The Hong Kong University of Science and Technology

Personal Data Privacy Policy

Approved by University Administrative Committee on 20 June 2019

I. Introduction

The Personal Data (Privacy) Ordinance of Hong Kong of 1996, and its associated amendment of 2012, seeks to protect the privacy of individuals with respect to the collection, usage, and handling of their personal data.

According to the Ordinance, personal data would include any data that could be used to directly or indirectly ascertain the identity of a living individual (*data subject*) and which are in a form in which access or processing is possible. The holder (*data user*) of such data is required to take the necessary actions to comply with the requirements of the Ordinance.

The Hong Kong University of Science and Technology, as a *data user*, needs to ensure that the requirements of the Ordinance are complied with and that the personal data being held are accurate, secure, and used for the purposes stated when such data are collected (and will not be used for any other purpose except in accordance with the law). *Data subjects*, in our case, would include (but not limited to) our staff and their dependents and affiliates, students, alumni, applicants, donors, and others involved in research, experiments, seminars, exchanges, recruitments, and other University activities.

Personal data privacy is a University-wide matter and it is necessary for ***all staff members and agents (including their representatives)*** of the University (such as student unions/societies of the University, staff associations of the University, third party contractors or third-party service providers engaged by the University or associated members of the University, including individuals who serve on Councils and Council committees) who handle personal data to observe the relevant rules and regulations and to take the necessary precaution and steps to ensure the privacy of personal data.

This document applies to all staff members and agents (including their representatives) of the University and outlines the position of the University in this regard. This document is confidential information of the University and is only intended for the University's staff members and agents (including their representatives). It must not be disclosed to any other person without the written consent of Data Privacy Officer.

II. Principles of the Personal Data (Privacy) Ordinance

The Personal Data (Privacy) Ordinance revolves around 6 basic principles. They are, in summary:

1. Data Collection – personal data collected about a *data subject* must (a) be done lawfully and fairly for lawful purpose(s) directly related to a function or activity of the *data user* and the collection is necessary or directly related to such purpose(s) (b) not be excessive in relation to such purpose(s), and (c) be made aware to the *data subject* concerned with certain prescribed information having been disclosed to the *data subject*.

2. Data Accuracy and Retention – *data users* should pay attention to the personal data they collect and ensure that such data are kept accurate, correct, up-to-date, and retained for only as long as necessary to fulfill the purpose(s) for which they were collected (including any directly related purpose) and not use any personal data which is inaccurate (or ensure that such inaccurate personal data is erased).

3. Data Usage – personal data should only be used for the purpose(s) for which they were collected (or a directly related purpose), unless express consent is given voluntarily by the *data subject* or a relevant person (e.g. parent / legal guardian).

4. Data Security – *data users* should put in place appropriate security measures to safeguard against unauthorized or accidental access, processing, erasure, loss or use of the personal data collected.

5. Policy and Practices – the *data user* should formulate policies and practices in relation to personal data (including information on the kinds of personal data held and the purpose for which such personal data are to be used) and make such information generally available.

6. Access and Correction – the *data subject* has the right to access his/her own personal data being held by the *data user* and to request correction to such data as necessary.

To comply with these principles, the University will undertake a number of actions, as outlined in the following sections.

III. Governance and Responsibilities

The University is a comprehensive and highly diverse community. Its many operating units function *independently* in fulfilling their respective roles and responsibilities and *collectively* toward achieving the goals and missions of the University.

Personal data privacy matters will also have to be addressed within this context, following a distributed but yet collaborative approach.

At the University level, it is necessary to provide *common* purpose and values, and to establish *common* ground work and address matters requiring co-ordination. At the execution level, on the other hand, it is necessary to rely on the vigilance and observance of *each and every unit* that deals with personal data (as it will not be possible for any central units to be aware of every such aspect at the unit level). There will have to be collaboration between the two levels.

The structure and responsibilities are discussed below:

1. Governance structure

   A formal governance structure will be adopted by the University to provide the necessary common focus and policies, and to establish a framework for co-ordination in personal data privacy matters.

   This governance structure includes the following:

   a) Data Privacy Officer

      The University will appoint a senior official to assume the role of *Data Privacy Officer*.

      The *Data Privacy Officer* will formulate data privacy policies and oversee the implementation, monitoring, promotion, resourcing, and incident management of data

privacy related matters. The *Vice President for Administration and Business* shall assume this role.

The *Data Privacy Officer* will be supported by a number of units/centers in the implementation and operation of data privacy policies, notably:

- the Information Systems Office, which will provide first line support to the *Data Privacy Officer* in overseeing the on-going operation of matters related to personal data privacy.

- the Information Technology Services Center, which will work with the Information Systems Office to facilitate the implementation of personal data privacy related actions, in particular with respect to the technical and technology aspects of such implementation.

The two offices above will work hand-in-hand in carrying out the decisions of the *Data Privacy Officer*, and will liaise with other University schools/departments/units/offices as required.

A group of key *data users* that deal substantially with personal data in their daily operation (see the section on Central Data Users below) will also act as early implementers of established data privacy policies and practices.

b) Data Privacy Advisory Committee

The *Data Privacy Advisory Committee* will consist of a group of major *data users* in the University. The committee will:

- form a platform/forum for discussion of issues, concerns, and solutions;
- advise the *Data Privacy Officer* in the formulation of policies and actions; and
- review the implementation of policies and recommend improvements.

The standing composition of the *Data Privacy Advisory Committee* is given in *Appendix A.* It is expected that the committee will co-opt additional members as required, in particular other central and major users of personal data.

c) Central Data Users (also known as *Central Data Custodians*)

The University typically holds personal data on the following groups of *data subjects*:

- Staff, dependents, affiliates, job applicants
- Students, recruitment prospects, applicants for admission
- Graduates and alumni
- Donors, contributors, partners, and associates
- Prospective employers, external student mentors/advisors, activity contacts
- Vendors, service providers, contractors
- Associates of the University including court, council, and other notable members

- Contacts collected through various University activities (e.g. seminars, training, conferences, fund raising, other special events)
- Others (e.g. key government personnel with which the University has dealings)

A number of central departments/offices, by virtue of their designated responsibilities, deal extensively with the personal data in the above groupings and are logically the *first-line* users of the data that fall within their respective areas of responsibility ("Central Data Users"). Note that the bulk of personal data in the above categories are held in central databases and maintained/processed via central administrative system functions.

As Central Data Users, these offices/departments will:

- ensure that the personal data held in respective central database(s) are captured, processed, kept current, and retrieved in accordance with the principles of the Ordinance;

- review and scrutinize requests by *other data users* for the use of such central data;

- advise *other data users* regarding the proper handling of personal data entrusted/released for their use;

- keep track of *data users* who had been given standing access permissions to central data and to review such periodically;

- be one of the primary contact points to handle requests from *data subjects* regarding review/correction of the recorded personal data;

- advise *other data users* in relation to their dealings with agents that handle and use personal data;

- require *other data users* to periodically provide status updates on the personal data transferred to agents and confirm that the transfer, handling and use of the personal data is in all respects in compliance with the Personal Data (Privacy) Ordinance, the University Data Privacy Policy Statement and the Personal Information Collection Statement relating to the personal data, as well as the mandate stipulated by such *other data users*.

