LINGNAN UNIVERSITY

Code of Practice for Handling Personal Data

I. Introduction

The University recognizes the individual's right to privacy and is committed to protecting the personal privacy of members of the University community. The mutual trust and freedom of thought and expression essential to the University rest on confidence that privacy will be respected and disclosure of personal data will be made in accordance with the requirements of relevant laws. While the data users collecting and having custody of personal data are immediately responsible for its protection, the ultimate protection comes from a university-wide awareness of the importance of privacy and the requirements of the relevant laws.

This Code of Practice for Handling Personal Data (the code) is based on the underlying principles and guidelines published in the Code of Practice on Human Resource Management issued by the Privacy Commissioner for Personal Data (PCPD) under the Personal Data (Privacy) Ordinance.

The primary purpose of the code is to provide practical guidance to University employees on how to properly handle personal data in the carrying out of University functions and activities. It deals with issues concerning collection, holding, accuracy, use and security, and subject access and correction in relation to the personal data of prospective, current and former employees and students of the University. All University employees are required to make reference to this code in determining their practices in handling personal data and must observe the provisions of the code. The consequence of mishandling personal data will range from receiving instruction on proper handling of such data to corrective or disciplinary actions.

II. Interpretation

Unless the context otherwise requires, the terms used in the code have the following meanings:

"data" means any representation of information (including an expression of opinion) in any document, and includes a personal identifier.

"data subject", in relation to personal data, is an individual who is the subject of the data.

"data user", in relation to personal data, is a person who, either alone or jointly or in common with other persons, controls the collection, holding, processing or use of the data.

"discrimination ordinances" means the Sex Discrimination Ordinance (Cap. 480), the Disability Discrimination Ordinance (Cap. 487), and the Family Status

Discrimination Ordinance (Cap. 527), and Race Discrimination Ordinance (Cap. 602).

"document" includes, in addition to a document in writing –

(a) a disc, tape or other device in which data other than visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced from the disc, tape or other device; and
(b) a film, tape or other device in which visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced from the film, tape or other device.

"DPP" means a Data Protection Principle in Schedule 1 of the PD(P)O. (Please refer to Section I of Annex 1.)

"PD(P)O" and "the Ordinance" – both terms refer to the Personal Data (Privacy) Ordinance.

"permitted purpose" in relation to personal data means a lawful purpose directly related to University functions or activities for which the data were to be used at the time of their collection; a directly-related purpose for which the data were or are used; the fulfillment of a relevant statutory requirement; or a purpose for which the data were or are used where the data subject has given his or her express consent to that use.

"personal data" means any data relating directly or indirectly to a living person; from which it is practicable for the identity of the individual to be directly or indirectly ascertained; and in a form in which access to or processing of the data is practicable.

"personal identifier" means an identifier assigned to an individual by a data user to uniquely identify that individual in relation to the data user for the purpose of the operations of the user.

"Personal Information Collection Statement" means a statement made to an individual in respect of whom personal data are collected by the person providing the statement in compliance with the requirements of DPP1(3). (Please refer to Section I of Annex 1)

"prescribed consent" is the express consent of the person given voluntarily, which has not been withdrawn by notice in writing.

"requestor", in relation to personal data, means the data subject or a person authorized by the data subject to act on his/her behalf to make a data access or correction request.

"University" means the University and its Affiliated Institutions such as Lingnan Institute of Further Education (LIFE).

Words denoting the gender or the neuter shall be deemed to include both genders and the neuter.

III. Obligations of Employees of the University in Handling Personal Data

1. While all University employees who are data users have to comply with the requirements of the Ordinance, this code has been prepared for the reference of all employees who have to handle personal data at work. For the purpose of this code, University employees who are directly or indirectly related to the collection, holding, processing and use of personal data in the course of their work are regarded as University personal data users (UPD user).

2. Recognizing that specific personal data of current as well as former students and members of the University community must be maintained for employment, educational, research and other institutional purposes, it is the University's policy that such data be collected, maintained, and used by the University only for appropriate, necessary, and clearly defined purposes, and that such data be controlled and safeguarded properly to ensure the protection of personal privacy to the extent permitted by law.

3. All staff members of the academic departments, administrative and service units and research institutes/centres of the University who collect or are given personal data of prospective, current and former students and members of the University for them to carry out their work are bound by this code.

4. Heads of departments/units (HoDs) that collect and/or hold personal data are required to establish or observe appropriate rules for the collection, use, retention and disposal of such data for relevant operational processes. They are also required to establish appropriate practices for their staff members to ensure that such personal data are maintained with accuracy, relevance, timeliness, and completeness, and appropriate and reasonable safeguards are implemented for data security and confidentiality. The guidelines on processing personal data for specific employment-related and student-related processes are found at Annexes 2 and 3.

5. All personal data collected and held by the University shall only be handled by the HoD or a staff member of the department/unit designated by him/her to be responsible for handling such data. HoDs should forward a list detailing the name(s) and position(s) of the designated staff, types of data to be handled, authorized duration (if applicable), etc. to the Chief Data Protection Officer (Chief DPO) for record and a copy of such list to the Human Resources Office (HRO) [for employment-related personal data] and the Registry/Registry of Lingnan Institute of Further Education (LIFE) [for student data]. The HoDs shall inform the Chief DPO and HRO/Registry/Registry of LIFE when there is any change in the information.

6. Employees with assigned responsibility for personal data must exercise care and follow the requirements of the Ordinance and this code. For policy clarification and details, employees are advised to contact the Chief DPO, Data Protection Officer of each department/unit or the HRO/Registry/Registry of LIFE.

7. All employees should not use personal data held by the University for personal reasons.

8. Where there are reasonable grounds to believe that personal data have become inaccurate since the data were collected, the UPD user is required to either erase the data or refrain from using such data until such time as the data have been properly updated.

IV. Broad Categories of Personal Data kept by the University

1. Employment-related personal data

Employment-related personal data held by the University comprise the following:

- personal particulars
- family details
- health records
- qualifications, skills and professional expertise
- recruitment details and appointment documents
- salary data
- leave records
- benefits details (including supporting documents)
- performance or work assessment data
- outside practice records
- staff development details
- research records
- insurance coverage details
- tax data

2. Personal data of students

Student personal data held by the University comprise the following:

- personal particulars
- family background
- financial situation
- educational qualifications (including previous schools & examination results)
- enrolment records (including exchange programmes, if any)
- assessment records, academic standing, and degree awarded (including classification)
- payment records
- books on loan records

- ♦ scholarships and bursaries records
- ♦ extra-curricular activities
- ♦ leave records
- ♦ health problems/disabilities (if applicable)
- ♦ disciplinary records (if any)
- ♦ profession & salary data (graduates/alumni)

3. Personal data of donors

- ♦ personal particulars
- ♦ profession
- ♦ education background (department, programme, graduation year)
- ♦ credit card information

4. Personal data published in public lists, such as University Calendar, University Communication Directory, University and personal webpages, etc., which may include name, rank/title, educational qualifications, dates of employment, office telephone numbers, office/electronic mail address, department/unit, are regarded as published information and therefore not covered under the provision of this code.

5. It is the University's policy that personal data, other than those specified in (4) above, should not be released to unauthorized parties within or outside the University without the express consent of the individual concerned, except in cases of exemption as provided by the PD(P)O.

V. Data Management Roles and Responsibilities

1. Definition

Banner Data – Any data that reside on, are transmitted to, or extracted from any Banner system, including databases or database tables/views, file systems and directories, and forms.

Banner System – This includes the modules, namely Student, Human Resources, Finance, Payroll, Alumni; and any other interfaces to these systems, such as the Infosilem TPHi Timetabling, DegreeWorks and home-grown applications.

Data Owners – Data Owners are individuals or business units that can determine who should have access to data within their jurisdiction, and what those access privileges should be. Responsibilities for implementing security measures may be delegated, though accountability remains with the owner of the data.

Data Managers - Data Managers oversee data management functions related to the capture, maintenance and dissemination of data for a particular operational area. They are responsible for the general administration of user access to data within their area(s) of responsibility. Data Managers are appointed by the respective Data Owner.

Data Guardian – Data Guardian of the Banner System is Information Technology Services Centre (ITSC). Its role is to ensure all the personal data kept in the system are secure and available for its authorized use under the approval of the respective data owner(s). In the case of student system in which there are multiple data owners and upon submitting the data access request from the requester to the Secretary of Personal Data Privacy Committee (PDPC), a panel member appointed by the Chairman of PDPC should decide whether the request for data access should be approved upon understanding the use of the data by the requester and measures taken by the requester to protect privacy. ITSC will act on the decision of such panel member to release the requested data or not.

