# Protect your personal data while engaging in IT related activities

## Personal Data (Privacy) Ordinance – Six Data Protection Principles

*Principle 1 – purpose and manner of collection of personal data*

Collection of personal data shall be related to a function or activity of the data user and the data collected are not excessive; the means of collection are lawful and fair; data subjects are informed of the purpose of collection and the use of the data.

*Principle 2 – accuracy and duration of retention of personal data*

Practicable steps shall be taken to ensure the accuracy of the personal data, and the data shall be erased after the fulfillment of the purposes for which the data are used.

*Principle 3 – use of personal data*

Unless the data subject gives consent, personal data should be used for the purposes for which they were collected or a directly related purpose.

*Principle 4 – security of personal data*

Practicable steps shall be taken to ensure that personal data are protected against unauthorized or accidental access, processing or erasure.

*Principle 5 – information to be generally available*

Policies and practices in relation to personal data should be formulated and made available.

*Principle 6 – access to personal data*

Data subjects have the rights of access to and correction of personal data.

## Table of Contents

## The Office of the Privacy Commissioner for Personal Data and Your Privacy Right

The Office of the Privacy Commissioner for Personal Data ("PCPD") is an independent statutory body set up to oversee the enforcement of the Personal Data (Privacy) Ordinance ("the Ordinance") which came into force on 20 December 1996 aiming at the protection of the privacy of individuals in relation to personal data.

Under the Ordinance, the right of personal data privacy includes: collection of personal data by fair means; being informed of the use of the data; providing only the necessary personal data; the use of the personal data can only be changed with consent; requesting for accuracy of personal data; requesting that personal data are not kept longer than necessary; requesting that security measures for personal data are taken; access to and correction of personal data; and requesting for disclosure of privacy policies by organizations.

According to the Data Protection Principle on the security of personal data, a data user should take all practicable security steps to ensure that personal data held by the data user are protected against unauthorized or accidental access, processing or erasure having particular regard to the kind of data and the harm that could result if any of those things should occur. Therefore, the requirements of the Principle will be contravened if no appropriate measure is taken to protect personal data or there is leakage of personal data due to inappropriate computer disposal.

## Computer Safety

Most of the personal data leakage incidents happened recently related to computer. In the past, functions of computer were simple and networks were not well developed. With the development of computer technology, especially the rapid advancement of the Internet, we can enjoy the convenience brought by computer. However, we also have to take heed of various accompanying risks, and most serious of which is leakage of personal data.

Apart from general word processing, computer nowadays can be used for blog writing, MSN Messenger communication, online banking, etc. If your email password or online banking password is stolen, the problems arose may be far more serious than you can imagine.

## Computer Viruses and Privacy (I)

A computer virus is a kind of malicious software which causes not only computer damage, but also data leakage or computer malfunction. New generation of computer viruses can even hide in computer for a long time and wait for the opportune moment to steal users' personal data. Therefore, installation of anti-virus software with regular updating can effectively eliminate the problem of data leakage caused by computer viruses.

There are various kinds of anti-virus software in the market. In addition to paid software, there are also free products for users, e.g. AVG Free, Avast! Home Edition, Avira AntiVir, etc. It is better to have them installed than not, though their functions may not be as sophisticated as paid software.

Apart from anti-virus software, users are also advised to install personal firewall software in computer. In addition to the built-in firewall software in the operating system, users can also install firewall software provided by a third party software supplier to enhance security. A firewall works like a filter filtering out different dangerous information on the network. Most of the security software companies have launched integrated Internet Security products with the functions of anti-virus and firewall to give users comprehensive protection in one product. Moreover, there are some firewall software packages with satisfactory functions, e.g. Comodo (http://www.personalfirewall.comodo.com/index.html).

Users should also activate the auto update function of their security software to guard against the latest threat. In the Information Security website (http://www.infosec.gov.hk) set up by the Government, common firewall software, anti-virus software and security patches from renowned manufacturers can be downloaded.

Websites for free anti-virus software:

AVG Free
Website: http://free.grisoft.com
Description: Free anti-virus and anti-spyware software compatible with Windows XP and Windows Vista for home users.

