November 15, 2018

To: All Department Chairmen/School Directors/Unit Heads
All staff members and students

Management and Security of Personal Data

Introduction

1. Personal data is recorded information relating to an identifiable living individual. Examples of personal data include identification documents such as Hong Kong Identity Cards and staff/student cards, names, addresses, telephone numbers, medical and employment records, recordings, videos and photos. Personal data privacy is an integral part of privacy and is protected by the Personal Data (Privacy) Ordinance ("the Ordinance").

2. As a data user and a responsible public institution, The Chinese University of Hong Kong ("the University") undertakes to comply with the requirements of the 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 and students of the University who handle identifiable personal data should take extra precaution to ensure that the relevant laws on personal data (privacy) 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 members, students, alumni, patients, clients, donors, job applicants and other data subjects involved in research/experiments/surveys.

3. You are requested to read the Ordinance and relevant Codes of Practice and Guidelines, especially the six data protection principles which are listed in the University's website on "Protection of Personal Data (Privacy)": http://www.cuhk.edu.hk/policy/pdo/. For other information of the Ordinance, please consult the Office of the Privacy Commissioner for Personal Data, Hong Kong (PCPD): http://www.pcpd.org.hk.

4. Mr. Eric, S.P. Ng, Vice-President (Administration) and University Secretary, serves as the Data Protection Officer of the University.

Precautionary Measures

5. All Department Chairmen/School Directors/Unit Heads of the University are requested to critically review and improve the procedures and other relevant internal arrangements that are within their purview, in accordance with the guidelines published from time to time by the Information Technology Services Centre (ITSC) and other relevant administrative units of the University (e.g. Human Resources Circular on employment-related personal data issued in October 2018), which can be found on the University's website on "Protection of Personal Data (Privacy)". Special attention should be paid to protect the identifiable personal and sensitive data by encryption and security password. To protect the personal data held by your offices, all files containing identifiable personal and sensitive data on desktop personal computers, laptops and portable devices should be encrypted or password protected <https://www.itsc.cuhk.edu.hk/user-trainings/information-security-best-practices/guidelines-for-data-protection/use-encryption-to-protect-confidential-data>, or engaging Azure Information Protection (AIP) <https://www.itsc.cuhk.edu.hk/images/content/privacy-security/aip/AIP_User_Guide-v2.0.pdf>. Staff members and students wishing to send emails with attachments

containing identifiable personal and sensitive data must ensure that all personal or sensitive information is encrypted or password protected, and that such email is sent only to the intended recipient (see tips/guidelines at <http://www.cuhk.edu.hk/policy/pdo/>). Advice and assistance may also be obtained from ITSC where necessary: http://servicedesk.itsc.cuhk.edu.hk.

All Department Chairmen/School Directors/Unit Heads should also make sure that an effective mechanism is in place within their respective Faculty/Department/School/Unit to determine whether it is really necessary to use mobile computing devices and removable storage media to handle identifiable personal and sensitive data, and to make sure that such devices are securely kept and the data carried therein are properly encrypted and/or password protected. Furthermore, members of the University are recommended to use mobile/removable devices owned by the offices, instead of personal mobile/removable devices, if such storage media have to be used. Please read the *Guidelines for Securely Managing Mobile / Removable Devices* <https://www.itsc.cuhk.edu.hk/user-trainings/information-security-best-practices/guidelines-for-securely-managing-mobile-removable-devices> and the *Guidance on the Use of Portable Storage Devices* <http://www.cuhk.edu.hk/policy/pdo/en/doc/portable_storage_e.pdf>.

Direct Marketing

6. Staff members and students are also requested to pay attention to the provisions of The Personal Data (Privacy) (Amendment) Ordinance 2012 relating to direct marketing under which, a data user, before using or transferring the personal data of data subjects to a third party for "direct marketing" purposes, must notify the data subjects and obtain their explicit consent to such use, i.e. an absence of response to the notification does not imply consent. In the University's context, direct marketing activities will not only refer to the solicitation of donations or contributions, but also advertising programme/course/service information to students, alumni and other stakeholders. For details, please refer to the information leaflet "New Guidance on Direct Marketing" <http://www.pcpd.org.hk/english/publications/files/GN_DM_e.pdf>.

European Union (EU) - General Data Protection Regulation (GDPR)

7. The EU General Data Protection Regulation (GDPR), adopted in 2016, has come into force on 25 May 2018. The GDPR, which involves new provisions and enhanced rights, has replaced existing data protection laws throughout Europe and introduced significant changes and additional requirements that will have a wide ranging impact on businesses around the world, irrespective of where they operate. For details, please refer to the information leaflet European Union – General Data Protection Regulation 2016 < https://www.pcpd.org.hk/english/data_privacy_law/eu/files/eugdpr_e.pdf>.

Engagement of Third-Party Service Providers

8. 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. Please refer to the University's website on "Protection of Personal Data (Privacy)" for detailed information and samples of Agreement.

Information Security Incident Report Policy

9. If you encounter any incident or suspected incident of violation of the personal data

(privacy) laws such as the loss of devices or document which carry identifiable personal or sensitive data, you should:

(1) fill in the "Information Security Incident Reporting Form";
(2) send the form directly and immediately to the Director of ITSC (IT-related incidents) or the Secretariat (non IT-related incidents); and
(3) report the incident to the Department Chairmen/School Directors/Unit Heads concerned as soon as possible, in order that remedial actions can be taken to prevent or minimize the damages caused to the data subjects, the University and all other parties concerned. Please refer to the University's website on "Protection of Personal Data (Privacy)" for details of the policy and the form.

Full Compliance

10. The privacy of our data subjects is of utmost importance and we thank you for your 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).

Eric S.P. Ng
Vice-President (Administration) and University Secretary