香港教育城 HKedCity

www.hkedcity.net

Policies and Framework for Privacy and Information Security in School

私隱及資訊保安 - 政策和框架

25 September 2019

Information Security Management System

- Based on ISO 27001
  - (US : NIST)
- Describe “organised approach” – whole school
- Based on Risk Management
- Address Confidentiality, Integrity and Availability
- Anchor on :
  - People, Process, IT System

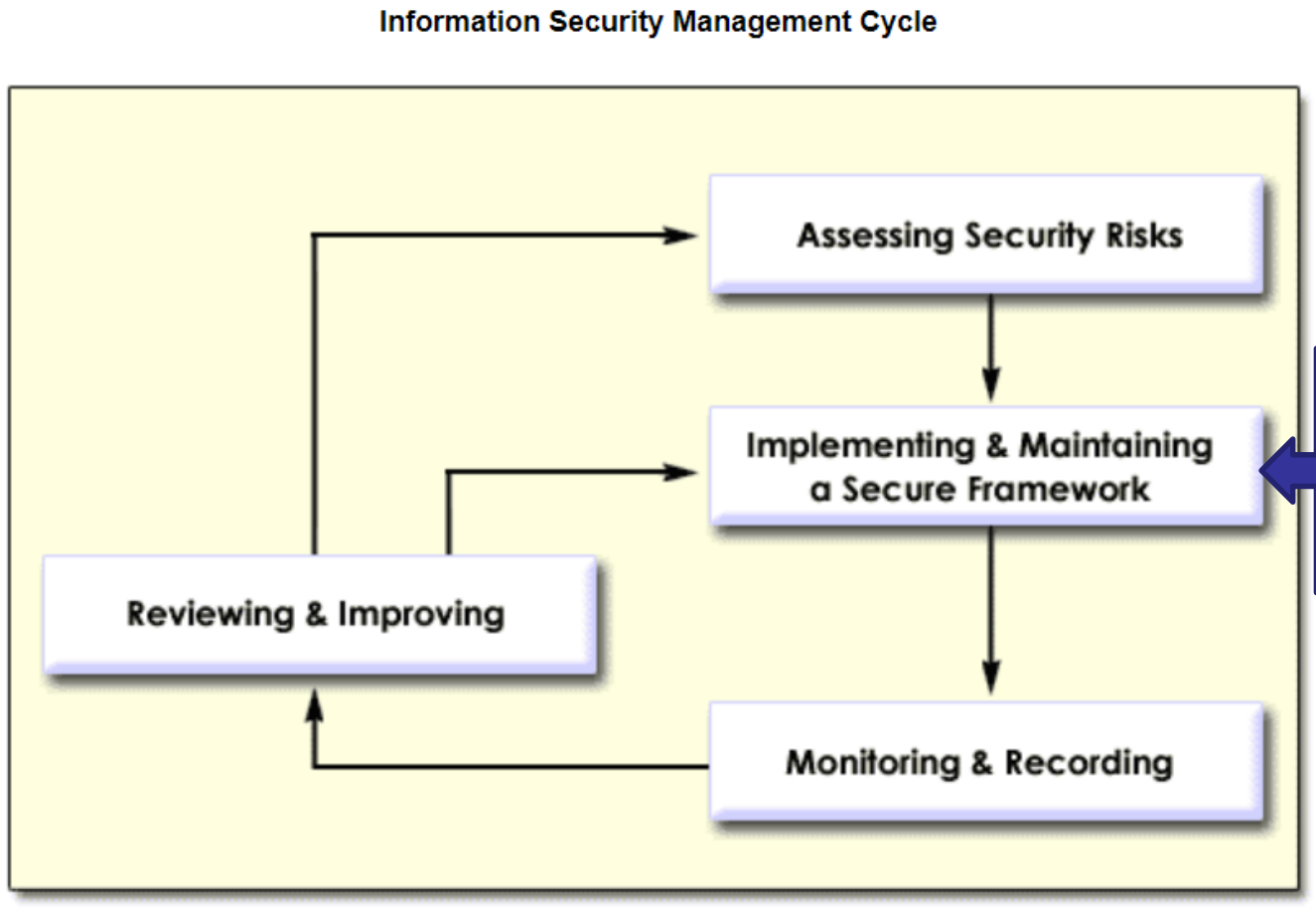
https://www.anitechconsulting.com.au/what-is-isms-and-how-will-it-impact-your-business/