To accomplish the above, it is expected the Central Data Users will put in place a clear and systematic *approval and tracking process* for data requests and usage. In doing so, Central Data Users shall also ensure that they will not do anything that would be inconsistent with such directions and/or guidance as may be given by the Data Privacy Officer from time to time.

2. *Other data users* in the University

Individual schools/departments/units/offices in the University may have the need and are holding personal data locally in their respective offices/sites. While the formal governance structure (discussed above) provides the framework for policies and co-ordination, the

assurance of compliance is necessarily distributed and is shared by every unit that deals with personal data.

Personal data kept/used locally at the school/department/unit/office are *typically* acquired through:

- extraction/download of such data from central databases, with permission from the relevant Central Data User office(s);

- contact channels available to and specific to the school/department/unit/office.

Irrespective of the source of data, schools/departments/units/offices dealing with such data should adhere to the principles of the Ordinance. The head of the concerned school/department/unit/office should ensure that an effective mechanism is in place for such purpose and also ensure that its school/department/unit/office will not do anything that would be inconsistent with such directions and/or guidance as may be given by the Data Privacy Officer from time to time.

The list of Central and Major Data Users for the various groups of *data subjects* are identified in *Appendix B*.

3. *Agents* of the University

From time to time, personal data collected by the University through its various arms may be transferred to agents of the University for use and handling on behalf of the University. Examples are as follows:

- Individual schools/departments/units/offices in the University may transfer personal data to student unions/societies and staff associations in connection with organizing and coordinating student/staff activities and events on behalf of the University.

- Central departments/offices may transfer personal data to Council members or Council committee members to handle matters on behalf of the University that fall within their jurisdiction.

- Central departments/offices may transfer personal data to contractors or third-party service providers engaged by the University to provide services to or on behalf of the University (e.g. bankers and insurance providers).

Schools/departments/units/offices shall only transfer personal data to a third party in accordance with the Personal Data (Privacy) Ordinance, the University Data Privacy Policy Statement and the relevant Personal Information Collection Statement, whether or not the recipient is an agent, and whether or not the recipient is within or outside the University.

However, if personal data is transferred to an agent of the University, the relevant school/department/unit/office shall bring this document to the attention of the agent and take steps to ensure that the agent complies with this document, the Personal Data (Privacy) Ordinance, the University Data Privacy Policy Statement and the Personal Information Collection Statement relating to the personal data. The relevant school/department/units/office must also establish a mandate governing the purpose, use and handling of the personal data by the agent and take steps to ensure the mandate is complied with.

More generally, schools/departments/units/offices shall ensure that they comply with the requirements in the Personal Data (Privacy) Ordinance and the guidelines issued by the Office of the Privacy Commissioner relating to transferring personal data to a *data processor* in the event the agent is a data processor.

Under the Personal Data (Privacy) Ordinance, a data processor means a person who processes personal data on behalf of another person and *does not* process the data for any of the person's *own purposes*.

The Personal Data (Privacy) Ordinance imposes two specific obligations on data users who engage data processors. If a data user engages a data processor, whether within or outside Hong Kong, to process personal data on the data user's behalf, the data user must adopt *contractual or other means* to prevent:

- any personal data transferred to the data processor from being kept longer than is necessary for processing the data; and

- unauthorized or accidental access, processing, erasure, loss or use of the data transferred to the data processor for processing.

The Office of the Privacy Commissioner has issued an information leaflet to provide guidelines to data users in complying with these requirements. The information leaflet can be accessed at: https://www.pcpd.org.hk//english/resources_centre/publications/files/dataprocessors_e.pdf.

Very often, schools/departments/units/offices may need to issue tenders for services where the potential bidder, if successful, will be regarded as a data processor. In this connection, the University has prepared suggested wordings for contracts and guidelines (*see Appendix F and G*) to help those who need to engage data processors. These illustrate the obligations imposed on data users who engage data processors explained above and how the information leaflet issued by the Office of the Privacy Commissioner relates to this context. Staff are reminded that these documents are only samples and staff should carefully read the guidance notes in the samples when using them. Staff are further reminded that these documents are not a substitute for reading the information leaflet issued by the Office of the Privacy Commissioner or this document. These samples can also serve as a general reference for entering into contracts with agents in generally.

If schools/departments/units/offices are not sure whether a third party is an agent and/or data processor and/or whether personal data can be transferred to a third party (whether or not an agent and/or data processor and whether or not within or outside the University), the relevant school/department/unit/office shall consult the Data Privacy Officer before making any arrangements for personal data to be transferred. Schools/departments/units/offices should also be mindful of the requirements of section 33 of the Personal Data (Privacy) Ordinance. See further section V below.

It is important for agents to remember that they are acting on behalf and upon the authority of the University. Therefore, agents receiving personal data shall only handle and use personal data in accordance with this document, the University Data Privacy Policy Statement and the Personal Information Collection Statement relating to the personal data. Agents must also only use and handle personal data in accordance with the mandate stipulated by the relevant school/department/unit/office that transferred the personal data to them.

More generally, agents shall familiarize themselves with the Personal Data (Privacy) Ordinance and ensure they are in compliance its provisions at all times.

Schools/departments/units/offices and agents should also be reminded that in the event there is infringing conduct, both the University and the agent could be held liable for the infringing conduct. The University reserves the right to take legal action against the agent. It is particularly important that schools/departments/units/offices ensure appropriate terms are incorporated into contracts with agents governing the obligations of agents in relation to protecting personal data and that agents act prudently at all times.

IV. Implementation and On-going Monitoring

To complement the University's data privacy efforts a number of facilities/action will be undertaken. These are identified below.

1. To ensure continued awareness/alert

   Periodic reminders will be issued by the Data Privacy Officer to *data users* and heads of schools/department/units/offices to reinforce the importance of proper handling of personal data. This will be done by:

   - all staff email – for general awareness of the principles of personal data privacy and reminder to be cautious about handling of such data.

   - email to the heads of school/department/unit/office – as reminder of the personal data privacy principles and the need to have a mechanism in place to comply with such principles, including alert reminder to concerned staff handling such data.

   Such reminders will typically be dispatched at the start of each semester (i.e. in September and February).

   Other forms of notification / reminders will be taken as appropriate from time to time to reinforce the awareness of the University community.

   Those who transfer personal data to agents must periodically remind the agents that they must handle and use the personal data transferred to them in accordance with this document, the Personal Data (Privacy) Ordinance, the University Data Privacy Policy Statement and the Personal Information Collection Statement relating to the personal data and that they must only handle and use personal data in accordance with the mandate stipulated by the relevant school/department/unit/office that transferred the personal data to them.

   From time to time, the Data Privacy Officer may also issue reminders to heads of school/department/unit/office on issues relevant to agents. In such case, it is the responsibility of the school/department/unit/office to ensure they circulate the reminder to the agents and draw those issues to the attention of the agents.

2. Education / Training

- Forums and seminars on the handling of personal data will be arranged on a periodic basis. These forums and seminars will provide the opportunity for the sharing of best practice across the institution, and help to ensure a common approach to data privacy issues.

  Where appropriate, the Office of the Privacy Commissioner on Personal Data may be invited to participate to provide first-hand information and comments/feedback.

- Special security training will be arranged for technical staff as necessary.

The objective is to provide staff members and agents who have to deal with personal data with the necessary information and/or techniques.

