



CHILDREN ONLINE PRIVACY

Practical Tips for Parents and Teachers



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

PCPD.org.hk

保障·尊重個人資料
Protect, Respect Personal Data

Introduction

This leaflet aims to provide tips to parents and teachers on helping children¹ under their care to protect their personal data in the online environment.

The Privacy Rights of Children



Everyone's personal data privacy right should be protected and respected regardless of their age. So, children should enjoy the right:

- to give personal data only where necessary;
- to fair collection of their personal data for lawful purposes;
- to be informed about intended use of their personal data;
- to personal data accuracy and security;
- to non-excessive retention of their personal data;
- to withhold consent to change of use;
- to be informed about the policies and practices of organisations which handle their personal data; and
- of access and correction of personal data.

Parents and teachers have a significant role to play in the exercise of the right, depending the age and maturity of the child in individual cases.



¹ Generally "children" means those under the age of 18.

Advice to Parents and Teachers



Online technologies bring enormous benefits to our daily lives yet their rapid development makes their privacy risks difficult to manage. Parents and teachers should however not shy away from such risks but learn and discuss with children the smart use of technologies and their related risks.

STEP 1 Getting Involved



1 Trying it out

The best way to learn technology is to try them. Parents and teachers should be able to gain first-hand knowledge in online platforms/systems by using them so that they can share their experience and communicate with children on how to protect the personal data privacy right.

Parents and teachers can experiment with online platforms/systems by creating online accounts using separate email addresses and pseudonyms. This should enable them to control what personal data is required and accessible, and avoid over-disclosure.



2 Participating in children's online activities

Parents and teachers are encouraged to find suitable ways to engage with children in the online activities. If parents and teachers are excluded from children's online world, they cannot be there to share experience and protect them.

3 Exploring parental controls

Some online platforms/systems offer parental controls (or "dashboards") that allow parents to monitor or configure the settings to protect children from undesirable contents or contacts. For younger children, parents could explore how these facilities may help.

STEP 2

Back to Basics



If children share or disclose their personal data casually, or if personal data is disclosed without authorisation or consent, the personal data may be misused to obtain gains, to cause them embarrassment or harm, or to draw inferences about them which may be untrue or damaging in the long run.

1 Privacy protection starting with self-help security

Many personal data breaches are caused by the lack of good security practice on the part of users themselves. Parents and teachers are also advised to read the leaflet *Protecting Privacy – Using Computers and the Internet Wisely*² with their children to understand more about essential security measures when using online platforms/systems, including how to protect their computers and smartphones, safe use of Internet and Wi-Fi, protection of accounts and passwords, and steps to take before disposal of equipment.

2 Be vigilant about digital footprints

Most people are conscious of protecting personal data such as names, phone numbers, addresses, dates of birth, and more sensitive data such as HK Identity card numbers, but may be less vigilant about safeguarding other “indirect” or seemingly less sensitive personal data – such as photos, schools attended, location trails, and data stored in smartphones. We need to be aware, however, that when enough indirect information is gathered, our identities may be ascertained by others without our knowledge.

Parents and teachers should remind children not to rush to provide or share information – even though the information appears to be indirect or fragmented – when registering for a new service or using it. They should be encouraged to consult their parents and teachers before providing or sharing their personal data.

2 See www.pcpd.org.hk/english/resources_centre/publications/files/computer_wisely_e.pdf



More specifically, parents and teachers are advised to read with children the leaflets *Protecting Online Privacy – Be Smart on Social Networks*³ and *Protect Privacy by Smart Use of Smartphones*⁴ and discuss how they can better protect themselves.

3 Checking default settings

Many online platforms/systems allow users to change privacy settings, such as who can see their information and what information would be retained by the system. Such settings are, however, often set by default to “sharing with everyone” rather than limiting the sharing and use of the information. Parents and teachers should therefore sensitise children to examine these settings critically before choosing to use new platforms/systems.

4 Nothing is private in the online world

Even when appropriate privacy settings have been carefully chosen, children should be reminded that it is not always easy or practicable to keep information private in the online world. Information may be disclosed where settings are misunderstood or misconfigured, or it may be deliberately copied and pasted to open forums by closed-circle “friends”. Children should be warned that sharing information including photographs online willingly or inadvertently means that the information will be accessed by members of the public.