香港教育城 HKedCity

ISMS Key Issues

- Risk Management
- Information Security Policy
  - Roles and Responsibilities
  - Controls, Technical Implementation
  - Guidelines, Procedures

Information Security Management Cycle



Source :
https://www.infosec.gov.hk/english/business/security_smc.html

Risk Assessment – School Example

Confidentiality	Integrity	Availability
Student Data	Accounting	Network / WiFi
Teacher / HR Data	Payroll	School email system
Exam papers	Exam Grades / Assessment Data	Admin / Learning Systems

香港教育城 HKedCity

Risk Registry

Vulnerabilities	Impact	Likelihood	Risk Level
Student Data	High	High	High
Payroll Data	Medium	Medium	Medium
Exam papers	High	Medium	High
Attendance Record	Low	Low	Low

Risk Mitigation Analysis - States

Description	Storage	Processing and I/O	Transmission
Student Data	eClass server, WebSAMS, Cloud Storage Backup, USB, Paper Document	Excel, Server, Paper Form Filling	School network, public network, Email, File sharing, Paper mails
Payroll	Payroll System, School Server, Paper forms	Payroll System, Excel, Calculator	LAN only, Letter distribution
Exam papers	Teacher Personal Storage School Server	MS Office Other editing tools Grading Tools	LAN only, Paper distribution

Related Legislations

- 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

Policies, Standards, Guidelines, Procedures

Policies

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

Standards

- Compliance – data centre, encryption

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

Details:
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)	• Approve policies • Delegate authority to Principals • Risk Management • Crisis Management
IT Committee under IMC	• Delegated with the above duties by the Council
School Supervisor	• Execution and Monitoring of the above
School Principal	• Implement IS policy • Resource (budget, manpower) provision • Overall responsibilities covering IT and non-IT
IT Head (Information Security Officer)	• Overall responsibility of IT related issues • Implement the IT infrastructure and procedures accordingly • Formulate IT guidelines and procedures
IT technical staff	• Carry out duties according to guidelines and procedures
Teachers with IT related duties (sensitive data, privileged accounts)	• Understanding the guidelines and procedures related to their special duties
Teacher Users	• Follow the guidelines and procedures • Comply with legal requirements • Comply with teacher code of conducts
Student Users	• 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

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

Use school provided accounts instead of personal accounts (cloud account)	✓
Use school provided email instead of personal emails	✓
Automatic removal of rights after staff / student leaving	✓
Not using real name with third party systems	✓

香港教育城 HKedCity

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)

