CYBER-BULLYING WHAT YOU NEED TO KNOW

PCPD
HK

PCPD.org.hk

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

Introduction

Nowadays, people are connected by a variety of electronic means and devices. Through instant messaging services and social media accounts, people share their daily life experiences and interact with friends and family, thereby sharing ideas, building relationships and having fun. Online, a person can access information shared by others with little or no restriction.

While technological innovations have made human interactions more efficient and more creative, increased connectivity may lead to problems when strangers, critics, bystanders or even friends interact irresponsibly and without due regard to people's right to privacy. People's lives offline may be adversely affected as a result. One notable example of such unfortunate consequences is cyber-bullying.

This leaflet provides examples of cyber-bullying to remind the members of the public of the privacy and legal issues involved in cyber-bullying and calls on Internet users to respect the privacy right of others in the cyber world. For tips on how to protect privacy when using social network platforms, please refer to the Privacy Commissioner for Personal Data, Hong Kong (the "**Commissioner**")'s leaflet entitled *Protecting Online Privacy – Be Smart on Social Networks*[1].

Different Forms of Cyber-bullying

- Example 1 — "Standard" Wedding Gift
- Example 2 — Avengers?
- Example 3 — Bus Incident
- Example 4 — Internet Justice?
- Example 5 — Fake Online Boyfriend
- Example 6 — Online Flaming War
- Example 7 — Compensated Dating Rumours

Legal Protection

1. www.pcpd.org.hk//english/resources_centre/publications/files/SN2015_e.pdf

Different Forms of Cyber-bullying

Cyber-bullying generally refers to bullying that involves the use of email, images or text messages sent to web pages, blogs, chat rooms, discussion forums, online gaming network, mobile phones, or other information and communication technology platforms. Behaviour of cyber-bullying includes harassment, denigration, disclosure of real-world identities, framing, impersonation, trickery and exclusion. Children as well as adults can be the victims of cyber-bullying. Whatever the mode, cyber-bullying can cause great distress to the victim and in the extreme cases lead to the most tragic of consequences: suicide.

Like their counterparts in the physical world, cyber-bullies sometimes try to persuade or bully other people into joining in with the abuse.

The difference is that cyber-bullies are able to hide their identities on the Internet and they require neither the physical nor social prowess that may be needed for traditional bullying. Instead, online communication technology allows for continuous onslaught unrestrained by physical boundary. It is difficult to effectively stop cyber-bullying.

Example 1 — "Standard" Wedding Gift

Incident

A bride-to-be passed remarks on a social networking site, expressing her dissatisfaction with the wedding presents received. Shortly afterwards, users of various Internet forums criticised her attitude, and her wedding date and venue were made public. She was put under tremendous pressure and had to apologise in public.

Tips

There is no simple "Delete" button that can delete the information disclosed online.

Though you may regret making an off the cuff remark on the Internet and wish to delete it after posting, but by then, it may have already been read and forwarded to a great many other people.

What goes online stays online. Hence do not post any information online that you would not share publicly offline. Always assume that your "private" conversations will be published and become known one day, either by mistake or through the acts of your "friends".

Example 2 • Avengers?

Incident

A girl posted a message to her friends online complaining that she had been dumped by her boyfriend. She accused her ex-boyfriend to have injured her by pushing her down a staircase. As a result, her “friends”, in cyber space parlance, showed their support by displaying the personal data of her ex-boyfriend including his name, photo and residential address on their sites. The “accused” sought relief by skipping classes for days and clarifying in a radio programme that the allegation was made with no factual basis. Some netizens avenged in the name of her ex-boyfriend and posted the girl’s personal data online.

Tips

Think twice before posting any message, information or photo. Even with access limited to only “friends”, you have no control over what your “friends” share online. Your “friends” may not seek your permission or even inform you before re-posting your messages on their accounts or sites.

Posting comments or sending messages impulsively (e.g. when you are angry) are often regretted subsequently.

Example 3 — Bus Incident

Incident

Two passengers on a bus quarrelled over a seat. The dispute was captured by another passenger with a smartphone camera who then shared it online. Internet users went on to disclose the names and phone numbers of the protagonists on the Internet after uncovering their identities, who as a result faced tremendous pressure. Criticisms of the two passengers' behaviour swamped most online forums.

Tips

Beware that smartphone users often capture incidents that take place in public and then publish the same online, and if you are picked on for your uncivil behaviour or just for a practical joke, you may attract bad publicity on the Internet.

