

54th APPA Forum (Virtual)

Future of remote work and learning: Privacy and cybersecurity challenges with remote working

“Remote Working: Symbiosis of Technology, Privacy and Security?”

9 December 2020 (Wednesday)

Tony LAM

Deputy Privacy Commissioner for Personal Data,
Hong Kong, China

PCPD



HK



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

Media Statements / Guidance issued by PCPD

Personal data
privacy
versus
mandatory
quarantine

Feb
2020

Fighting COVID-19 pandemic:
Advice for
Employers &
Employees

Mar
2020

Data Security of Video-
conferencing Software
/ Apps
&
Children's Privacy
during the Pandemic

Apr 2020

Cybersecurity
risks amid COVID-
19 pandemic

Jun
2020

Premise Operators
on Temperature
Measurement &
Collection of
Relevant Personal
Data

Jul
2020

Guidance on
protecting personal
data of teachers,
staff and students

Sep
2020

3 Guidance
Notes relating
to Work-from-
Home
Arrangements

Nov
2020

Our Data Protection Principles



1 Lawful purpose / purpose specification / data minimisation

2 Data accuracy / retention limitation

3 Use limitation

4 All practicable steps be taken on security

5 Openness / transparency

6 Data access / correction rights

Three Guidance Notes Relating to Work-from-home Arrangements

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

Guidance Note

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 arrangements¹; 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 employees².

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

Protecting Personal Data under Work-from-home Arrangements: Guidance for Organisations 1 November 2020

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

Guidance Note

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 process¹.

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

Protecting Personal Data under Work-from-home Arrangements: Guidance for Employees 1 November 2020

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

Guidance Note

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 privacy¹.
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.