3. Addressing on-going operational questions and concerns

In their daily operations, University units may come across situations when it is not obvious whether personal data is (or should be) involved and, if so, how it should be handled.

It is expected that most operational concerns/questions could typically be addressed in discussion with the concerned Central Data User office(s) (see *Appendix B*).

Concerned matters could also be brought to the attention of the Data Privacy Officer and email to ispdpo@ust.hk, especially when:

- it is not certain which Central Data User office should be contacted to discuss the matter, or

- the matter is non-trivial and/or requires policy considerations, and cannot be resolved via discussion with the Central Data User office(s) concerned.

This will ensure that *data users* will have a clear avenue to bring forward their operational questions/concerns for discussion/resolution, and, enable consistent handling among units for similar situations.

In the event agents have any questions or concerns about the use and handling of the personal data transferred to them, they should forthwith contact the relevant school/department/unit/office that transferred the personal data to them. If the relevant school/department/unit/office is unable to address the enquiry, it shall forward the enquiry to the Data Privacy Officer.

4. Making data privacy information generally available

Information about the University's policy and practices regarding personal data will be made available through:

- University Data Privacy Policy Statement (see *Appendix C*) – available on the University's intranet

- Personal Information Collection Statement (see *Appendix D*)– available at various points of data collection

- Personal Data Privacy Policy (i.e. this document) – from the website of the University Data Privacy Officer (via the website of the Office of the Vice President for Administration and Business)

- Other information regarding data privacy practices will be published from time to time via the website of the University Data Privacy Officer

5. Incident reporting

Incidents or suspected incidents involving the breach of personal data privacy (including any leakage of personal data, actual or suspected) should immediately be brought to the attention of the head of the concerned school/department/unit/office, who in turn should promptly report the incident to the Data Privacy Officer.

Agents should forthwith report incidents or suspected incidents to the head of the school/department/unit/office that transferred the personal data to it, who in turn shall promptly report the incident to the Data Privacy Officer.

The Data Privacy Officer will determine the severity of the incident (drawing from his advisory committee where necessary) and report the case to the *Privacy Commissioner for Personal Data* and/or the affected data subjects as appropriate/necessary.

Proper documentation should be maintained for each such case, typically including such information as:

- cause of the incident,
- action(s) taken,
- recommendation(s) to mitigate the risk(s) of further incidents.

6. Reviews and monitoring

All data users should review their respective personal data handling procedures and processes on a periodic (e.g. annual) basis and to remind concerned staff and agents regarding proper practices.

Periodic audits will also be conducted to ensure compliance.

V. Overseas Jurisdictions

This policy only relates to the Hong Kong law requirements on personal data privacy. However, there may be situations where the personal data privacy requirements of overseas jurisdictions will also be relevant. For example, when the University needs to enter into a collaboration contract with an academic institution abroad and personal data will be handled by both parties. When the laws of more than one jurisdiction are relevant, there may be conflicting legal requirements on personal data privacy.

The possible handling of a situation where there is a conflict of legal requirements depends on the actual facts. Relevant factors may include where the data is held and where it is processed. Specific advice will need to be sought in the event of an actual case of conflict arising.

It is therefore better to try to avoid situations of conflicting legal requirements and see how differences can be mitigated upfront. A good starting point in situations where there are cross-border personal data needs is to try to enter into a contract governed by Hong Kong law, where possible. Staff could then require the overseas institution to have the contract reviewed for compliance with their local laws. If the contract needs to be governed by foreign law, it should be reviewed to ensure that provisions relating to personal data would also suit Hong Kong law compliance. Staff should carefully consider what their personal data needs are during the contract negotiation stage so that appropriate arrangements that are compatible with the laws of both jurisdictions could be set out in the contract to minimize the risk of uncertainty later on. For example, whether there is a specific need for the school/department/unit/office to access certain personal data such that if access is not granted, the school/department/unit/office won't be able to carry out a particular function (e.g. print academic certificates).

Staff should also be mindful of section 33 of the Personal Data (Privacy) Ordinance. Section 33 prohibits the transfer of personal data to a place outside Hong Kong unless one of the preconditions are satisfied. Normally, the easiest precondition to satisfy is to ensure the data subject has consented in writing to the transfer. It is important to note that section 33 is currently not yet in force and there is no timeline when it will come into operation. However, as good practice data users are encouraged to comply with it as if it is already in force so that when it does take effect they would already be in compliance with the requirements. Broadly speaking, if a data subject signs a Personal Information Collection Statement that informs the data subject that his/her personal data will be transferred outside Hong Kong, this should be sufficient for section 33 purposes. The Office of the Privacy Commissioner on Personal Data has issued a guidance note on section 33. Staff dealing with situations involving cross-border personal data needs should further consult this guidance note which can be accessed at:
https://www.pcpd.org.hk/english/resources_centre/publications/files/GN_crossborder_e.pdf

Staff are also reminded that situations involving cross-border personal data needs can be complicated and there will likely be differences in legal requirements on the subject of personal data privacy. Each case turns on its own facts. Therefore, in situations where there are cross-border personal data needs, staff should seek specific legal advice on how to ensure personal data privacy requirements of the relevant jurisdictions are complied with while addressing actual personal data needs.

VI. Privacy Impact Assessments

It is advisable that a "privacy-by-design" approach be adopted at the design stage of a new project or initiative that might have a significant impact on personal data privacy. By going through a privacy impact assessment, the project will be checked against the privacy principles which helps to identify privacy concerns. Mitigating action can then be planned and implemented in the early stages to address privacy issues and to minimize the risk of non-compliance.
It is important that we adopt a critical and objective approach in conducting the privacy impact assessment. Depending on the nature of the project concerned and the type of personal data involved, various offices shall be involved in providing input to the assessment.

Appendix A - Membership of the Data Privacy Advisory Committee

Recommended *standing* composition of the Data Privacy Advisory Committee is:

Chair:	Vice President for Administration and Business in the capacity of Data Privacy Officer
Secretary:	Director of Information Systems
Members:	Senior representatives of

- Academic Registry
- Human Resources Office
- Office of the Dean of Students
- Information Technology Services Center

It is expected that the committee will co-opt *additional* members as required, in particular other central and major users of personal data.

Appendix B – List of Central and Major Users of Personal Data *

* The list of Central and Major Users of Personal Data is not exhaustive and will be reviewed from time to time.