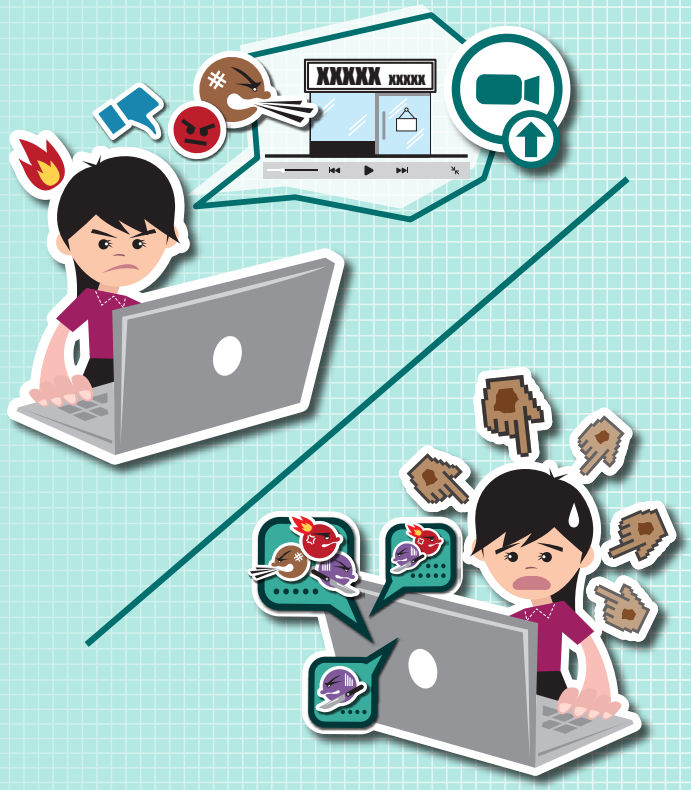
Beware that there are some Internet forums known for their members' prowess in uncovering the identity of the persons featured in the online video clips. Even if you and your friends have only left fragmented information about you on different sites, others can find ways to collate all information about you without your knowledge.

For minor incidents of cyber-bullying, e.g. a mean or nasty comment, the best response could be no response.

Example 4 — Internet Justice?

Incident

A grumpy customer posted a video to rally netizens' opposition against a shop for its poor customer service. She expressed her anger at the shop with nasty words. To her surprise, netizens found her actions unreasonable and she became the target of attack. Her photo, home and office addresses were published on the Internet. A social network group was set up calling for her apology.



Tips

What you say or share online can draw scrutiny beyond your expectation.

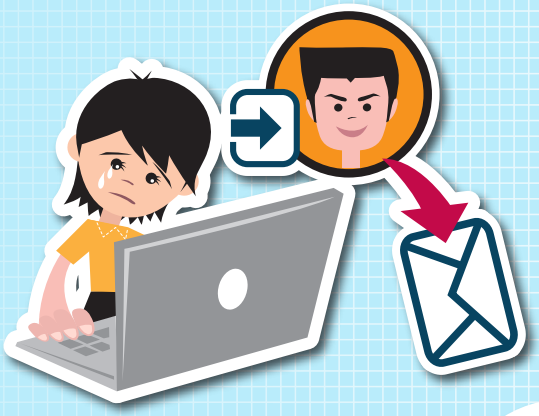
The information you shared with others could be targeted by cyber-bullies naming and shaming individuals in the name of Internet justice. They put you on trial over your online words or behaviour and give their verdicts. It is not uncommon that an "attacker" may end up as a victim when the tide turns.

Think twice before joining a heated discussion. Treat others the way you would like to be treated. You could be the next victim!

Example 5 — Fake Online Boyfriend

Incident

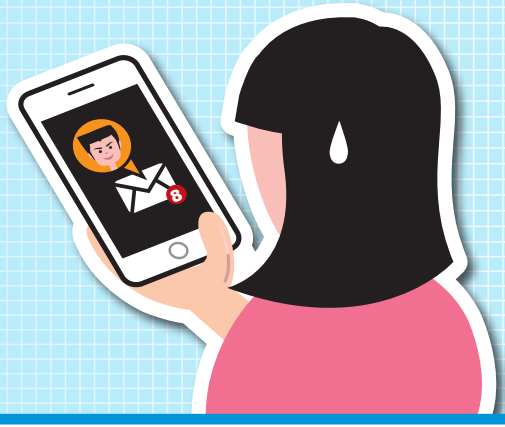
Soon after a love relationship began, the boy shared his social network account password with his girlfriend. To her disappointment, the girl found from the boy's social network activity logs posts relating to his previous relationships which were unknown to her. The girl then impersonated the boy and sent harassing messages to his ex-girlfriends.



Tips

Cyber-bullying may also occur when someone poses as the victim and uses the victim's account to send out offensive, harassing, inappropriate messages or "hate" mail to friends and family on the "friend" list, thus misleading them to believe the communication was sent by the victim.

You may complain directly to the social network operator as abusive contents may be a violation of its acceptable use policy and subject to removal. Most social network sites have a link to their customer service department that allows individuals to report offensive messages, information or photos so that they can take action to remove them.



Example 6 — Online Flaming War

Incident

A couple broke up, both vented their anger at each other on an online forum. Both had their own supporters, and their offensive remarks were reported to the Online Service Provider ("OSP") by the opposite side as inappropriate, leading to the termination of their accounts with the OSP.

Tips

Cyber-bullies may set up their victims by making them angry so that they respond with an irate or offensive remark. Once the victim so responds, the cyber-bully will click on the inappropriate content button on his social network or chat screen and notify the OSP that there is objectionable content in the victim's account.

