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 Organisations

Introduction

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

2. This Guidance serves to provide practical advice to organisations (including business entities) 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. Organisations that implement WFH arrangements should adhere to the following principles:

(1) setting out clear policies on the handling of data (including personal data) during WFH arrangements[1] ; 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 data and documents are transferred to employees[2].

1 Data Protection Principle (DPP) 5 in Schedule 1 to the Personal Data (Privacy) Ordinance (Cap. 486 of the Laws of Hong Kong)
2 DPP 4

Practical advice to organisations

4. Organisations, as data users and employers, are primarily responsible for safeguarding the security of personal data and protecting their employees' personal data privacy. The following measures should be implemented by organisations in order to give effect to the general principles for WFH arrangements.

Risk assessment

5. WFH arrangements may be unprecedented or new to many organisations. Organisations should therefore assess the risks on data security and employees' personal data privacy in order to formulate appropriate safeguards.

Policies and guidance

6. In light of the results of risk assessment, organisations should review their existing policies and practices, make necessary adjustments and provide sufficient guidance to their employees. Such policies and guidance may cover the following areas:

   (1) transfer of data and documents out of the organisations' premises and corporate networks;

   (2) remote access to the corporate networks and data;

   (3) erasure and destruction of unnecessary data and materials; and

   (4) handling of data breach incidents.

Staff training and support

7. Organisations should provide sufficient training and support to their employees for WFH arrangements to ensure data security. Training and support may cover the following areas:

   (1) data security techniques such as password management, use of encryption and secure use of Wi-Fi; and

   (2) awareness about cybersecurity threats and trends, such as phishing, malware and telephone scams.

8. Organisations should deploy designated staff to answer questions from employees and provide necessary support.

Device management

9. Organisations may provide their employees with electronic devices (such as smartphones and notebook computers) under WFH arrangements. The following steps should be taken to ensure the security of the data, including personal data, stored in the electronic devices-

(1) installing proper anti-malware software, firewalls and the latest security patches in the devices;

(2) performing regular system updates for the devices;

(3) ensuring that all work-related information in the devices are encrypted;

(4) setting up strong access controls, such as requiring the use of strong passwords (with a combination of letters, numbers, and symbols), requiring changing of passwords regularly and using multi-factor authentication; limiting the number of failed log-in attempts;

(5) preventing the transfer of data from corporate devices to personal devices;

(6) enabling remote wipe function so that information in the devices can be erased if the devices are lost; and

(7) avoid putting the names, logos and other identifiers of the organisations on the devices conspicuously to avoid unwarranted attention.

Virtual Private Network (VPN)

10. VPN is an important and popular tool for WFH arrangements because it enables employees to access corporate networks remotely and more securely via the internet. Organisations should ensure the security of VPN by, for example:

(1) using multi-factor authentication for connecting to the VPN;

(2) keeping security setting of the VPN platform up-to-date;

(3) using handshake protocol (such as Internet Protocol Security (IPSec), Secure Socket Layers (SSL), Transport Layer Security (TLS), etc.) for establishing secure communication channels between employees' devices and the corporate networks;

(4) using full-tunnel VPN where possible (using split-tunnel VPN only when necessary, such as in circumstances of insufficient bandwidth); and

(5) blocking the connection from insecure devices.

Remote access

11. In addition to using VPN, organisations should implement further security measures for remote access to their corporate networks. Practicable measures include-

    (1) implementing network segmentation to divide a network into multiple segments or subnets, thereby reducing the risk and magnitude of data breach incidents as well as enhancing the protection for critical and sensitive data;

    (2) granting assess rights to employees on a need basis, for instance, using role-based access control;

    (3) enabling account lockout function to prevent login by a user after multiple failed login attempts; and

    (4) reviewing logs of remote access to identify any suspicious activities.

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

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

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

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 on the Use of Video Conferencing Software

Introduction

1. Work-from-home (WFH) arrangements have been made from time to time during COVID-19 pandemic. As a result, video conferencing has fast become the new normal. The increasingly prevalent use of video conferencing software creates new risks to data security and personal data privacy[1].

2. This Guidance serves to provide practical advice to organisations and their employees to enhance data security and the protection of personal data privacy when they use video conferencing software. This Guidance is also applicable to other users of video conferencing software, such as teachers and students.

Practical guidance on the use of video conferencing software

3. Organisations (including business entities) should review and assess the policies and measures on security and protection of personal data privacy of different video conferencing software in order to choose the ones that meet their requirements. For example, organisations may wish to use a video conferencing software with end-to-end encryption if they cannot avoid using the software for discussing confidential matters.

4. Users of video conferencing software should pay heed to the following general security measures-

   (1) safeguard their user accounts by setting up strong passwords, changing the passwords regularly, and activating multi-factor authentication, if available;

   (2) ensure that the video conferencing software is up-to-date and the latest security patches have been installed; and

   (3) use reliable and secure internet connection for conducting video conferencing.

5. To ensure the security and protection of personal data privacy during a video conference, the host of the conference should-

   (1) set up a unique meeting ID as well as a strong and unique password for the conference; provide the meeting ID and the passwords to the intended participants only, and through different means (such as email and instant messaging), whenever possible;

   (2) where possible, arrange one more "host" (in addition to the main host who is chairing the meeting) to deal with administrative, technical and other contingent issues during the video conference;

[1] Data Protection Principle 4 in Schedule 1 to the Personal Data (Privacy) Ordinance (Cap. 486 of the Laws of Hong Kong) requires data users to take all practicable steps to protect the personal data they hold against unauthorised or accidental access, processing, erasure, loss or use.

(3) set up a virtual waiting room and validate participants' identities before allowing them to join the conference; "lock" the meeting when all participants have been admitted to prevent unauthorised access;

(4) only allow those participants who need to make presentations to share their screens or documents;

(5) inform all participants and obtain their consents before recording the conference; prohibit participants from recording the conference; and

(6) store the records of the conference (such as video recording and chat messages) securely, such as by using password protection or encryption and delete the records when they are no longer necessary.

6. For participants of a video conference, to protect their personal data privacy, they should-

(1) be aware of their backgrounds, which may be captured by their cameras and may reveal their personal or sensitive information to other participants; use virtual backgrounds if necessary;

(2) turn off the microphones (or even the cameras) when they are not speaking;

(3) avoid discussing personal or sensitive information during the video conference as far as practicable; and

(4) close unnecessary documents and windows (such as windows showing email accounts) before the sharing of screen to avoid disclosing sensitive information to other participants.

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

PCPD website

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**

Download this publication

First published in November 2020