

# **Personal Data Compliance Manual**

(Effective from September 2019)

Legal, Risk and Compliance Unit  
Office of the Executive Vice President

(updated: February 2022)

**Contents**

<b>1. Introduction</b>	4
1.1 Purpose	4
1.2 Scope	4
1.3 Definitions and Interpretations	5
1.4 Accountability	7
1.5 Questions and Support	7
<b>2. Overview of the Ordinance</b>	8
2.1 Data Protection Principles	8
2.2 Statutory Exemptions	10
2.3 Consequences of and Liability for Non-compliance	11
<b>3. Personal Data Management</b>	12
3.1 Collection of Personal Data	12
3.2 Personal Data - HKID or Document of Identity	13
3.3 Personal Data - Images	13
3.4 Personal Data – International Student Applicants from the European Economic Area	15
3.5 Proactive Compliance Planning	16
<b>4. Direct Marketing</b>	17
4.1 Requirements and Procedures	18
4.2 To Students by Email @connect.polyu.hk	19
4.3 To Staff by Email @polyu.edu.hk	19
<b>5. Use of CCTV</b>	20
5.1 Privacy and Personal Data Perspective	20
5.2 Planning	20
5.3 Compliance Measures	22
<b>6. Data Access and Correction Requests</b>	24
6.1 Applicability	24
6.2 Data Subjects and Request-Handling Departments	25
6.3 Handling DAR	25
6.4 Handling DCR	29
<b>7. Personal Data Privacy Enquiries</b>	32
<b>8. Data Incidents</b>	33
<b>9. Frequently Asked Questions</b>	38
<b>Appendix A – Template of the Generic PICS</b>	43
<b>Appendix B – Template of the Consent Form for Recording</b>	45

**INTERNAL USE**

**Appendix C – Notice for Applicants from the European Economic Area** .....47

**Appendix D – Template for Direct Marketing**..... 50

**Appendix E – CCTV Installation Assessment Form**.....51

**Appendix F – Grounds for Refusal of Data Access/Correction Request(s)**.....53

**Appendix G – Illustration on Redacting** ..... 54

**Appendix H – Template of the Letter for Refusing Data Access Request(s) / Data  
Correction Request(s)**.....55

**Appendix I – Data Incident Information Sheet** .....56

## **1. Introduction**

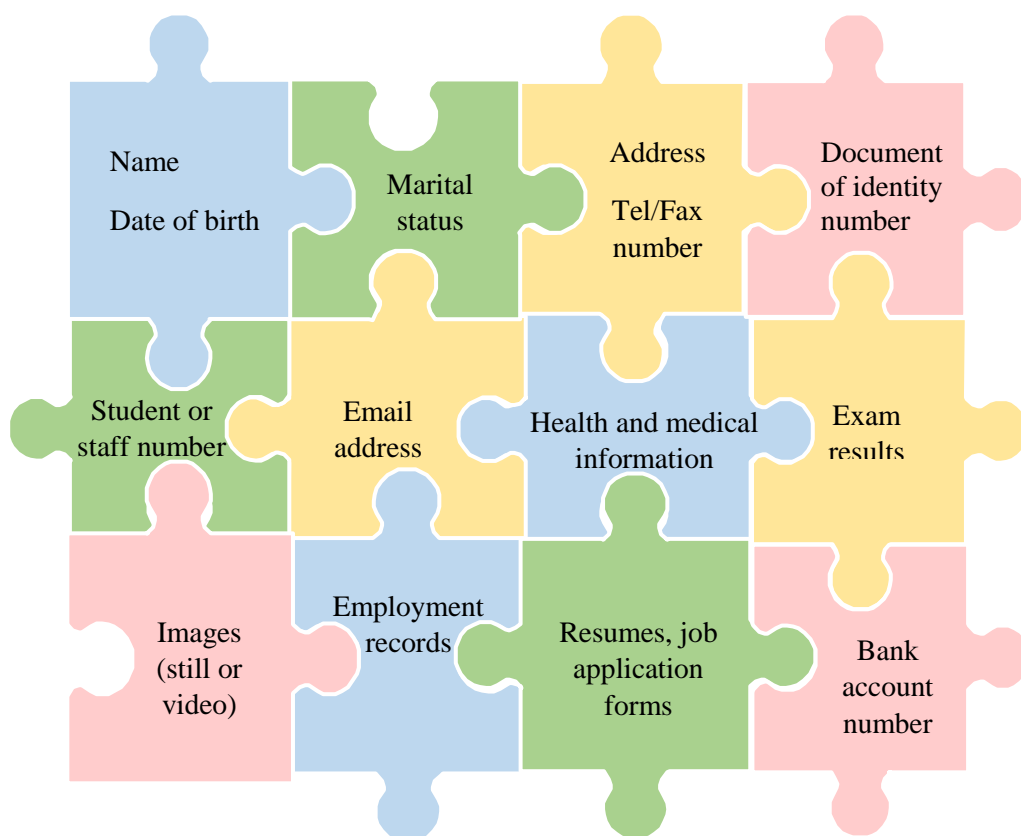
### **1.1 Purpose**

This Personal Data Compliance Manual (the “Manual”) sets out the practices of the University on personal data as a compliance guide to staff members when carrying out their duties. The Manual can be found at the University Portal ([https://www2.polyu.edu.hk/DAG/PD\\_Manual.pdf](https://www2.polyu.edu.hk/DAG/PD_Manual.pdf)) together with other related materials, for example:

- a) Guidelines for Handling Applicant/Student Data with Reference to the Personal Data (Privacy) Ordinance prepared by the Academic Registry; and
- b) Departmental Guidelines on Handling Staff Personal Data prepared by the Human Resources Office.

### **1.2 Scope**

The Manual applies to personal data that the University collects or creates in the course of its operation.



### **1.3 Definitions and Interpretations**

In the Manual, unless the context requires otherwise:

**Anonymized Data** means data that do not carry specific identifiable personal information;

**CCTV** means closed circuit television;

**Commissioner** means the Privacy Commissioner for Personal Data<sup>1</sup> ;

**Request Administrator** means a staff member appointed by the Head of Department to handle Data Access Request(s) or Data Correction Request(s);

**Data Access Request** or **DAR** means a request made by an individual, or a relevant person on behalf of the individual<sup>2</sup>:

- a) to be informed by a Data User whether the Data User holds Personal Data of which the individual is the Data Subject; and
- b) if the Data User holds such data, to be supplied by the Data User with a copy of such data;

**Data Correction Request** or **DCR** means where a copy of Personal Data has been supplied by a Data User in compliance with a Data Access Request, and the individual, or the relevant person on behalf of the individual, who is the Data Subject considers that the data is inaccurate, then that individual may make a request that the Data User make the necessary correction to the data<sup>3</sup>;

**Data Incident** means an incident when there is actual or potential loss, unauthorized or accidental access, copying, alteration, erasure or use of Personal Data;

**Data Processor** means a person who

- a) processes Personal Data on behalf of another person; and
- b) does not process the Personal Data for any of the person's own purposes;

**Data Protection Principle** or **DPP** means any of the data protection principles set out in the Ordinance<sup>4</sup>;

**Data Requestor** means a person who makes a Data Access Request or Data Correction Request;

**Data Subject** means the individual who is the subject of the Personal Data concerned<sup>5</sup>;

**Data Steward** means the Head/ Director of Department or his/her deputy, who is entrusted for managing the data that pertains to his/her functional area or under his/her purview<sup>6</sup>;

**Data User** means a person who, either alone or jointly or in common with other persons, controls the collection, holding, processing or use of Personal Data<sup>7</sup>;

---

<sup>1</sup> Section 2 and Section 5(1) of the Ordinance.

<sup>2</sup> Section 2 and Section 18(1) of the Ordinance.

<sup>3</sup> Section 2 and Section 22(1) of the Ordinance.

<sup>4</sup> Section 2 and Schedule 1 of the Ordinance.

<sup>5</sup> Section 2 of the Ordinance.

<sup>6</sup> Chapter 3 of the Data Governance Framework ([https://www2.polyu.edu.hk/DAG/Data Governance Framework.pdf](https://www2.polyu.edu.hk/DAG/Data%20Governance%20Framework.pdf)).

<sup>7</sup> Section 2 of the Ordinance.

**Department** means a Faculty, School, Department, Functional Unit or Office of the University;

**Direct Marketing**<sup>8</sup> means:

- 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, recreational, political or other purposes, through Direct Marketing Means;

**Direct Marketing Means**<sup>9</sup> is defined as:

- a) sending information or goods, addressed to specific persons by name, by mail, fax, electronic mail or other means of communication; or
- b) making telephone calls to specific persons;

**DM Administrator** means a staff member appointed by the Head of Department to manage departmental direct marketing activities;

**DPDO** means the departmental personal data officer;

**Head of Department** means the Head of a Department, Dean of a Faculty or School, or Head or Director of a Functional Unit or Office;

**Manual** means this Personal Data Compliance Manual;

**Ordinance** means the Personal Data (Privacy) Ordinance;

**Personal Data**<sup>10</sup> means any data:

- a) relating directly or indirectly to a living individual;
- b) from which it is practicable for the identity of the individual to be directly or indirectly ascertained; and
- c) in a form in which access to or processing of the data is practicable;

**Personal Identifier** means an identifier a) that is assigned to an individual by a Data User for the purpose of the operations of the user; and b) that uniquely identifies that individual in relation to the Data User. It does not include an individual's name used to identify that individual;

**Personal Information Collection Statement** or **PICS** means a statement given by the Data User for the purpose of complying with the notification requirements under Data Protection Principle 1(3) of the Ordinance<sup>11</sup>; and

**PolyU or University** means The Hong Kong Polytechnic University.

Mandatory requirements of the Manual are indicated by “**shall**” and “**is/are required**”. Optional requirements are indicated by **may** and **should**.

---

<sup>8</sup> Section 35A of the Ordinance.

<sup>9</sup> Section 35A of the Ordinance.

<sup>10</sup> Section 2 of the Ordinance.

<sup>11</sup> “*Guidance on Preparing Personal Information Collection Statement and Privacy Policy Statement*” issued by the Commissioner in July 2013.

## **1.4 Accountability**

### **Primary Ownership and Accountability – Departments**

The primary ownership and accountability on Personal Data management rest with the Departments. According to the Data Governance Framework, the Head of Departments or their deputy are Data Stewards of the data that pertains to their functional area or under their purview.

### **Heads of Department**

- a) Overall responsible and accountable for compliance with the Ordinance, the Manual and departmental procedures;
- b) Establish departmental procedures that align with the Manual and University policies and standards that are applicable to Personal Data;
- c) Appoint staff members to administer the process specified in Chapter 4 (DM Administrator), Chapter 5 (Data Steward of the recordings of the CCTV system), Chapter 6 (Request Administrator) and serve as the Departmental Personal Data Officer (DPDO)<sup>12</sup>; and
- d) Make the necessary arrangement so that all staff members (part-time and full-time), students and student helpers who may have access to or handle Personal Data on behalf of the University are aware of the requirements of the Manual.

### **Departmental Personal Data Officers (DPDOs)**

The terms of reference of DPDOs can be found at the University Portal.

### **Staff Members**

Staff members shall follow the Manual and departmental procedures.

## **Oversight – Legal, Risk and Compliance Unit, Office of the Executive Vice President (LRC Unit)**

### **LRC Unit**

- a) Oversees institutional compliance with the Ordinance and the Manual;
- b) Provides guidance to Departments on the requirements under the Manual and management of data breach risks;
- c) Reviews and updates the Manual annually according to the prevailing statutory requirements, best practices and trends of enforcement;
- d) Provides support to Departments on Data Incident cases;
- e) Handles enquiries by the Commissioner; and
- f) Assesses the impact of changes in statutory and regulatory requirements on Personal Data and communicates the requirements with the stakeholders of the University.

## **1.5 Questions and support**

The DPDO shall handle the enquiries of fellow colleagues of the Department on Personal Data protection and privacy related matters. See Chapter 9 for frequently asked questions. If the DPDO is in doubt, he/she shall discuss with the LRC Unit.



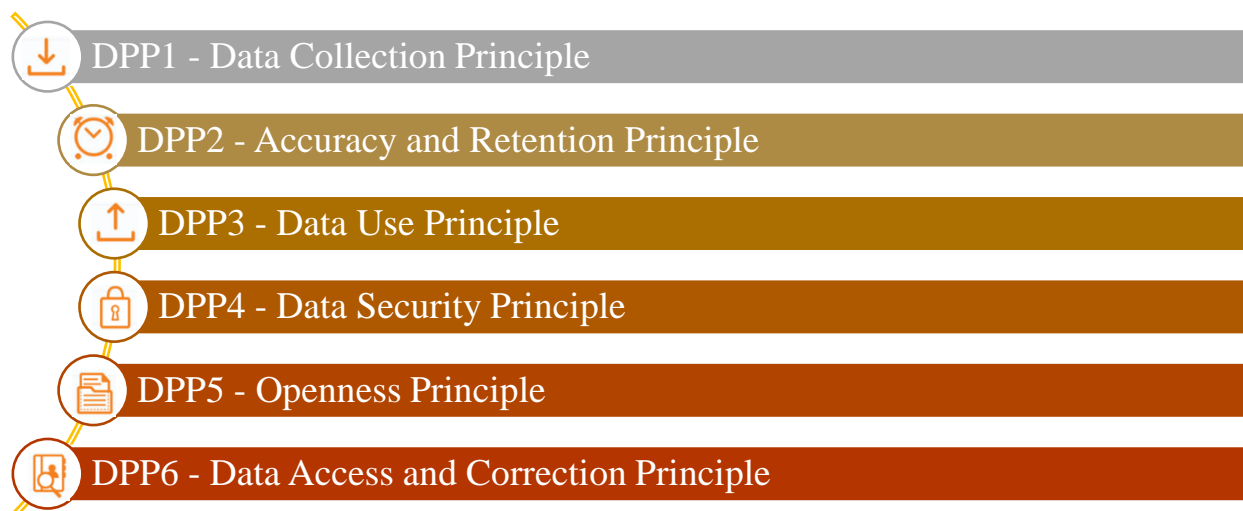
---

<sup>12</sup> The DM Administrator, Data Steward of the recordings of the CCTV system, Request Administrator and DPDO can be the same or different staff members. The Head of Department may take up personally some or all of these roles.