2. Area of Responsibility

Module	Data Owner(s)
Student System Banner forms that begin with the letter "S" (except for SR and SA forms which are Recruit/Admissions), as well as most of the forms that begin with the letter "G". Examples are SPAIDEN, SFAREGQ, SFASLST, SGASTDN, GOAEMAL.	Registrar (Undergraduate Programmes); Dean of School of Graduate Studies (Research Postgraduate Programmes); Programme Directors (Taught Postgraduate Programmes); Director of Lingnan Institute of Further Education
Finance System Banner forms that begin with the letter "F" - like FPAREQN.	Director of Finance
Human Resources System Banner forms that begin with the letters "P" or "N" - like PHATIME, or NBIJLST. Banner forms that begin with the letter "G", like GZAPINR	Director of Human Resources
Payroll Banner forms that begin with the letters "P" or "N"- like PHATIME, or NBIJLST.	Director of Finance
Alumni / Advancement Banner forms that begin with the letter "A" - like APASBIO.	Director of Institutional Advancement and Public Affairs

Module	Data Manager(s)
Student System	Team leaders in Registry (Undergraduate Programmes); Administrative head of School of Graduate Studies (Research Postgraduate Programmes); Associate Director of Student Affairs; Associate Programme Directors (Taught Postgraduate Programmes); Assistant/Associate Director (Quality Assurance and Registry) of LIFE
Finance System	Associate Director of Finance
Finance System - Research Projects	Principal Investigator
Human Resources System	Associate Director of Human Resources
Payroll	Associate Director of Finance
Alumni / Advancement	Senior Alumni Affairs Manager Institutional Advancement Manager

VI. Data Processor Management

1. When the University shares personal data it controls with a third party to perform tasks in relation to that data on behalf of the University, this third party is then a "data processor".

   (a) The University and the data processor should have a binding contract that the data processor will commit to certain standards, including but not limited to data security, following the requirements of the Code, ensuring the University to meet its legal requirement with regards to individual's data privacy and protection.

2. When the University shares personal data it controls with a third party for joint purposes, this third party is then a "joint data user". The sharing of such data can be one-off or long-term.

   (a) The University and the joint data controller shall have a documented arrangement stating their respective roles and responsibilities with regards to individual's data privacy and protection.

   (b) The joint data controller shall not share such data to another third party without the University's consent. A new documented arrangement shall be made if necessary.

3. When the University shares personal data it controls with a third party for the said third party to carry out its own functions, the University and the third party then becomes two separate "data user".

   (a) It is normally not advised for the University to have this practice, unless the third party is closely related to the University (such as a University Trust, a University Donor, a University Student Union, and a University Student Society), or unless required by law.

   (b) Extra precaution shall be taken if sharing of such data to a third party that is not closely related to the University is indeed justified, that is necessary for important public interest (e.g. to fulfil tax and finance auditing, to assist genuine criminal investigation, or to assist major public health initiatives), or that sharing such data is to protect a University member's vital interest where he or she is in a critical situation and a consent is not obtainable. Agreements, preferably written, shall be made to ensure that the third party does not use the data for profit, that the third party have the necessary measures to safeguard the personal data.

4. When working with third party data processors, the University shall, whenever possible, have a contractual relationship with its data processor, joint data user and data user whom the University shares data with.

(a) When entering into a contract, the University shall duly consider whether principles listed below have been covered in the contract with a data processor. Data processor includes data processor defined in VI-1, joint data user defined in VI-2 and separate data user defined in VI-3:

i. Necessary security measures shall be included to protect the personal data.
ii. The data processor shall not keep personal data longer than necessary. The data processor shall return, delete or destruct the personal data it withholds in a timely manner.
iii. The data processor is not allowed to use or disclose the personal data it withholds for purposes that are not specified in the contract unless a new contract or agreement is reached with the University.
iv. The data processor cannot sub-contract its services to a third party unless a new contract or agreement is reached.
v. In the circumstances that sub-contracting is necessary, the sub-contractor shall have the same obligations, but the primary data processor is fully liable to the data user with regards to fulfilling the data processor's obligations.
vi. In the case that any abnormalities are found, such as a potential data breach, the data processor must make immediate report to the data user.
vii. The data processor shall ensure compliance of agreed obligations by taking necessary measures, such as developing personal data protection policies and training for responsible staff, and such measures shall be included as part of the service in data processing.
viii. As the data user, the University has rights to audit and inspect the services provided by the data processor.
ix. In a contract, the University and the data processor shall agree on clauses that specify the consequences of violation of contractual terms.

VII. Purpose and Use of Personal Data

1. All personal data kept by a UPD user should be used only for the purpose for which they are collected or for a directly related purpose. If a UPD user wishes to use the data for a purpose other than a purpose for which the data were collected, he must, before using the data, seek explicit consent of the data subject in writing for the use of the data.

2. <u>Employment-related personal data</u>

(a) In general, employment-related personal data are collected, processed, used and kept by the University for the following employment-related purposes:

- manpower planning
- recruitment and appointment
- administration and payment of wages and other benefits
- staff appraisal and performance assessment
- administration of personnel actions
- staff training and development
- compliance with University policy and/or legislation in relation to employment-related matters
- University promotional and public relation activities
- tax matters

(b) Specifically, academic teaching staff are requested to give explicit consent to the release of their Course Teaching and Learning Evaluation scores to enrolled or prospective students to facilitate programme and course selection.

3. Student data

In general, students' personal data are collected and maintained by the University for purposes in relation to their studies at the University which may include:

- admission and registration
- academic advising
- hostel
- payment
- grant/loan
- books borrowing
- using University facilities
- scholarship, subsidies, financial assistance and bursaries
- counselling
- special educational needs
- international programmes
- student training and development
- society experience
- assessment
- transcript (academic and non-academic)
- testimonials
- degree certificates
- disciplinary matters
- contact and communication
- compliance with University policy and regulations, and/or registration in relation to health and safety, and other study-related matters
- alumni and graduates

4. Donor data

In general, donors' personal data are collected and maintained by the University for purposes in relation to their donations and sponsorships to the University which may include:

- solicitation
- donation and sponsorship receipts
- tax deduction
- contact and communications

5. Direct marketing

A UPD user who intends to use a data subject's personal data in direct marketing must inform the data subject of the UPD user's intention and obtain the consent from the data subject. The obligation on the UPD user applies even if the data were collected from a third party.

"Direct marketing" is defined as:

(a) the offering, or advertising of the availability, of goods, facilities or services; or

(b) the solicitation of donations or contributions for charitable, cultural, philanthropic, recreation, political or other purposes, through

  i. sending information or goods, addressed to specific persons by name, by mail, fax, electronic mail or other means of communication; or

  ii. making telephone calls to specific persons

A UPD user must inform the data subject as early as possible, preferably on or before the data are collected, the UPD user's intention to use the data subject's personal data for direct marketing.

The data subject must be informed of the following:

(a) the UPD user's intention to use the personal data of the data subject for direct marketing;

(b) the UPD user will not use the data without the data subject's consent;

(c) the kind of personal data to be used;

(d) the classes of marketing subjects in relation to which the data are to be used; and

(e) the response channel through which the data subject may give consent to the intended use.

The UPD user must also notify the data subject of his/her right to opt-out, orally or in writing, from the direct marketing list at any time. The UPD user must maintain a list of all customers who have indicated that they do not wish to receive further marketing approaches (the "Opt-Out List"). A UPD user must erase the personal data which are no longer required for the original purpose.

Under the same principle, a UPD user must not provide personal data to other third parties for direct marketing without explicit consents from data subjects.

