



「混合式學習新常態： 學校資訊保安及數據管理」 網上研討會

2020 年11月5日

學校資訊保安框架

香港教育城行政總監 鄭弼亮先生
香港教育城科技部主管 雷正先生

01

「混合式學習下的學校資訊保安及數據管理」論壇

Microsoft 香港雲端技術員 湯文軒先生
天主教領島學校 李安迪校長
保良局王賜豪（田心谷）小學資訊
科技統籌教師 潘濬仁先生
香港教育城行政總監 鄭弼亮先生

03

在學習新常態下 保障個人資料私隱

香港個人資料私隱專員公署助理個人
資料私隱專員（公共事務）
謝敏傑先生

02

加強學校數據管理： 全新教城帳戶管理

香港教育城發展部主管
洪婉玲女士
香港教育城系統經理
李文傑先生

04



01

學校資訊保安框架



香港保安觀察報告 Hong Kong Security Watch Report

HKCERT is pleased to bring to you the "Hong Kong Security Watch Report" for the second quarter of 2020.

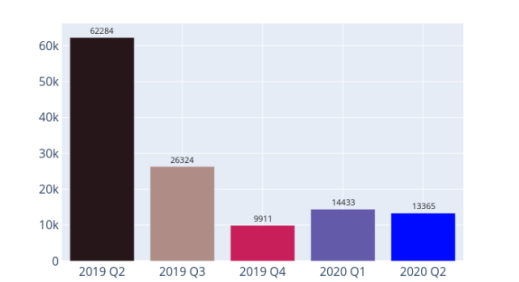
Nowadays, many networked digital devices, such as computers, smartphones, tablets, are being compromised without the user's knowledge. The data on them may be mined and exposed every day, and even be used for various criminal activities.

The Hong Kong Security Watch Report aims to raise public awareness of the problem of compromised systems in Hong Kong, enabling them to make better decision in information security. The data in this quarterly report focuses on the activities of compromised systems in Hong Kong which suffer from, or have participated in various types of cyber attacks, including web defacement, phishing, malware hosting, botnet command and control centres (C&C) or bots. "Computers in Hong Kong" refer to those whose network geolocation is Hong Kong, or the top level domain of their host name is ".hk" or ".香港".

Highlight of Report

In 2020 Q2, there were 13,365 unique security events related to Hong Kong used for analysis in this report. Data were collected through IFAS¹ with 10 sources of information², and not collected from the incident reports received by HKCERT.

Trend of security events




「混合式學習新常態」

Ensure on-premise security controls still apply to systems when they are not on the internal network.

<https://www.pwccn.com/en/issues/cybersecurity-and-data-privacy/covid-19-impact-mar2020.pdf>

Managing the impact of COVID-19 on cyber security

The COVID-19 outbreak has been declared a pandemic by the World Health Organisation, causing huge impact on people's lives, families and communities. This has had an immediate effect on organisations, changing the ways employees work and bringing with it new cyber risks.

As the international response continues to develop, we know that organisations are facing potentially significant challenges to which they need to respond rapidly. Many organisations and employees are needing to rethink ways of working in light of considerable operational and financial challenges. Without appropriate considerations, this could fundamentally increase the risk of cyber security attacks.

We are seeing both the likelihood and impact of cyber attacks increasing and cyber security good practices may fall by the wayside as organisations become more technology dependent than ever. We are also beginning to see the nature of the threat changing, as attackers exploit uncertainty, unprecedented situations, and rapid IT and organisational change.

Organisations should take three key actions to mitigate these emerging risks:

1

Secure their newly implemented remote working practices.

2

Ensure the continuity of critical security functions.

3

Counter opportunistic threats that may be looking to take advantage of the situation.