## **2. Overview of the Ordinance**

### **2.1 Data Protection Principles**

The University, as a Data User, shall comply with the six DPPs<sup>13</sup>.



#### **DPP1 – Data Collection Principle**

Personal Data shall only be collected in a lawful and fair manner, for a purpose directly related to a function/activity of the University. Personal Data collected shall be necessary but not excessive.

When collecting Personal Data from a Data Subject, the Department shall provide the Data Subject with the following information:

- the purpose of data collection;
- whether it is obligatory or voluntary for the data subject to supply the data;
- where it is obligatory for the Data Subject to supply the data, the consequences for him/her if he/she fails to supply the data;
- the use of the Personal Data, or the provision of the Personal Data to another person for use, for Direct Marketing (if applicable);
- the classes of persons to whom the data may be transferred; and
- the name (or post title) and contact details to which DARs may be made.

#### **Example(s)**

##### **Unfair means of collecting Personal Data:**

Collection of job applicants' Personal Data under the guise of a recruitment exercise.

##### **Excessive collection of Personal Data:**

Collection of residential address from subscribers of e-newsletters of the University.

<sup>13</sup> The DPPs are set out in Schedule 1 of the Ordinance.





### **DPP2 – Accuracy and Retention Principle**

Data Users are required to ensure that the Personal Data are accurate and be deleted or disposed of when no longer required for the purpose for which they were originally collected.

If a Department engages a Data Processor to process Personal Data, the Department shall follow the requirements of the Data Governance Framework of the University<sup>14</sup> for the disclosure/transmission of data to a third party.



### **DPP3 – Data Use Principle**

Personal Data shall be used for the purpose for which the data is collected or for a directly related purpose. Prescribed consent of the Data Subject is needed before using his/ her Personal Data for a new purpose.

- “Prescribed consent” means the express consent given voluntarily by the Data Subject.
- “New purpose” means any purpose other than (i) the purposes for which the data was collected; or (ii) purposes directly related to those in (i).

#### **Example(s)**

##### **Use of Personal Data for a new purpose:**

A seminar participant provided his name and email address to the seminar-hosting Department to obtain the seminar presentations by email. The Department shall **only use the collected Personal Data for sending the requested materials**. The Department is **not allowed to use the Personal Data for a new purpose**, e.g. distributing e-newsletter of the Department, without the prescribed consent of the seminar participant.



### **DPP4 – Data Security Principle**

A Data User needs to take practicable steps to safeguard Personal Data from unauthorized or accidental access, processing, erasure, loss or use. Personal Data shall be safeguarded in accordance with the Data Handling Guidelines<sup>15</sup>.



### **DPP5 – Openness Principle**

A Data User shall take all practicable steps to make Personal Data policies and practices known to the public regarding the types of Personal Data it holds and how the data is used. The University’s Privacy Policy Statement is available on the University’s website:

[https://www.polyu.edu.hk/web/en/privacy\\_policy\\_statement/index.html](https://www.polyu.edu.hk/web/en/privacy_policy_statement/index.html)



### **DPP6 – Data Access and Correction Principle**

A Data Subject shall be given access to his/her Personal Data and allowed to make corrections if it is inaccurate.

<sup>14</sup> See Chapter 5 of the Data Governance Framework.

<sup>15</sup> See Appendix B of the Data Governance Framework.

## 2.2 Statutory Exemptions


The Ordinance specifically provides for exemptions under Part 8 of the Ordinance.

The following are some of the relevant exemptions to DPP3 – Data Use Principle:

- **Section 58:** where Personal Data is used for the purpose of prevention or detection of crime or for prevention, preclusion or remedying (including punishment) of unlawful or serious improper conduct or dishonesty or malpractice by persons, etc.
- **Section 59:** the disclosure of the identity, location and health data (physical or mental) of a Data Subject where non-disclosure may likely cause serious harm to the physical or mental health of the Data Subject or any other individual
- **Section 60B:** where the use of the Personal Data is required or authorized by Hong Kong law or in connection with any legal proceedings in Hong Kong or is required for establishing, exercising or defending legal rights in Hong Kong
- **Section 61:** the disclosure of Personal Data by a person to a Data User whose business consists of a news activity and there is reasonable ground for that person to believe that the publication or broadcasting of the Personal Data is in the public interest
- **Section 62:** where Personal Data is used solely for preparing statistics or carrying out research and the resulting statistics or research does not identify the Data Subjects
- **Section 63C:** where the use of the Personal Data is to identify an individual who is reasonably suspected to be, or is involved in a life-threatening situation and to carry out emergency rescue operations, provide emergency relief services, or to inform the individual's immediate family members/ relevant persons of the individual's involvement in the life-threatening situation.

The following are some of the relevant exemptions to DPP6 – Data Access and Correction Principle and section 18(1)(b):

- **Sections 53, 55:** Personal Data which consists of information relevant to staff planning proposal related to filling a series of employment positions or ceasing a group of individuals' employment until the completion of that process. Personal Data being considered for determining eligibility or suitability for (i) employment, promotion, discipline and dismissal in an employment situation; or (ii) in connection with the awarding of contracts, awards, scholarships, honours or other benefits, until the completion that process;
- **Section 56:** Personal reference given by an individual other than in the ordinary course of his occupation and relevant to another individual's suitability or otherwise to fill any position of employment or office;
- **Section 60:** Personal Data in respect of which a claim of legal professional privilege could be maintained in law;
- **Section 60A:** Personal Data the disclosure of which might incriminate the University in any proceedings for any offence other than an offence under the Ordinance.

 *The burden of proof that the use of Personal Data is so exempted lies on the Data User who wishes to rely on the exemption. The Department shall seek the advice of the LRC Unit on the application of the exemption(s).*

### **2.3 Consequences of and Liability for Non-compliance**

The University is the Data User of Personal Data that the respective Departments collects/creates, uses/accesses, retains, or discloses/transmits. Each Department is required to comply with the DPPs and the Ordinance.

The University takes a serious view on compliance with legal and regulatory requirements. Contravention of DPPs or the Ordinance affects the rights of the Data Subject. It would also damage the reputation of the University.

The Commissioner may, upon investigations and findings that the University has breached one or more of the DPPS, serve an enforcement notice to direct the University, as the Data User, to remedy the contravention. If the University fails to comply with the enforcement notice, the University commits a criminal offence and is liable on conviction to a fine for up to HK\$50,000 and imprisonment for 2 years.

Any act of misfeasance or omission of the duty of care by a staff member in handling Personal Data in the course of employment at the University may result in liability of the staff member and the University. The University may defend itself in law by showing that it has taken practicable steps to prevent the staff member from being non-compliant with the Ordinance.

#### **Example(s)**

##### **Personal liability for non-compliance with the Ordinance:**

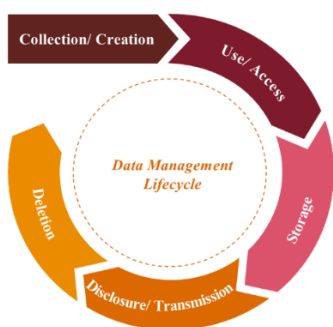
A staff member abuses the access right granted and contacts the participants of a departmental seminar to conduct a survey for a project under her own Master of Business studies. The staff member is in breach of the departmental policies and procedures, and the Ordinance. **The staff member may be liable personally for the breach of the Ordinance** and subject to disciplinary proceedings of the University.

The University may not be liable for this incident if it has provided training and taken practicable steps to prevent the staff member from being non-compliant with the Ordinance<sup>16</sup>, such as regularly monitoring the effective implementation of its policies related to Personal Data by staff members.

---

<sup>16</sup> Section 65(3) of the Ordinance.

### 3. Personal Data Management



Personal Data falls in the “Confidential” category under the Data Classification Scheme of the Data Governance Framework<sup>17</sup>. Some Personal Data may fall in the “Restricted” category. Departments shall follow the requirements of the Data Governance Framework of the University for the collection or creation, use or access, storage, disclosure or transmission, and deletion<sup>18</sup> of data, as well as the Data Handling Guidelines<sup>19</sup> that are applicable to the relevant classification categories of Personal Data.

#### 3.1 Collection of Personal Data

When collecting Personal Data from a Data Subject, the Department shall provide the information as required under DPP1 to the Data Subject. It is a common practice to set out the requisite information in a PICS. The PICS for key groups of Data Subjects can be found at:

Data Subjects	Custodian Department for PICS	Hyperlink/Location of PICS
Student Applicants and Students	AR	<a href="http://www.polyu.edu.hk/as/PICS.pdf">http://www.polyu.edu.hk/as/PICS.pdf</a> In the website above, Student Handbook, eAdmission platform, and eStudent platform
Staff Members	HRO	<a href="http://www.polyu.edu.hk/hro/pics_staff.pdf">http://www.polyu.edu.hk/hro/pics_staff.pdf</a> In the website above, Departmental Guidelines on Handling Personal Data, and Staff Handbook
Donors and Alumni	AADO	<a href="http://www.polyu.edu.hk/aado/PICS.pdf">http://www.polyu.edu.hk/aado/PICS.pdf</a>
Users of University Health Service	UHS	<a href="https://www.polyu.edu.hk/uhs/en/personal-information-collection-statement">https://www.polyu.edu.hk/uhs/en/personal-information-collection-statement</a> In the website above and reception area of UHS
Users of centres established by Departments	BME	Jockey Club Rehabilitation Engineering Clinic: <a href="https://www.polyu.edu.hk/bme/services/jockey-club-rehabilitation-engineering-clinic/personal-information-collection-statement/">https://www.polyu.edu.hk/bme/services/jockey-club-rehabilitation-engineering-clinic/personal-information-collection-statement/</a>
		Jockey Club Smart Ageing Hub <a href="https://www.polyu.edu.hk/Ageing/en/pics.php">https://www.polyu.edu.hk/Ageing/en/pics.php</a>
	CBS	Speech Therapy Unit: in the reception area
	RS	Rehabilitation Clinic: <a href="https://www.polyu.edu.hk/rs/rehabclinic/en/contact-us/personal-information-collection-statement/index.html">https://www.polyu.edu.hk/rs/rehabclinic/en/contact-us/personal-information-collection-statement/index.html</a> In the website above and reception area
	SN	Integrative Health Clinic: in the reception area
	SO	Optometry Clinic: in the reception area

<sup>17</sup> See Chapter 4 of the Data Governance Framework.

<sup>18</sup> See Chapter 5 of the Data Governance Framework.

<sup>19</sup> See Appendix B of the Data Governance Framework.

Data Subjects	Custodian Department for PICS	Hyperlink/Location of PICS
Participants of departmental activities	Departments	In the website of the relevant Department and/or in hard copy. See <b>Appendix A</b> for the template.

The DPDOs of the respective custodian Departments for PICS shall put the PICS in their respective departmental websites as a master document. When the Department is going to organize or host any activity whereby it will collect Personal Data from an individual (e.g. seminar audience, respondents of surveys or questionnaires), the DPDO shall ask the staff in charge of the activity to make the master PICS available to the individual by incorporating a hyperlink of the PICS into the application form or registration form, the website or other media channels, or providing a hard copy of the PICS.

### 3.2 Personal Data - HKID or Document of Identity

A Department shall **not** collect the HKID number or a copy of the HKID Card:



- a) merely for identity verification. The identity of a student or staff member can be verified by checking the student ID number or staff ID number. The identity of an external party (e.g. contractor, donor, event participant, visitor, etc.) can be confirmed by his/her name; or
- b) merely to safeguard against any clerical error.

In the event it is required to retain a copy of the HKID (e.g. for appointment of new staff), mark it with “copy” in the presence of the Data Subject.

The practices above mentioned in relation to the HKID apply to other documents of identity, such as the Mainland ID and the passport.

### 3.3 Personal Data - Images

An image of an identifiable individual captured in a photograph or video recording is the Personal Data of that individual.



#### **(A) Video Recordings of Academic Activities**

The recording of academic activities (e.g. lectures, seminars, laboratory demonstrations, presentations, etc.) can serve as a valuable resource for students (e.g. as an aid for students’ revision or post-lecture review, to enable complex ideas/concepts to be revisited and reflected upon by students, etc.) and for public interest (e.g. seminars open to the public).