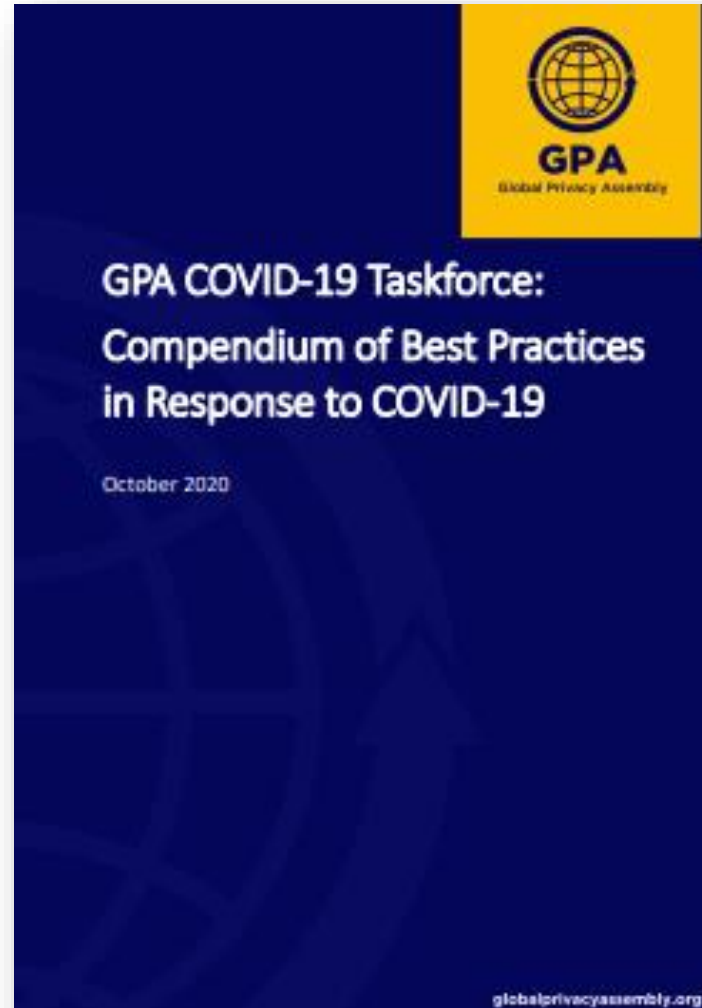
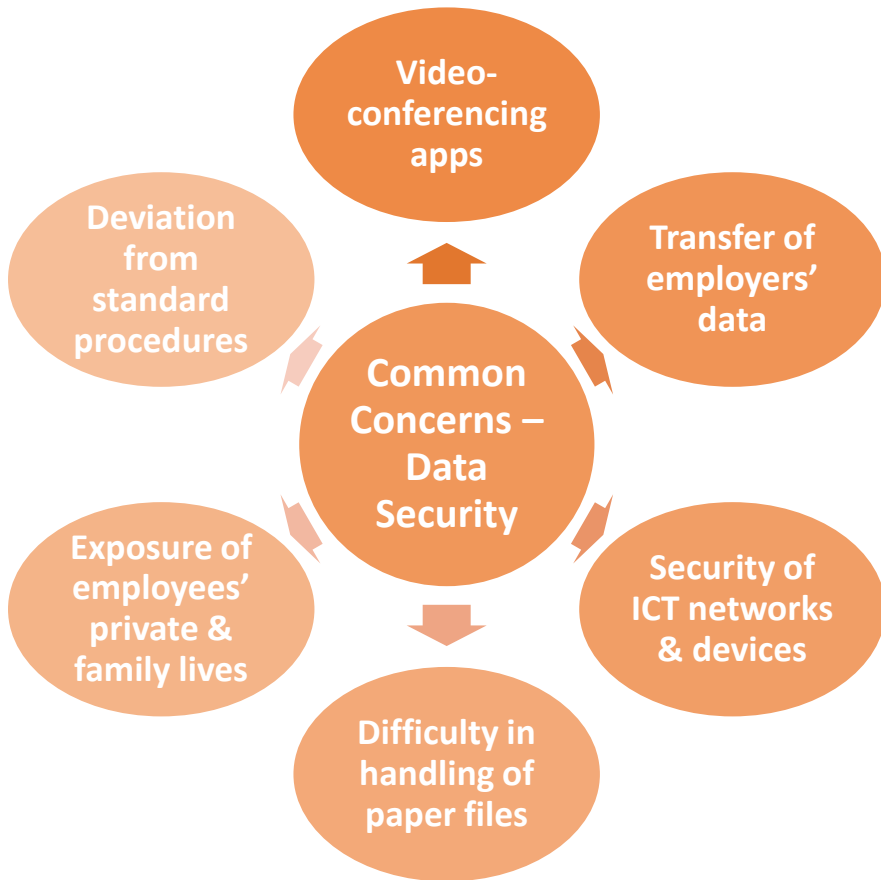
Practical guidance on the use of video conferencing software

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;

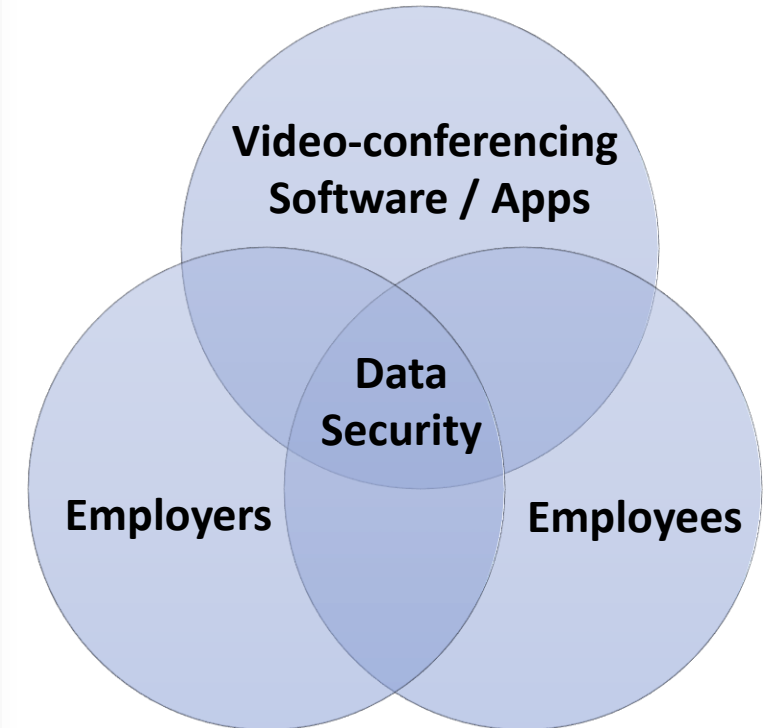
¹ Data Protection Principle 4 in Schedule 1 to the Personal Data (Privacy) Ordinance (Cap. 486 of the Laws of Hong Kong) requires data users to take all practicable steps to protect the personal data they hold against unauthorised or accidental access, processing, erasure, loss or use.