Data Subject Group	Central Data User Office	Responsible Officer (to be recommended)
Staff, Dependents, and Affiliates; University associates	Human Resources Office	
Job Applicants	Human Resources Office	
Recruits and Admission Prospects (UG)	Undergraduate Recruitment and Admission Office	
Recruits and Admission Prospects (PG)	Office of Postgraduate Studies	
Student records	Academic Registry	
Records of Scholarship and Financial Aid, and related donors	Office of the Dean of Students (Scholarships and Financial Aid Office)	
Records of Non-academic and Career related activities (including Employers and Mentors)	Student Affairs Office / Office of the Dean of Students	
Payment and Payroll records of Staff and Students	Finance Office	
Graduates and Alumni	Development and Alumni Office	
Donors, Prospective Donors, and Friends of HKUST	Development and Alumni Office	
Vendors, contractors	Purchasing Office	
Court, Council, and notable associates of the University	Court, Council, and Senate Secretariat	
Data Subject Group	**Major Data User**	**Responsible Officer (to be recommended)**
Student, alumni, student applicants, etc.	School of Business & Management	
Student, alumni, student applicants, etc.	School of Engineering	
Student, alumni, student applicants, etc.	School of Humanities & Social Science	
Student, alumni, student applicants, etc.	School of Science	
Student, alumni, student applicants, etc.	HKUST Fok Ying Tung Graduate School	
Student, alumni, student applicants, etc.	Interdisciplinary Programs Office	

Appendix C – University Data Privacy Policy Statement ("PPS")

Statement of Policy

The Hong Kong University of Science and Technology (the "University") respects the personal data privacy of all individuals and pledges to be in compliance with the requirements of the Personal Data (Privacy) Ordinance of Hong Kong ("PDPO") so that the privacy of your personal data is protected in accordance with the standard required by law. In doing so, we require all our staff and agents to comply with the PDPO in the same manner as the PDPO applies to the University as a whole and adhere to the strictest standards of security and confidentiality.

Statement of Practice

1. Kinds of personal data held

   The following explains the types of records / personal data held by the University.

   (a) Personnel records, which include but not limited to job applications, teaching and non-teaching staff files (containing personal details, job particulars, details of salary, payments, benefits etc.), leave and training records, group medical and dental insurance records, mandatory provident fund (and equivalent retirement) schemes participation records, performance appraisals, disciplinary records, information about dependents and affiliates necessary for administrative and operational activities;

   (b) Records of students and alumni, which include but not limited to various University related applications and operations (such as for enrolment in courses, programs or activities run by the University; grants, loans or other assistance by the University; and accommodation at the University, etc.) which contain student personal details, academic records (such as examination/test results or transcript, and so on), student reports, assignment/essay papers, examination papers, administrative records (such as payments, charges and fines, disciplinary information, etc.), non-academic and co-curricula records (such as internship, community activities, student union and other societal participation, and so on);

   (c) Records collected from the University's website / intranet, which include but not limited to records containing email addresses and personal details, preferences of web-users, location information (including IP addresses); and

   (d) Other records, which include but not limited to administration and operational files, records holding personal data provided to the University from associates of the University, individuals participating in activities organized or run by the University (including promotional, educational, or training activities), log records on the use of data facilities, services, or participation in activities, records of requests to access / correct personal data and enquiries from the public, research findings and related publications.

2. Main purposes of collecting and keeping personal data

   Personal data will only be used for the purposes stated at the time the data is collected, which broadly speaking, covers academic, educational/teaching, administrative, research, and related activities that are consistent with the University's mission (which is to advance learning and knowledge through teaching and research, particularly in science, technology, engineering, management and business studies, and at the postgraduate level; and to assist in the economic

and social development of Hong Kong). However, specific purposes will vary depending on the nature of the personal data held.

Examples of specific purposes are explained further below.

Personal data held in:

(a) Personnel records are collected and kept for corresponding with staff, recruitment and human resource management purposes including but not limited to obtaining reference checks, maintaining employee records and assessing work performance, consideration for eligibility for staff benefits, training and development, emergency purposes, and organizing social and other activities and events;

(b) Records of students and alumni are collected and kept for purposes including but not limited to providing education and assistance to students, facilitating communications between the University and its students and alumni, facilitating the provision of information upon request by students or alumni in relation to their affairs at the University (such as requests for academic certificates and transcripts), compiling statistics on enrolment at the University, facilitate academic planning and management, and organizing social and other activities and events;

(c) Records collected from the University's website / intranet are collected and kept for purposes including but not limited to handling various applications submitted through the University's website / intranet, sending newsletters to subscribers registered through the University's website, responding to requests submitted through the University's website / intranet, facilitating website access and compiling statistics on website usage; and

(d) Other records are collected and kept for purposes which vary according to the nature of the record, including purposes such as facilitating administration or office functions, organizing and delivering activities, compiling, summarizing, aggregating and/or de-personalizing personal data in connection with research or statistical/analytical activities carried on by the University in furtherance of the University's mission, conducting direct marketing activities (such as communicating information to individuals about the University's courses and programs) in connection with furthering the University's mission, facilitating publication of research or other publications relating to the University.

3. Collection of personal data

(a) General: When the University collects personal data from individuals, the University will provide them with a Personal Information Collection Statement ("PICS") on or before the collection in an appropriate format and manner in compliance with the PDPO.

(b) Personal data of minors: The PDPO does not impose any additional obligation on data users to seek the express consent of the minor (or his / her parent / guardian) on top of having to disclose the requisite information just because the data subject is a minor. Notwithstanding this, data users are generally not advised to collect personal data from minors (particularly those who are incapable of making an informed decision) without prior consent from a person with parental responsibility of the minor.

There are situations where the University may need to collect personal data of minors but it may not be practicable to obtain the consent of the parent because, for example:

- the occasion is not one where parents may accompany the minor;
- filling in an online application through the internet which the minor may be able to complete on his / her own, etc.

Under the circumstances, the University will ask for an indication that the minor has consulted his / her parents before providing the personal data.

(c) Personal data from the University's website / intranet: In order to provide web-users with a smooth browsing experience, we may need to use technical means (such as cookies) to collect information from web-users when they visit the University's website / intranet. If you are given the option whether or not to accept cookies and you do not accept, you may not be able to access the full content of our website / intranet.

(d) Direct marketing: Where it is intended that the personal data collected will be used for direct marketing purposes, the University will provide the individual with all the necessary information required to be given by law such as information about the direct marketing means and the classes of marketing subjects before making the collection. The University will not use an individual's personal data in direct marketing unless it has obtained the express consent of the individual concerned and such consent has not been withdrawn.

4. Duration of retention of personal data

The University will only hold personal data for as long as it is necessary to fulfill the purpose or a directly related purpose for which they are collected.

5. Disclosure of personal data

The University will take all practicable steps to keep the personal data you have provided confidential. However, the University may need to disclose, transfer or assign personal data collected by it to such outside third-parties to facilitate the purpose for which the personal data was collected. In general, the parties to which we may disclose, transfer or assign personal data include medical practitioners providing medical services to the University's staff, if applicable, any agent, contractor or third-party service provider engaged by the University to provide services to or on behalf of the University (e.g. bankers, insurance providers and payroll service providers) and any person to whom the University is under an obligation to make disclosure under any requirements of any law or for the purposes of any guidelines or codes of practice with which the University is expected to comply. We may also disclose, transfer or assign personal data internally within the University (on a need-to-know basis) to facilitate the purpose for which the personal data was collected or a directly related purpose. The personal data may be disclosed, transferred or assigned within or outside Hong Kong. In case it is to a place outside Hong Kong, while the University will take appropriate steps to protect the privacy of the personal data, it should be noted that such place may not have in place data protection laws which are substantially similar to, or serve the same purposes as, the PDPO so personal data located outside Hong Kong may not be protected to the same or similar level as in Hong Kong.

6. Security of personal data

The University will take appropriate steps to protect the personal data held by it against unauthorized or accidental access use, loss, processing, erasure, transmission, modification or disclosure. When the University needs to disclose, transfer or assign personal data to outside

third-parties, the University will take appropriate steps to protect the privacy of the personal data to be disclosed, transferred or assigned (for example, requiring our service providers to keep confidential any personal data with which it comes into contact).