#### ***Use of the Video Recording***

The recordings<sup>20</sup> are data of the University and shall be managed according to the Data Governance Framework. When planning to deploy video recording, the Department shall ensure that appropriate controls and policies for different phases of the data management lifecycle are in place, communicate and conduct awareness training to relevant staff and students on these requirements.

<sup>20</sup> The copyright and other intellectual property of video recordings made by or on behalf of the University belong to the University.

**Staff members shall only make video recording of academic activities for learning, teaching and research purposes. Students are only permitted to view the video recording for their own studies.**

### ***Before Recording***

Before recording the academic activities, the instructor or organiser shall take the necessary steps to protect the Personal Data of the students, guests (e.g. guest speakers, panellists, etc.) or other members of the audience, if any. The names and images of students and guests shall not be captured in the video recording if it is not necessary for the purposes of the activities concerned. If students and guests are captured in the background but are **not identifiable from the video recording**, such as if the image is too small or obscured, then there is less concern in relation to Personal Data.

- (i) Guests – If the video recording will capture the images of the guests, the invitation to the guests shall **specify that the event will be recorded, the purpose of the video recording, how the video recording will be used, and enclose a written confirmation** (see **Appendix B** for the template of the suggested wording in the invitation and the written confirmation) for the guests to sign and return to the Department on or before the starting date of the activity to be recorded.
- (ii) Students – The instructor or organiser shall **inform the students before the scheduled recording takes place that the event will be recorded, the purpose of the recording, and how the recording will be used** (e.g. be made available to students who are registered in the course, be posted on the website of the University for the public). The instructor or organiser shall identify and designate a zone **outside the recording area** for students who do not wish to be captured in the recording.

### ***During Recording***

The instructor or organiser shall display conspicuous notice to remind the students and guests, or any other member of the audience, at the beginning of the academic activity that it is to be recorded. The notice may read as follows:

*“This [nature of academic activity (e.g. seminar, tutorial)] will be recorded for the purpose of [purpose of the recording] and the recording may be made available to [name/group of individuals] on the [channels or media]. The recorded images will be handled by [Name of Department/ Office] according to the prevailing policy of The Hong Kong Polytechnic University. Enquiries shall be addressed to the [Post Title of the responsible officer and contact details].”*

The red light outside the venue to indicate the recording has commenced (if available) shall be switched on.

If a student or any other member of the audience indicates that he/she does not wish to be recorded, the instructor or organiser shall (1) ask the student or member of the audience to stay outside the recording area, or (2) edit the recording later (see the “After Recording” paragraph below), if such capturing is unavoidable (e.g. in a small classroom).

### *After Recording*

After recording, the instructor or organiser shall review the recording to **remove any captured images of the individuals (from which the individuals are identifiable) who indicated that they do not wish to be captured in the recording.**

### **(B) Taking Photographs or Videos during Events**

Before a Department takes photographs or videos during an event (e.g. a seminar/workshop), it shall notify the participants in the event invitation, during the registration or in the event confirmation. The notice may read as follows:

*“[Name of Department/ Office] of The Hong Kong Polytechnic University may take photographs/ video recording during this event and use such images in publicity or marketing activities. The recorded images will be handled by [Name of Department/ Office] according to the prevailing policy of The Hong Kong Polytechnic University. Enquiries shall be addressed to the [Post Title of the responsible officer and contact details].”*

### **3.4 Personal Data – International Student Applicants from the European Economic Area**



The EU General Data Protection Regulation (“GDPR”) applies outside the European Economic Area (“EEA”) countries in relation to Personal Data submitted by student applicants from the EEA countries **while the applicants are in their respective home countries.** The applicants provide their Personal Data to the University in order to facilitate the University’s assessment of their eligibility for the relevant curriculum for studies.

Once the accepted applicants have arrived in Hong Kong for studies, their Personal Data collected thereafter are no longer subject to GDPR. **For unsuccessful applicants, the personal data collected during the process is governed by GDPR as well as the Ordinance. Departments that recruit students from the EEA countries have to make the notice in Appendix C available to the said student applicants before collecting their Personal Data.**

### **3.5 Proactive Compliance Planning**

When planning a new initiative or project that needs to use Personal Data, the initiative or project owner (“the owner”) shall be mindful of the need to comply with the requirements of the Manual. The owner shall raise the issue with the Head of Department if he/she foresees or encounters any potential compliance issues or difficulties at the planning or implementation stage.

The common pitfalls are:

- Collecting excessive or irrelevant Personal Data
- Access right to Personal Data is too broad or not defined
- Inadequate security protection of Personal Data
- Use of Personal Data beyond the scope of the relevant PICS provided to the Data Subjects
- Use of Personal Data in Direct Marketing without the express consent of the Data Subjects

Personal Data are classified as “Confidential” pursuant to the Data Classification Scheme of the Data Governance Framework. The owner **shall refer to the Data Governance Framework which sets out the various stages of the data management lifecycle and guidelines for handling Personal Data and plan ahead to comply with the applicable requirements.**



## **4. Direct Marketing**

Use of Personal Data in Direct Marketing is an important subject under the Ordinance. Non-compliance with the Ordinance in relation to Direct Marketing may constitute criminal offences, and from time to time draw the attention of the public and the media. They may eventually lead to inquiries or investigation by the Commissioner, which would have adverse impact on the reputation of the non-compliant Data User.

The University is concerned to ensure that the Departments comply with the statutory requirements on Direct Marketing in managing their respective departmental activities. The Department shall follow the procedures described in this Chapter to obtain **express consent** of the Data Subjects **before** using the Personal Data in Direct Marketing.

### **Example(s)**

#### **Direct Marketing through “Direct Marketing Means”:**

- A personalized offer (“personalized” means addressing the recipient by his or her name) of discounts on computers and laptops sent via SMS.
- A personalized email regarding the opening of a new café near the campus.
- A personalized letter to alumni soliciting donations.

#### **The following activities are not Direct Marketing:**

- Sending marketing materials by post to an address **without the name of a specific person or simply to the “occupant”**.
- Soliciting donations **face-to-face** from another person.
- Introducing a fundraising programme **exclusively for corporations or organizations, not any specific person.**

## **4.1 Requirements and Procedures**

### **(A) DM Administrator(s)**

The Head of Department shall designate its staff member(s) as DM Administrator(s) to manage its departmental Direct Marketing activities. For Departments that conduct more than one streams of Direct Marketing activities, it is advisable to work out whether all units/sections in the Department be referred to as the same Department or be segregated. This will have impact on the scope of consent to be obtained from third parties and the ease of future administration.

### **(B) Obtaining Prior Consent**

The DM Administrator(s) shall use the template (see **Appendix D**) to obtain the **express consent** of the Data Subject **before** using the Personal Data, or providing the Personal Data for use, in Direct Marketing. **Such consent shall always be obtained in writing (either online or in paper form).**<sup>21</sup>

The said template may be appended to the end of the PICS when Personal Data are first collected from the Data Subjects, or be sent separately to obtain the express consent.

### **(C) Sending Direct Marketing Information**

The DM Administrator(s) shall send information falling under the scope of Direct Marketing (“Direct Marketing information”) only to the Data Subjects who consented to receive it<sup>22</sup>. The DM Administrator(s) shall also inform the Data Subjects of their opt-out right<sup>23</sup> (i.e. the right to cease to allow his or her Personal Data to be used for Direct Marketing at any time) by including an opt-out channel (see **Appendix D**) in each set of Direct Marketing information (e.g. to each separate email, letter or SMS) to be sent to the

<sup>21</sup> The Ordinance allows consent from the Data Subjects to be obtained either in writing or orally but oral consent has to be confirmed in writing within 14 days thereafter. Departments **shall always** obtain Direct Marketing consent **in writing** to avoid any miscommunication with or misunderstanding by the Data Subjects.

Data Subjects who have given their express consent.

Direct Marketing information shall be sent by:

- a) email by the Mailing List Management System (“MLM”); or
- b) mail in hard copy.

MLM is preferred for reducing the chance of human error in managing opt-out requests (see Sub-section (D) of this Section for the details) by:

- ✓ automatically incorporating the opt-out channel; and
- ✓ recording the opt-out request of the Data Subject and updating the database automatically.

Departments shall refer to the MLM website of ITS for the details.

### **(D) Opt-out Request**

The Data Subjects may exercise their opt-out right at any time after giving their prior express consent, by submitting an opt-out request through one of the following channels:

- a) Email via MLM – The Data Subject may click the “unsubscribe” link in the email. MLM will update the list of Data Subjects accordingly.
- b) General email, mail or oral notice – the DM Administrator(s) shall add the Data Subject’s name to the manually maintained opt-out list and acknowledge the Data Subject’s request by way of a written or electronic confirmation that the request has been processed.

<sup>22</sup> It is an offence under Section 35E of the Ordinance to use a Data Subject’s Personal Data in Direct Marketing without the Data Subject’s consent. Offenders are liable on conviction to a fine of HK\$500,000 and to imprisonment for 3 years.

<sup>23</sup> Sections 35G and 35L of the Ordinance.

No Direct Marketing information shall be sent to Data Subjects who have submitted the opt-out request.

#### **4.2 To Students by Email @connect.polyu.hk**

The University provides email accounts to its students (@connect.polyu.hk) for all-round development and education-related purposes and to facilitate communications with students, notify students of learning and development activities, benefits and welfare, updates and news of the University, and privileges and other activities offered by the University. Messages sent to the above-mentioned email accounts for students for the above stated purposes are not Direct Marketing information.

In case Personal Data of students are to be used in Direct Marketing, the requirements and procedures outlined in Section 4.1 of the Manual shall be followed.

#### **4.3 To Staff by Email @polyu.edu.hk**

The University provides work email accounts (@polyu.edu.hk) to staff for work-related purposes and to facilitate communications with the staff, notify staff of training and development activities, benefits and welfare, updates and news of its Departments, and privileges and other activities offered by the Departments and affiliated organizations of the University. Messages sent to the above-mentioned work email accounts for staff for the above stated purposes are not Direct Marketing information.

In case Personal Data of staff are to be used in Direct Marketing, the requirements and procedures outlined in Section 4.1 of the Manual shall be followed.

#### **4.4 To Alumni by Email @connect.polyu.hk**

The University provides email accounts to its alumni (@connect.polyu.hk) to facilitate communications with alumni, notify alumni of benefits and welfare, updates and news of the University, and privileges and other activities offered by the University. Messages sent to the above-mentioned email accounts for alumni for the above stated purposes are not Direct Marketing information.

In case Personal Data of alumni are to be used in Direct Marketing, the requirements and procedures outlined in Section 4.1 of the Manual shall be followed.

## **5. Use of CCTV**

### **5.1 Privacy and Personal Data Perspective**

The images captured and recorded by closed-circuit television (“CCTV”) systems are extensive and may constitute Personal Data under the Ordinance. It is necessary to carefully consider the potential impact of CCTV surveillance on the privacy of individuals and ensure that its use is properly controlled to avoid unnecessary intrusion into the privacy of individuals.



#### **Example(s)**

The following use of CCTV do not result in collection of Personal Data:

A CCTV is installed to collect the real-time data of pedestrian flow at a busy footbridge between the University and Hung Hom station. The CCTV does not capture any individual’s facial image and therefore no Personal Data is being collected.

A CCTV without recording function is NOT collecting Personal Data, and therefore the use of this CCTV system does not fall under the purview of the Ordinance.

CCTV systems in the University are either owned (i.e. installed and operated) by the Facilities Management Office (“FMO”) (for communal areas and common corridors) or a Department (for the premises of the Department). The owner or the intended owner of CCTV system(s) are required to comply with the requirements under the Manual when planning to install new/additional, re-locate, replace or upgrade CCTV system(s). The owner of CCTV system(s) shall review the need to continue to use the installed CCTV system(s) at least every 3 years with reference to the criteria and parameters in the Manual.

### **5.2 Planning**

When a Department plans to install a CCTV system, the Head of Department shall consider the following factors<sup>24</sup>:

- Assessment – Is it appropriate, necessary and proportionate for the given purposes or circumstance to use CCTV?
- Alternatives – Are there other less privacy-intrusive means than the use of CCTV to achieve the same objective?
- Accountability – Has the Department acted and been seen to have acted responsibly and transparently, in terms of its policy, controls, and compliance with the Ordinance, in the use of CCTV?

<sup>24</sup> “Guidance on CCTV Surveillance and Use of Drones” issued by the Commissioner in March 2017.

**(A) Purpose and Circumstances of Installing CCTV System(s)**

It is justifiable to install a CCTV system and rely on the images recorded for a number of legitimate purposes. Some typical examples are as follows:

- a) To prevent unlawful or unauthorized activity;
- b) To monitor the security of high-value assets (e.g. vehicles in car parks and expensive equipment in laboratories); or
- c) To protect the safety of staff members, students and visitors to the campus.

The Head of Department shall review the geographical scope and the period of surveillance according to the defined purpose(s).

For example, to prevent unauthorized access to high-value equipment or confidential data in a room, the surveillance scope shall be limited to that location. The CCTV cameras shall be positioned in a way that will not unnecessarily intrude into the privacy of individuals. **No** CCTV cameras shall be installed in places where privacy is reasonably expected (e.g. changing rooms).

**Using CCTV system(s) to monitor target person(s) or to conduct covert monitoring** (i.e. the individuals who may be captured are not informed of the operation of the CCTV system) is highly intrusive to privacy. Prior approval by FMO and the LRC Unit is required. The approval will only be granted if there is a genuine need and no other less privacy-intrusive arrangements or alternatives are available.