VIII. General requirements in handling personal data

1. Personal Information Collection Statements[1]

When a UPD user collects personal data from a job applicant, employee or former employee, prospective and current students, alumni and other members of the University community, he/she must explicitly inform the individual on or before collecting the data of the following information. Personal Information Collection Statement Template is found on Annex 5:

(a) the purpose for which the data are to be used;
(b) the duration for which the data will be kept;
(c) the classes of third parties[2] (within or outside the University) to whom the data may be transferred for one or more of the purposes given in (a) above or a directly related purpose;
(d) whether or not it is obligatory to supply the data and, if not obvious from the circumstances, the consequences of not providing such data;
(e) the rights of data subjects to request access to and corrections of their personal data; and
(f) the name and address of the officer to whom such requests should be made; and
(g) if the personal data will be used for direct marketing activities, the UPD user shall:
    i. inform data subjects on the purpose and intention to use their personal data for direct marketing;
    ii. obtain consent from the data subject, and if applicable any transfers of data to a third person for direct marketing;
    iii. identify the kinds of personal data to be used for direct marketing;
    iv. solicit the classes of goods, facility or services offered/advertised or the purpose for which donations or contributions (i.e. marketing subjects); and
    v. provide an option and a response channel for data subject to express consent or opt-out.

[1] A UPD user is not required to give such a statement in relation to personal data collected before 20 December 1996 and may continue to use such data without obtaining the consent of the individuals concerned as long as the purposes for which the data are used come within the reasonable scope of the purpose(s) for which the data were originally collected.

[2] Government departments to which a UPD user is required by law to transfer certain personal data, for example the Inland Revenue Department, need not be included in a statement of such third party. There is also no requirement for the UPD users to name other internal departments/units or employees of the University to whom personal data may be transferred for the purposes of employment. More information on exemption is found in Section II of Annex 1.

2. The identity card number and other personal identifiers in employee / student records

In accordance with University policy and the Code of Practice on the Identity Card Number and other Personal Identifiers issued by the PCPD:

(a) The HRO may collect the HKID number and copy of the identity card of an employee. Such data, however, should only be kept in the confidential employee personal files kept in the HRO. A Staff Card shall be issued to each serving employee, which shall be used as an official identifier of the staff for University functions and activities.

(b) The Registry/Registry of LIFE keeps the students' HKID number in its internal records. Other units such as the Finance Office, Office of Student Affairs and Office of Institutional Advancement and Public Affairs (OIAPA)/Student Development Office and Communication and Public Relations of LIFE may also keep HKID number of the students/graduates for their uses as appropriate. A student ID Card with a unique student ID number shall be issued to each registered student, which shall be used as an official identifier of the student within the University.

3. Definition of records of personal data held by the University

(a) All data collected by a UPD user shall be kept in an official document of the University (including official copies of electronic data stored in a computer system, e.g. HRIS and payroll system, managed by an authorized data user).

(b) Only official records of personal data kept by the University shall be regarded as personal data in the custody of the University and be provided to a data subject upon request in accordance with relevant procedures.

4. Security of personal data

(a) Confidentiality and security are the responsibility of and should be fully observed by every University employee in handling all University functions and activities so that official information and personal data may be passed from one department or party to another with confidence that such information will be handled properly in accordance with relevant regulations and law.

(b) A UPD user should implement security measures to ensure the privacy of personal data to whom he/she is given access for him/her to carry out his/her work for "permitted purposes".

i. Collection, Processing and Use of personal data

a. The collection, processing and use of personal data should be restricted to the head of department/unit concerned and those who are authorized and designated by him/her to assist in the handling of the documents.

b. Employees handling the personal data must not discuss in public areas any such personal data.

ii. Storage

a. The officer in charge of the use of personal data shall apply appropriate security protection to personal data against unauthorized or accidental access, processing or destruction of those data. As a matter of good practice, personal data should be kept in confidential files locked in cabinets located in a controlled area accessible only to staff cleared to handle such personal data or kept in password controlled electronic files.

b. A "clear desk" policy is required of employees who are given access to personal data. They must file or put in cabinets all documents and papers containing personal data in locked cabinets before leaving his working position for an extended time or at the end of each working day. If a "clear desk" policy is not feasible, such documents should be kept inside a locked room.

c. Documents containing personal data and confidential information in use or taken to official meetings must not be left unattended.

iii. Transmission of personal data

a. The "need-to-know" principle should be applied in the handling of all documents containing personal data, i.e. the circulation of confidential personal data should be no wider than what is required for the efficient performance of duties.

b. Employees granted access to personal data should not make private copies of or communicate to unauthorized parties within or outside the University any such personal data. If a UPD user is required to make personal data available to employees outside his/her own department/unit (or other members of the University community), he/she should ensure that such people are made aware of the need to apply appropriate security protection to such data.

c. When sending documents containing personal data to another data user, such documents must be sealed in envelope and to be opened by the addressee or the authorized person only.

d. If it comes to the knowledge of the UPD user who has collected personal data and subsequently transmitted such data to another data user for permitted purposes that such personal data are no longer accurate, he/she must notify the other data user of the inaccuracy. In addition, the former should provide the latter with such particulars as are necessary to ensure that the data are accurate.

iv. Data on electronic information system

a. Data on computer systems

All UPD users should ensure that access to personal data held on an automated system is controlled by security features such as account names and secured passwords or an audit trail or a warning feature that could deter unauthorized attempts to access the data.

b. All authorized users of such data should take steps to eliminate all unofficial documents in relation to an official document as soon as practical (e.g. draft copies) and to prevent the establishment of unauthorized copies of such documents on computers that are outside such controls as are applied to the authorized copy.

c. Internet/Network Usage

The UPD users of personal data are required to take adequate steps to secure the data as it travels on any network and when it reaches a server computer. They are required to consult the ITSC for practical advice for the effective implementation of such measures. Examples of the measures include:

i. establish a secure network channel such as a VPN connection before data transmission is carried out;
ii. employ WPA2 encryption for WiFi connection before data are transmitted through the air;
iii. avoid transmission of sensitive data in public access computers such as public computers in Internet cafés or public libraries.

d. Emails

It is also the responsibility of the data users to take adequate steps to protect and dispose of properly all personal data that they include in, or attach to, any email to be sent on a network. Employees are requested to note that multiple copies of the data may be established after the first transmission of the email containing such data; (e.g. a copy of the email may reside in the transmitting email server computer and another copy may remain in the receiving server). Also, emails encrypted using certain methods (e.g. S/MIME) are only protected during transmission but may be read by any person having access to the sender's or the recipient's computer. All UPD users should implement practices with respect to the proper destruction of emails and attachments to emails that contain personal data. Examples of good practices include:

i. always use the Lingnan University Campus Email to avoid sending sensitive data over public Internet email that may result in a copy being stored or archived by a third-party server.

ii. password protect the data file using tools such as Word, Excel, Acrobat, etc. when it is necessary to send sensitive data using email. The password should be sent via a separate email message or different mean.

e. Data Storage on Computer Devices

Sensitive data should be stored on a secure network drive instead of a mobile device to prevent data leakage in case of losing the device. Sensitive data should be encrypted before transferred into removable media or via email. The UPD users can consult ITSC on the most updated encryption software. Encrypted USB storage device may be used for additional level of protection. Proper security should be enabled to prevent the loss or theft of a computer, mobile device or USB storage device. Virus scanning is important to prevent data leakage. Files downloaded from the Internet, email attachments or external storage devices should be scanned for virus before opened or saved on a computer.

5. <u>Disposal of personal data</u>

(a) Personal data no longer required for the purpose for which they were to be used shall be destroyed in accordance with the requirements of this set of guidelines and the PD(P)O. The UPD users must ensure that the physical destruction of personal data of a prospective employee/student, current employee/student or

former employee/student held on paper or other non-erasable medium is undertaken with appropriate security measures, to avoid their inadvertent disclosure or transfer to unauthorized parties prior to destruction. However, the waste for secure disposal may be collected in special containers in a controlled area accessible only to staff cleared to handle personal data of the type being disposed of.

(b) Officer in charge may arrange for large volumes of personal data to be stored or destroyed by a reputable storage or waste disposal company.

(c) Notwithstanding this requirement to dispose of personal data, such data must be retained where erasure is prohibited under any law or where there are reasonable grounds to believe that it is in the public interest not to dispose of the data.

(d) Where it is desirable to retain certain personal data, for example, for statistical or precedent purposes, measures should be taken as far as feasible to erase any information from such data which directly or indirectly identifies or from which the identity of an individual can be deduced. Such data from which the identity of the data subject cannot be directly or indirectly ascertained will cease to be personal data and hence will not be governed by the requirements of the PD(P)O.