• Policies, Standards, Guidelines, Procedures

Policies

- Principles, intentions, directional
- Clearly defines **AUTHORITIES, ROLES and RESPONSIBILITIES**

Standards

- Compliance – device standards, Windows version

Guidelines

- More detail description to guide operation

Procedures

- Detailed step - by - step instructions that should be followed



Roles and Responsibilities

Information Security in Schools - Recommended Practice (Sept 2019) Chapter 2 Security Management

- 2.4.3 Set up and Implement
Management and Administrative
Processes

(a)(i) Assign roles and responsibilities

- ✓ School Management
- ✓ IT Head
- ✓ IT Committee Members
- ✓ Technical Support Staff

Chapter 1	About this Document
Chapter 2	Security Management
Chapter 3	Security Incident Handling
Chapter 4	Physical Security
Chapter 5	Access Control
Chapter 6	Data Security
Chapter 7	Network and Communication Security
Chapter 8	Website & Web Application Security
Chapter 9	Mobile Device and Mobile Application Protection
Chapter 10	Malware Protection
Chapter 11	Cloud Service
Chapter 12	Resources of Reference on IT Security

<https://www.edb.gov.hk/en/edu-system/primary-secondary/applicable-to-primary-secondary/it-in-edu/Information-Security/information-security-in-school.html>



	Responsibilities
Incorporated Management Committee (IMC)	<ul style="list-style-type: none"> • Approve policies • Delegate authority to Principals • Risk Management • Crisis Management
IT Committee under IMC	<ul style="list-style-type: none"> • Delegated with the above duties by the IMC
School Supervisor	<ul style="list-style-type: none"> • Execution and Monitoring of the above
School Principal	<ul style="list-style-type: none"> • Implement IS policy • Resource (budget, manpower) provision • Overall responsibilities covering IT and non-IT
IT Head (Information Security Officer)	<ul style="list-style-type: none"> • Overall responsibility of IT related issues • Implement the IT infrastructure and procedures accordingly • Formulate IT guidelines and procedures
IT technical staff	<ul style="list-style-type: none"> • Carry out duties according to guidelines and procedures
Teachers with IT related duties (sensitive data, privileged accounts)	<ul style="list-style-type: none"> • Understanding the guidelines and procedures related to their special duties
Teacher Users	<ul style="list-style-type: none"> • Follow the guidelines and procedures • Comply with legal requirements • Comply with teacher code of conducts
Student Users	<ul style="list-style-type: none"> • Understand AUP • Comply with school requirements for students (conduct, discipline) • Comply with legal requirements



• IMC and Principal

- Conduct Risk Assessment
- Develop IS Policies
- Assign Roles and Responsibilities
- Monitoring and Review



• Related Legislations

- Access to computer with criminal or dishonest intent
- Theft and damage of property (digital assets)
- Personal data protection
- Copyright / IP rights
- Software Asset Management
- Digital marketing and unsolicited electronic messages
- Electronic Transactions Ordinance
- Safety in the use of Display Screen Equipment



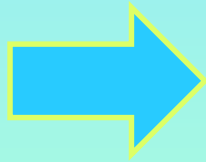
FOR IT HEAD- Infrastructure and Systems Related

- **Network** Security – private network, remote access
- **Server** security – patch and upgrades, rights management
- **Classifying** sensitive data (personal data, mailbox, exam papers etc.)
- Managing **file** storage, backup and cloud services, IT **Assets** (keys)
- Security in IT Procurement and Service Contracts, **third party services**
- Managing Technical **Support Staff** – security training, procedures, monitoring
- Reviewing system statistics and **logs**
- Managing privileged / **admin accounts**
- Managing staff / student **accounts**



Security - as - a - Service

- ISO 27001 / IS Policy
- Network Security (router, firewall, VPN, VLAN..).
- Server / Web / Cloud Security
- Application / App Security
- Data / File Security
- Forensics
- Related Laws
- *COVID-19 – remote everything*
- ...