The Head of Department shall also consider the operating hours of the CCTV. In some cases, it may only be necessary to operate for a certain period (e.g. after office hours) rather than throughout the day.

**(B) Availability of Alternatives**

The Head of Department shall assess the options available to achieve the purpose.

Example(s)
<p>Purpose: To prevent and deter unauthorised use, damage or loss of certain laboratory equipment.</p> <p>Options available: Installing smartcard access control system, installing alarm system, patrol by security guard and/or CCTV surveillance.</p> <p>The use of CCTV system is only justified if these alternatives are proven ineffective or impracticable.</p>

To facilitate future reference of the due process being undertaken for compliance with the aforesaid requirements, the DPDO shall submit the completed CCTV Installation Assessment Form (see **Appendix E**) to the Head of Department. If the Head of Department considers that the planned installation is justified, he/she shall be **accountable for compliance with the Ordinance and the Manual**. The Head of Department may take up personally the role as Data Steward of the recordings of the CCTV system or designate his/ her deputy or other staff members as Data Steward(s) of the recordings of the CCTV system to comply with the requirements set out in Section 5.3 of the Manual.

**(C) Review of Continuing Use**

The Head of Department shall review the justification for continuing the use of the CCTV system at least every 3 years, to ensure that it is still serving the purpose(s) for which it was first installed, with reference to the criteria and parameters in the Manual. If the use of the CCTV system is no longer relevant or necessary, or if less privacy-intrusive alternatives can be used to achieve the same purpose(s), the Head of Department shall discontinue the use of the CCTV system.

**5.3 Compliance Measures**

The Data Steward(s) of the recordings of the CCTV system shall put in place the following measures:

**(A) CCTV Notice**

Display conspicuous notices in the area under CCTV surveillance to duly inform the people in the area that they are subject to CCTV surveillance. The CCTV notice shall read as follows:

*“CCTV in Operation*

*Closed-circuit television (“CCTV”) are in operation on these premises for security and safety purposes. The recorded images will be handled by the [Name of Department/Office] in accordance with the relevant guidelines of The Hong Kong Polytechnic University.*

*Enquiries or reports shall be addressed to the [Post Title of the responsible officer and contact details].”*

**(B) Control on Access to Recordings**

Ensure that there are written procedures and guidelines on handling requests to view or obtain a copy of the recordings and assess the requests to access the recordings accordingly<sup>25</sup>.

**(C) Security and Maintenance**

Ensure that the CCTV systems (both the equipment and the recordings) are properly protected<sup>26</sup> from vandalism or unlawful access. The CCTV systems equipment shall be stored in a secured place (e.g. inside a locked room or a cabinet where only authorized personnel have access).

Conduct regular maintenance of the CCTV systems to ensure their normal operation. If necessary, consult FMO for information on CCTV system maintenance.

**(D) Retention and Deletion**

Delete the recordings upon expiry of the retention period specified on the approved CCTV Installation Assessment Form. If the recordings eventually need to be retained beyond the originally specified

---

<sup>25</sup> See Chapters 5 and 6 of the Data Governance Framework.

<sup>26</sup> See Chapter 5 and Appendix B of the Data Governance Framework.

retention period, the Data Steward(s) shall put the justifications and extended retention period on record, and delete the recordings upon expiry of the extended retention period. The Data Steward(s) shall follow the requirements of the Data Governance Framework<sup>27</sup> in relation to the security and protection of the recorded images as well as the deletion upon the expiry of the specified retention period.

**(E) Maintaining Records**

Record the requests for viewing, copying and transferring the recordings in a log book for future reference. The log book shall include the following:



- a) Purpose of viewing/copying/transferring the recording (e.g. to verify the circumstances under which a reported personal injury claim occurred);
- b) Scope of the requests (e.g. the location, the starting and ending times of the relevant part of the recording)
- c) Name and other particulars of the requestor (e.g. the post name or title), organization (if the requestor is not a staff member or student of the University) and the date of request;
- d) Name of the approver (including the post name or title) and date of approval; and
- e) Date of compliance with the request.

**Note:**

The Data Steward(s) of the recordings of the CCTV system shall consult the LRC Unit upon receipt of requests from the law enforcement authorities to view or obtain any CCTV records, as these authorities have other statutory powers that need to be considered under the Ordinance. The Ordinance contains exemptions from the application of DPP3 and DPP6 (e.g. for the prevention or detection of crime).

---

<sup>27</sup> See Chapter 5 and Appendix B of the Data Governance Framework.

## **6. Data Access and Correction Requests**

### **6.1 Applicability**

The Data Subject has the right to access (i.e. to make a DAR) and make correction of his/her Personal Data (i.e. to make a DCR) under the Ordinance. Specifically, the Data Subject is entitled<sup>28</sup> to:

- a) ascertain whether the University holds his/her Personal Data;
- b) request a copy of such Personal Data held by the University, if any; and
- c) request to correct<sup>29</sup> such Personal Data held by the University if it is found to be inaccurate.



According to the Ordinance, the Data Requestor should use the Form OPS003 (the DAR form prescribed by the Commissioner<sup>30</sup>) for making a DAR. The Data User may charge a processing fee that is not excessive for handling a DAR, but **no** processing fees may be charged for a DCR.

**Note:** As recommended by the Commissioner, **even if the DAR is not made by using the Commissioner’s DAR Form (Form OPS003)**, Data Users are still advised to respond to that request as if it were a DAR proper (i.e. by sending a copy of the requested Personal Data to the Data Requestor) if it **substantially** contains the scope and details of the requested data and the identity of the Data Requestor.

The Head of Department shall designate staff member(s) to handle the DAR and DCR (“Request Administrator”) according to Sections 6.3 and 6.4 of the Manual respectively. The Request Administrator may also be the DPDO. The Request Administrator shall maintain records of DARs and DCRs received and processed by the Department in a log book (see below for a template).

<b>Data Access Request (DAR)/ Data Correction Request (DCR)</b>	<b>Date of First Receipt of Request</b>	<b>Data Subject Category</b>	<b>Ref.</b>	<b>Date of Reply to Data Requestor (within 40 calendar days of Date of First Receipt of Request)</b>	<b>(If DAR/ DCR is refused) Reason(s) for Refusal</b>
<i>e.g. DAR</i>		<i>e.g. Student</i>			
<i>e.g. DCR</i>		<i>e.g. Staff</i>			

<sup>28</sup> Schedule 1 of the Ordinance: DPP6 – Access to Personal Data.

<sup>29</sup> According to section 22(1) of the Ordinance, the DCR is applicable only to the Personal Data that has been supplied in compliance with an earlier DAR by the Data Requestor, who considers the supplied Personal Data to be inaccurate. The University adopts a flexible approach and will accept requests to correct Personal Data that are not supplied pursuant to a prior DAR.

<sup>30</sup> English version: <https://www.pcpd.org.hk/english/publications/files/Dforme.pdf> or Chinese version: [https://www.pcpd.org.hk/tc\\_chi/publications/files/Dformc.pdf](https://www.pcpd.org.hk/tc_chi/publications/files/Dformc.pdf)



## **6.2 Data Subjects and Request-Handling Departments**

DARs and DCRs are handled by the relevant Departments listed below:

<b>Data Subject</b>	<b>Request-Handling Department</b>
Student applicants and students <sup>31</sup>	AR
Donors and Alumni	AADO
Job applicants, staff members and former staff members <sup>32</sup>	HRO
Members/ users of centres established by Departments, and participants of events organized by Departments	The respective Departments
Users of University Health Service	UHS

## **6.3 Handling DAR**

DARs for the Personal Data of students and staff members should be handled in accordance with the procedures stipulated by AR (see the “Application for Personal Data Access under the Personal Data (Privacy) Ordinance” released by AR) and HRO (see the “Departmental Guidelines for Handling Staff Personal Data” released by HRO) respectively. If the Data Requestor can access the Personal Data direct, the Request Administrator shall advise the Data Requestor to access such Personal Data accordingly. Students should access their Personal Data via the eStudent System (for sub-degree, undergraduate and taught postgraduate students) and the University Portal (for research postgraduate students). Staff members should access their Personal Data via the Computerised Human Resources Information System (CHRIS).

### **Stage DAR1 – Preparation**

Check if the DAR is to be handled by one’s own Department or another Department. Refer to Section 6.2 of the Manual for the relevant request-handling Departments. If the DAR is to be handled by another Department, forward the DAR to the DPDO of the relevant Department **within 2 working days after receiving the DAR from the Data Requestor (i.e. first receipt).**



(Go to the next page.)

<sup>31</sup> See the “Application for Personal Data Access under the Personal Data (Privacy) Ordinance” released by AR.

<sup>32</sup> See the “Departmental Guidelines for Handling Staff Personal Data” released by HRO, and the Data Governance Framework regarding DARs by staff members for their own Personal Data.

Record the date of first receipt of the DAR and other relevant particulars in the log book. It is a **statutory requirement** to comply with a DAR **within 40 calendar days (not working days) of first receipt**<sup>33</sup> (the “40-day period”). If the DAR is transferred from another Department, the Request Administrator shall ascertain the date of first receipt of the DAR by seeking clarification from the Department that first received the DAR (as needed).

**Stage DAR2 – Review**

Check the validity of the DAR.

**Note:**

A valid DAR shall either be made on the Form OPS003 (the form prescribed by the Commissioner as stated in Section 6.1 of the Manual), **or in other written form(s) in Chinese or English** specifying:

- a) the identity information of the Data Subject (e.g. name, student ID number/staff ID number, address, telephone number);
- b) if the DAR is submitted by a “relevant person”<sup>34</sup> on behalf of the Data Subject, such written request shall also include the identity information of the relevant person, the written authorization signed by the Data Subject to authorise the relevant person to make a DAR on his/her behalf and a copy of the Data Subject’s identification document; and
- c) information which can help to locate the requested Personal Data (e.g. the kind of document which contains the requested data, the Department that collected the data, where and when the data was collected, etc.).

If any of the information/document(s) in a), b) (if applicable) or c) is missing from the DAR, ask the requestor for the missing information/document(s). If the Data Requestor does not provide the required information/document by the expiry of the 40-day period, refuse the DAR (refer to Stage DAR3b below).



Assess whether any of the relevant exemptions in Section 2.2 of the Manual or the examples of grounds for refusal (outright or partial) in **Appendix F** is applicable. If the Request Administrator considers that any or more of them may be applicable, seek advice from the LRC Unit **not later than 10 calendar days from the date of first receipt of the DAR**. If the LRC Unit advises that the request is exempted and may be refused, go to Stage DAR3b.

<sup>33</sup> Section 19(1) of the Ordinance.

<sup>34</sup> Section 17A of the Ordinance.

**Stage DAR3a –Comply with the DAR**

Gather the requested data. For data maintained by another Department, the Request Administrator shall coordinate with the DPDO(s) of the other Department(s) to locate the requested data.

The Request Administrator shall check the data to be supplied to the Data Requestor carefully and redact the Personal Data of other Data Subject(s). See **Appendix G** for an illustration of redacting. Do **not** tamper with or destroy any data in the course of gathering and supplying the requested Personal Data.



Assess the processing fee (which may include a photocopying fee if photocopies of documents are made for the Data Requestor) as appropriate for the DAR, and inform the Data Requestor to pay the said fee by expiry of the 40-day period. Check that the Data Requestor has paid the said fee by the said date<sup>35</sup>.

**Note:**

If the Data Requestor fails to pay the photocopying fee before the expiry of the 40-day period, the Request Administrator shall issue a written reminder to him/her asking for payment and state that the Personal Data requested will be made available upon receipt of the payment.

The processing fee can only be charged if the Department is going to comply with a DAR.



**If the Request Administrator is not able to fully comply with the request within the 40-day period** (e.g. the requested data is voluminous, so only part of the requested data can be gathered), perform this step, otherwise go to the next step:

The Request Administrator shall, within the said period, prepare a draft reply to the Data Requestor for endorsement by the Head of Department. The draft reply shall explain the reasons for the delay in gathering all the requested data<sup>36</sup>. The endorsed draft shall be further submitted to the LRC Unit for review **not later than 30 calendar days from the date of first receipt of the DAR**. Incorporate the comments (if any) of LRC Unit.

Send the reply with the data gathered as of the expiry of the said 40-day period to the Data Requestor by the expiry of the said 40-day period. Full compliance with the request shall be made **as soon as practicable after the said period**.



(Go to the next page.)

<sup>35</sup> Section 28(5) of the Ordinance allows the Data User to refuse to comply with a DAR unless and until the fee imposed by the Data User has been paid.

<sup>36</sup> Section 19(2) of the Ordinance.

## INTERNAL USE

Submit the DAR and a requested copy of the Personal Data to be provided to the Data Requestor to the Head of Department for review and endorsement.

Release the copy of Personal Data to the Data Requestor by ordinary mail (or by registered mail if specified by the Data Requestor on his/her DAR) **within the 40-day period**. If the Data Requestor collects the copy in person, confirm his/her identity by checking his/her PolyU staff/student ID card or HKID Card (for non-PolyU members).

Record the date of reply to the Data Requestor and other relevant information in the log book, and file a copy of the reply for record. The completed DAR Form and relevant documents are recommended to be retained on file **for 1 year from the date of first receipt of the DAR** for future reference or possible follow-up actions.