(e) The data retention and disposal handling procedures should at a minimum, consist of the following key elements:

i. The procedure to identify each type of records, digital or physical for retention or erasure purpose;
ii. The retention period of each type of record;
iii. The procedure to identify all copies of the personal data including photocopies, backup or digital copies;
iv. The erasure method to be used for each type of records, which must match with the type of storage technology (i.e. the shredded wastes should be specially handled or can be thrown away with normal office waste, and the transporting personal data outside the data user's premises);
v. The procedure to securely delete digital or destroy paper records that are no longer required in a defined response timeframe;
vi. The procedure to identify the erased records in backup media and to ensure such information cannot be accessed and/or used;
vii. The documentation requirement of the erasure record;
viii. Roles and responsibilities of relevant parties (e.g. the Data Owner, the Panel, DPO and the ITSC) in disposal process; and
ix. A process for periodic review (at least on an annual basis) of the data retention and disposal mechanism cause and changes in the internal control environment or external requirements.

(f) Data disposal record should be constructed to document data disposal activities. A Personal Data Inventory template can be found in Annex 6. The data disposal record should at least include the following information:

i. Department / Unit / Team
ii. Record Name / Format / Medium / Location
iii. Record reference number
iv. Reason for Disposal
v. Method of Disposal / Destruction
vi. Whether all copied, including backups, are disposed
vii. Preparer and approver (name, position and contacts)
viii. Date of disposal

6. Handling procedure on EU residents' personal data

(a) The University is accountable to guarantee its members who are EU residents have rights to:

- be notified on data processing of his or her personal data,
- be able to delete his or her personal data without undue delay under circumstances, including where the personal data are no longer necessary in relation to the purposes for which it is collected, where the consent is withdrawn, where there is no overriding legitimate interest,
- be able to object to data processing,
- restrict data processing to an interim period
- be able to obtain from the University and to transfer to another data controller a copy of his or her personal data in an orderly, common and machine-readable manner upon request.

IX. General requirements in handling data requests

1. Data access requests by data subjects

(a) Generally speaking, an individual whose personal data are held by the University is entitled to:

- check whether the University holds his personal data;
- request to be given a copy of such data; and
- require the University to correct any of such data if such data are inaccurate.

(b) In accordance with the Ordinance, a UPD data user responding to a data access request from a data subject must not disclose to the individual seeking access any data identifying any other individual unless that other individual consents explicitly. In accordance with Section 20(2) of the PD(P)O, when providing relevant documents (e.g. extracts of meeting minutes) concerning an employment issue of a data subject (e.g. performance review, termination of an employment, etc.) in compliance with a data access request, copy of the requested personal data contained in the relevant document will be provided to the data subject with

omission of personal data of any third parties (e.g. the names and other identifying particulars of other individuals which would disclose the identity of such other individuals).

(c) Generally speaking, where one document contains personal data of more than one data subject, the University as a data user will comply with a data access request from one or more data subjects by providing the personal data relevant to each requestor (data subject) only.

(d) When personal data are collected for a process which has not been completed and which later includes an appeal mechanism, the University is entitled to refuse to comply with a data access request until the completion of the process.

2. Types of personal data to be provided in response to a data request

(a) In order to save cost and time for both the data subject and the University, only employment/student related personal data specifically required by a data subject shall be provided in response to a request.

(b) However, unless otherwise specifically required by the data subject, the following types of employment-related personal data will not be normally included in a response:

i. Documents in the personal files
- Curriculum vitae and copies of certificates, transcripts, testimonials
- Appointment letter
- Terms of Service
- Leave records
- Personal Particulars Form
- Personal Data Update Form
- Benefits applications, attachments, claims
- Personnel Actions documents submitted by the data subject
- Reference letters submitted by data subject

ii. Any official document a copy of which has been already given to the data subject in his/her capacity as a participating party (e.g. a member of a committee) in the business concerned at the time when such a document is produced or after it is formally signed/confirmed/recorded. Examples of such kind of documents include:
- minutes/notes of meetings,
- Staff Appraisal Reports (copy signed by both the appraiser and the appraisee)
- letters/memos written by the data subject
- letters/memos directly addressed/formally copied to the data subject,
- email memos/notices sent to or by the data subject.

3. Procedures for handling a data request for personal data

(a) Upon receipt of a data request transmitted by the Chief DPO, HoD or the designated employee responsible for handling data requests (i.e. Data Protection Officer (DPO) of each department/office and the research units/centres/programmes to be taken care by the Faculty DPO concerned) shall forward a list of personal data on the data subject kept in the department/unit to the Chief DPO.

(b) To ensure confidentiality, uniformity, and accuracy of personal data to be provided, the HRO and the Registry/Registry of LIFE will be responsible for coordinating all the documents in relation to data requests from current or former employees or students of the University respectively. The Chief DPO will forward all the lists prepared by other UPD users to the HRO/Registry/Registry of LIFE. HRO/Registry/Registry of LIFE will compare its own list with these lists, and to avoid unnecessary duplication of documents, will inform the department/unit concerned to forward only a copy of the documents needed to the HRO/Registry/Registry of LIFE for consolidation, and if necessary, for editing.

(c) As provided by the PD(P)O, the HRO/Registry/Registry of LIFE will be responsible for editing the documents in accordance with the provisions of the PD(P)O to ensure that only personal data belonging to the data subject will be provided to him/her. All information other than personal data or personal data belonging to other individuals shall not be provided in response to a data access request.

(d) HRO/Registry/Registry of LIFE will forward to the Chief DPO the edited copies of the documents contained in a sealed envelope marked with "to be opened by the addressee only" for his/her transmission to the requestor.

(e) The University has decided to levy charges on the requestor to meet some of the cost of handling data requests. HoD and HRO/Registry/Registry of LIFE should complete and forward to the Chief DPO a timesheet which logs the amount of time spent on preparing the documentation for the data request for his/her calculation of the charges. In cases of doubt or need for information, the Chief DPO may request the HoD/HRO/Registry/Registry of LIFE to provide further input for dealing with the requests and charges.

(f) The University shall respond to each request not later than 40 days after receiving the request.

(g) The HRO/Registry/Registry of LIFE will keep a record of personal data provided in response to a data access request for a period of 12 months or until the case closes, whichever is earlier.

4. Procedures for handling a data correction request

(a) A data subject who has been provided with a copy of personal data is entitled to ask the data user to correct any inaccurate data in that copy.

(b) If such a correction request relates to data that are an expression of opinion or evaluative comments (e.g. on performance), and the data user is not satisfied that the data are inaccurate, the data user may refuse to make the correction. In the event of refusing to correct a record of an opinion, the data user must make a note of the requestor's and his/her view on the inaccuracy of the data, which must be attached to the data user's copy of the data in such a way that it will be seen by anyone who uses the data. A copy of the note shall also be sent to the data subject together with the data user's notice of refusal to comply with the correction request as required by the PD(P)O.

5. The procedure for application for employment-related or student-related personal data access and/or correction is set out in Annex 4, and enquiries on these guidelines should be directed to the HRO or the Registry/Registry of LIFE.

X. Handling of Data Breach Incident

1. The University as a data user shall take remedial actions to mitigate the damage that may inflict to the data subjects in a data breach.

(a) Gathering of essential information relating to the breach shall be promptly taken by PDPC. The Chairman shall be informed in a timely manner.

(b) Necessary containment measures shall be taken to reduce harm to the data subjects. It may be necessary to notify the law enforcement agencies, the relevant regulators, and the data processors.

(c) In the event that such data breach is due to the negligence of a delegated data processor, the data processor is required to take immediate remedial measures and inform the University.

(d) Assessment of risks and harm shall be taken to prevent similar data breach from happening in the future.

(e) The University is recommended to inform its members about the data breach, so its members can stay alerted.