7. Personal data access and correction

   Individuals have the right to request access to and to correct their personal data held by the University.

   Personal data may be made available to concerned individuals via different means, including (a) authenticated on-line enquiries and/or (b) completion of prescribed forms provided by concerned offices and sending the completed form by email to ispdpo@ust.hk.

   Similarly, requests to correct personal data held by the University may be made via on-line functions where available and/or by submitting such requests by email to ispdpo@ust.hk, using prescribed forms provided by concerned offices.

   In accordance with the Personal Data (Privacy) Ordinance, data access requests will normally be addressed within a 40-day period. A fee reflecting the cost of processing the data request may be levied.

8. Enquiries

   Any enquiries regarding personal data privacy policy and practice may be addressed to the University's Data Privacy Officer and email to ispdpo@ust.hk.

Appendix D - Personal Information Collection Statement ("PICS")

A PICS will determine how personal data is to be used/stored/retained subsequent to collection. As such, the statement should be well planned.

Factors to be considered for a PICS:

- A PICS shall be included on all hardcopy forms, web pages, or any other medium that are used for data collection (e.g. student admission, job application, appointment letter, student registration form, seminar sign-up form, etc.).

- A PICS shall at a minimum contain the following information :
  - Statement of purpose (i.e. the purpose for which data is to be used)
  - Clearly indicate which data are obligatory and which data are voluntary and the consequence(s) of not providing the obligatory data
  - Statement about disclosure (i.e. clearly indicate to whom data may be disclosed, and clearly indicate whether data may be transferred to third parties and the classes of third parties to whom data may be transferred)
  - Statement about security (i.e. that practical steps shall be taken to ensure data are protected against unauthorized or accidental access, processing, erasure, loss or use)
  - Statement about duration of retention (i.e. ensure that data is not kept longer than is necessary for fulfilling the purpose for which it is collected)
  - Statement about the right to access and correct data (i.e. data subject can request access to his/her data and request correction of his/her data)
  - Provision(s) for enquiries to be made (i.e. the name of office concerned and the contact address/email to whom a data access and/or correction request may be made)

- Each such statement should be reviewed and ***tailored to suit the context*** concerned.

- The statement should cover those uses of the data for which the data needs to be collected. It may be broad but should not be overly vague as to render it meaningless.

  As personal data can only be used for the original purpose of collection (or a *purpose directly related to the original purpose)*, it would be prudent to set out in the PICS at the outset the other purposes you envisage for which personal data may be used to avoid argument and so that you can use the personal data for those other purposes without the need to seek the individual's consent each time.

- The availability and content of PICS statements and the provision for consent should be reviewed on a periodic basis (e.g. annually).

- The use of the data for *research purpose*

  - While the initial collection of data may primarily be for administrative/operational use, where envisaged, the potential use of data for research should be *incorporated into* the PICS. Statements such as the following can be considered:

    … It is expected that personal data will also be used for research or statistical/analytical purposes to further the University's mission (i.e. to advance learning and knowledge through teaching and research, particularly in science, technology, engineering,

management and business studies, and at the postgraduate level; and to assist in the economic and social development of Hong Kong ….

- Where research is not explicitly mentioned in the original PICS, it will be necessary to establish that research is an activity that is ***directly related*** to a stated purpose in the original PICS, in order for the data to be used.

- If neither of the above applies, the personal data can still be used for research (under Section 62 of the PDPO) if ***all*** of the following criteria are met:

  √ the personal data is to be used for preparing statistics or carrying out research;

  √ the personal data will not be used for purpose(s) other than the original purpose(s) or a directly related purpose or in preparing statistics or carrying out research;

  √ the resulting statistics or results of the research are ***not*** made available in a form which identifies the data subjects or any of them.

  Accordingly, as long as the requirements in Section 62 are satisfied (in particular, that the personal data will be *fully* depersonalized in the results), personal data originally collected for other purposes can be subsequently used in research (as a new purpose) without the need to seek prescribed consent from the individual.

  However, if the personal data ***will not be depersonalized*** in the results or ***despite efforts to depersonalize, it is still be possible for the individual to be identified from the results (e.g. due to a small data pool)*** then section 62 cannot be relied upon and prescribed consent is needed before you can use the personal data in research as a new purpose.

- Further guidelines on preparation of PICS

  The Office of the Privacy Commissioner for Personal Data has issued a Guidance Note on preparing PICS. Members of staff who are required to prepare PICS are advised to further consult this Guidance Note, which can be accessed at:

  http://www.pcpd.org.hk/english/publications/files/GN_picspps_e.pdf.

- Sample PICS

  In order to better illustrate the requirements of a PICS, the University has prepared a sample PICS (*see Appendix H*). Staff are reminded that this is only a sample and staff should carefully read the guidance notes in the sample when using the sample. Staff are further reminded that the sample is not a substitute for reading the Guidance Note issued by the Office of the Privacy Commissioner or this document.

Appendix E - Useful Links and Further References

1. Website of the Office of the Privacy Commissioner for Personal Data http://www.pcpd.org.hk/

2. The Personal Data (Privacy) Ordinance - Principles
   https://www.pcpd.org.hk/english/data_privacy_law/6_data_protection_principles/principles.html

3. The Personal Data (Privacy) Ordinance
   https://www.pcpd.org.hk/english/data_privacy_law/ordinance_at_a_Glance/ordinance.html

4. The Personal Data (Privacy) Amendment Ordinance
   https://www.pcpd.org.hk/english/data_privacy_law/amendments_2012/amendment_2012.html

5. Office of the Privacy Commissioner for Personal Data - Guidance Note on Personal Information Collection Statement:
   http://www.pcpd.org.hk/english/publications/files/GN_picspps_e.pdf

6. Office of the Privacy Commissioner for Personal Data - Code of Practice on Human Resource Management and frequently asked questions
   https://www.pcpd.org.hk/english/data_privacy_law/code_of_practices/files/PCPD_HR_Booklet_Eng_AW07_Web.pdf
   https://www.pcpd.org.hk/english/data_privacy_law/code_of_practices/files/faq_recruitment_e.pdf

7. Office of the Privacy Commissioner for Personal Data –Data Access Request form
   http://www.pcpd.org.hk/english/publications/files/Dforme.pdf

8. Office of the Privacy Commissioner for Personal Data – Information Leaflet on Outsourcing the Processing of Personal Data to Data Processors
   https://www.pcpd.org.hk//english/resources_centre/publications/files/dataprocessors_e.pdf

9. Office of the Privacy Commissioner for Personal Data – Guidance on Personal Data Protection in Cross-border Data Transfer
   https://www.pcpd.org.hk/english/resources_centre/publications/files/GN_crossborder_e.pdf

10. Office of the Privacy Commissioner for Personal Data – Privacy Impact Assessments
    https://www.pcpd.org.hk/english/resources_centre/publications/files/InfoLeaflet_PIA_ENG_web.pdf

11. Information Technology Services Center – Cybersecurity
    http://itsc.ust.hk/cyber-security

12. HKUST website on Personal Data Privacy
    https://dataprivacy.ust.hk/

Appendix F – Sample re Tenders For Services Where The Potential Bidder, If Successful, Will Be Regarded As A Data Processor.

