Joint Universities Computer Centre Limited (“JUCC”)

Information Security Awareness Training- Session Three

Privacy and Personal Data

Agenda

Overview of Privacy and Personal Data

- Definition of personal data
- Personal data in universities

Roles and Responsibilities in Privacy and Personal Data

Privacy Ordinance and Relevant Regulations

- Hong Kong Personal Data (Privacy) Ordinance
- Six data protection principles
- Practicing the data protection principles

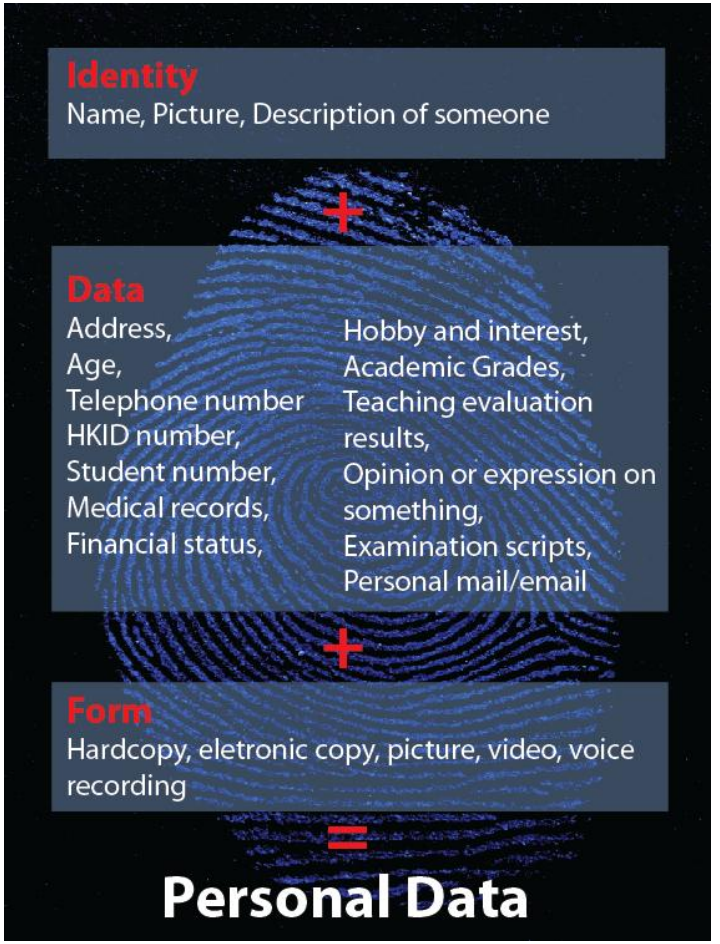
Case Study on Data Leakage in Universities

Protecting Data while Surfing the Internet

Overview of Privacy and Personal Data

Definition of Personal Data

- Relating directly or indirectly to a living individual
- From which it is practicable for the identity of the individual to be directly or indirectly ascertained
- In a form in which access to or processing of the data is practicable



Personal Data in Universities

- Any data relating directly or indirectly to a living individual
  - Name and HKID card number;
  - Address and telephone number;
  - Student number and examination transcripts;
  - The details of your academic research project;
  - Teaching evaluation results;
  - Your opinion or expression in sensitive topics;
  - Religious views;
  - Medical records and financial status; and
  - The personal data of others obtained through academic research (e.g. personal data obtained through surveys, interviews or other information gathering techniques).

Definition of Privacy

- A concept applies to Data Subject (a living individual to whom personal data relates)
- The agreed protection of personal data
- The right of an individual to decide who has access to his personal information and how that information should be used
- Privacy not only guarantees the confidentiality of data, but also data's level of privacy

Roles and Responsibilities

- Data owners, data custodians and users should be defined for each type of personal data
  - Consider establishing a roles and responsibility matrix
  - For employees, job duties should state the type of data that person is responsible for

Roles and Responsibilities in Privacy and Personal Data

Data Owners

- Authority to collect, create, retain and maintain information and information systems within their assigned area of control
- Usually senior personnel or faculty unit managers
- Responsibilities include:
  - Assigning custody of the information
  - Authorising access to the Information
  - Specifying controls to ensure confidentiality, integrity and availability
  - Communicating the control requirements to the data custodian and users of the information

Roles and Responsibilities in Privacy and Personal Data

Data Custodians

- Responsible for the administration of controls as specified by the data owner
- Tasks include:
  - Implementing physical and or technical controls
  - Administering access to information
  - Ensuring the availability of information

Data Users

- Granted explicit authorisation by the relevant Data Owner to access, alter, destroy, or use information within an information system
- Responsible for:
  - Using the information only for the purpose intended by the owner
  - Complying with all controls established by the owner and custodian
  - Ensuring that classified or sensitive information is not disclosed to anyone without permission of the owner

Example - Roles and responsibilities of student records

- **Data Owner**
  - Head of Student Records

- **Data Custodian**
  - Student Records Officer
  - Administration Officer

- **Data User**
  - Student (which the information belongs to)
  - Teachers

Hong Kong Personal Data (Privacy) Ordinance

Objectives

To protect the privacy interests of living individuals in relation to personal data. It also contributes to Hong Kong's continued economic well being by safeguarding the free flow of personal data to Hong Kong from restrictions by countries that already have data protection laws.

Scope of Coverage

The Ordinance covers any data relating directly or indirectly to a living individual (data subject)… It applies to any person (data user) that controls the collection, holding, processing or use of personal data.