XI. Training and education

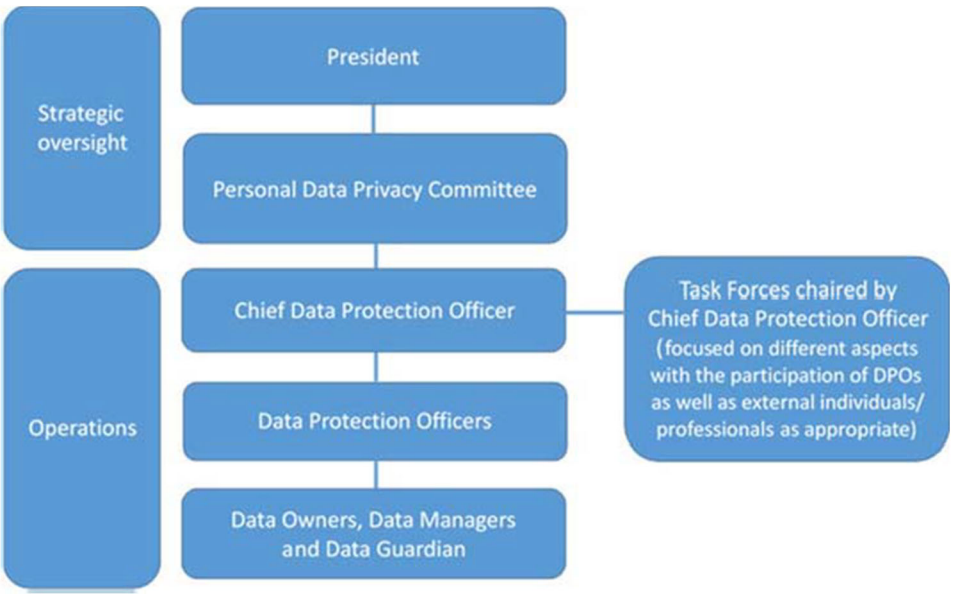
1. The University as a data user is committed to complying with the requirements of the PD(P)O and all staff members and students are required to observe and act in accordance with all relevant provisions of the PD(P)O. In order to promote the awareness on matters relating to data privacy and data protection and to enhance the understanding of the PD(P)O, the University should regularly organize publicity and education programmes for all new comers, staff and students through seminars, talks and other awareness campaigns.

2. Mandatory education programme tailored to specified needs would be provided to the DPOs and related personnel handling personal data as deemed appropriate.

3. Regular quizzes on PD(P)O should be given to staff and students.

XII. Reporting and monitoring of the Code of Practice

1. The University's data privacy governance framework and reporting structure are set out as follows:



2. The Code will be subject to review annually by PDPC. Any variations and amendments to the document will be announced to members of the University in due course.

3. The secretary of PDPC is responsible for coordinating members of the PDPC in the last quarter of each calendar year for reporting and revision on the Code and matters related to Data Privacy and Protection of the University. PDPC shall decide the format (e.g. verbal communication, written report and/or meetings) to monitor the progress or consolidate solutions to matters arising from the annual review.

Last updated: April 2023

Extraction from the Personal Data (Privacy) Ordinance

I. Data Protection Principles

1. Principle 1 - purpose and manner of collection of personal data

(1) Personal data shall not be collected unless -
- (a) the data is collected for a lawful purpose directly related to a function or activity of the data user who is to use the data;
- (b) subject to paragraph (c), the collection of the data is necessary for or directly related to that purpose; and
- (c) the data is adequate but not excessive in relation to that purpose.

(2) Personal data shall be collected by means which are -
- (a) lawful; and
- (b) fair in the circumstances of the case.

(3) Where the person from whom personal data is or is to be collected is the data subject, all practicable steps shall be taken to ensure that - *(Amended 18 of 2012 s. 40)*
- (a) he is explicitly or implicitly informed, on or before collecting the data, of -
  - (i) whether it is obligatory or voluntary for him to supply the data; and
  - (ii) where it is obligatory for him to supply the data, the consequences for him if he fails to supply the data; and
- (b) he is explicitly informed -
  - (i) on or before collecting the data, of -
    - (A) the purpose (in general or specific terms) for which the data is to be used; and
    - (B) the classes of persons to whom the data may be transferred; and
  - (ii) on or before first use of the data for the purpose for which it was collected, of - *(Amended 18 of 2012 s. 40)*
    - (A) his rights to request access to and to request the correction of the data; and
    - (B) the name or job title, and address, of the individual who is to handle any such request made to the data user, *(Replaced 18 of 2012 s. 40)*

unless to comply with the provisions of this subsection would be likely to prejudice the purpose for which the data was collected and that purpose is specified in Part 8 of this Ordinance as a purpose in relation to which personal data is exempt from the provisions of data protection principle 6.

(Amended 18 of 2012 s. 40; E.R. 1 of 2013)

2. Principle 2 - accuracy and duration of retention of personal data

(1) All practicable steps shall be taken to ensure that -

(a) personal data is accurate having regard to the purpose (including any directly related purpose) for which the personal data is or is to be used;

(b) where there are reasonable grounds for believing that personal data is inaccurate having regard to the purpose (including any directly related purpose) for which the data is or is to be used - *(Amended 18 of 2012 s. 40)*

(i) the data is not used for that purpose unless and until those grounds cease to be applicable to the data, whether by the rectification of the data or otherwise; or

(ii) the data is erased;

(c) where it is practicable in all the circumstances of the case to know that -

(i) personal data disclosed on or after the appointed day to a third party is materially inaccurate having regard to the purpose (including any directly related purpose) for which the data is or is to be used by the third party; and

(ii) that data was inaccurate at the time of such disclosure, that the third party -

(A) is informed that the data is inaccurate; and

(B) is provided with such particulars as will enable the third party to rectify the data having regard to that purpose. *(Amended 18 of 2012 s. 40)*

(2) All practicable steps must be taken to ensure that personal data is not kept longer than is necessary for the fulfillment of the purpose (including any directly related purpose) for which the data is or is to be used. *(Amended 18 of 2012 s. 40)*

(3) Without limiting subsection (2), 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 of the data. *(Added 18 of 2012 s. 40)*

(4) In subsection (3) –

data processor (資料處理者) means a person who -

(a) processes personal data on behalf of another person; and

(b) does not process the data for any of the person's own purposes. *(Added 18 of 2012 s. 40)*

3. Principle 3 - use of personal data

(1) Personal data shall not, without the prescribed consent of the data subject, be used for a new purpose. *(Amended 18 of 2012 s. 40)*

(2) A relevant person in relation to a data subject may, on his or her behalf, give the prescribed consent required for using his or her personal data for a new purpose if –

(a) the data subject is –
  (i) a minor;
  (ii) incapable of managing his or her own affairs; or
  (iii) mentally incapacitated within the meaning of section 2 of the Mental Health Ordinance (Cap. 136);

(b) the data subject is incapable of understanding the new purpose and deciding whether to give the prescribed consent; and

(c) the relevant person has reasonable grounds for believing that the use of the data for the new purpose is clearly in the interest of the data subject. (Added 18 of 2012 s. 40)

(3) A data user must not use the personal data of a data subject for a new purpose even if the prescribed consent for so using that data has been given under subsection (2) by a relevant person, unless the data user has reasonable grounds for believing that the use of that data for the new purpose is clearly in the interest of the data subject. *(Added 18 of 2012 s. 40)*

(4) In this section-
new purpose (新目的), in relation to the use of personal data, means any purpose other than—

(a) the purpose for which the data was to be used at the time of the collection of the data; or

(b) a purpose directly related to the purpose referred to in paragraph (a). *(Added 18 of 2012 s. 40)*

4. Principle 4 - security of personal data

(1) All practicable steps shall be taken to ensure that any personal data (including data in a form in which access to or processing of the data is not practicable) held by a data user is protected against unauthorized or accidental access, processing, erasure, loss or use having particular regard to -– *(Amended 18 of 2012 s. 40; 17 of 2018 s. 129)*

(a) the kind of data and the harm that could result if any of those things should occur;

(b) the physical location where the data is stored; *(Amended 18 of 2012 s. 40)*

(c) any security measures incorporated (whether by automated means or otherwise) into any equipment in which the data is stored; *(Amended 18 of 2012 s. 40)*

(d) any measures taken for ensuring the integrity, prudence and competence of persons having access to the data; and

(e) any measures taken for ensuring the secure transmission of the data.

(2) Without limiting subsection (1), 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 unauthorized or accidental access, processing, erasure, loss or use of the data transferred to the data processor for processing. *(Added 18 of 2012 s. 40)*

(3) In subsection (2)—
data processor (資料處理者) has the same meaning given by subsection (4) of data protection principle 2. *(Added 18 of 2012 s. 40)*

5. Principle 5 - information to be generally available

All practicable steps shall be taken to ensure that a person can -

(a) ascertain a data user's policies and practices in relation to personal data;

(b) be informed of the kind of personal data held by a data user;

(c) be informed of the main purposes for which personal data held by a data user is or is to be used. (Amended 18 of 2012 s. 40)

6. Principle 6 - access to personal data

A data subject shall be entitled to -

(a) ascertain whether a data user holds personal data of which he is the data subject;

(b) request access to personal data -
(i) within a reasonable time;
(ii) at a fee, if any, that is not excessive;
(iii) in a reasonable manner; and
(iv) in a form that is intelligible;

(c) be given reasons if a request referred to in paragraph (b) is refused;

(d) object to a refusal referred to in paragraph (c);

(e) request the correction of personal data;

(f) be given reasons if a request referred to in paragraph (e) is refused; and

(g) object to a refusal referred to in paragraph (f).