SAMPLE

Guidance notes for users of this sample

- *This sample is drafted for tenders for services where the potential bidder, if successful, will be regarded as a data processor. A data processor is a person who processes personal data on behalf of another person (e.g. the University or a University unit) and does not process the data for any of its own purposes.*

- *The Personal Data (Privacy) Ordinance requires that where a data user (e.g. the University or a University unit) engages a data processor, whether within or outside Hong Kong, to process personal data on the data user's behalf, the data user must adopt contractual or other means to prevent (i) personal data transferred to the data processor from being kept longer than is necessary for processing the data and (ii) unauthorized or accidental access, processing, erasure, loss or use of the data transferred to the data processor for processing.*

- *The purpose of this sample is to provide guidance to address these requirements. While contractual or other means appear to be alternatives, as a matter of good practice, it is advisable to still consider what other non-contractual measures could be taken in addition to incorporating express terms into the contract.*

- *This sample is divided into two parts. Part 1 provides suggested wording to be included in tender documents for the purposes of informing potential bidders of the kinds of contractual obligations relating to personal data that they will be expected to comply with in the event their bid is successful. Part 2 provides suggestions on non-contractual measures that could be taken in relation to tendering and reviewing bids submitted.*

- *Items in square brackets with "e.g." indicated are examples which the user of this sample will need to amend as appropriate.*

- *Please note this document is only a sample and not exhaustive. The extent to which the subject of personal data needs to be addressed in tender documents and in relation to tendering and reviewing bids submitted will ultimately depend on actual circumstances and users will need to make their own judgement. Users are also reminded that actual wording to be included in tender documents and actual measures taken on the subject of personal data must be tailored to suit the context concerned.*

Part 1: Suggested wording for tender documents

Personal data privacy

In the event your bid is successful, you will enter into a contract with the [e.g. the University or insert relevant University unit] in relation to the subject matter of this tender under which you will be required to observe certain contractual obligations in relation to personal data privacy. The actual scope and wording of the contractual obligations will be negotiated in due course should your bid be successful. However, you should expect to have imposed on you contractual obligations covering the following areas:

- Compliance with the Personal Data (Privacy) Ordinance.

- Compliance with local laws on personal data privacy in jurisdictions outside Hong Kong, where applicable.

- Compliance with our Data Privacy Policy Statement (also known as PPS).

- Compliance with the Personal Information Collection Statement (also known as PICS) applicable to the service that we are engaging you to provide.

- Security measures required to be taken by you to protect personal data entrusted to you. This includes measures to prevent unauthorized or accidental access, processing, erasure, loss or use of the data entrusted to you. We will require you to take the same security measures that we would have to take if we were processing the personal data ourselves. We will also require you to protect personal data in accordance with the data protection principles under the Personal Data (Privacy) Ordinance.

- Timely return, destruction and/or deletion of personal data entrusted to you when it is no longer required for the purpose for which it is entrusted to you. Personal data entrusted to you shall not be kept longer than is necessary for processing the data.

- Prohibition against any use or disclosure of personal data by you for a purpose other than the purpose for which the data is entrusted to you.

- Absolute or qualified prohibition against you from sub-contracting the service that we are engaging you to provide.

- In the event we permit you to sub-contract the service that we are engaging you to provide, we will require you to impose on the sub-contractor the same obligations in relation to handling and processing personal data as we impose on you and where the sub-contractor fails to fulfil its obligations, you shall remain fully liable to us for the fulfilment of those obligations.

- Immediate reporting of any sign of abnormalities or security breaches.

- Measures required to be taken by you to ensure that your staff will carry out the security measures and comply with the obligations under your contract with us regarding handling of personal data.

- Our right to audit and inspect how you handle and store personal data. We will also require you to keep proper records of all personal data that have been transferred to you for processing; and

- Consequences for violations of your contract with us.

Please note that this list is not exhaustive. As explained above, the actual scope of the contractual obligations will be negotiated in due course should your bid be successful. We may impose on you other contractual obligations relating to personal data as we deem

necessary given the nature of the service that we are engaging you to provide and the particulars set out in your bid.

Part 2: Suggested non-contractual measures in relation to tendering and reviewing bids submitted

Some good practice recommendations may include the following:

1. When considering to issue a tender for services from data processors, consider whether anonymized or dummy data by data processors can equally serve the purpose. If all or part of the data could be anonymized or dummy data, this would be less privacy intrusive. The amount and scope of personal data potentially involved in the project shall be limited to that which is absolutely necessary.

2. Carefully review the background and competence of short-listed bidders. Only choose a bidder if you are satisfied that the bidder has good reputation in the industry, is known for delivering high quality services, promotes ethical practices, has a good track record on personal data protection and has the technical competence and infrastructure to enable personal data to be handled and processed with adequate protection.

3. Carefully review the personal data privacy policies of short-listed bidders and consider if they are in line with the University's personal data privacy policy and practices. If the bidder's policies are not readily available on their website, it would be advisable to obtain a copy from the bidder for consideration. Only choose a bidder if you are satisfied that the bidder has robust policies in places and whose personal data privacy policies and practices are consistent with those of the University.

4. Ascertain details from short-listed bidders about any training which they provide their staff on handling and processing personal data and what actual security measures they take to ensure that personal data in their care is properly safeguarded and not kept for longer than is necessary. Only choose a bidder if you are satisfied that the bidder provides adequate training to their staff and implements effective security measures that are no less stringent than those of the University.

5. Ask short-listed bidders how they would handle any sign of abnormalities (for example, audit trail shows unusual frequent access of personal data by a staff member at odd hours) or security breaches (for example, missing personal data). Only choose a bidder if you are satisfied that the bidder handles signs of abnormalities and security breaches in a prompt and proper manner.

Appendix G – Sample re Entering Into Contracts With Successful Bidders Of Tenders Who Are Regarded As Data Processors

SAMPLE

Guidance notes for users of this sample

- *This sample is drafted for entering into contracts with successful bidders of tenders who are regarded as data processors. A data processor is a person who processes personal data on behalf of another person (e.g. the University or a University unit) and does not process the data for any of its own purposes.*

- *The Personal Data (Privacy) Ordinance requires that where a data user (e.g. the University or a University unit) engages a data processor, whether within or outside Hong Kong, to process personal data on the data user's behalf, the data user must adopt contractual or other means to prevent (i) personal data transferred to the data processor from being kept longer than is necessary for processing the data and (ii) unauthorized or accidental access, processing, erasure, loss or use of the data transferred to the data processor for processing.*

- *The purpose of this sample is to provide guidance to address these requirements. While contractual or other means appear to be alternatives, as a matter of good practice, it is advisable to still consider what other non-contractual measures could be taken in addition to incorporating express terms into the contract.*

- *This sample is divided into two parts. Part 1 provides suggested wording to be included in contracts with data processors. Part 2 provides suggestions on non-contractual measures that could be taken in relation to engaging data processors.*

- *Items in square brackets with "e.g." indicated are examples which the user of this sample will need to amend as appropriate. Where appropriate, additional guidance notes have been added in the main body of this sample.*

- *Please note this document is only a sample and not exhaustive. The extent to which the subject of personal data needs to be addressed in the contracts with data processors will ultimately depend on actual circumstances and users will need to make their own judgement. Users are also reminded that actual wording to be included in contracts with data processors and actual measures taken on the subject of personal data must be tailored to suit the context concerned.*

Part 1: Suggested wording for contracts with data processors

Personal data privacy

1. You shall at all times comply with the Personal Data (Privacy) Ordinance ("PDPO").

2. You shall at all times comply with the laws of [e.g. United Kingdom] on personal data privacy to the extent they do not contradict Hong Kong law or your obligations under this contract ***[Note: Applicable if the data processor is located outside HK and personal data will be held outside HK]***

3. You shall at all times comply with the University's Data Privacy Policy Statement ("PPS"), as in force from time to time. A copy of the current PPS will be provided to you separately.