- **Security - as - a - Service**
 - Policy
 - Health Check
 - Implementation
 - Incident Management
 - Audit & Review
 - Training



Handling Staff Accounts

Use school provided accounts instead of personal accounts (e.g. Google, Yahoo)	✓
Use school provided email instead of personal emails	✓
Automatic removal of accounts after staff / student leaving	✓
Only school created accounts can access student data	✓



Handling Personal Data

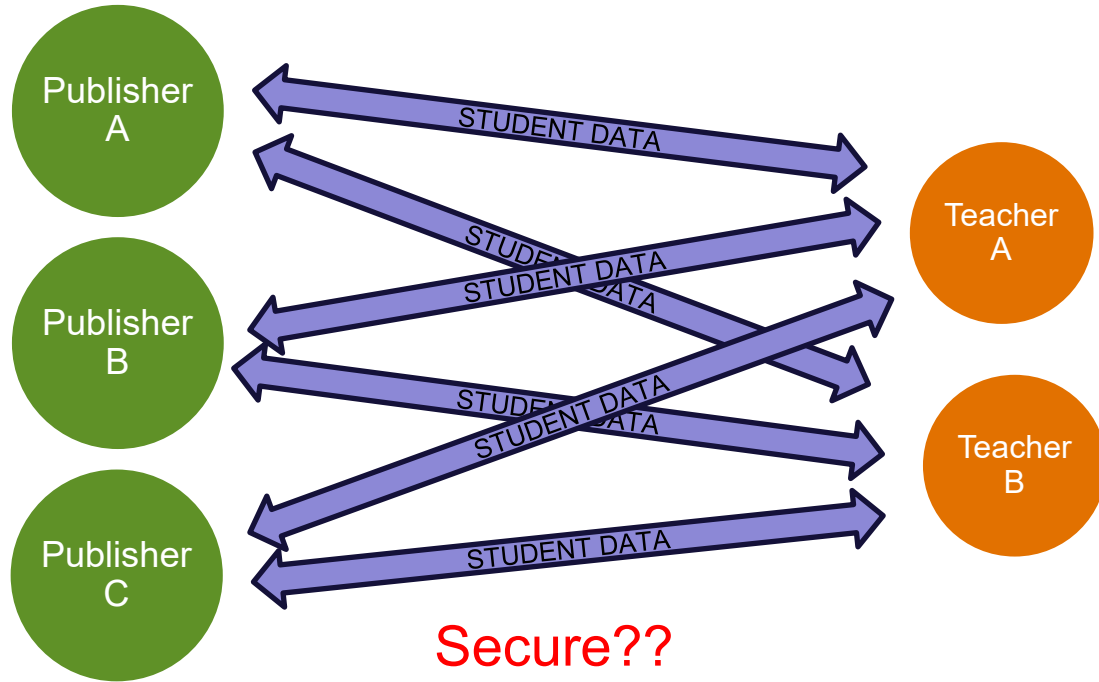


Personal Data Handling

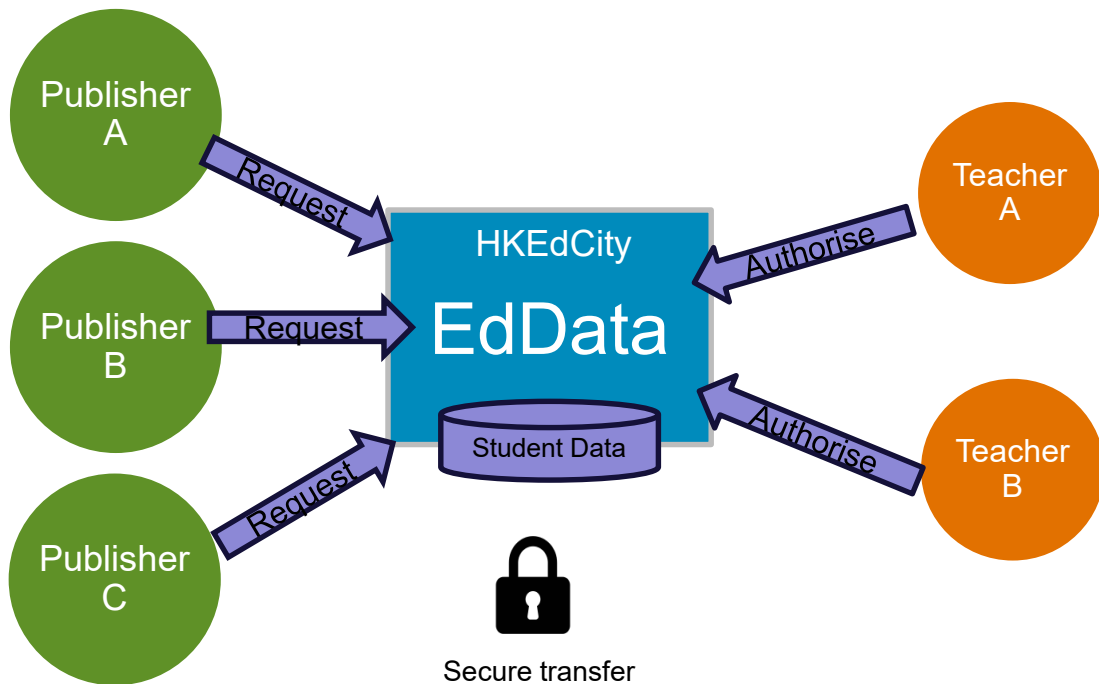
- Collection – PICS / Consent Form
- Minimum data – no unnecessary HKID, address, phone in student list, email, reports etc.
- Encryption – in storage, processing and transmission
 - Especially : USB, email, Excel
- Hash Key – Integrity of data
- **Transfer to third parties (e.g. publishers)**



Personal Data Handling



Personal Data Handling












Third Party Data Transfer Checklist

Agreement with third parties on purpose and usage of personal data	✓
Clear authority on who can transfer data	✓
Encryption in storage and transmission	✓
Hash Key to protect integrity and reduce liability	✓
Contractual rights to request removing data upon request	✓
Clear record of who transferred the data	✓
Choose what data fields to be transferred	✓
Clear record what data has been transferred	✓
Secure transfer system (not email, WhatsApp etc).	✓



EdData – facilitate third party data transfer

Checklist for Effective and Secure Data Access			
Task	Responsible Parties		
	Publishers / Providers	HKEdCity	Schools
<ul style="list-style-type: none"> Signing of Agreement, that clearly states <ol style="list-style-type: none"> 1) The purpose and usage of personal data 2) The contractual rights to request for data removal (Revoke Function) 			
<ul style="list-style-type: none"> Clear authority on who can transfer data 			
<ul style="list-style-type: none"> Choose what data needs to be accessed 			
<ul style="list-style-type: none"> Choose to approve what data to be accessed 			
<ul style="list-style-type: none"> Provide a safe data transfer platform, including <ol style="list-style-type: none"> 1) Encryption in storage and transmission 2) Hash Key to protect integrity 			
<ul style="list-style-type: none"> Provide a comprehensive and clear data transfer logs, listing out the data access details 			
<ul style="list-style-type: none"> Check publishers' / providers' data access details from the data transfer logs 			



THANKS!