If there are continuous bullying messages and you decide that the best strategy is to isolate yourself from those messages, you may use the social network sites' blocking feature to stop receiving such messages. Most social networking sites as well as instant messaging programs have profile settings that allow a user to block other users from contacting them or showing comments on their accounts. (Note: Typically this option cannot stop bullies from continuing to post message and prevent others from seeing them.)

Example 7 — Compensated Dating Rumours

Incident

A girl, who had no social network account, was falsely accused by her classmate of being involved in "compensated dating". The rumour spread on an online forum. Some of the girl's friends posted her photo and telephone number for "investigation". As a result, the girl received thousands of nuisance calls for sex service.

Tips

You may believe that you are safe from cyber-bullying because you have never disclosed your personal data or communicated with others on the Internet. However, as the Internet is so closely wired, any individual, Internet user or not, is vulnerable to irresponsible online behaviour.

Children may not understand the long-term implications of posting silly or offensive remarks or pictures. They may not appreciate it is not acceptable to harass, spread gossip, or make mean or disparaging comments towards others online. Parents need to educate children about their rights and responsibilities as netizens.

Children should seek help from parents, teachers or adults that they can trust. They should not shy away from showing to trusted adults any messages that include threatening or harassing statements.

Legal Protection

There is no statute law in Hong Kong on cyber-bullying, and as cyber-bullying activities are wide-ranging and cover defamation, criminal intimidation and infringement of intellectual property, etc., they have to be addressed by relying on different branches of the law. Various law enforcement bodies are involved.

If the post carries criminal element e.g. criminal intimidation, or if it is indicative of a civil wrong, e.g. defamation or injurious falsehood, you may report it to the Police or seek legal advice as to the appropriate recourse. If you do not know who sends or posts the messages, the messages should be saved to help identify the perpetrator.

Where cyber-bullying engages the collection and use of personal data, the requirements of the Data Protection Principles ("**DPPs**") under the Personal Data (Privacy) Ordinance are relevant. DPPs 1 and 3 are particularly important:

- DPP1 – This principle requires the data user to collect only the personal data for a purpose directly related to its function or activity; collect data as necessary and not excessively; and collect data by means which are lawful and fair. For instance, collection of personal data for the purpose of criminal intimidation is not for a lawful purpose and is therefore prohibited under DPP1.

- DPP3 – This principle stipulates that unless the data subject has given explicit and voluntary consent, personal data shall only be used for the purpose for which it was originally collected or a directly related purpose.

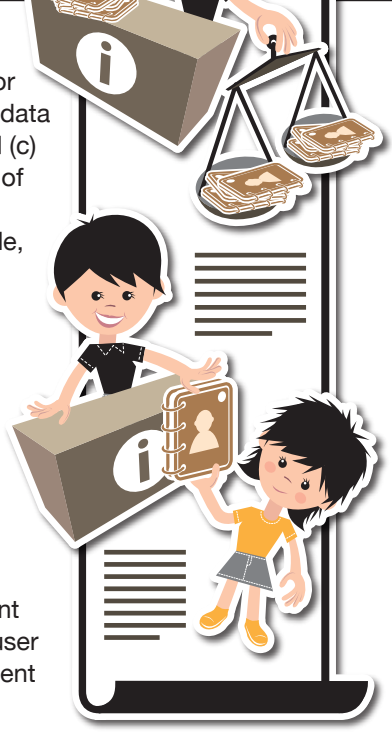
  There is no exemption from DPP3 for personal data obtained from the public domain through channels such as public registers, search engines or public directories. In other words, cyber-bullying based on the use of personal data of targeted persons collected from these public sources could be a contravention of DPP3.

The fact that an individual's personal data can be obtained from the public domain must not be taken to mean that the individual has given blanket consent for further use of his personal data for whatever purposes. Due regard must be given to (a) the original purpose of making the personal data available in the public domain, (b) the restrictions, if any, imposed on further uses of the data and (c) the reasonable expectation of personal data privacy of the individual. The legitimate expectation of privacy can be ascertained by asking whether a reasonable person in the shoes of the individual concerned would find the re-use of the data unexpected, inappropriate or otherwise objectionable, taking into account all factors in the circumstances. It is unlikely that a victim of cyber-bullying would accept that his personal data found in the public domain can be used to his detriment.

More detailed explanations on how DPP3 governs the use of personal data in the public domain are found in the Commissioner's *Guidance on the Use of Personal Data Obtained from the Public Domain*[2].

DPPs 1 and 3 may be exempted under section 52 of the said Ordinance where personal data is held by an individual and is (a) concerned only with the management of his personal, family or household affairs; or (b) so held only for recreational purposes.

Contravention of a DPP per se is not an offence, but the Commissioner may serve an enforcement notice on the data user concerned to remedy the contravention and it is an offence for the data user not to comply with the enforcement notice. The offence attracts a fine of $50,000 and imprisonment for two years and, in the case of a continuing offence, a daily fine of $1,000.



2. www.pcpd.org.hk/english/publications/files/GN_public_domain_e.pdf

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**

First published in October 2014
March 2017 (First Revision)