### Stage DAR3b – Refuse the DAR (if applicable)

Prepare a draft written notification to the Data Requestor for endorsement by the Head of Department. Refer to **Appendix H** for the template of the letter for refusing a DAR. The endorsed written notification shall be further submitted to the LRC Unit for review **not later than 30 calendar days from the date of first receipt of the DAR**. Incorporate the comments (if any) of the LRC Unit.

Issue the notification to the Data Requestor **within the 40-day period**.

Record the refusal case and the reason(s) for the refusal in the log book, and file the relevant DAR documents. Retain the refusal records and documents for **4 years from the date of making the entry to the log book**<sup>37</sup>.

---

<sup>37</sup> Section 27(1) of the Ordinance.

**6.4 Handling DCR**

DCR can be raised by a Data Subject to make corrections to his/her Personal Data, with proper supporting information/document(s) and/or after the Data Subject has received his/her Personal Data from the Data User via a DAR.

DCRs for the Personal Data of students and staff members should be handled in accordance with the procedures stipulated by AR (see Section 6.2 of this Chapter) and HRO (see Section 6.2 of this Chapter) respectively. If the Data Requestor can correct the requested Personal Data direct, the Request Administrator shall advise the Data Requestor to do so accordingly. Students should make correction to their Personal Data via the eStudent System (for sub-degree, undergraduate and taught postgraduate students) and the University Portal (for research postgraduate students). Staff members should make such corrections via the Computerised Human Resources Information System (CHRIS).

**Stage DCR1 – Preparation**

Check if the DCR is to be handled by one's own Department or another Department. Refer to Section 6.2 of the Manual for the relevant request-handling Departments. If the DCR is to be handled by another Department, forward the DCR to the DPDO of the relevant Department **within 2 working days after first receipt** of the DCR.



Record the date of first receipt and other particulars in the log book. It is a statutory requirement to comply with a DCR **not later than 40 calendar days (not working days) of first receipt of it<sup>38</sup> (the "40-day period")**.

If the Request Administrator receives the DCR from another Department, he/she shall ascertain the date of first receipt of the DCR by seeking clarification from the Department that first received the DCR (as needed).

<sup>38</sup> Section 23(1) of the Ordinance.

**Stage DCR2 – Review**

Check the validity of the DCR (There is no specific DCR form prescribed by the Commissioner):

- a) A DCR under the Ordinance shall be made by the Data Subject with appropriate supporting documentation to show the inaccuracy of the Personal Data concerned.
- b) If the DCR is submitted by a “relevant person”<sup>39</sup> on behalf of the Data Subject, the DCR shall include the identity information of the relevant person, and be attached with an authorization letter signed by the Data Subject together with a copy of the identification document of the Data Subject.

If any of the information/document(s) in a) or b) (if applicable) is missing from the DCR, ask the Data Requestor for the missing information/document(s). If the requestor does not provide the required information/document(s) by the expiry of the 40-day period, refuse the DCR (refer to Stage DCR3b below).



Assess whether the relevant exemption(s) in Section 2.2 of the Manual or the grounds for refusal in **Appendix F** is/are applicable. If the Request Administrator considers that any or more of them may be applicable, seek advice from the LRC Unit **not later than 10 calendar days from the date of first receipt of the DCR**. If the LRC Unit advises that the request is exempted or may be refused, go to Stage DCR3b.

**Stage DCR3a – Comply with the DCR**

Correct or update the Personal Data concerned. If the Personal Data to be corrected are not held by the request-handling Department, the Request Administrator shall coordinate with the DPDO(s) of the relevant Department(s) to correct the Personal Data.

Let the Data Requestor have a copy of the corrected Personal Data as appropriate by, for example, sending him/her a letter setting out the corrected data and the date of correction. **The DCR shall be handled free of charge.**

Record the date of reply in the log book, and file a copy of the reply for record. DCR documents are recommended to be retained on file for **1 year from the date of first receipt of the DCR** for future reference or possible follow-up actions.

<sup>39</sup> Section 17A of the Ordinance.

**Stage DCR3b – Refuse the DCR (if applicable)**

Prepare a draft written notification to the Data Requestor for endorsement by the Head of Department. Refer to **Appendix H** for the template of the letter for refusing a DCR. The endorsed written notification shall be further submitted to the LRC Unit for review **not later than 30 calendar days from the date of first receipt of the DCR**. Incorporate the comments (if any) of LRC Unit.

Issue the notification to the Data Requestor **within the 40-day period**.

Record the refusal case and the reason(s) for the refusal in the log book, and file the relevant DCR documents. Retain the refusal records and documents for **4 years from the date of first receipt of the DCR**<sup>40</sup>.

---

<sup>40</sup> Section 27(1) of the Ordinance.

## 7. Personal Data Privacy Enquiries

This Chapter describes the process for handling enquiries about information or requests for clarification on the University’s privacy policies, procedures and practices, or how Personal Data is collected/created, used/accessed, retained, disclosed/transmitted or deleted by the University. Enquiries from the media (e.g. news reporters, journalists, etc.) shall be handled by CPA.

The records are recommended to be retained on file for 1 year from the date of first receipt of the enquiry for future reference or possible follow-up actions.

Source of Enquiry	Owner	Action
Commissioner	DPDO	Enquiries <b>from the Commissioner</b> shall be reported to the Head of Department and forwarded to the LRC Unit <u>immediately or as soon as practicable, preferably within 2 working days</u> . The Head of Department shall assign a staff member to coordinate with the LRC Unit to collect the relevant facts and provide other necessary information for handling the enquiry.
Any party other than the media or the Commissioner	All staff members	Refer the enquirer or forward the enquiry to the DPDO of his/her Department, <u>preferably within 2 working days</u> .
	DPDO	<ol style="list-style-type: none"> <li>1. If the enquiry is related to Personal Data handled by another Department, then <u>promptly, preferably within 2 working days of first receipt of the enquiry</u>, forward the enquiry to the DPDO of the relevant Department.</li> <li>2. Respond to the enquiry according to the following principles:               <ol style="list-style-type: none"> <li>a) If the required information can be checked/retrieved by the enquirer from an online database (e.g. eAdmission System, eStudent System or Computerised Human Resources Information System), the DPDO shall direct the enquirer to the appropriate database;</li> <li>b) If the enquiry is straightforward and the DPDO can answer readily, the DPDO shall answer the enquiry promptly; or</li> <li>c) In other cases, the DPDO shall consult the Head of Department for guidance. The Head of Department may consult the LRC Unit (if needed).</li> </ol> </li> <li>3. In the event the enquiry is in writing or a written response is needed, the DPDO shall a) prepare and submit the draft response to the Head of Department for review and endorsement; b) submit the endorsed draft to the LRC Unit for review; c) incorporate the comments (if any) of the LRC Unit; and d) finalise and despatch the response to the enquirer.</li> </ol>



## **8. Data Incidents**

It is vital to handle a Data Incident properly to minimize its impact and prevent a recurrence.

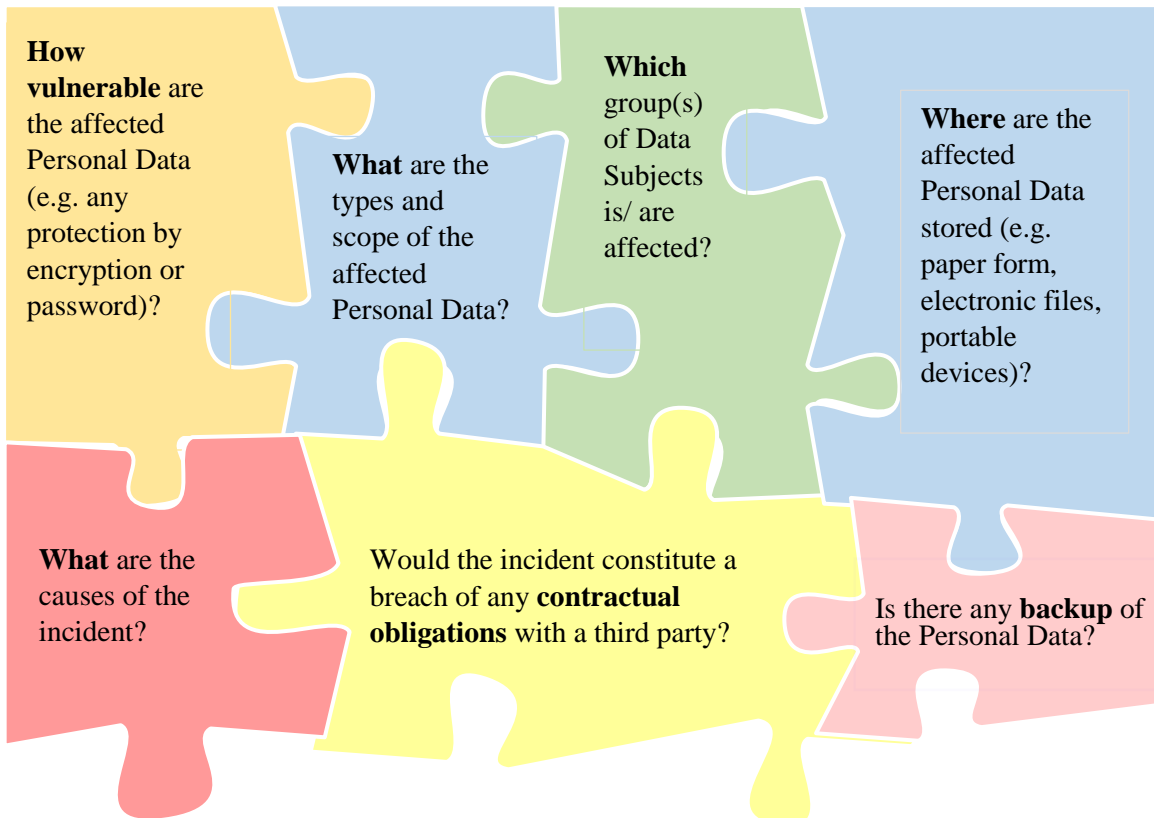
### **1 Detection**



#### **(1) Initial Assessment**

When a staff member is aware of a Data Incident, he/she shall report the incident to the Head of Department and the DPDO of the Department within 24 hours or as soon as practicable. An initial assessment shall be carried out by the Head of Department and/or DPDO of the Department. As Anonymized Data do not carry identifiable personal information, an incident involving Anonymized Data is not a Data Incident.

With the directive from the Head of Department, the DPDO shall promptly work with the Data Steward of the affected Personal Data and gather the following information about the Data Incident:



Data Incidents involving Personal Data collected or processed by a student during fieldwork, internship or placement shall be reported by the student, subject teacher or Head of Department to the student's fieldwork/ internship/ placement supervisor as soon as practicable.

**(2) Data Incident Involving the Commissioner**

If the Department is notified by the Commissioner of a Data Incident (or the Commissioner becomes involved), the incident shall be passed to the LRC Unit for handling. The Head of Department shall assign a staff member, as appropriate, to coordinate with the LRC Unit to collect the relevant facts and provide other necessary information for handling the incident.

**2 Impact Containment, Risk Assessment and Reporting**



**(1) Impact Containment**

Depending on the cause of the Data Incident and with the directive of the Head of Department, the DPDO, Data Steward of the affected Personal Data and relevant IT supporting personnel (if applicable) shall undertake appropriate containment and rectification measures to contain the impact of the Data Incident. For example:

- a) Shutdown the affected system(s);
- b) Change users' passwords and system configurations to control access and use (i.e. assign access roles on a need-to-know basis);
- c) Cease or change the access rights of individuals suspected to have committed or contributed to the Data Incident;
- d) Intercept or delete the Personal Data (e.g. recalling emails and asking unintended recipients to delete the wrong emails received or mail back the documents containing the Personal Data);
- e) Enhance or rectify physical security control (e.g. replace the broken lock); and/or
- f) Report the Data Incident to the law enforcement agencies as appropriate (e.g. the Police, if theft or other crime is suspected). The Head of Department shall consult the LRC Unit prior to reporting to the law enforcement agencies.

**(2) Risk Assessment**

The Head of Department shall assess the risk of harm caused by the Data Incident to the Data Subjects and the University.

- a) Potential harm to Data Subjects:
  - Threat to personal safety
  - Identity theft
  - Financial loss
  - Embarrassment, adverse impact on emotional well-being and/or personal image
- b) Potential harm to the University:
  - Interruption to operation
  - Negative impact on reputation
  - Breach of contractual obligation(s) to the Data Subject(s) and/or third parties
  - Non-compliance with the Ordinance and being subject to sanctions
  - Financial loss

**(3) Reporting**

Indicators of high risk of harm:

- The Data Incident affects the Personal Data of a large group of people (e.g. all students of the Department).
- The affected Personal Data in aggregate (e.g. HKID Card details, date of birth, address, and bank account information) could be exploited for theft of identity.
- The affected Personal Data are not secured in accordance with the Data Handling Guidelines under the Data Governance Framework.
- The impact of the Data Incident cannot be contained within a reasonable time despite implementation of all practicable measures.