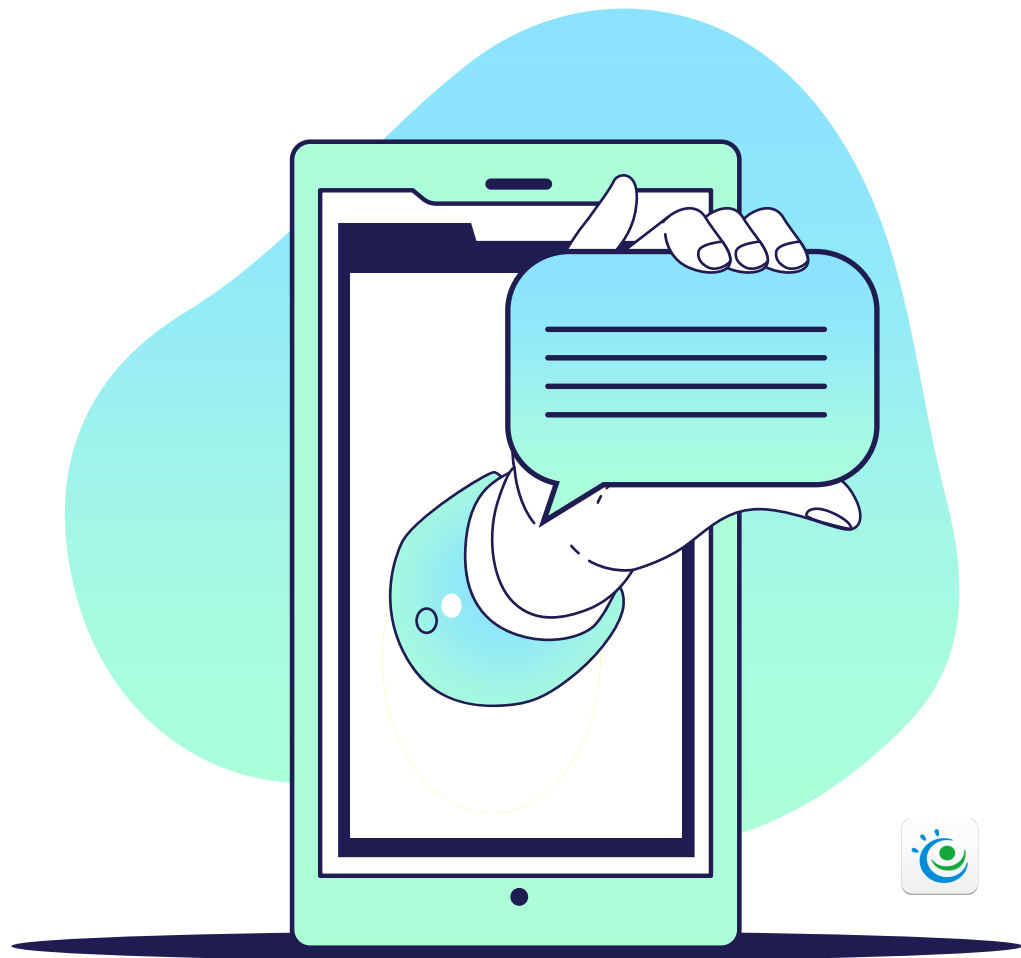
查詢

熱線: +852 2624 1000

電郵: info@hkedcity.net

網站: www.hkedcity.net

CREDITS: This presentation template was created by **Slidesgo**, including icons by **Flaticon**, infographics & images by **Freepik** and illustrations by **Stories**