4. You shall comply with the Personal Information Collection Statement ("PICS") applicable to the service that we are engaging you to provide, as in force from time to time. A copy of the current PICS will be provided to you separately.

5. You shall implement all practicable security measures to protect personal data entrusted to you. This includes implementing measures to prevent unauthorized or accidental access, processing, erasure, loss or use of the data entrusted to you. You shall upon our request give details of the measures taken and agree to make any amendments as we may reasonably require. You further acknowledge and agree that if for any reason, you are unable to provide security measures to our satisfaction then given that protecting the privacy of data subjects is our utmost priority, we reserve the right to terminate this contract forthwith in such situation. At a minimum, we require you to take the following measures:

    a. Generally, you shall:

        i. take the same security measures that we would have to take if we were processing the personal data ourselves. Details will be provided separately;

        ii. protect personal data in accordance with the data protection principles under the PDPO;

    b. Without limitation to the generality of the foregoing:

        i. All hard copy documents containing personal data shall be stored in locked cabinets and only be accessible by authorized staff;

        ii. All soft copy documents or electronic mediums containing personal data shall be password protected and only be accessible by authorized staff;

        iii. Documents containing personal data, in whatever format and however stored, shall only be accessed by, disclosed to and/or used by those staff who need to know, strictly for the purpose of performing the services that we are engaging you to provide;

        iv. Personal data shall only be erased, deleted or destroyed in accordance with this contract or with our express consent ***[Note: Please amend the specific measures as appropriate having regard to factors such as the amount of personal data involved, sensitivity of the personal data, the nature of the data processing service and the harm that may result from a security breach]***.

6. If at any time during the course of performing the services under this contract, we require you (for whatever reason) to return any personal data entrusted to you or any personal data entrusted to you is no longer required, you shall forthwith and in any

event no later than [e.g. 14 days] return the same to us and confirm that you have not retained any copies of such personal data. Upon the termination of this contract, for whatever reason, you shall forthwith and in any event no later than [e.g. 14 days] return to us all personal data entrusted to you and confirm that you have not retained any copies of such personal data. In the event personal data to be returned to us is stored electronically, you shall ensure a copy of such personal data is sent to us and after we have confirmed due receipt of the same, you shall proceed to permanently erase or delete the electronic copies of such personal data held by you and confirm that the same has been permanently erased or deleted. Where personal data is contained in hard copy documents, we may require you to destroy the hard copy documents (e.g. by shredding the hard copy documents) instead of returning the same to us and if that is the case, details of the arrangement will be provided separately.

7. You are strictly prohibited from using or disclosing personal data entrusted to you for any purpose other than to perform the services that we are engaging you to provide.

8. [You are strictly prohibited from sub-contracting to others the service that we are engaging you to provide.]

   OR

   [Subject to such terms and conditions to be separately agreed, you may sub-contract the service that we are engaging you to provide provided that you will impose on the sub-contractor the same obligations in relation to handling and processing personal data as we impose on you. Specifically, you shall procure and demonstrate to our satisfaction that your obligations in relation to handling and processing personal data under in this contract are incorporated into your contract with the sub-contractor mutatis mutandis. Your choice of sub-contractor must also be approved by us. You acknowledge and agree that in the event the sub-contractor fails to fulfil its obligations, you shall remain fully and solely liable to us for the fulfilment of those obligations and shall fully indemnify us and hold us harmless from and against any and all claims, demands, liabilities, losses or damage which may arise in this connection.]***[Note: Please choose the desired option for your situation. The first option is where no sub-contracting is permitted. The second option is where sub-contracting is permitted]***

9. You shall forthwith and in any event no later than [e.g. 24 hours] report to us in writing any sign of abnormalities (for example, audit trail shows unusual frequent access of personal data by a staff member at odd hours) or security breaches (for example, missing personal data) in relation to personal data entrusted to you that has come to your attention and give details of the remedial measures you have taken. You shall also provide any additional details and take any actions that we may require.

10. You shall procure that all authorized staff involved in performing the services under this contract observe the obligations regarding handling of personal data as set out in this section in the same manner mutatis mutandis as they apply to you. In this connection, you shall demonstrate to our satisfaction that you have implemented personal data protection policies and procedures and provided adequate training to your staff.

11. We reserve the right to audit and inspect at any time how you handle and store personal data entrusted to you and you shall fully cooperate whenever we exercise such right. You shall keep proper records of all personal data that have been transferred to you for handling and processing and how they have been handled and processed, including records of personal data which have been returned, deleted, erased or destroyed in accordance with this contract. You shall also keep records of all signs of abnormalities and security breaches and how they have been handled.

12. You acknowledge and agree that in the event you fail to comply with your obligations hereunder or under the PDPO, you shall remain fully and solely liable to us for the fulfilment of such obligations and shall fully indemnify us and hold us harmless from and against any and all claims, demands, liabilities, losses or damage which may arise in this connection. We also reserve the right to terminate this contract forthwith. We further reserve the right to take action against you, whether legal or otherwise.

Part 2: Suggested non-contractual measures in relation to engaging data processors

Some good practice recommendations may include the following:

1. If it is envisaged that personal data will be processed by data processors, ensure that when collecting personal data it has been made plain and clear in understandable language to data subjects in the PICS that their personal data may be disclosed or transferred to data processors and processed by data processors. Where practicable, data subjects should be requested to sign such PICS to the effect that they expressly consent to their personal data being so disclosed, transferred and processed. This is especially if their personal data will be disclosed, transferred and processed overseas. Data subjects should also be assured that security measures will be taken to protect their personal data.

2. If the data processor is not situated in Hong Kong, legal advice should be obtained to ensure that the contract is enforceable in both Hong Kong and the jurisdiction in which the data processor is situated.

3. Ensure that the use of technical and legal terms such as “personal data” are clearly defined in the contract. This is especially important if the data processor is not situated in Hong Kong as the meaning of technical and legal terms may vary with jurisdictions. Technical and legal terms should be defined to suit compliance with Hong Kong law requirements.

4. Regularly audit and inspect how data processors handle and store personal data entrusted to it. Regularly inspect the records kept by the data processor pertaining to the personal data entrusted to it to ensure that they are kept in order. Questions should be raised and answered if any audit or inspection reveals any defect or deficiencies.

5. Properly document all the measures you have taken to ensure that personal data entrusted to the data processor is properly safeguarded. This includes at a minimum:

    a. Ensure that the process of selecting the chosen data processor and the reasons for choosing such data processor, especially in terms of personal data protection, is documented in writing;

b. Ensure that a copy of the signed contract with the data processor containing contractual obligations imposed on the data processor in relation to protecting personal data is safely kept;

c. Ensure that as data user, a record of the personal data transferred to the data processor is kept. The record should be updated regularly and reconciled with the records of the data processor. Any discrepancies should be checked and the reasons for it should be documented and kept on record.

d. Ensure that details of all audits and inspections conducted with the data processor and the findings, actions taken and outcomes are documented in writing and kept on record.

