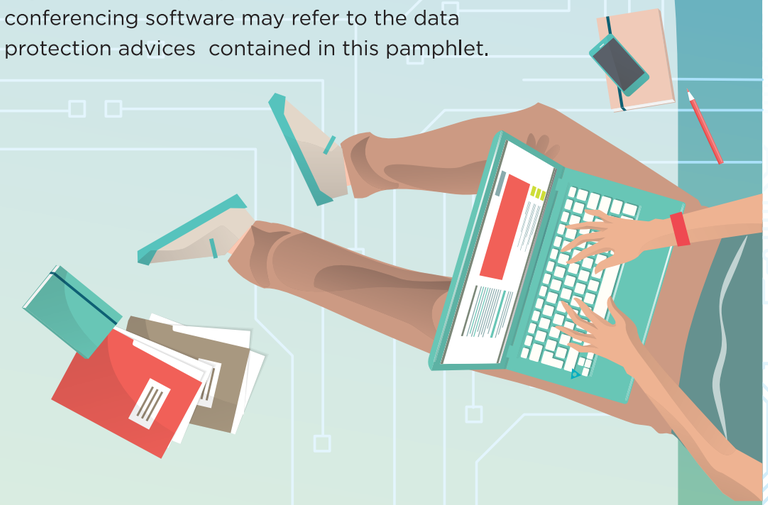
Introduction

Work-from-home (WFH) arrangements have been made from time to time during the COVID-19 pandemic. This inevitably increases risks to the security and privacy of personal data.

Organisations (including their employees) should enhance their awareness of and measures for data security and ensure that the handling of personal data complies with the requirements of the Personal Data (Privacy) Ordinance (Cap. 486). For this purpose, organisations, employees, and users of video conferencing software may refer to the data protection advices contained in this pamphlet.



For details, please refer to the three Guidance Notes issued by the Office of the Privacy Commissioner for Personal Data, Hong Kong, under the series "Protecting Personal Data under Work-from-Home Arrangements" for organisations, employees, and users of video conferencing software.

Download this publication:

Download the Guidance Notes:

Enquiry Hotline	2827 2827
Fax	2877 7026
Address	Room 1303, 13/F, Dah Sing Financial Centre, 248 Queen's Road East, Wanchai,Hong Kong.
Email	communications@pcpd.org.hk

Protecting Personal Data under Work-from-Home Arrangements

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

Organisations

1. Assess the risks to data security and personal data privacy in order to devise appropriate protection measures.

2. Provide employees with electronic devices (such as smartphones and notebook computers) as far as practicable and ensure that appropriate security settings are enabled for the devices.

3. Devise policies and guidance on the transfer of data and documents, remote access to the corporate networks and handling of data breach incidents.

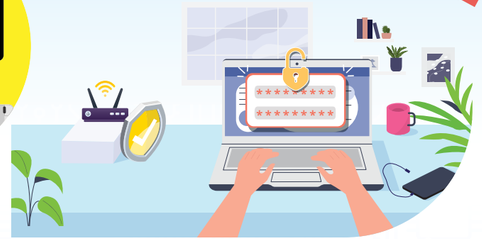
4. Ensure that appropriate security settings have been adopted for virtual private networks (VPNs) and activate multi-factor authentication.

5. Provide employees with appropriate training covering areas such as password management, encryption and awareness of cybersecurity threats.

Employees

1. Adhere to employers' policies on the handling of data.

2. Use only corporate electronic devices and email accounts for work as far as practicable.



3. Use wired network connections or secure Wi-Fi connections (such as those adopting WPA3 or WPA2 security protocols).

4. Avoid working in public places or using public Wi-Fi for work.

Users of video conferencing software

1. Choose the appropriate video conferencing software, such as the ones with end-to-end encryption.

2. Set up strong passwords for user accounts and activate multi-factor authentication.

3. Ensure that the video conferencing software is up-to-date and the latest security patches have been installed.

4. Set up a unique meeting ID and a strong password for each video conference.

5. Set up a virtual waiting room to validate participants' identities before the video conferences.