The Six Data Protection Principles

- Principle 1: Purpose and manner of collection of personal data
  - Collect personal data for a lawful purpose and by fair means
  - Purpose of collection must be directly related to a function or activity of the data user
  - No excessive collection of data

The Six Data Protection Principles

- Principle 2: Accuracy and duration of retention of personal data
  - Keep data accurate and up-to-date and no longer than its necessary period

The Six Data Protection Principles

- Principle 3: User of personal data
  - Use data for the purpose stated at the time of collection or for a directly related purpose
- Principle 4: Security of personal data
  - Apply appropriate safeguard for data protection
  - Protect the data from unauthorised access

The Six Data Protection Principles

- Principle 5: Information to be generally available
  - Openness about what kinds of data is hold and the main purpose of using it.
- Principle 6: Access to personal data
  - Make data access and data correction requests in respect of individual’s personal data

Practicing the data protection principles

Obtain Consent

- Obtain consent before acquiring, holding or using personal data
- Include a statement explaining the following when gathering personal data:
  - which kind of data is to be used for?
  - who will access the data?
- Keep and use data strictly only on the necessary purpose especially for sensitive data

Practicing the data protection principles

Records Handling

- Review files regularly and discard unnecessary or obsolete data
- Delete unnecessary electronic records
- Do not give away or sell university computers or data storage media
- Shred unnecessary paper records
- Dispose data securely
- Implement security measures to protect data (e.g. Locked file cabinets, password and encryption, clean desk policy, etc)

Practicing the data protection principles

Maintain Data Accuracy

- Keep all personal data up-to-date and accurate
- Responsibilities of staff
  - Provide accurate and up-to-date personal information to the University
  - Inform the University of any errors or changes to information which they have provided

Practicing the data protection principles

Third Party Data Processor

- Establish a written contract on information confidentiality and security between university and the third party processor
- Non-disclosure agreement
- Compliance with the Personal Data (Privacy) Ordinance

Individual Staff/ Student Rights

- Maintain an open attitude with staff/ students regarding the personal data being held about them

Data Disclosure

- Obtain consent of the data subject before revealing the personal data to the 3rd party
- Can only disclose student data to the 3rd party which is used for students' studies and to meet regulation requirements
- Handle all the requests for the personal data carefully and ensure they are genuine and legitimate

Practicing the data protection principles

Research

- Personal data collected for research complied with university's data protection rules and the Personal Data (Privacy) Ordinance
- Do not keep personal data longer than is necessary for the purpose (Principle 2)
- Use the obtained personal data only for the purpose stated at the time of collection (Principle 3)
- Researcher should consider:
  - Obtain minimum amount of data
  - Clear academic objective?
  - Security over data storage
  - Duration of data retention period
  - Anonymous data

Examination Results

- Obtain consent from students concerned before publishing
- Do not publish list of student names and candidate numbers if the department wishes to publish examination results with exam candidate numbers
- Authentication is required if a student wants to obtain the results by telephone

Feedback on Teaching and Training

- Regarded as personal data of the teacher
- Obtain permission from the data subject who provided the information before disclosing it or keep information identity anonymous

Marketing Information

- Do not disclose personal data to marketing organisation without permission from data subject
- The personal data should only be used for the purpose stated at the time of collection (Principle 3)

Practicing the data protection principles

- In general, the university should
  - Always use student number instead of HKID number
  - Provide guidelines and regular training to staff on personal data protection
  - Always comply with the Personal Data (Privacy) Ordinance

Case Study on Data Leakage in Universities
Case 1

Disclosure of teaching evaluation results to students

- Evaluation results = personal data of the teacher
- Personal data may not be used for a purpose other than the purpose of the data where to be used when they were collected
- Can be disclosed to all students?

Disclosure of teaching evaluation results to students

- Possible Solutions
  - Acknowledge the purpose of teaching evaluation result disclosure for which the data concerned are collected
  - Notice those individual before disclosing the result

Examination Scripts

- Generally not considered as personal data
- No specific retention time limit imposed
- Exception:
  - The answers require personal information
  - Examination scripts contain comments or evaluation of the student’s answer

Case 2 (cont' d)

Recommendation on Examination Scripts

- Mark comments on separate mark sheet instead of the examination script
- Keep records until academic appeal has completed

Protecting Data while Surfing the Internet

Recommendations on using shared computer

(*Shared computers include public computers in the library, computer labs, canteens and other public areas.*)

- Don't check the "Remember My ID" box;
- Don't save passwords;
- Always remember to logoff using the logoff button;
- Get into the habit of changing passwords frequently (every 90 days);
- Delete the contents of the browser's cache;
- Don't trust the bookmark of the browser, always key in the URL;
- Don't login to a computer and leave it unattended; and
- Avoid transactions involving financial data.

BEST PRACTICE: Do not login to any website (e.g. student registrar, bank account, email) unless absolutely necessary.

Protecting Data while surfing the Internet

Recommendations on using personal computer

(*Personal computers include the computer at your workplace or any personal computer used solely by yourself)*

- Install security patches to your system (e.g. Windows service pack)
- Use anti-virus and anti-spyware in your computer;
- Do not provide personal information to untrusted or suspicious website;
- Be skeptical, do not download any suspicious attachments provided by anyone;
- Always consult IT helpdesk when in doubt about suspicious links and attachments;
- Do not download pirated material, including music and video, as they may trick you to install malware to play them; and
- Log out or lock your computer when left unattended.

Privacy and Personal Data

- Definition of Personal Data
- Personal Data in Universities
- Roles and Responsibilities in Data Protection
- The Ordinance & 6 DPPs
- DPP in Practice

Q&A