The DPDO shall document all of the information gathered, actions taken and analysis performed as outlined above under Part A of the Data Incident Information Sheet (see **Appendix I**), and submit it to the Head of Department for review and endorsement. The Head of Department shall submit the Data Incident Information Sheet to the following parties **within 48 hours of being aware of the Data Incident or as soon as practicable**:

<b>Person(s) Whose Personal Data is Affected by the Incident</b>	<b>Recipient of the Data Incident Information Sheet</b>
All cases	Executive Vice President Head, Legal, Risk and Compliance Director of Communications and Public Affairs
Students	Registrar
Staff members	Director of Human Resources
All cases related to IT system(s)	Director of Information Technology

3

**Notification** (if applicable)



**(1) To the Data Subject**

The Head of Department shall, upon consultation with the Director of Communications and Public Affairs and the Head, Legal, Risk and Compliance, notify the Data Subjects about the Data Incident. The notification to the Data Subjects may include the following:

- a) A general description of how and when the Data Incident occurred;
- b) A list of the types of Personal Data affected by the Data Incident;
- c) A description of the measures already taken or to be taken to contain the impact of the Data Incident;
- d) Information and advice on actions the Data Subjects can take to protect themselves from the adverse effects of the Data Incident e.g. identity theft or fraud; and
- e) Means to contact the University for further information or assistance.

## **INTERNAL USE**

If there is a contractual obligation (e.g. with third parties) to protect the relevant Personal Data, the Head of Department shall consider the appropriate action to address the potential breach of contract. If theft or other crime is suspected, the Head of Department may also report the matter to the Police.

### **(2) To the Commissioner**

Depending on the circumstances of the case, a notification may be given to the Commissioner. The Head of Department shall consult EVP and the LRC Unit to decide whether such notification shall be given.

If EVP and the LRC Unit are of the view that a notification to the Commissioner is needed, the Head of Department shall complete a Data Breach Notification Form, which is available at the Commissioner's website below:

[https://www.pcpd.org.hk/english/enforcement/data\\_breach\\_notification/files/DBN\\_e.pdf](https://www.pcpd.org.hk/english/enforcement/data_breach_notification/files/DBN_e.pdf)

The completed Data Breach Notification Form shall be submitted to the LRC Unit for review prior to submitting it to the Commissioner. The completed form shall be uploaded onto the Commissioner's website below:

[https://www.pcpd.org.hk/english/enforcement/data\\_breach\\_notification/dbn.html](https://www.pcpd.org.hk/english/enforcement/data_breach_notification/dbn.html)

**Note:** Reporting a Data Incident to the Commissioner does not preclude the Commissioner from receiving complaints and conducting an enquiry or investigation of the case (whether in response to a complaint or on the Commissioner's own motion).

### **(3) Recording of Notification of Data Incident**

All notifications shall be made in writing and endorsed by the Head of Department and be recorded in Part B of the Data Incident Information Sheet (**Appendix I**).

**4 Post-Incident Review**



After the Data Incident is handled and the consequences are managed, the Head of Department, Data Steward of the affected Personal Data and the DPDO shall review the causes and evaluate if existing protection and prevention measures are sufficient to prevent similar incidents from occurring.

***Typical issues to be considered at the post-incident review:***

- Are there processes that can be streamlined or introduced to prevent similar Data Incidents from occurring in the future?
- Are there weaknesses in existing working practices or security measures to protect Personal Data (e.g. use of outdated software and protection measures, insufficient staff awareness of the proper practices for handling Personal Data)?
- Are the methods for accessing and transmitting Personal Data sufficiently secure (e.g. access limited to authorized personnel only)?
- Is there a need to amend or reinforce existing policies and practices for managing or safeguarding Personal Data?

The DPDO shall document the recommended changes identified from this review in Part C of the Data Incident Information Sheet (**Appendix I**), and submit the completed Data Incident Information Sheet to the Head of Department for review and endorsement.

The DPDO shall then file a copy of the completed Data Incident Information Sheet for record and copy the same to the parties involved within one month after detection or acquiring knowledge of the Data Incident.

The Head of Department shall conduct periodic review (at least on an annual basis) of its Data Incident(s) and the results of the post-incident review(s) for identifying the lessons to be learned (e.g. from the patterns of incidents) and weaknesses that need to be addressed.

## **9. Frequently Asked Questions**



**a) My Department arranges a number of activities for members of the public. How can I incorporate the PICS in the registration form of these activities?**

As a start, the DPDO of your Department shall use the generic template of the PICS in **Appendix A** and incorporate the requisite details such as Department name and contact details for access or correction of data. Then the DPDO shall host the PICS in the departmental website as a master document. You can then incorporate a hyperlink to the PICS into the application or registration form, website or other media channels, to comply with Data Protection Principle 1 of the Ordinance. Alternatively, you may append the full text of the PICS to the end of the application or registration form.

**b) How should I handle Personal Data during my work?**

You shall follow the requirements outlined in the Data Handling Guidelines<sup>41</sup> when handling Personal Data.

**c) May I continue to send Direct Marketing information to someone who has made an opt-out request?**

You shall not send any Direct Marketing information to the Data Subjects that have made an opt-out request. Failure to comply with an opt-out request may constitute an offence under the Ordinance. Contact the DPDO of your Department for assistance to send Direct Marketing information by the Mailing List Management System, via which anyone who has made an opt-out request will be removed from the system.

**d) Is it permissible to charge the Data Subject a fee for making an opt-out request to the University for the purpose of Direct Marketing?**

This is not permissible. Under the Ordinance, the University (as the Data User) shall not charge the Data Subject a fee for complying with his/her opt-out request.

**e) If the Police asks for the residential address and phone number of a student, shall I comply with this request?**

There are a number of exemptions to the Data Protection Principles under the Ordinance (see Section 2.2 of the Manual), which includes the Police's request for Personal Data held by the University by relying on section 58 of the Ordinance. While the University is under the legal obligation to cooperate with and assist the Police in its law enforcement duties as necessary, it shall also exercise due diligence to ensure that any disclosure of Personal Data for this purpose does not violate the Ordinance. Ask the Police to send the request in writing, setting out the basis of the request in the context of the requirements under the Ordinance. Enquire with the law enforcement agents to understand the details of the case if these are not clear. Analyze the basis

---

<sup>41</sup> See Appendix B of the Data Governance Framework.

of the request in the context of the Ordinance. The University may comply with the request when it is reasonably satisfied that failure to supply the requested data would be likely to prejudice the investigation<sup>42</sup>. You may also refer the request of the Police to the DPDO of your Department or the LRC Unit for advice.

**f) Is it necessary to have a PICS available on collection of Personal Data by CCTV?**

The University has put up CCTV notice(s) on the premises where CCTV surveillance is in operation to inform the affected individuals of the purpose of collection of Personal Data and to provide the means of contact for reporting issues and making inquiries. It is therefore not necessary to have a PICS for CCTV.

**g) CCTV is installed to collect the real time data of pedestrian flow at a busy footbridge between the University and Hung Hom station. The CCTV neither captures any individual's facial image nor has any recording function. Does the Manual apply?**

Applying the definition of Personal Data under the Ordinance, there is no collection of Personal Data in a form in which it is practicable to access or process, so the Manual does not apply to this CCTV system. (Refer to Chapter 5 on the use of CCTV systems for collecting Personal Data.)

**h) Our CCTV system captures and records low resolution images in a public area taken at such an angle that the facial images of the individual cannot be determined. Does the Manual apply?**

Images from which the identity of the individuals cannot be determined are not Personal Data. The Manual does not apply to this type of CCTV system and the images recorded. (Refer to Chapter 5 on the use of CCTV systems for collecting Personal Data.)

**i) Can our Department collect the "ID number + surname" from the visitors of Student Halls of Residence for security purposes e.g. if a visitor violated the Hall Regulations, he/she will be barred from entering the premises in future?**

Under the DPP1, collection of Personal Data shall be necessary for or directly related to the purpose(s) of use, and shall be adequate but not excessive. According to the "Code of Practice on the Identity Card Number and Other Personal Identifiers Compliance Guide for Data Users" issued by the Commissioner in July 2016, collection of HKID Card numbers by the Data User is permitted for future identification of an individual who is permitted to enter premises where monitoring of his/her activities in the premises is not reasonably practicable.

In view of the above, your Department shall demonstrate that the collection of "ID number + surname" for security purposes are not excessive, and monitoring of the activities of the individual inside the premises is not reasonably practicable.

1. Visitors who are staff members or students of PolyU shall only be required to provide their staff ID or student ID numbers. Your Department shall not collect their "ID number + surname";

---

<sup>42</sup> Section 58(2) of the Ordinance; and the Commissioner's Case Note 2010C06.

## INTERNAL USE

2. Your Department shall not collect the ID number of a visitor if it is reasonably practicable to monitor the visitor's activities in hall premises e.g. the visitor is attending an event hosted by hall staff/ tutors; and
3. If the visitor is neither a staff member nor a student, and it is not reasonably practicable to monitor the visitor's activities in the hall, you may collect the visitor's "ID number + surname".

The staff/student ID numbers or ID numbers (and surname) collected shall be properly managed and protected in accordance with the Manual and the University's Data Governance Framework (the "Framework"). According to Section 3.4 of the Framework, it is the responsibility of the Data Stewards (i.e. your Department) to ensure that the said retention periods are defined, and to develop processes to securely delete the Personal Data at the end of the relevant retention periods. Section 5.6 of the Framework stipulates that the Data Custodians shall securely delete the Personal Data upon the expiry of the relevant retention period(s) and with the approval from the respective Data Steward (please refer to the Data Handling Guidelines in the Framework for the details).

**j) Is it true that only part-time staff members need to be directly provided with a copy of the Manual? How about full-time staff members?**

All staff members of PolyU (both full-time and part-time) shall abide by the requirements set out in the Manual. A copy of the Manual is available under the Administration page on the University Portal ([https://www2.polyu.edu.hk/DAG/PD\\_Manual.pdf](https://www2.polyu.edu.hk/DAG/PD_Manual.pdf)). Departments shall ask their full-time staff members who are required to have access to or handle Personal Data to read this Manual via the said page. As some part-time staff members may not have access to the University Portal, Departments shall provide the part-time staff members whose job responsibilities may require them to have access to or handle Personal Data, with a copy of the Manual.

**k) I have questions on the Manual. How can I seek assistance?**

You should contact the DPDO of your department. You can find out who is your DPDO from the Administration page on the University Portal ([https://www2.polyu.edu.hk/DAG/List\\_of\\_Dept\\_PD\\_Officers.pdf](https://www2.polyu.edu.hk/DAG/List_of_Dept_PD_Officers.pdf)). The DPDO shall handle the enquiries of fellow colleagues of the Department on Personal Data protection and privacy related matters. If the DPDO is in doubt, he/she shall discuss with the LRC Unit.



**Students' Personal Data**

**l) Can I publish students' academic results in a public venue?**

The student names/ student ID numbers and their respective results shall not be posted in any public venue (e.g. notice boards). Alternatively, Departments may consider posting academic results within secure systems (such as the eStudent System) that require individual students to authenticate their identity for access to their own results.

**m) I am an academic staff member and I want to record my lecture on video. What do I need to consider before I do this?**

If you are doing the recording for your own reference and no images of students will be captured, there is less concern on compliance. As a matter of courtesy, inform the students before recording the lecture.

If you are doing the recording which will be made available to the students for revision, you need to consider the following:

Before recording the lecture, you shall ensure that the privacy of the students and guests (e.g. guest speaker, panellists, etc.) is assured for all video recordings. The names and images of the students and guests shall not be captured in the video recording if it is not necessary. If the video recording will capture the images of the guests, you shall obtain the consent of the guests prior to the commencement of the recording. You have to inform the students of the recording arrangement, including the purposes of use of the recording, in advance. If the students' facial images will likely be captured, seek their agreement beforehand and respect their choices. You shall also inform the general audience and remind the guests of the recording arrangement above at the beginning of the lecture to be recorded. Refer to Section 3.3 of the Manual for more information.

**n) A student disclosed to me her health and personal circumstances which affected her studies. Can I inform the student's other lecturers about this?**

The information you received should only be used for the purpose for which it was provided. Unless you have the student's express consent, you should not pass the information to other lecturers.

**o) Are examination answer books Personal Data of students?**

Examination answer books contain the student ID number, the grades/scores and examiners' written remarks, which are the examiners' evaluation of the students' performance, so they shall be handled as documents containing the Personal Data of the respective students.

**p) Can I distribute graded assignments to students by asking them to pick up from a pile of other graded assignments left on a table at the back of the classroom?**

Student assignments shall not be left unattended. The best practice is to hand them back to students individually and directly, to avoid inadvertent disclosure of a student's Personal Data (e.g. student name, student ID number, grade, etc.).

- q) Our Department records students' presentations only if the students agree to it. We started this practice so that the teaching staff may refer to the recordings to respond to students' queries on their assessment grades/scores or other comments on their presentations. Can we use these recordings as a teaching tool for other students during classes?**

The recording contains the student's Personal Data (e.g. face and voice), so it falls within the ambit of the Ordinance. You shall also comply with the Data Governance Framework (the "Framework") of the University from the creation to the deletion of the recordings, which fall into the "Confidential" category under the Data Classification Scheme of the Framework.