II. Exemptions

The PD(P)O provides specific exemptions from the requirements of the Ordinance, which are summarized below:

1. Domestic purposes
   Personal data held for domestic or recreational purposes are given a broad exemption from the provisions of the Ordinance.

2. Transitional provisions for personal data
   Personal data held by the University before 20 December 1996 and provided by an individual on the specific understanding that the data would not be made available to the data subject (e.g. performance evaluation reports) are exempted from data access request to such data until 3 August 2002.

3. Employment-related purposes
   Exemptions from the requirements of data access are given to the following catergories of personal data collected and/or used for certain employment-related purposes:
   - ♦ data relating to staff planning;
   - ♦ data for an evaluative process (e.g. personnel actions) prior to a decision being taken and where an appeal can be made against such a decision; and
   - ♦ a personal reference in relation to an applicant for an appointment until the time when he has been informed of the outcome in writing.

4. Public and Competing Interests
   Exemptions from requirements on data access and/or use limitation apply when the application of those provisions to the data would be likely to prejudice any of the matters of public or competing interests listed in the PD(P)O, such as security, defence or international relations in respect of Hong Kong; prevention and/or detection of crime; the assessment or collection of any tax or duty; the prevention or preclusion of significant financial loss arising from unlawful or imprudent business/personal activities; health; legal proceedings and news activities.

A University data user with reasonable grounds for believing that the situation falls within one of those areas specified above and Part 8 of the PD(P)O is required to inform and consult the DPO, the HRO or the Registry/Registry of LIFE before using/releasing the data or refusing a data request.

LINGNAN UNIVERSITY

Guidelines for Handling Personal Data in Employment-related Processes

I. These guidelines provide guidance to staff members of the University in handling personal data in specific employment-related processes. For the general guidelines and procedures for handling personal data in the University, staff members are advised to refer to the University's *Code of Practice for Handling Personal Data*.

II. Employment-related Personal Data

The University establishes and maintains, for the administration of personnel programmes, only personnel records pertaining to individuals as current or former employees of the University or as applicants for positions, as are relevant and necessary to the management of its human resources. Employment-related personal data held by the University comprise the following:

- Personal particulars, including the personal identity documents, address, contact number, emergency contact number & photo
- Curriculum vitae, including qualifications, skills, work & professional experiences
- Salary data (past and current)
- Appointment documents
- Leave records
- Employee benefits information, including insurance, medical records, family details
- Performance appraisal and work assessment information
- Research related information, if applicable
- Teaching related information, including teaching & learning evaluation scores, if applicable
- Outside practice records
- Training & development information
- Tax reporting data
- External assessments/references, if applicable

III. Handling Personal Data for Employment-related Processes

1. Recruitment

(a) Job applicants have to be specifically informed of the purposes(s) for collecting their personal data and the way(s) these data will be used on or before the collection.

(b) Mechanisms should be in place to verify the accuracy of the data of the job applicants in accordance with University guidelines and the *Code of Practice on the Identity Card Number and Other Personal*

Identifiers issued by the Office of the Privacy Commissioner for Personal Data (PCPD).

(c) Application documents should be handled, used and kept by officers responsible for relevant recruitment matters. The information contained therein should only be used for recruitment and other employment-related purposes in the University. Such data should be accessible only to offices, committees and persons who process recruitment and appointment matters. All application documents should be disposed immediately or returned to the Human Resources Office (HRO) immediately after use.

(d) Personal data of unsuccessful applicants, including references and external assessments, are normally destroyed in accordance with the published guidelines after the successful applicant(s) has/have formally accepted the offer(s) of appointment at the completion of the recruitment exercise. If the personal data of unsuccessful applicants are retained for future reference purposes, such data should not be kept for a period in excess of 24 months.

(e) When references or assessment reports have to be sought from any third parties within or outside the University, the referee or assessor should be informed on or before the collection of the data that such data shall be made available to the data subject on request in accordance with the requirements of the Personal Data (Privacy) Ordinance (PD(P)O).

(f) For any recruitment exercise administered by a department/unitother than the HRO, the head of the home department (HoD) should establish and observe appropriate rules for the collection, processing and disposal of personal data of applicants as set out in this set of guidelines or the PD(P)O.

(g) There is no appeal procedure for recruitment. The "relevant process" of a recruitment exercise commences when posts are advertised and the process ends as soon as an appointee has given written consent to his contract of employment.

2. Appointment

(a) Successful applicants, on becoming employees of the University, will be assigned a personal file in the HRO which holds their employment-related personal data.

(b) The HRO will transmit relevant employment-related personal data to the HoD of the employees and to other authorized University users on a need basis.

(c) Each HoD should keep such data in a confidential file for individual members of his department/unit, accessible only to authorized users in the department/unit. When required, such data should only be transmitted in sealed envelopes or password controlled electronic files directly addressed to another authorized user.

(d) Upon the expiry of the appointment of a HoD or any changes in a headship, the HoD concerned should, prior to his departure/expiry of his term, return all such data back to the HRO or inform HRO of the agreed arrangement/storage of such data during a transitional period.

(e) For any appointment directly administered by a department/unit other than the HRO, the HoD concerned should establish and observe appropriate rules for the collection, processing and disposal of personal data of the appointees as set out in this set of guidelines or the PD(P)O.

3. Performance Review

(a) Performance review is conducted regularly for all staff members on long-term appointment.

(b) Data collected during the performance review process will be used for various human resources management purposes, including but not limited to performance management, staff planning and making personnel decisions by the University via the relevant review parties.

(c) The performance review reports will be made available to supervisors and relevant staff review committees/assessment panels in the consideration of personnel actions.

4. Personnel Actions

(a) Data are collected including recommendations from supervisors, the relevant parties and where appropriate from external assessors and stakeholders for the purpose of determining the outcome of personnel actions such as probation review, contract renewal, performance-based salary increment, substantiation, promotion, and promotion with substantiation.

(b) Upon completion of the personnel actions exercises, if there are legitimate reasons to retain such data, such data can be retained for no longer than 7 years upon the employees' cessation of employment.

5. Termination

(a) Upon the departure/transfer/redeployment/retirement of an employee, the HoD concerned should return all employment-related personal data of the staff member concerned to the HRO, or dispose all such data immediately, as appropriate

(b) All personal data of former employees maintained in the personal files by the HRO or at the Banner System will be scheduled for destruction within seven years of their departure or completion of any appeal/compliant/judicial review/court proceedings, whichever is later, except otherwise required by law.

(c) For personal data of former employees directly administered by a department/unit, if required by law, the HoD concerned shall establish and observe appropriate rules and procedures for

i. the proper retention, updating and use of such data for the required period to fulfill such permitted purposes;

ii. the subsequent proper disposal of such data as set out in this set of guidelines or the PD(P)O.

(d) For any appointment directly administered by a department/unit other than the HRO, the HoD concerned should establish and observe appropriate rules for the collection, processing and disposal of personal data of the appointees as set out in this set of guidelines, the Code of Practice for Handling Personal Data or the PD(P)O.

IV. The procedure for application for employment-related personal data access and/or correction is set out in Annex 4, and enquiries on these guidelines should be directed to the HRO.

LINGNAN UNIVERSITY

Guidelines for Handling Personal Data for Student-related Matters

I. These guidelines provide guidance to staff members and students of the University in handling personal data for student-related matters. For the general guidelines and procedures for handling personal data in the University, staff members are advised to refer to the University's *Code of Practice for Handling Personal Data*.

