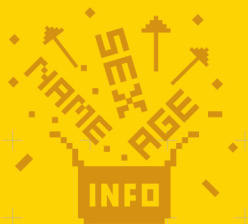
How to protect your personal data – data security and personal safety

- Social networks may ask you to log in your email account or synchronise your smartphone address book to find friends for you. Beware that they may import the entire address book from your account/ smartphone to the social network, and undoing this arrangement could be difficult.

- Social networks provide a convenient tool to get in touch with one another but are often full of malicious links or files. Make sure your anti-virus programme and its virus definition files are up-to-date.

- Social networks provide test ground for all sorts of new ideas. Often the privacy implications have not been well-considered. So, use new features with caution and find out how to turn them off to protect yourself, if necessary.

- Remember to remove accounts in sites that you no longer use or you are not interested in any more to reduce the fragmented information you leave on the Internet. Keep a list of accounts you have created so you can remove them later.

- It is difficult to verify information provided by others on the Internet including their true identities, so think twice before meeting others you got to know on the Internet, or acceding to their request for information, money or help.

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

**Office of the Privacy Commissioner
for Personal Data, Hong Kong**

Enquiry Hotline : (852) 2827 2827

Fax : (852) 2877 7026

Address : 12/F, 248 Queen's Road East, Wanchai, Hong Kong

Website : www.pcpd.org.hk

Email : enquiry@pcpd.org.hk

Learn more about

上私隱要自保
Think PRIVACY Be SMART Online

www.pcpd.org.hk/besmartonline