Protecting Personal Data under Work-from-home Arrangements: Guidance on the Use of Video Conferencing Software 1 November 2020

Remote Working – A Global Issue



Best Practices:



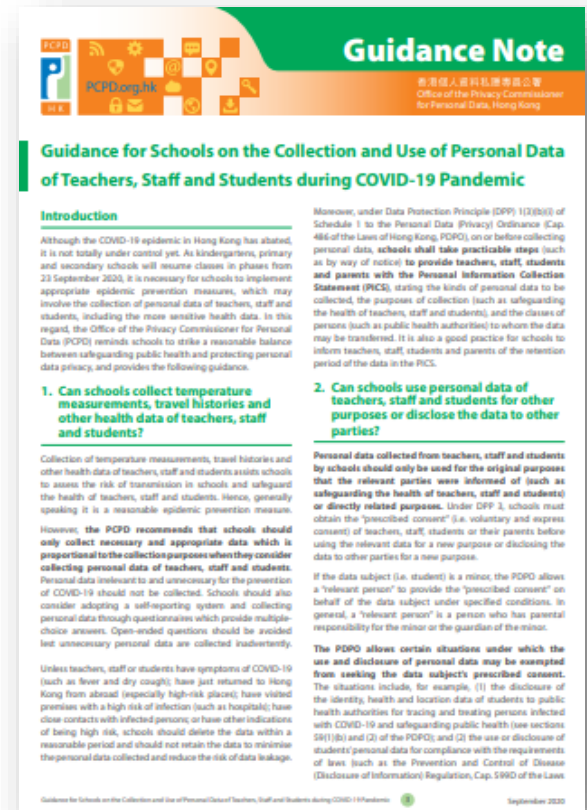
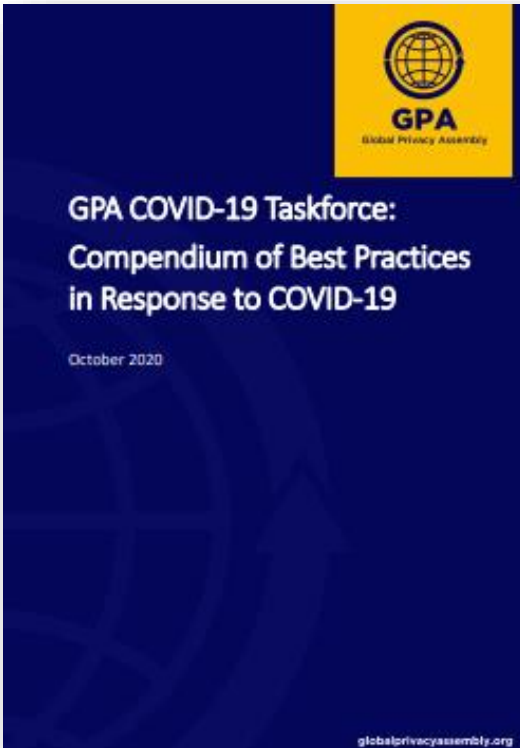
Return to work / schools

Common Concerns

- Proportionality
- Data security
- Use & disclosure of data
- Data retention period

Advice / Guidance

- Purpose well informed
- Self-reporting mechanisms preferred
- Practicable steps to ensure data security
- Disclose data only when necessary
- Destroy data when not necessary



Data Security & Personal Data Privacy

Network security determined by its weakest link

Manage both external and internal aspects

Human actors most unpredictable

Our Sharing Spinning

DIGITAL TRANSFORMATION

DIGITAL COMES FIRST

DATA UBIQUITOUS;
PERSONAL DATA PRIVACY EVER EXPECTED

Thank you

Website: www.pcpd.org.hk

E-mail: communications@pcpd.org.hk