II. Student-related Personal Data

1. The student data collected and held by the University shall only be handled by the Head of Department/Unit or designated staff member(s) of the Department/Unit. Student-related personal data held by the University comprise the following:

    - ♦ personal particulars
    - ♦ family background
    - ♦ financial situation
    - ♦ educational qualifications (including previous schools & examination results)
    - ♦ enrolment records (including exchange programmes, if any)
    - ♦ assessment records, academic standing, and degree awarded (including classification)
    - ♦ payment records
    - ♦ books on loan records
    - ♦ scholarships and bursaries records
    - ♦ extra-curricular activities
    - ♦ leave records
    - ♦ health problems/disabilities (if applicable)
    - ♦ disciplinary records (if any)
    - ♦ profession & salary data (graduates/alumni)

2. In general, students' personal data are collected and maintained by the University for purposes in relation to their studies at the University and alumni affairs which may include:

    - ♦ admission and registration
    - ♦ academic advising
    - ♦ hostel
    - ♦ payment
    - ♦ grant/loan
    - ♦ books borrowing
    - ♦ using University facilities
    - ♦ scholarship, subsidies, financial assistance and bursaries
    - ♦ counseling

- special educational needs
- international programmes
- student training and development
- society experience
- assessment
- transcript (academic and non-academic)
- testimonials
- degree certificates
- disciplinary matters
- contact and communication
- compliance with University policy and regulations, and/or registration in relation to health and safety, and other study-related matters
- alumni and graduates

III. Data of Applicants for Admission

1. Upon collection of personal particulars (including HKID/passport number), academic and other information from applicants for admission considerations, the applicants shall be informed of the purpose of collecting the data, how the data will be used, his/her rights to request access to and correct the information provided, and how such requests may be made. These shall be spelt out in the application form.

2. Measures shall be taken to verify the accuracy of the data of the applicants, e.g. to check against the source documents as far as practicable and to have the confirmation after checking recorded.

3. Retention of personal data of applicants shall only be kept as long as necessary but not exceeding 6 months after the completion of the admissions exercise, except those who have been admitted to become students or those who have paid fees on accepting the University's offer.

4. Personal data of the applicants shall not be used outside the specified purposes, except with the expressed consent of the applicants.

5. Personal data of applicants shall be kept under proper security by the Registry/Registry of Lingnan Institute of Further Education (LIFE), the School of Graduate Studies (GS) and Programme Offices of individual taught postgraduate programmes, and the Information Technology Services Centre (ITSC) and only be released for confidential use by personnel of academic departments and parties concerned for the purposes of selection for admission.

6. Applicants shall have access to their personal data kept by the University. They may be required to pay a fee for searching and processing of the data and to cover any relevant costs if deemed necessary.

7. Academic references received from referees will only be disclosed to the applicants concerned upon their requests when the admissions process is

completed. If the disclosure cannot be made within 40 days of the request, the applicant shall be informed of the reasons in writing.

8. Any public display of admission results (e.g. in newspapers or University notices) shall not include a display of the applicants' names together with application numbers or any other personal identifiers.

IV. Non-Financial Data of Students

1. Data (including personal particulars, academic qualifications and other relevant information) of applicants for admission to study programmes, after being accepted by the University, will be transferred to the student records databases which are kept for a specified period, or permanently maintained, by the Finance Office (FO), Registry/ Registry of LIFE, GS/ individual TPg Programme Offices, ITSC, Library, Office of Student Affairs (OSA)/ Student Development Office of LIFE and Office of Institutional Advancement and Public Affairs (OIAPA)/ Communication and Public Relations of LIFE.

   Data (including personal particulars and other relevant information) of applicants who have paid the admission fee but subsequently withdraw their study, will be kept by the FO for the period required for the processing of refunds or claims arising from the fees paid on accepting the University's offer.

   A student's name, student number and/or ID card number together shall not be made visible to other students or anyone who does not need to carry out activities related to the permitted uses of the ID card number.

2. To ensure accuracy of student records, each student shall be able to access via the University's computer system his/her own personal particulars and enrollment records upon completion of registration and enrollment in each term of the academic years.

3. In the process of addition, alteration and deletion of student information, proper mechanisms shall be adopted to ensure its accuracy and appropriateness.

   A Student ID Card shall be issued to each registered student. The issuance of Student ID Cards shall be made under close supervision to safeguard against the unauthorized assignment of student numbers or production of Student ID Cards.

   The student ID card number shall be unique to each student and shall be used as an official identifier of the student as an alternative to the student's HKID card number. Student ID card numbers, instead of HKID card numbers, shall be used for student identification in most internal documentation unless otherwise required.

   A student shall be allowed to use a valid Student ID Card issued to him/her as a personal identifier for obtaining services on campus.

4. Each student upon graduation shall be given a copy of his/her transcript for information. To facilitate future liaison, in addition to the records kept by the Registry/ Registry of LIFE, GS or individual TPg Programme Offices, relevant student records of those who left or graduated from the University will be transferred to the OIAPA/Communication and Public Relations of LIFE.

5. Student data are accessed only by responsible staff members of the University or be distributed by the ITSC and the Registry/ Registry of LIFE/individual TPg Programme Offices to responsible persons of relevant academic and administrative departments and units concerned for their use.

6. Occasional requests from departments or units for student records shall be made by responsible officers to GS or individual TPg Programme Offices, Registry/ Registry of LIFE with full justification for the requests. The data obtained shall not be kept longer than is necessary for the specified purposes.

7. Each student or graduate or his/her authorized representative can have access to his/her own data being kept by the University, or authorize the University to release such information to a third party, e.g. another higher education institution, by way of issuance of certification documents such as transcript and testimonial. A fee will be charged for data searching, processing and to cover any relevant costs.

   In the provision of services to students and graduates, units may accept HKID Card, or its photocopy, or Student ID Card as an identity alternative to the physical production of the card by the student or graduate if he/she is not able to present such identity card in person to the unit concerned.

   They should not compulsorily require any students to furnish their HKID Card copies unless permitted by law (such as to fulfil section 17J of the Immigration Ordinance in case of employing a student as a helper).

   All units should cease the collection of HKID Card copies from students, and destroy all copies which have been previously collected from students.

8. The University's policies, practices and purposes regarding personal data of students will be made known to students via notices.

9. Students have the right to correct his/her personal data. A printed form for changing personal particulars is available in Registry/ Registry of LIFE for use by students.

10. Co-curricular Programmes refer to Integrated Learning Programme (ILP) and Civic Engagement Programme (CE). OSA asks for students' full name, email address, study programme and year, gender, and contact phone number, when students enroll in the programmes. After the attendance record is compiled, all raw data will be destroyed at the end of each academic year, except the attendance records.

11. Counselling Record of Students
    For each counselling and advising appointment, the following data are collected:
    - ♦ student's name
    - ♦ student ID number
    - ♦ gender
    - ♦ study programme and year
    - ♦ contact phone number

    An individual counselling record of the student that records his/her case history is kept confidential, and access to the records is restricted to supervisor and counsellors. The clerical officer is assigned to look after the filing. Individual counselling record of a student will be kept for three years after the student graduates or leaves the University.

12. Student Activities
    After the attendance record is compiled, all raw data will be destroyed at the end of each academic year

13. Student Hostels
    All raw data about student hostel applications will be destroyed at the end of each academic year. Room records will be destroyed after the student graduates or leaves the University.

14. Surveys and Test Data
    The following data are collected for General Health Questionnaire Survey (GHQ): student ID number, gender, study programme and year, age, email address, hostel room number, and contact phone number. The survey data are kept for one year after student graduates or leaves the University.

    The data forms collected for other surveys conducted by OSA are destroyed after the completion of the survey. The data of the survey will be stored in electronic form. Test record sheets are kept until the students graduate or leave the University. However, for research purposes, any links that could reveal a test subject's identity with his/her test results are deleted.

V. Financial Data of Students

The scholarships and bursaries data are recorded in donors' files which will be kept by the OSA until they discontinue their donation to the University. The following two password protected records of students will be kept for seven years after graduation:

1. The Government Local Student Finance Scheme (LSFS) and Non-means Tested Loan Scheme (NLS) records. The information provided in the LSFS and NLS records will be used for assessment of students' applications for University Student Finance Scheme. These records are kept for audit purpose.

2. The interest-free loan records including the forms of undertaking signed by successful applicants and guarantee forms. These records are kept for repayment purpose.

VI. Data of Alumni and Donors

1. The bank account information will be kept from the student records database by the Finance Office and donor records database by Office of Institutional Advancement and Public Affairs for the period required for the processing of refunds, claims or donation.

2. For the Career Advisory Network, the data of graduates are kept in the written and disk format, with their consent.

3. The alumni activity enrollment forms collected from alumni through different channels will be destroyed within 6 months upon completion of an event. Donation forms and forms bearing financial data which will have impact on tax payment will be kept for 7 years, as required by Law.

4. The contact update forms received from alumni through different channels will be destroyed within 6 months.

   Final year students will be informed in advance that their personal data will be kept by the University for communication purposes after their graduation and they are provided channels to give their consent if they would like to continue receiving the information and news from the University.

