The IHP’s Policy & Guidelines in Protection of Personal Data (Privacy)

The IHP as a data user undertakes to comply with the requirements of the Personal Data (Privacy) Ordinance to ensure that personal data kept are accurate, securely kept and used only for the purpose for which they have been collected.

All staff members of the IHP who handle identifiable personal data should take extra precaution to ensure that the relevant laws on personal data (privacy) and the University Guidelines are complied with and that effective security measures are adopted to protect personal and sensitive data concerning a wide spectrum of data subjects such as staff, students, alumni, research subjects, job applicants and other data subjects involved in enrollment / research / experiments / surveys.

1. Personal Data (Privacy) Ordinance

The Personal Data (Privacy) Ordinance was brought into force on 20 December 1996 to protect the privacy interests of living individuals in relation to personal data. The Ordinance covers any data relating directly or indirectly to a living individual (data subject), from which it is practicable to ascertain the identity of the individual and which are in a form in which access or processing is practicable. It applies to any person (data user) that controls the collection, holding, processing or use of personal data.

Please read carefully and comply with the following Ordinance and relevant Codes of Practice and Guidelines. For other information of the Ordinance please consult the Office of the Privacy Commissioner for Personal Data, Hong Kong (PCPD) (http://www.pccd.org.hk).

Some useful resources available from the HKSAR Government’s / PCPD’s website are as follows:

- Personal Data (Privacy) Ordinance (Chapter 486 Full Text)
- Schedule 1 of the Personal Data (Privacy) Ordinance — Details of the 6 Data Protection Principles
- Privacy Guidelines: Monitoring and Personal Data Privacy at Work
- Code of Practice on Human Resource Management
- Code of Practice on the Identity Card Number and Other Personal Identifiers — A Compliance Guide for Data Users
- Personal Data Privacy and the Internet — A Guide for Data Users
- Guidance on the Use of Portable Storage Devices
Personal Data (Privacy) (Amendment) Ordinance 2012
The Personal Data (Privacy) (Amendment) Ordinance 2012 introduced various amendments to the Personal Data (Privacy) Ordinance to enhance the protection of personal data privacy of individuals. The majority of the provisions under the Amendment Ordinance have come into effect from 1 October 2012, while provisions relating to direct marketing and the legal assistance scheme take effect from 1 April 2013. Under the New Guidance on Direct Marketing ("the Guidance"), a data user is required to take specified action before using personal data in direct marketing and data user must not use or provide personal data to others for use in direct marketing without data subject’s consent or indication of no objection. The Guidance provides practical tips to data users on how to comply with the new direct marketing requirements under the amended Personal Data (Privacy) Ordinance.

- An Overview of the Major Provisions of the Personal Data (Privacy) (Amendment) Ordinance 2012
- New Guidance on Direct Marketing

2. The IHP’s Guidelines in Protection of Personal Data (Privacy)
All staff members are required to comply with all relevant provisions of the Ordinance and observe the following six Data Protection Principles under the Ordinance in the collection, use, disclosure and retention of personal data:

6 Data Protection Principles:

- **Principle 1 - Purpose and Manner of Collection**
  This provides for the lawful and fair collection of personal data and sets out the information a data user must give to a data subject when collecting personal data from that subject.

- **Principle 2 - Accuracy and Duration of Retention**
  This provides that personal data should be accurate, up-to-date and kept no longer than necessary.

- **Principle 3 - Use of Personal Data**
  This provides that unless the data subject gives consent otherwise personal data should be used for the purposes for which they were collected or a directly related purpose.

- **Principle 4 - Security of Personal Data**
  This requires appropriate security measures to be applied to personal data (including data in a form in which access to or processing of the data is not practicable).

- **Principle 5 - Information to be Generally Available**
  This provides for openness by data users about the kinds of personal data they hold and the main purposes for which personal data are used.
Principle 6 - Access to Personal Data
This provides for data subjects to have rights of access to and correction of their personal data.

All line managers of the IHP are requested to critically review and improve the procedures and other relevant internal arrangements that are within their purview, in accordance with the following guidelines published from time to time by the Information Technology Services (ITS), University Data Protection Officer and other relevant administrative units of the University.

Special attention should be paid to protect the identifiable personal and sensitive data by encryption and security password (i.e. by means of the Data Leakage Protection software and the encrypted USB drives provided by the University). Further advice and assistance may be obtained from ITS’ webpage on Information security: http://www.its.hku.hk/services/infosec as necessary.

3. Engagement of Third-Party Service Providers
To avoid the loss or unauthorized use or disclosure of personal and sensitive data, it is recommended that a Non-Disclosure Agreement be signed in all situations with student helpers and contractors when acquiring third-party service that may give rise to access to personal and sensitive data or restricted information.

4. Maintenance and Disposal of Computing Devices
Regarding the maintenance and disposal of all the IHP-owned computers, mobile computing devices and removable storage devices/media, all staff should assign responsible staff member(s) to ensure that all identifiable personal and sensitive data therein contained are properly erased before these devices are dispatched for maintenance or disposal, to minimize the risk of loss, unlawful disclosure or unauthorized use of such data. Staff who are required to use maintenance or repair service for computing devices, are advised to enter into Non-Disclosure Agreements with the relevant service providers.

5. Information Security Incident Report Policy
It is important that any incident or suspected incident of violation of the personal data (privacy) laws such as the loss of devices which carry identifiable personal or sensitive data, is reported to the University as soon as possible so that remedial actions can be taken to prevent or minimize the damages caused to the data subjects, the University and all other parties concerned. All incidents should be reported to Mr Ivan Ho, Personal Data Protection Coordinator of the IHP, at 2817-5457 or hoivan@hku.hk immediately.
6. **Data Access and Correction Request**

All data subjects have the right to request access to and correction of personally identifiable information about themselves that is held by the IHP. If they wish to access their personal data held by the IHP, they could make a written request to ihphku@hku.hk.

7. **Full Compliance**

The privacy of our data subjects is of utmost importance and we thank all staff’s cooperation in our efforts to protect the personal data collected and managed by the University and to ensure full compliance with the relevant laws on personal data (privacy).