Avast! Home Edition
Website: http://www.avast.com/eng/free_software.html
Description: Free use of anti-virus software upon registration. In addition to anti-virus and anti-spyware, Avast! offers anti-rootkit, P2P file transfer and IM (e.g. MSN Messenger) protection. Chinese version is available.

Avira AntiVir
Website: http://www.free-av.com
Description: In addition to scanning for malicious programs such as viruses, worms and Trojans, it can also detect Rootkit and phishing websites. It is only available for home users in single computer use.

**Computer Viruses and Privacy (II)**

Even if you have installed anti-virus and firewall software, you still cannot lower your guard because security software may not keep up with the development of network attack. Relying solely on security software cannot completely avoid personal data leakage caused by network attack. For better protection, the use habit of users is essential. For example, you should not download unknown files arbitrarily, open suspicious email attachments, or input your personal data (including user name, password, date of birth, ID card number, etc.) in websites recklessly; otherwise it is useless to have powerful security software installed.

## Security of USB Flash Drives

In addition to easy portability, USB flash drives offer high storage capacity. Many young people like to store their coursework and even their photos in USB flash drives. As the size of a USB flash drive is rather small, such device can be easily lost, resulting in personal data leakage. In fact, users can use encrypted USB flash drives, or they can use encryption software, e.g. TrueCrypt (http://www.truecrypt.org) to encrypt those USB flash drives without built in encryption feature. For any access to an encrypted USB flash drive, users have to input a password, which protects the data from leakage.

## Security Tips for Using IM/Email/Blog/Facebook

IM (Instant Messaging) is a real time communication system, allowing two or more persons make instant text message, file, voice and video communication on the Internet. For commonly used IM software, such as MSN Messenger, there is not much risk in file transmission. If users have installed anti-virus software and do not install unknown software, most problems can be avoided. Users should bear in mind that they should not recklessly disclose their personal data to other people because there is "History" function in most IM software. If your record is retrieved by others, the consequence may be very serious. Moreover, as some IM software programs have "File sharing" function, users should be careful about the setting to avoid sharing of their personal data by others.

Recently, more and more website links with viruses have been sent through MSN Messenger. You should not trust that a message sent by your friend is definitely virus free. It is because when these websites are infected, they will automatically send website links with viruses to your friends in Messenger Communication. Once they click on the Internet, their computers are infected and viruses will be widely spread. Therefore, in addition to installation of anti-virus software, before clicking the website links sent by your friends, to play safe, you should ask your friends what they have sent.

Regarding email, users should avoid clicking website links and opening attachments recklessly. For sending mail in bulk, the "bcc" function should be used to avoid disclosing the email addresses of the recipients or virus attacks.

Apart from MSN Messenger, many people also have the habit of writing blogs and browsing Facebook. Although basic security is provided in such services, users should not post their personal data on the Internet. Once the data are posted on the web, every one can see them. To protect yourself, you should carefully decide what data should be posted on the web. Furthermore, if you want to share your group photos in your blog or social networking websites, you'd better notify your friends first because not every one likes to be shown.

In Facebook, you can set the access right of different users to your personal data. In short, your good friends can see more information about you, and for better protection, you may deny others access to your personal data.

## How to Transmit and Store Important Personal Data

Before sending sensitive personal data by email, the file should be encrypted. To open the file, the recipient needs to input a password. Such arrangement can protect the data as well.

Moreover, "password protect" function is available in Microsoft Office. Users can password protect their Word, Excel and Powerpoint files (Steps: "File" → "Save As" → "Tools" → "General Options" → "Protect Password"). Compression software, such as Winzip and WinRAR can also password protect your files when the files are compressed.

For more effective and powerful encryption function, professional encryption software, such as EntrustEntelligence and DriveCrypt can be used.