5 Teach children to respect the privacy of others

Parents and teachers should also encourage children to respect privacy of others in the way they would like to be respected. For example, children should be encouraged to have regard to the personal consent of their friends and families when they plan to share or tag their photographs.



³ See www.pcpd.org.hk/english/resources_centre/publications/files/SN_e.pdf

⁴ See www.pcpd.org.hk/english/resources_centre/publications/files/leaflet_smartphones_e.pdf

STEP 3

Setting a Good Example



Parents and teachers are role models for children. They should set good examples by protecting their own personal data and respecting others' personal data privacy.

On protecting their own personal data privacy, parents and teachers should set an example by understanding the privacy implications of using online platforms/systems. For example, assessing the advantages and risks of using various online services so as to demonstrate to children the steps needed to protect themselves while enjoying the benefits of online services.

On respecting the personal data privacy of others, parents and teachers should set an example by consulting others before sharing personal data of friends or third parties. In terms of sharing children's information (such as photographs, examination results and participation in sporting events), parents and teachers should invariably take into account the interest of the children, including physical harm and potential embarrassment in the future. However, as children's expectations and ability to make decisions may vary depending on individual maturity and intellectual development, parents and teachers are encouraged to discuss with them frequently and frankly on their online practices.



The Reality of Online Technologies



• Cyberbullying

Cyberbullying is a complex issue and not solely related to the sharing of personal data. However, sometimes the over-disclosure of personal data, including passwords, can serve as a means to cause harm in some circumstances (such as when a friendship turns sour and a friend becomes a bully). Most importantly, children should be made aware that they need to seek advice from parents and teachers when faced with cyberbullying.

• Free service having a price tag

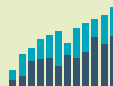
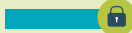
Children should be taught to consider the motive behind many “free” services available on the Internet. It is likely that they are paying for such “free” services at the price of sacrificing their personal data. Personal data (including our interests, purchasing habits, health conditions etc.) is a valuable and tradeable commodity to many enterprises or organisations. On the other hand, children may be victimised by the misuse or disclosure of their personal data without realising it until it is too late. Parents and teachers should assist the children in understanding and realising that they may not genuinely be benefitted by trading off their personal data.

• Online identities not being what they appear

Children should be reminded that the online community is very different from the real world. Even genuine users of online services often use pseudonyms or even false information to register their accounts, and can deceitfully portray themselves as whoever they want to be. Worse still, if a friend's account is hacked, anyone can easily pretend to be your friend with intent to defraud you. “Friend of a friend” on the Internet is just a stranger and should never be trusted. Parents and teachers should alert children of the potential dangers of personal safety and loss of property when communicating online.

Login

Password



• No “delete” button on the Internet

Children should be told that not many of the online platforms/systems offer the means to have their activities and information deleted. Even if they do, the effectiveness of the deletion is often unclear. Given that it may not be easy to get in touch with these online platforms/systems for redress, children should be taught to think twice before sharing information.

Furthermore, any information disclosed online could be searched, transferred, downloaded or archived by others. Children should understand that anything they disclose online could potentially be made available to the public without their knowledge, and that there is virtually no way to completely remove such information once it is circulated on the Internet.



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

PCPD.org.hk

Enquiry Hotline : (852) 2827 2827

Fax : (852) 2877 7026

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

Email : enquiry@pcpd.org.hk

Copyright: Reproduction of all or any parts of this publication is permitted on condition that it is for non-profit making purposes and an acknowledgement of this work is duly made in reproduction. **Disclaimer:** The information provided in this publication is for general reference only. It does not provide an exhaustive guide to the application of the Personal Data (Privacy) Ordinance (the "Ordinance"). For a complete and definitive statement of law, direct reference should be made to the Ordinance itself. The Privacy Commissioner for Personal Data (the "Commissioner") makes no express or implied warranties of accuracy or fitness for a particular purpose or use with respect to the above information. The above suggestions provided will not affect the functions and power conferred upon the Commissioner under the Ordinance.

© Office of the Privacy Commissioner for Personal Data, Hong Kong. First published in December 2015.