Using the recordings during classes as a teaching tool for other students constitutes a "new purpose" under the Ordinance. According to Data Protection Principle 3 of the Ordinance, you need to further obtain the student's express consent before you do so. Alternatively, you may wish to state both purposes when you initially seek the student's consent in one-go to make the recordings. It would be advisable to state in the request for consent the expected period for the use of the recordings for the teaching purpose. You shall ensure that the recordings containing the Personal Data are deleted thereafter, in accordance with the Framework and the Data Protection Principle 2 of the Ordinance which stipulates that Personal Data should not be kept longer than is necessary or the fulfilment of the purpose for which the data is collected.

- r) Who is the Data Subject of the teaching evaluation results?**

The teaching evaluation results (e.g. Student Feedback Questionnaire) of teachers are the Personal Data of the teachers concerned, so the latter are the Data Subjects of the results.

## **Appendix A – Template of the Generic PICs**

This is a personal information collection statement under the Personal Data (Privacy) Ordinance (“the Ordinance”).

**Notes to user:**

1. Please fill in the particulars in square brackets and marked with an asterisk \*.
2. If you need to modify this template, please consult the LRC Unit of EVP Office.

### 1. Purpose of Collection

The personal data provided by you to [Department/Office Name]\* of The Hong Kong Polytechnic University (“PolyU”) will be collected, retained, processed, used and transferred (within or outside of Hong Kong) for the following purposes:

- Processing your inquiries, application, registration or request for services, activities and facilities;
  - Facilitating communications with you;
  - Facilitating implementation of PolyU’s policies and procedures, and monitoring compliance with the same;
  - Enabling PolyU to comply with any applicable procedures, laws, regulations or court orders (in each case whether in Hong Kong or overseas), any requests by government, statutory, regulatory or law enforcement authority, and valid legal processes, ordinances obligations;
  - Conducting quality assurance, surveys and review, statistical analysis, and research; and
  - Other purposes directly relating to any of the above.
2. You are required to provide your personal data, other than those items indicated as optional. Failure to provide such data may lead to inability to process your application, registration or request for services, activities and facilities, or maintain contact with you.

### 3. Disclosure and Transfer of Personal Data

PolyU will keep your personal data confidential and only authorized members will have access to and handle your personal data. PolyU may disclose or transfer your personal data to service providers and contractors engaged in activities on behalf of PolyU within or outside Hong Kong solely for the purposes set out in paragraph 1 above.

PolyU may also disclose your personal data when authorized or required by law and in response to requests from law enforcement agencies, government departments or regulatory authorities, or where required to protect PolyU’s rights or properties.

### 4. Access and Correction of Personal Data

You have the right to request for access and correction of your personal data held by PolyU. Any data access and correction request according to the Ordinance should be made in writing to the Departmental Personal Data Officer of [Department/Office Name]\* at [address]\* or by email at [email address]\*. A fee may be imposed for processing your data access request.

5. Security, Accuracy and Retention of your Personal Data

PolyU takes reasonable precautions to prevent the loss, misappropriation, unauthorized access or destruction of your data. PolyU also takes reasonable steps to ensure that all personal data held by it is accurate, complete, correct and reliable for the intended use.

Your personal data will be retained by PolyU according to its policy on retention of data and records.

6. Privacy Policy Statement

You may refer to [https://www.polyu.edu.hk/web/en/privacy\\_policy\\_statement/](https://www.polyu.edu.hk/web/en/privacy_policy_statement/) for the Privacy Policy Statement of PolyU.

## **Appendix B – Template of the Consent Form for Recording**

### **Suggested wording in the invitation to the guest:**

This [name and date of educational activities] will be recorded for the purpose(s) of [purpose of the recording]. The recording will be made available to [name/group of individuals] on the [channels or media].

### **Written confirmation from the guest before commencement of the recording:**

Notes to user:

Please fill in the particulars in square brackets. This duly completed form shall be returned to the Department on or before the date of the activity to be recorded.

I, [name of the Guest], authorize The Hong Kong Polytechnic University (the "University") and its agents to make audio and video recordings by any means and in any media (the "Recordings") of my presentation, lecture or programme described below (the "Presentation") and to use my name, photograph and biographical information in connection with the reproduction and distribution of the Presentation and the Recordings. I understand that the University will credit me as the author or source of the Presentation.

Presentation at the [name of the Department] of the University

*Title of Event:*

*Title of Presentation:*

*Date of Presentation:*

*Location of Presentation:*

I retain any copyrights I may have in the Presentation. Nothing in this document shall limit my rights to publish or use the Presentation as I see fit.

I agree that the University will own the Recordings and all copyrights and other rights therein ("IP rights"). I agree that the University will have the irrevocable, worldwide right to make, copy, edit, publish, distribute, play, show, display and otherwise use and make available the Recordings and any works that may be derived from the Recordings, by any means and in any media now existing or hereafter invented, and to authorize others to do the same.

**INTERNAL USE**

I will do such thing and/or execute such document as may be requested by the University to effectively transfer/assign all the IP rights of the Recordings to the University.

\*While I receive an honorarium for the Presentation, I understand and agree that I will not receive any royalties or other payment in connection with either the IP rights I have granted to the University in this document or the use and dissemination of the Recordings.

I warrant that neither my Presentation nor the grant of the IP rights I have made to the University in this document infringes or violates any copyright or other right of, or breaches any obligation I have to, any other person or entity.

Signature:

Name: [name of the Guest]

Date:

\* delete if not applicable

## **Appendix C – Notice for Applicants from the European Economic Area**

### **Notice for Applicant from the European Economic Area**

#### **1. What is the purpose of this document?**

The Hong Kong Polytechnic University (the “University”) is committed to protecting the privacy and security of your personal information. This notice describes how we collect and use your personal data during the application for admission process in accordance with the General Data Protection Regulation (“GDPR”). The University is the “data controller” for the information that we obtain from you or others as a result of your application for undergraduate or postgraduate study.

#### **2. Glossary**

In this notice, your “personal data” means any recorded information that is about you and from which you can be identified. It does not include data where your identity has been removed (anonymous data). “Processing” of your personal data means anything that we do with that information, including collection, use, storage, disclosure, deletion or retention.

#### **3. The types of data we hold about you**

The information we hold about you may include the following:

Personal details such as name, title, address, telephone number, email address, date of birth, sex and gender;

- Education and employment information;
- Visa, passport and immigration information;
- Funding and financial support information.

We may also process the following "special categories" of more sensitive personal data:

- Information about your race or ethnicity;
- Information about your health, including any disability and/or medical condition;
- Information about criminal convictions and offences (if applicable to your course).

Special category data will not be used to assess your application and will only be used in accordance with paragraph 6.

#### **4. How did the University obtain your data**

Most of the information we hold comes from your application, for example, via [www.polyu.edu.hk](http://www.polyu.edu.hk). We may also collect additional information directly from you and from other parties, such as your current or former school(s), referees, and government departments and agencies.

#### **5. How the University uses your data**

We process your data for the purpose of processing and assessing your application for study, and for purposes related to your application, such as assessing your eligibility for funding and your financial status. Access to your data will be provided to our staff who need to view it as part of their work in carrying out the purposes. We set out below examples of circumstances where it is necessary for us to process your data. We may use the same information under more than one circumstances.

**(1) To consider your application**

We also need to process data under this heading where the University is working with a third party in order to offer you services, for example, those offered by the colleges or scholarship benefactors. See paragraph 7 on third party sharing.

**(2) To comply with a legal obligation**

Information processed for this purpose includes, but is not limited to, information relating to the monitoring of equal opportunities. We are also required by law to provide data to various Government departments, such as immigration, visa.

**(3) To meet our legitimate interests**

We also need to process your data in order to meet our legitimate interests or the legitimate interests of others. For example:

- asking you to provide additional information on your application;
- notifying you of changes to course information; and
- inviting you to take part in applicant surveys or enabling third parties to conduct applicant surveys on our behalf.

**If you fail to provide personal information under 5(1) or 5(2) above**

If you fail to provide certain information when requested under the circumstances described in paragraphs 5(1) and 5(2) above, we may not be able to meet our contractual obligation to consider your application or to comply with our other legal obligations.

**Change of purpose**

We will only process your personal data for the purposes for which we collected it, unless we reasonably consider that we need to use it for another related reason and that reason is compatible with the original purpose. If we need to use your data for an unrelated purpose, we will seek your consent to use it for that new purpose.

Please note that we may process your data without your knowledge or consent where this is required or permitted by law.

**6. Special category data**

Special category data require a higher level of protection. Listed below are examples of processing activities that we regularly undertake in respect of these types of data. In addition to the activities listed below, it may sometimes be necessary to process this sort of information for exceptional reasons, for example, because it is necessary to protect your vital interests or those of another person.

**Disability**

We will process data you have volunteered about any disability in order to make any arrangements or adjustments required in relation to your application (e.g. to arrange access for interviews) and/or to monitor equal opportunities.

**7. Data sharing with third parties**

In order to perform our contractual and other legal responsibilities or purposes, we may, where relevant and necessary, need to share your information with the following types of organization:

- Your referees;
- The governmental departments or agencies responsible for immigration and study visa;
- Sponsors or benefactors of funding and financial support;

Where information is shared with third parties, we will seek to share the minimum amount.

All third-party service providers that process data on our behalf are required to take appropriate security measures to protect your data in line with our policies. We do not allow them to use your data for their own purposes. We permit them to process your data only for specified purposes and in accordance with our instructions.



## **8. Retention Period**

We will retain your data only for as long as we need it to meet our purposes, including any relating to legal, accounting, or reporting requirements.

## **9. Your rights**

Under certain circumstances, by law you have the right to:

- **Request access** to your data (commonly known as a “subject access request”). This enables you to receive a copy of your data and to check that we are lawfully processing it.
- **Request correction** of your data. This enables you to ask us to correct any incomplete or inaccurate data we hold about you.
- **Request erasure** of your data. This enables you to ask us to delete or remove your data in certain circumstances, for example, if you consider that there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your data where you have exercised your right to object to processing (see below).
- **Object to processing** of your data where we are relying on our legitimate interests (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your data for direct marketing purposes.
- **Request the restriction of processing** of your data. This enables you to ask us to suspend the processing of your data, for example if you want us to establish its accuracy or the reason for processing it.
- **Request the transfer** of your data to another party.

Depending on the circumstances and the nature of your request it may not be possible for us to do what you have, for example, where there is a statutory or contractual requirement for us to process your data and it would not be possible to fulfil our legal obligations if we were to stop. Where you have consented to the processing (for example, by asking us to send you certain types of communication), you can withdraw your consent at any time, by emailing us at [\[insert email\]](#). Upon your withdrawal of the consent, we will stop the processing as soon as we can. The withdrawal will not invalidate past processing.

If you want to exercise any of the rights described above or are dissatisfied with the way we have used your information, please email the [\[Academic Registry/ International Affairs Office/ Faculty of XXXX\]](#) of the University at [\[insert email\]](#). We will seek to deal with your request without undue delay, and in any event in accordance with the requirements of the GDPR. Please note that we may keep a record of your communications to help us resolve any issues which you raise.

## **10. Keeping your data up-to-date**

It is important that the data we hold about you is accurate and current. You can access, amend and delete your data yourself until the point at which you submit your application to the University. Please keep us informed of any changes after you submit your application.

## **11. Changes to this privacy policy**

We reserve the right to update this privacy policy at any time, and will seek to inform you of substantial updates. We may also notify you in other ways from time to time about the processing of your personal data.

The Hong Kong Polytechnic University  
[\[month and year\]](#)

## **Appendix D – Template for Direct Marketing**

**Notes to user:**

1. Please fill in the particulars in square brackets and marked with an asterisk \*.
2. If you need to modify this template, please consult the LRC Unit of EVP Office.

### **Obtaining Consent for Direct Marketing**

#### Use of Personal Data in Direct Marketing

[Department/Office Name]\* of The Hong Kong Polytechnic University would like to use your name, address, telephone number, fax number and email address to inform you of the following activities, services and facilities (collectively, “the marketing subjects”):

- Activities, seminars or workshops organized by us alone, jointly with other parties or by other parties;
- Privileges, discounts and offers for services provided by us alone or jointly with other parties; and
- Charitable, educational, social and other activities that solicit contributions, donations or participation.

We cannot use your personal data for sending information on the above marketing subjects to you unless we have received your consent. Please tick (✓) the box below to indicate your agreement for us to use your personal data to send you information on the above marketing subjects.

You may withdraw from receiving information on the marketing subjects indicated above at any time by sending an email to the Departmental Personal Data Officer at [email address]\*.

I agree [Department/Office Name]\* of The Hong Kong Polytechnic University to use my personal data to send me information on the marketing subjects indicated above.

Name: \_\_\_\_\_

Signature: \_\_\_\_\_ Date: \_\_\_\_\_

### **Unsubscribe Statement**

You may withdraw from receiving direct marketing information from [Department/Office Name]\* by sending an email to the Departmental Personal Data Officer at [email address]\*.