## File-sharing Software

Foxy software is a kind of P2P software with the advantage of transferring files in high speed. As P2P networks are usually flooded with illegal software and files and users are unable to know whether a file is safe, in case a file is planted with a Trojan or virus, your computer will be completely unguarded. Not only data in your computer may be accessed by others, your computer may also be used to attack other computers, thus participating in crime without your notice. Furthermore, some P2P software programs require users to open many network transfer ports and this will render a computer more vulnerable to Internet attacks.

Recently, a series of personal data leakage incidents happened because working staff neglected the fact that the personal computers they used to handle their work had been installed with file-sharing software. Therefore, when using Foxy, users have to set up their “upload folders” carefully. It’s easy to do it: simply unclick the files that you do not want to be shared in the setting profile of “share folders”.

Can users then rest assured? Not yet. They have to carefully set the location of their “download folders” because the data inside the “download folders” will be automatically put on the Internet for searching and downloading by other Foxy users. Therefore, it is proposed to set the “download folder” as a blank folder that is only used for downloading and frequently clear up the folder by deleting those data/files that should not be shared.

## Safe Wi-Fi Internet Access

Following the popularity of Wi-Fi, users can be online at any time and at any place. However, as Wi-Fi uses airwaves for transmission, others can easily intercept the transmitting data. Therefore, when Wi-Fi is used, encryption system has to be activated to avoid illegal interception of data.

Most Wi-Fi networks can support WEP or WPA/WPA2 encryption technology, in which WPA2 is the safest option. If it is possible, users should use WPA2 encryption. In the Government Wi-Fi Programme, two Wi-Fi connections are provided to users to access the Internet: unencrypted connection and WPA2 encrypted connection. Users are advised to use the encrypted connection to minimize the risk that their data will be intercepted or decrypted. Moreover, when using public Wi-Fi access, users should be careful not to share their data folders.

## Computer Repair and Disposal

If our computers need repairing, how can we avoid leakage of our personal data? First of all, we should choose a reputable and reliable computer repair company by, for example, finding out the company's policies and practices in handling personal data, checking whether it has taken any measures to ensure the integrity and prudence of persons handling the data, etc. If it is necessary to repair the hard disk, a backup should be made before deleting the personal files. Moreover, computers should not be disposed of recklessly. There had been incidents of data leakage caused by careless disposal of computers by organizations. Therefore, you are advised to erase the data in your hard disk with file deletion software, e.g. WipeDrive, Inferno, etc., or you may completely erase the data by formatting your computer with the low level format software provided by the hard disk manufacturer.

Malicious software (Malware) – a collective term for computer viruses, Trojans, spyware, etc. Generally speaking, it is surreptitiously installed on a computer for data dissemination, destruction and search/transmission without the user's consent.

Security software – software including anti-virus software, anti-spyware, firewall, etc. designed to guard malicious software. In recent years, such functions have been integrated into the Internet Security Suite to provide comprehensive system protection.

P2P (peer to peer) technology – currently the most popular file transfer technology. Each node can simultaneously perform uploading and downloading in high speed, lightening the load of a central server in transmitting data to different clients.

WEP – the acronym for "Wired Equivalent Privacy", a kind of Wi-Fi encryption technology. It is an old encryption protocol using static encryption keys, but no longer meets the needs today.

WPA – the acronym for “Wi-Fi Protected Access”, a kind of Wi-Fi encryption technology. Its dynamic encryption capability can effectively lower the possibility of decryption during Wi-Fi transmission.

Disclaimer: The security measures and the use of products or software suggested in this booklet do not constitute our recommendation of any kind. Individuals have to consider their needs cautiously. The Privacy Commissioner for Personal Data (“the Commissioner”) shall not accept any liability for any loss or damage howsoever arising from any use of the products or software, and the functions and power conferred to the Commissioner under the Ordinance will remain unaffected.

Acknowledgement: Dr. Elizabeth Quat (Co-founder and Ex-president, Internet Professional Association)

The Office of the Privacy Commissioner for Personal Data, Hong Kong
Hotline: (852) 2827 2827
Fax: (852) 2877 7026
Address: 12/F, 248 Queen’s Road East, Wan Chai, Hong Kong
Website: www.pcpd.org.hk
Email: enquiry@pcpd.org.hk
August 2008