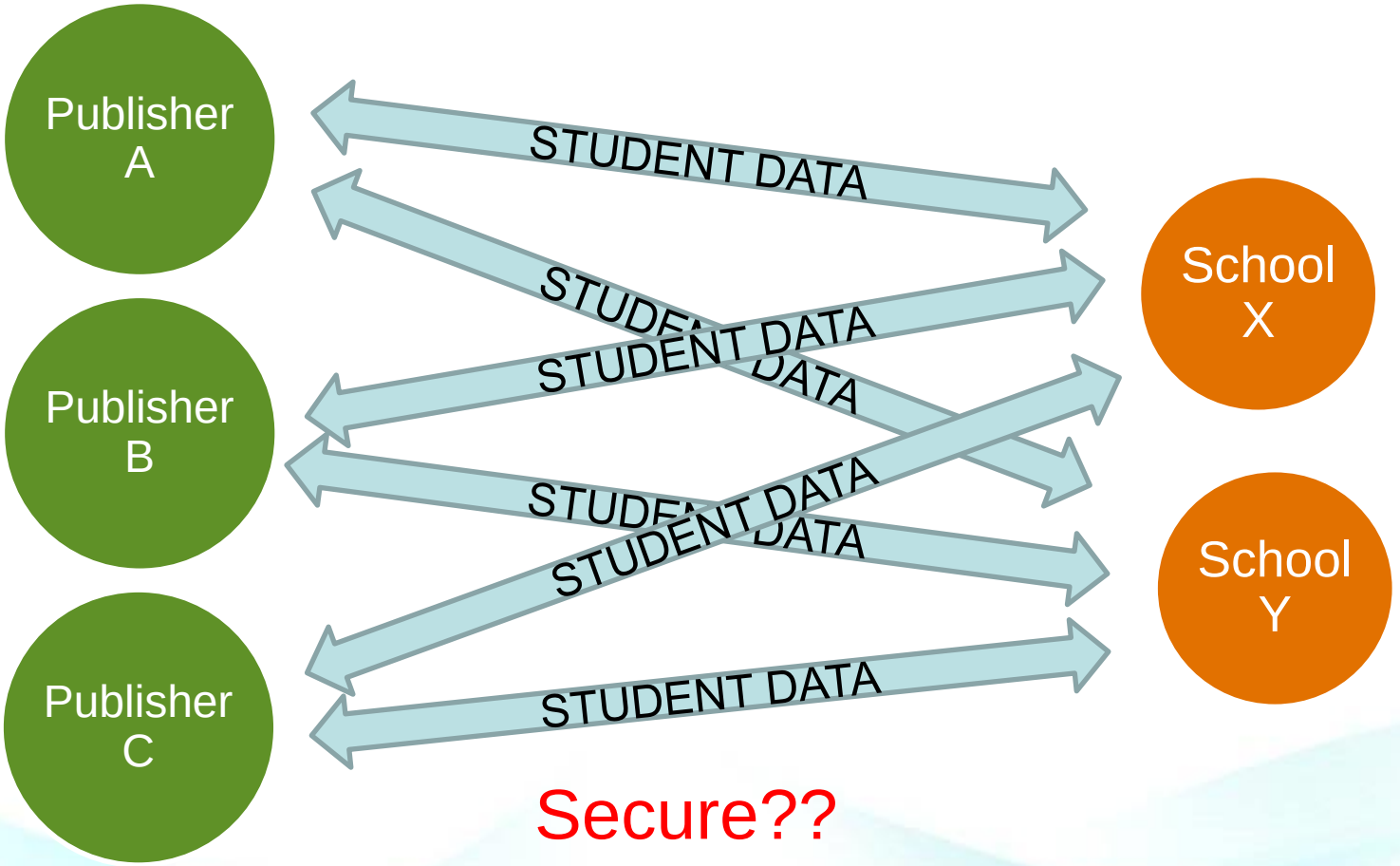
香港教育城 HKedCity

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).	✓

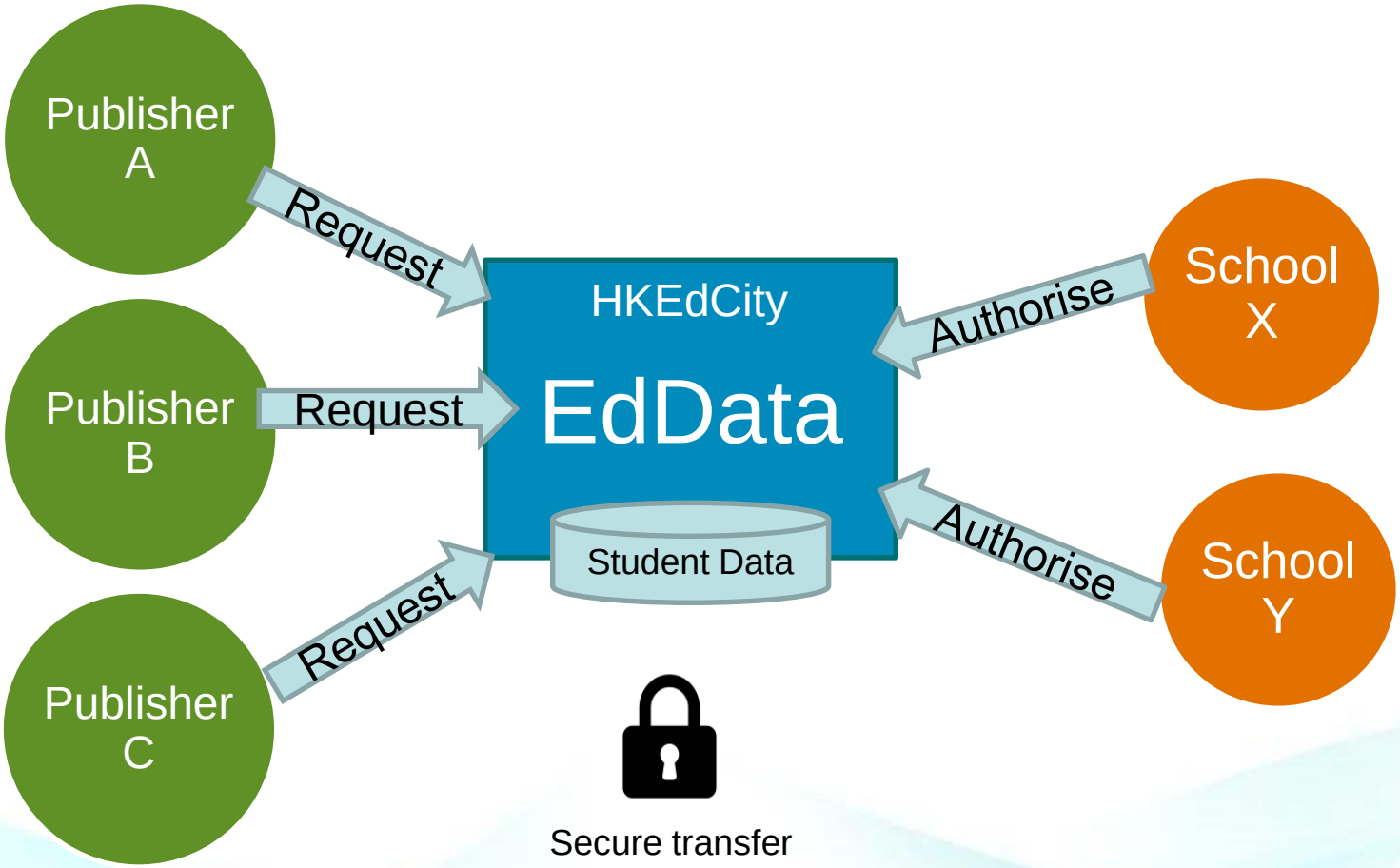
香港教育城 HKedCity

Transfer of Student Data