04

加強學校數據管理： 全新教城帳戶管理

- 概念
- 示範



帳戶管理的挑戰

學校管理層

- 整體的帳戶管理策劃
- 負責同工的權責
- 確保帳戶定時更新

學校管理員

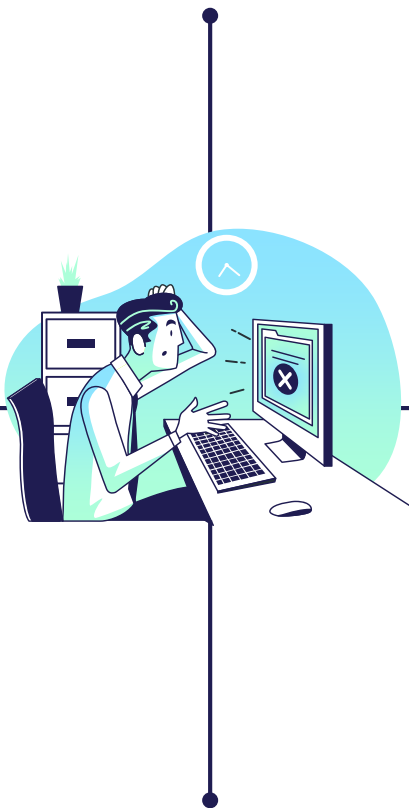
- 劃一帳戶管理
- 定時更新帳戶
- 支援師生適時使用電子資源

教師

- 不同平台的帳戶管理
- 學校及個人帳戶的混淆
- 適時使用電子資源

學生

- 不同平台不同帳戶
 - 忘記密碼
- 適時使用電子資源



全新教城帳戶管理 - 「校本教師帳戶」

目的

- 。加強保障只有授權的帳戶使用校本服務及閱取學生數據
- 。協助學校能更簡易安全地管理全校教師的帳戶



「校本教師帳戶」的特色

「校本教師帳戶」

統一為全校 教師開設

- 以教師持有的學校電郵登記
- 管理權屬於學校
- 管理員可重置或更改教師帳戶密碼，或新增、移除個別帳戶

教師帳戶需每學年更新

因應每學年的教 師任職情況更新

- 管理員按指示於系統上載相關資料，所有帳戶會即時更新，逾期帳戶會被移除
- 帳戶只在開設或更新的學年內有效，以提高帳戶的安全性及可靠性

學校無需批准連結「個人教師帳戶」

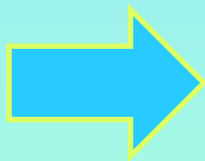
只需透過「校本 教師帳戶」建立 帳戶

- 在新系統推出前，已於教城開設的「個人教師帳戶」並已由學校批准連結學校的帳戶將不受影響
- 鼓勵學校逐步以「校本教師帳戶」取代「個人教師帳戶」



「個人教師帳戶」轉移為「校本教師帳戶」 - 教師使用帳戶的變動

- 以教城帳號 / 登入電郵或學校電郵登入
- 自行更新個人資料，如姓名
- 帳戶與e- Services 電郵連結
- 當離職後，除了校本服務，教師可繼續以帳戶使用非校本服務



- 以學校提供的教城帳號 / 學校電郵登入
- 學校的教城帳號以 <school_code>開始, 例如：
ntc-xxxx
- 個人姓名不可自行更新
- 學校管理員可協助重設密碼
- 當離職後，教師將不能繼續使用該帳戶



推行時間表

1/2021開始

協助「個人教師帳戶」
轉移為「校本教師帳戶」



28/10/2020

推出「校本教師帳戶」



8/2021

所有學校全面推行
「校本教師帳戶」



首階段 (28/10/2020 開始)



學校管理員

1. 於會員系統上載教師資料：
 - 為加入學校電郵
 - 開設新的教師帳戶
 - 設定帳戶到期日
2. 移除不適當帳戶



已由學校批准連結學校的
的「個人教師帳戶」

不受影響



新入職或未有帳戶的教師

向學校索取「校本教師帳戶」



下階段 (1/2021開始) - 「個人教師帳戶」轉移為「校本教師帳戶」



校長

決定：

1. 全校採用「校本教師帳戶」
2. 轉移的時間表



學校管理員

執行「個人教師帳戶」轉移為「校本教師帳戶」



已由學校批准連結學校的「個人教師帳戶」

1. 決定是否轉移為「校本教師帳戶」或繼續保留現有帳戶
2. 將有關教學資源*轉移至新的「校本教師帳戶」

*教學資源的覆蓋及轉移方法將稍後通知





04

示範



● 你的寶貴意見

<https://bit.ly/360Fg3c>



THANKS!

查詢

熱線: +852 2624 1000

電郵: info@hkedcity.net

網站: www.hkedcity.net

CREDITS: This presentation template was created by **Slidesgo**, including icons by **Flaticon**, infographics & images by **Freepik** and illustrations by **Stories**