5. The following data are collected for Graduate Employment Survey (GES): employment status, employer information, employment sector, job title, monthly income, no. of job offers, time taken in seeking employment, channel of obtaining job vacancy information and information on further studies, etc.

   It is obligatory to complete the GES as part of the academic dress collection procedures which is endorsed by the senior management in the past years. It is stated in the letter or email to graduates that the information they provide in the GES might be shared with other internal departments within the University and be used by the University Grants Committee (UGC) in reviewing and allocating resources to the University and for other statistical purposes. The questionnaires of the survey will be destroyed after the completion of the survey. The data of the survey which could identify individual's identity will be kept in the Business Intelligence for the purpose of analysis of graduates' employment trend, and development of career related strategy.

VII. Assessment Data

1. Data users of students' assessment records are responsible for 'ensuring an adequate level of protection for the personal data'. As regards External Academic Advisors who are provided with the examination scripts of students (with identities masked for moderation, they should also be reminded to handle the data with care.

2. Grades processing should only be handled by designated academic and administrative staff.

3. Only a master and a spare copy of Undergraduate Examinations Board (UEB)*/Boards of Examiners (BoE) papers/documents relating to student assessment should be kept by the Chairman and the Secretary respectively, while all other copies issued to members must be collected by the Secretary at the end of a meeting and destroyed afterwards.
(*Postgraduate Studies Committee for postgraduate programmes)

4. Raw marks and comments for individual assessment components (e.g. tests, term papers, assignments, examinations, etc.), and relevant extracts of documents containing information relating to individual students such as papers of UEB/BoE meeting are subject to data access after the relevant process.

5. When graded answer scripts are copied to students in order to comply with data access requests or are returned to students for feedback, students should be advised clearly that marks on the scripts are only raw marks and may be subject to any necessary adjustment.

6. Students may be shown examination scripts in the presence of the teacher concerned, but the scripts remain the property of the University.

7. Student assessment data will only be accessed by responsible staff members of the University or distributed by the Registry to responsible persons of units upon justified requests for their use. The data obtained shall not be kept longer than is necessary.

8. Students can have access to their assessment results via the Banner System in the form of academic reports/transcripts which indicate the grades for each course a student enrols, the number of credits obtained, the grade point average and any decision of the Senate, if applicable.

9. Students may appeal through the Registrar for a review of grades or a reassessment according to Regulations Governing University Examinations.

10. Apart from the retention of a selection of four to six scripts per course for three years for specific purposes, all answer scripts and raw assessment scores should be properly disposed of after the student assessment process and the appeal period of the term (about three months after the examination period of the term), to be in line with the Data Protection Principles.

11. For cases requiring a longer review period and course with an 'I' grade, the disposal of relevant documents or records concerning individual students should be deferred until the completion of all necessary procedures.

VIII. Application procedures for student-related personal data access and/or correction are set out in the Annex 4, and enquiries on these guidelines should be directed to GS, Registry or Registry of LIFE.

Procedures for Applications for Personal Data Access Request

1. The Chief Data Protection Officer maintains application procedures for access to and/or correction of personal data held by the University according to the provisions of the Personal Data (Privacy) Ordinance.

2. All enquiries concerning personal data access should be addressed to the Chief Data Protection Officer.

3. A data subject who wishes to make a request for access to or correction of his own personal data held by the University under the provisions of the Ordinance should complete an "Application for Personal Data Access Request" form (https://www.ln.edu.hk/f/upload/35939/Data%20Access%20and%20Correction%20Form.pdf) obtainable from the ITSC, MB401, Patrick Lee Wan Keung Academic Building, Lingnan University, Tuen Mun, N.T., Hong Kong.

4. The data subject should return the completed application form to the Chief Data Protection Officer in person, showing his student/staff card, and if not available, his HKID or passport for identification. Any requests on behalf of the data subject should be submitted with a written authorization and a copy of the data subject's Student/Staff ID card or HKID card/passport.

5. For data access request, the data subject is required to pay an application fee of $150 at the Finance Office and to complete a proforma indicating clearly the specific areas of data or documents to which they want to have access.

6. Upon showing the receipt of payment to the Chief Data Protection Officer, an acknowledgement slip will be issued to the data subject indicating that the request is accepted and the search will proceed.

7. The Chief Data Protection Officer will notify the data subject in writing of the outcome and/or progress of the request within 40 days from the date of submission.

8. A charge will be levied on the data subject for each request in accordance with the following schedule:

Photocopy of printed documents	$5 per page

9. If the request cannot be completed within the 40-day period, the data subject will be advised of the reasons for the delay and notified of a revised completion date.

Annex 5

Personal Information Collection Statement Template

1. The purpose(s) of collecting personal data by means of this form is/are to … [*].
2. In order to serve the specified purpose(s), the personal data collected may be transferred to … [†] … for … [‡]. All information provided will be destroyed by… [$].
3. Without your expressed approval, or unless required by law, the personal data collected herein will not be disclosed to third parties other than those specified in Point 2.
4. Unless indicated otherwise, all personal data requested in this form is required for its purpose(s). If such data is incomplete or inaccurate… [Ω].
5. Without your consent, the University will not use your personal information provided to us to conduct direct marketing
6. As a data subject, you have the right to request access to and correction of the personal data under the Personal Data (Privacy) Ordinance. For requests for access to personal data, please contact the Data Protection Officer at DPO@LN.edu.hk. For requests to correct/update personal data, please contact the responsible Department/Office at … [#].

* Please spell out the purpose(s). As an alternative to including item 1 in the statement, the title of the form should indicate its purposes clearly.

† Where applicable, please characterize (it may not be appropriate to list each one by name) any third parties (such as other administrative units within the University, and/or particular external agencies) who will or may receive the data.

‡ Where applicable, please state the related purpose(s), such as further processing, consideration, approval, etc., for which the data will be transferred.

$ Where applicable, please specify the date by which the record will be deleted.

Ω Where applicable, i.e., when not obvious from the context, please indicate possible adverse consequences of failure to provide the data, or of providing inaccurate data, e.g., the application will be void or delayed.

\# Please provide an extension no. and/or email that will reach the responsible officer.

A Personal Information Collection Statement should look like this:

1. The purpose of collecting personal data by means of this form is to use your contact information for Global Service-Learning Program in Country A. Office of Service-Learning will use your emails and phone numbers for communication with you.
2. In order to maintain necessary communication, the personal data collected in this form may be transferred to ABC University, Country A. All information provided will be destroyed after the Program is completed.
3. Without your expressed approval, or unless required by law, the personal data collected herein will not be disclosed to third parties other than those specified in Point 2.
4. Unless indicated otherwise, all personal data requested in this form is required for organizing this Program. If such data is incomplete or inaccurate, your application will be void or delayed.
5. Without your consent, Lingnan University and ABC University will not use your personal information provided to us to conduct direct marketing.
6. As a data subject, you have the right to request access to and correction of the personal data under the Personal Data (Privacy) Ordinance. For requests to access your personal data, please contact the Data Protection Officer at DPO@LN.edu.hk. For requests to correct/update personal data, please contact Office of Service-Learning (osl@LN.edu.hk).

Personal Data Inventory Template

Personal Data Inventory																																				
						Collection				Storage						Usage within Organisation		Transfer/Disclosure to External Parties						Retention & Disposal							Privacy Risk Assessement					
										Within Department		Other Department		Third Party				Within Lingnan			Outside Lingnan															
No.	Department	Application name	Data Subject	Personal Data Types	Consent collection	Collection Purpose - why Organisation collects personal data	Data Owner	Collection Source	Collection Medium	Physical Storage	Electronic Storage	Physical Storage	Electronic Storage	Physical Storage	Electronic Storage	Users of Personal Data and Purpose of Usage	Access to Personal Data by Departments	External Parties and Purpose of Transfer/ Disclosure	Types of Personal Data	Transfer Mode	External Parties and Purpose of Transfer/ Disclosure	Types of Personal Data	Transfer Mode	Retention Period	Disposal Methods	Planned Disposal Date	Disposed by	Actual Disposal Date	Authorised by	Authorisation Date	Step 1 Column H	Step 2	Step 3	Step 5	Step 6	Step 7
1																																				
2																																				
3																																				
4																																				
5																																				
6																																				
7																																				
8																																				
9																																				
10																																				