PCPD
H K
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

Protecting Personal Data under Work-from-Home Arrangements: Guidance for Employees

Introduction

1. Work-from-home (WFH) arrangements have been made from time to time during the COVID-19 pandemic. Under WFH arrangements, employees may have to access or transfer the data and documents of their employers through their home networks and own devices, which are less secure than the professionally managed corporate networks and devices of their employers. This inevitably increases risks to data security and personal data privacy.

2. This Guidance serves to provide practical advice to employees to enhance data security and the protection of personal data privacy under WFH arrangements.

General principles for WFH arrangements

3. Regardless of whether one works in the office or works from home, the same standard should apply to the security of personal data and the protection of personal data privacy. Employees should adhere to the following principles when they work from home:

   (1) adhering to their employers' policies on the handling of data (including personal data); and

   (2) taking all reasonably practicable steps to ensure the security of data, in particular when information and communications technology is used to facilitate WFH arrangements, or when the data and documents are transferred during the work process[1] .

[1] Data Protection Principle 4 in Schedule 1 to the Personal Data (Privacy) Ordinance (Cap. 486 of the Laws of Hong Kong)

Practical advice to employees

4. Employees may have to remotely access their employers' corporate networks during WFH period. They may also bring electronic and paper documents home for work. The following steps should be taken by employees to ensure data security.

Device management

5. Employees should as far as practicable use only corporate electronic devices for work. The following steps should be taken to ensure the security of the devices and the data therein:

   (1) setting strong passwords, changing the passwords regularly and not sharing the passwords with other devices and accounts;

   (2) not inserting personal devices (such as personal USB flash drive) into corporate devices because personal devices may be prone to containing malware or other security vulnerabilities;

   (3) encrypting the data if portable storage devices are used for transferring or storing data;

   (4) not sharing corporate devices with family members;

   (5) turning off or locking the devices when they are not in use; and

   (6) promptly reporting any loss of corporate devices to employers.

Work environment

6. Employees should avoid working in public places to prevent accidental disclosure of personal data or restricted information to third parties.

7. If it is unavoidable to work in public places-

   (1) screen filters should be used to protect information displayed on the screens of electronic devices; and

   (2) public Wi-Fi should not be used. Employees may use the hotspot sharing function of their mobile phones if internet connection is needed for other devices for work.

Wi-Fi connection

8. Wired network connection is generally more secure than using Wi-Fi. Employees should therefore opt for wired connection under WFH arrangements, where possible. If Wi-Fi is used, the following steps should be taken to enhance the security of the connection-

(1) adopting up-to-date security protocol such as Wi-Fi Protected Access 3 (WPA3) or Wi-Fi Protected Access 2 (WPA2) to encrypt the data in transit and safeguard against other attacks;

(2) setting strong passwords for the Wi-Fi networks and changing the passwords regularly; not using the default login names and passwords of the Wi-Fi routers;

(3) updating the firmware of the Wi-Fi routers in a timely manner; and

(4) reviewing the devices connected to the Wi-Fi networks regularly to identify and remove suspicious devices.

Electronic communications

9. Electronic communications such as email and instant messaging allow employers and employees to communicate efficiently under WFH arrangements. To ensure security of electronic communications, employees should-

(1) avoid using personal email accounts or personal instant messaging applications for work;

(2) use only corporate email accounts for sending and receiving work-related documents and information;

(3) encrypt emails and/or attachments if they contain personal data or restricted information;

(4) double-check the names of recipients carefully before sending emails and instant messages, especially when the emails or the messages contain personal data or restricted information; and

(5) beware of phishing and malicious emails; do not open suspicious links or attachments; verify the genuineness of suspicious emails and messages with the senders by other channels, such as telephone.

Paper document management

10. Transfer of paper documents out of office premises should be avoided as far as practicable, in particular for those documents containing personal data or restricted information. If it is necessary for employees to bring paper documents home for work, the following steps should be taken:

(1) seeking approval from supervisors;

(2) redacting or removing personal data, restricted information and other unnecessary information from the paper documents before leaving office, where practicable;

(3) keeping a register of paper documents that have been taken home;

(4) taking extra care of the paper documents when travelling;

(5) locking paper documents in a secure cabinet or drawer at home to prevent unauthorised access;

(6) returning the paper documents to offices as soon as possible when they are no longer necessary; and

(7) not disposing of work documents with personal data or restricted information at home. They should be shredded in accordance with established procedures in the office.

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

PCPD website

Download this publication

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

First published in November 2020