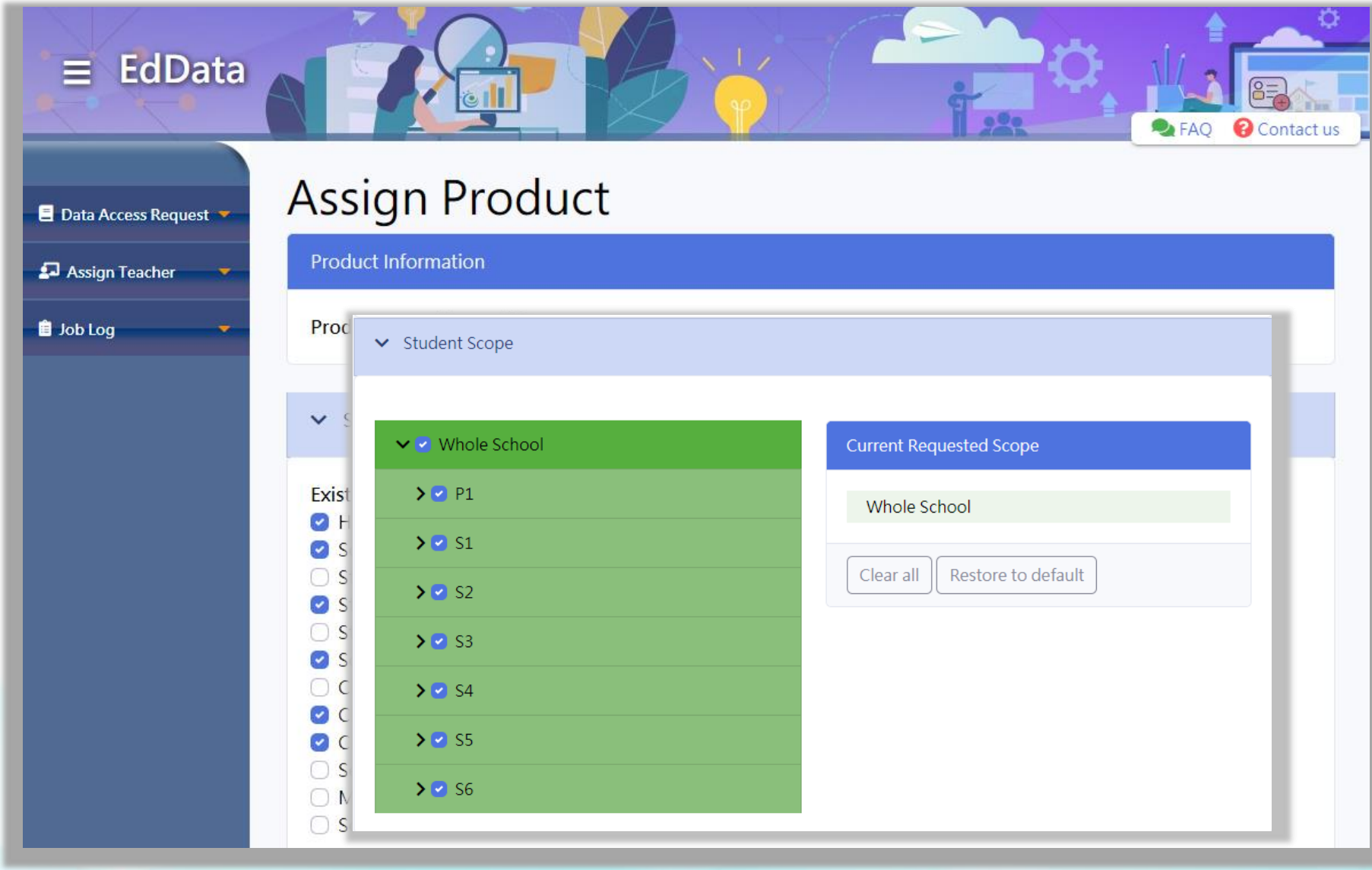


Secure??

EdData


Publisher A
Publisher B
Publisher C
Request
Request
Request
HKEdCity
EdData
Student Data
Authorise
Authorise
School X
School Y
Secure transfer

EdData


EdData
FAQ
Contact us
Data Access Request
Assign Teacher
Job Log
Assign Product
Product Information
Student Scope
Whole School
P1
S1
S2
S3
S4
S5
S6
Current Requested Scope
Whole School
Clear all
Restore to default