Appendix H – Sample PICS

SAMPLE

Guidance notes for users of this sample

- *The purpose of this sample is to provide suggested wording for a Personal Information Collection Statement ("PICS"). It is prepared using employment as the backdrop to make it easier for the user of this sample to follow through the examples given.*

- *Items in square brackets with "e.g." indicated are examples which the user of this sample will need to amend as appropriate. Where appropriate, additional guidance notes have been added in the main body of this sample.*

- *Please note this PICS is only a sample and not exhaustive. The actual content of a PICS will ultimately depend on actual circumstances and users will need to make their own judgement. Each PICS must be tailored to suit the context concerned. Users should also refer to the University's Data Privacy Statement for further guidance on how to prepare a PICS which shall have prevailing effect.*

Suggested Personal Information Collection Statement

Personal Information Collection Statement ("PICS")

1. Your Privacy

The Hong Kong University of Science and Technology (the "University") respects the personal data privacy of all individuals and pledges to be in compliance with the requirements of the Personal Data (Privacy) Ordinance of Hong Kong ("PDPO") so that the privacy of your personal data is protected in accordance with the standard required by law. In doing so, we require all our staff and agents to comply with the PDPO in the same manner as the PDPO applies to the University as a whole and adhere to the strictest standards of security and confidentiality.

"**Personal data**" means any personally identifying information or sensitive data from which it is practicable for the identity of an individual to be ascertained, such as: [e.g. name, age, marital status, occupation, income, address, contact details, HKID card or passport numbers and credit card information].

This PICS is provided by the [e.g. Human Resources Office] (the "[e.g. HRO]") for the purposes of complying with the notification requirements under the PDPO when collecting personal data. It should be read in conjunction with the University's Data Privacy Policy Statement ("PPS"). A copy of which is available at this link: ***[Note: Please insert]***

Please read this PICS and the PPS carefully to understand the policy and practices of the University and [e.g. HRO] regarding how your personal data will be treated.

This PICS may from time to time be revised, or otherwise changed as the [e.g. HRO] deems necessary but the [e.g. HRO] will endeavour to give you advance notice of any such revision or change where practicable.

2. Purposes for which your Personal Data will be used

The [e.g. HRO] collects your personal data [e.g. when you make an application for a position with the University and/or commence employment with the University].

You will also be required to supply the [e.g. HRO] with personal data from time to time [e.g. throughout your employment].

The purposes for which your personal data may be used are as follows:

(i) [e.g. For identification and determination of eligibility for employment generally and qualifications relevant to your employment with the University; assessing work performance, attendance and disciplinary record; providing and reviewing salaries, bonuses and other benefits; consideration for promotion, training, secondment or transfer; consideration for eligibility for staff benefits; providing employee references; obtaining or managing employment visa, where required; filing tax returns and making other legally required filings;]***[Note: Please amend purposes as appropriate]***

(ii) [It is expected that personal data will also be used for research or statistical/analytical purposes to further the University's mission (i.e. to advance learning and knowledge through teaching and research, particularly in science, technology, engineering, management and business studies, and at the postgraduate level; and to assist in the economic and social development of Hong Kong)]***[Note: Only if research is envisaged]***; and

(iii) For all other purposes ancillary to the above purposes.

Unless otherwise indicated, it is obligatory to supply the requested personal data. Failure to provide the requested personal data may result in the [e.g. HRO] not being able to [e.g. process your employment application or provide you with the necessary support during your employment with the University, as the case may be, or even result in disciplinary action]***[Note: Please amend consequences of not providing obligatory data]***.

3. Disclosure

The [e.g. HRO] will take all practicable steps to keep your personal data confidential but in connection with the above purposes, the [e.g. HRO] may need to disclose, transfer or assign the personal data you have provided within or outside Hong Kong to the following parties and you consent to the [e.g. HRO] doing so. You understand and acknowledge that in case your personal data is disclosed, transferred or assigned to a place outside Hong Kong, while the [e.g. HRO] will take appropriate steps to protect the privacy of your

personal data, such place may not have in place data protection laws which are substantially similar to, or serve the same purposes as, the PDPO so your personal data located outside Hong Kong may not be protected to the same or similar level as in Hong Kong:

(i) Outside third-parties such as:

[e.g. medical practitioners providing medical services to the University's staff, if applicable; any agent, contractor or third-party service provider engaged by the University to provide services to or on behalf of the University, including without limitation, bankers, insurance providers and payroll service providers; and any person to whom the University is under an obligation to make disclosure under any requirements of any law or for the purposes of any guidelines or codes of practice with which the University is expected to comply];

(ii) Parties and staff within University on a need-to-know basis; and

(iii) Any person with your express or implied consent.

4. Security

The [e.g. HRO] will take appropriate steps to protect the personal data held by it against unauthorized or accidental access, use, loss, processing, erasure, transmission, modification or disclosure. When the [e.g. HRO] needs to disclose, transfer or assign personal data to outside third-parties, the [e.g. HRO] will take appropriate steps to protect the privacy of the personal data to be disclosed, transferred or assigned (for example, requiring third-party service providers to keep confidential any personal data with which it comes into contact).

The personal data you have provided, however stored, will only be accessed by those who are authorized to do so. Staff members, agents, contractors and third-party service providers designated to handle personal data will be instructed to do so only in accordance with this PICS.

5. Retention of Personal Data

The [e.g. HRO] will keep your personal data only for as long as necessary to fulfil the purposes for which the personal data was collected or a directly related purpose.

Personal data which is no longer required will be destroyed.

6. Your Right to Access and Correction

You may at any time request access to and correction of your personal data in the records of the [e.g. HRO].

To exercise any of your rights, please contact the [e.g. Head of Human Resources] (see details below). Depending on the nature of the request, the [e.g.

Head of Human Resources] may need to forward the request to the University's Data Privacy Officer for further handling.

The [e.g. HRO] is required by law to respond to your requests within 40 days but the [e.g. HRO] may charge you a reasonable fee for doing so to the extent permitted by law.

7. Enquiries

For the purposes of this PICS and the functions/operations of the [e.g. HRO], the [e.g. Head of Human Resources] has been designated to handle requests/enquiries relating to personal data. Such requests/enquiries may include:

(i) Requests for access to or correction of personal data;
(ii) Enquiries about the kinds of personal data held;
(iii) Requests for information regarding the policies and practices of the University and [e.g. HRO] with respect to personal data; and
(iv) General questions or complaints regarding personal data.

The [e.g. Head of Human Resources] can be contacted as follows:

[e.g. Head of Human Resources]
[e.g. Human Resources Office]

Address: ***[Note: Please insert]***

Email: ***[Note: Please insert]***

Please mark all communications "Confidential".

I have read and understood the contents of this PICS and consent to the matters set out in this PICS.

Name: ***[Note: Please insert]***
Date: ***[Note: Please insert]***

[Note: The law does not require the data subject to sign a PICS but where practicable, it is suggested to require the data subject to sign it to prepare for section 33 compliance when it comes into force]