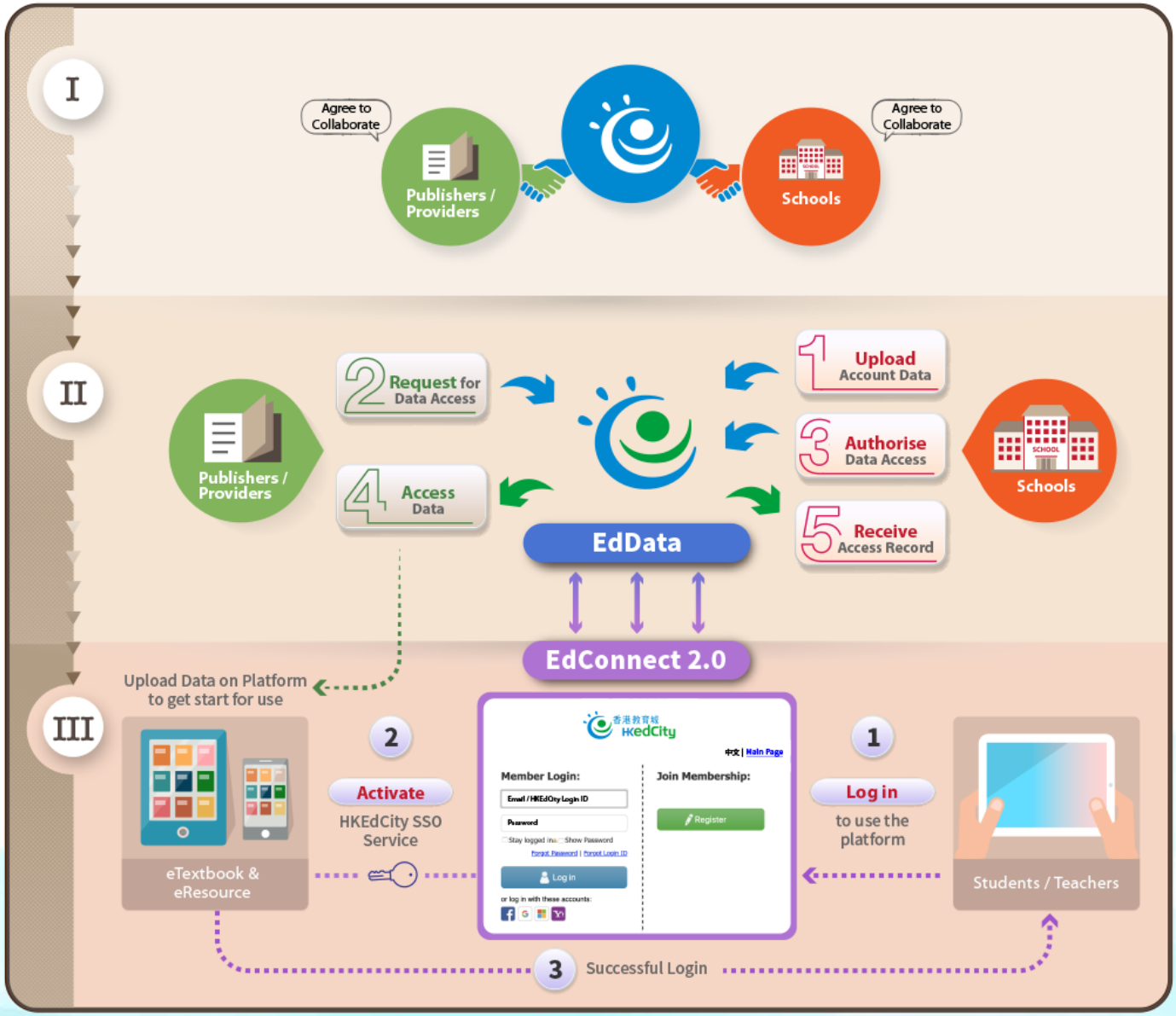
香港教育城 HKedCity

EdData

Checklist for Effective and Secure Data Access

Task	Responsible Parties: Publishers / Providers	HKEdCity	Schools
Signing of Agreement, that clearly states 1) The purpose and usage of personal data 2) The contractual rights to request for data removal (Revoke Function)	✓	✓	✓
Clear authority on who can transfer data			✓
Choose what data needs to be accessed	✓		
Choose to approve what data to be accessed			✓
Provide a safe data transfer platform, including 1) Encryption in storage and transmission 2) Hash Key to protect integrity		✓	
Provide a comprehensive and clear data transfer logs, listing out the data access details		✓	
Check publishers' / providers' data access details from the data transfer logs			✓

Technical Framework to Strengthen Privacy & Security



More info: https://www.hkedcity.net/eddata/

香港教育城
HKedCity

-END-

Thank you