## Appendix E – CCTV Installation Assessment Form

SECTION 1 – INITIAL SCREENING QUESTIONS		
		Yes / No
1.1	Will the CCTV system have the recording function (video or still pictures) that can capture the facial images of individuals?	
1.2	Is the purpose of installing the CCTV system to collect or compile information about identified individuals?	
<p>If you have answered “Yes” to any one of the above questions, please proceed and complete Section 2. Otherwise, you do not need to proceed further with this assessment as the CCTV system will not involve the collection of Personal Data as defined under the Personal Data (Privacy) Ordinance (the “Ordinance”), and is therefore not regulated under the Ordinance.</p>		
SECTION 2 – ASSESSMENT		
2.1	<p>Please provide detailed information about the CCTV system to be installed:</p> <ul style="list-style-type: none"> <li>a) Purpose(s) for installation (please also indicate the problem(s) to be addressed by the installation):</li> <li>b) Number of CCTV camera(s):</li> <li>c) Location of the CCTV camera(s):</li> <li>d) Resolution of the CCTV camera(s):</li> <li>e) CCTV camera operation times (e.g. after office hours and on holidays only, 24 hours a day or 7 days a week):</li> </ul>	
2.2	<p>Have you considered other less privacy-intrusive alternatives to CCTV surveillance which can also achieve the above-mentioned purpose(s)?</p> <p><input type="checkbox"/> Yes (Please specify the alternatives being considered, and explain why they are not feasible or effective for the specified purpose(s) above.)</p> <p>_____</p> <p><input type="checkbox"/> No (Please explain.)</p> <p>_____</p>	
2.3	<p>Will the CCTV system be used to monitor target persons or for covert monitoring?</p> <p><input type="checkbox"/> Yes (Go to Question 2.4.)</p> <p>_____</p> <p><input type="checkbox"/> No (Go to Question 2.5.)</p>	
2.4	<p>If the answer to Question 2.3 is “Yes”, have you obtained approval from FMO and the LRC Unit?</p> <p><input type="checkbox"/> Yes and I have attached the approval documents/correspondences.</p> <p>_____</p> <p><input type="checkbox"/> No This installation <u>cannot</u> proceed.</p>	
2.5	<p>In addition to the DPDO of the Department, please list out all the parties that will have/may have access to the CCTV records and the purposes for accessing those records:</p>	

**INTERNAL USE**

	<b>Post Title of Relevant Party</b>	<b>Organization (if external to the University)</b>	<b>Purpose</b>
2.6	The retention period of recorded images is _____		
2.7 (Please check all that apply.)	Where will the CCTV records be stored? <input type="checkbox"/> On campus <input type="checkbox"/> Off-campus <input type="checkbox"/> Locked cabinets <input type="checkbox"/> Restricted storage area / filing room <input type="checkbox"/> Other security measures (Please specify): _____ _____		
2.8	List out any other privacy risks identified and the actions you will take to remove or reduce the risk (if any):		
	<b>Risk</b>	<b>Action to Remove or Reduce the Risk</b>	
<b>Submitted by: DPDO</b>			
Signature: Name: Department: Date:			
<b>Approved by: Head of Department</b>			
Signature: Name: Date:			

**Appendix F – Grounds for Refusal of Data Access/Correction Request(s)**

A DAR may be refused if:

- a) there is no or not enough information for the Department to verify the identity of the Data Requestor;
- b) the Department cannot comply with the request without disclosing the Personal Data of a third party;
- c) the request is not written in Chinese or English;
- d) the DAR fee has not been paid;
- e) the Department is not supplied with information to locate the requested data;
- f) the DAR follows two or more similar requests, and it is unreasonable for the Department to comply with the DAR in the circumstances;
- g) another party controls the use of the requested data in a way that prohibits the Data User from complying with the DAR; or
- h) the Department is entitled under the Ordinance or any other Ordinance not to comply with the DAR.

**All DAR refusal cases shall be referred to the LRC Unit not later than 30 calendar days from the date of first receipt of the DAR for approval.**

A DCR may be refused if:

- a) there is no or not enough information for the Department to verify the identity of the Data Requestor;
- b) the DCR is not written in Chinese or English;
- c) the Department is not satisfied that the Personal Data to which the DCR relates is inaccurate;
- d) the Department is not provided with sufficient information to ascertain that the data is inaccurate;
- e) the Department is not satisfied that the correction provided in the DCR is accurate.

**All DCR refusal cases shall be referred to the LRC Unit not later than 30 calendar days from the date of first receipt of the DCR for approval.**

**Appendix G – Illustration on Redacting**

Original version

Attendance Records

On 4 September 2018, I was on duty from 9 a.m. to 4 p.m. At 12:30 p.m., I received a phone call from a person called John Chan who told me that he needed help at his unit on the 9<sup>th</sup> floor. I attended the location and rang the doorbell. A Chinese female answered the door and told me that there was no one called John Chan and she did not make the phone call. The lady identified herself as Phyllis Leung and her contact number was 9090 9090. I left the location at 12:48 p.m.

Chan Tai Man  
Staff number: 12345

---

Redacted version – in response to a Data Access Request by John Chan

Attendance Records

On 4 September 2018, I was on duty from 9 a.m. to 4 p.m. At 12:30 p.m., I received a phone call from a person called John Chan who told me that he needed help at his unit on the 9<sup>th</sup> floor. I attended the location and rang the doorbell. A Chinese female answered the door and told me that there was no one called John Chan and she did not make the phone call. The lady identified herself as [REDACTED] and her contact number was [REDACTED]. I left the location at 12:48 p.m.

[REDACTED]  
Staff number: [REDACTED]

---

Redacted version – in response to a Data Access Request by Phyllis Leung

Attendance Records

On 4 September 2018, I was on duty from 9 a.m. to 4 p.m. At 12:30 p.m., I received a phone call from a person called [REDACTED] who told me that he needed help at his unit on the 9<sup>th</sup> floor. I attended the location and rang the doorbell. A Chinese female answered the door and told me that there was no one called [REDACTED] and she did not make the phone call. The lady identified herself as Phyllis Leung and her contact number was 9090 9090. I left the location at 12:48 p.m.

[REDACTED]  
Staff number: [REDACTED]

**Appendix H – Template of the Letter for Refusing Data Access Request(s) / Data Correction Request(s)**

[On letterhead]

Reference No.:

[Date]

[Name of Data Requestor]

[Postal address of Data Requestor]

Dear [Name of Data Requestor],

**Re: Data Access/Correction\* Request**

We refer to your data access/correction\* request dated [date] for [scope of request].

We regret that we cannot comply with your request for the following reason(s): [explanation as appropriate]

Any queries pertaining to this matter can be directed to [Name of DPDO or designated officer] at [contact email address].

Yours sincerely,

[Signature]

[Name of Head of Department]

[Post title]

The Hong Kong Polytechnic University

\* Please delete as appropriate.

## Appendix I – Data Incident Information Sheet

**Notes:**

*Part A – To be completed by the DPDO. The DPDO shall then send the information sheet to the Head of Department for endorsement. The Head of Department shall submit the endorsed information sheet to the following parties **within 48 hours of being aware of the Data Incident or as soon as practicable:***

- *All cases - **Executive Vice President, Head, Legal, Risk and Compliance and Director of Communications and Public Affairs***
- *If the Personal Data of students are affected - **Registrar***
- *If the Personal Data of staff members are affected - **Director of Human Resources***
- *If the Data Incident is related to IT system(s) - **Director of Information Technology***

*Part B and Part C – To be completed by the DPDO and endorsed by the Head of Department. The DPDO to file the completed information sheet and copy the same to the parties involved in Part A within one month of the Data Incident.*

PART A – THE DATA INCIDENT AND RISK ASSESSMENT		
<b>A1. Incident:</b>	Date: Time:	Description:
<b>A2. Detection:</b>	Date: Time:	<u>Information of the Person who Detected the Incident</u> Name: Post Title/ Department (if applicable):
<b>A3. Personal Data Storage Medium:</b> <i>(Please check all that apply.)</i>	<input type="checkbox"/> Paper form <input type="checkbox"/> Electronic files (e.g. Microsoft Word files, spreadsheets, etc.) <input type="checkbox"/> Storage devices (e.g. USB flash drive, hard disk, etc.) <input type="checkbox"/> The University’s website <input type="checkbox"/> Others (Please specify): _____	
<b>A4. Are security measures (required under the Data Governance Framework) in place?</b>	<input type="checkbox"/> Yes (Please specify): _____ <input type="checkbox"/> No	
<b>A5. Estimated number of Data Subjects affected:</b>	<input type="checkbox"/> 1 - 100 <input type="checkbox"/> 101 – 1,000 <input type="checkbox"/> 1,001 – 10,000 <input type="checkbox"/> 10,001+	<input type="checkbox"/> Unknown (Please explain): _____ _____
<b>A6. Data Subjects:</b> <i>(Please check all that apply.)</i>	<input type="checkbox"/> Students of the sub-degree programmes, undergraduate programmes or taught postgraduate programmes <input type="checkbox"/> Students of the research postgraduate programmes <input type="checkbox"/> Staff members <input type="checkbox"/> Users of the University Health Service <input type="checkbox"/> Users of learning and teaching facilities (e.g. the Optometry Clinic, Rehabilitation Clinic, Integrative Health Clinic) <input type="checkbox"/> Alumni <input type="checkbox"/> Others (Please specify): _____	



<b>A7. Personal Data affected:</b> <i>(Please check all that apply.)</i>	<input type="checkbox"/> Name <input type="checkbox"/> Date of birth <input type="checkbox"/> Gender <input type="checkbox"/> HKID Card number, Mainland ID number, passport number <input type="checkbox"/> Student ID number, staff ID number, library card number <input type="checkbox"/> Address <input type="checkbox"/> Mobile Phone/Telephone number <input type="checkbox"/> Fax number <input type="checkbox"/> Email address <input type="checkbox"/> Marital status <input type="checkbox"/> Health information, medical records	<input type="checkbox"/> Emergency contact details <input type="checkbox"/> Images (still or video) of individuals (e.g. photographs or video recordings) <input type="checkbox"/> Academic records <input type="checkbox"/> Interview records (e.g. resumes, job application forms, interview assessment records) <input type="checkbox"/> Employment records <input type="checkbox"/> Performance appraisal records <input type="checkbox"/> Donation records <input type="checkbox"/> Bank account or credit card number <input type="checkbox"/> Others (Please specify): <hr/> <hr/>
<b>A8. Is a backup copy of the data available?</b>	<input type="checkbox"/> Yes <input type="checkbox"/> No	
<b>A9. Would the University be in breach of any agreement/contract as a result of the Data Incident?</b>	<input type="checkbox"/> Yes (Please attach a copy of the agreement document.) <input type="checkbox"/> No	
<b>A10. Cause of the Data Incident (if known):</b>	<hr/>	
<b>A11. Is there any risk of harm caused by the Data Incident?</b> <i>(Please check all that apply.)</i>	<input type="checkbox"/> No (Please explain): <hr/>	
	<b>To Data Subjects:</b> <input type="checkbox"/> Threat to personal safety <input type="checkbox"/> Identity theft <input type="checkbox"/> Emotional well-being, embarrassment <input type="checkbox"/> Financial loss	<b>To the University:</b> <input type="checkbox"/> Reputational damage <input type="checkbox"/> The loss of public trust in the University <input type="checkbox"/> Non-compliance with the Ordinance <input type="checkbox"/> Breach of contractual obligations <input type="checkbox"/> Financial loss
<b>A12. What actions have been taken to contain the impact (including the risk(s) of harm in A11 above) of the Data Incident, or to resolve the Data Incident?</b> <i>(Please check all that apply.)</i>	<input type="checkbox"/> Shutdown the affected system on _____(dd/mm/yyyy) <input type="checkbox"/> Change users' passwords and system configurations to control access and use on _____(dd/mm/yyyy) <input type="checkbox"/> Cease or change the access rights of individuals suspected to have committed or contributed to the Data Incident on _____(dd/mm/yyyy) <input type="checkbox"/> Intercept or delete the Personal Data (e.g. recalling emails and asking unintended recipients to delete the wrong emails received or mail back the documents containing the Personal Data) on _____(dd/mm/yyyy) <input type="checkbox"/> Enhance or rectify physical security control (e.g. replace the broken lock) on _____(dd/mm/yyyy) <input type="checkbox"/> Report to law enforcement agencies (e.g. the Police, if theft or other crime is suspected). ( <i>Note: The Head of Department shall consult the LRC Unit prior to reporting to law enforcement agencies.</i> ) <input type="checkbox"/> Others (Please specify): <hr/> <hr/> <hr/>	

ENDORSEMENT BY HEAD OF DEPARTMENT	
Name: Post Title and Department:  Date:	Signature:
PART B – NOTIFICATION	
<b>B1. Did you notify the Data Subjects about the Data Incident?</b> <i>(Note: Data Subjects shall be notified about the Data Incident as soon as practicable.)</i>	<input type="checkbox"/> Yes (Please specify the actions that have been taken to inform the Data Subjects, and the date of notification.) <hr/> <input type="checkbox"/> No (Please explain.) <hr/>
<b>B2. Did you notify other relevant parties about the Data Incident?</b> <i>(Please check all that apply.)</i>	<input type="checkbox"/> Yes <input type="checkbox"/> Police, if theft or other crime is suspected (Please specify the actions that have been taken and date of notification): <hr/> <input type="checkbox"/> External parties as required by contractual obligations (Please specify the party names, actions that have been taken and date of notification): <hr/> <input type="checkbox"/> Others (Please specify the party name, actions that have been taken and date of notification): <hr/> <input type="checkbox"/> No (Please explain): <hr/>
<b>B3. Did you notify the Commissioner about the Data Incident?</b>	<input type="checkbox"/> Yes (Please specify the actions that have been taken to inform the Commissioner, and the date of notification, and attach a copy of the submitted Data Breach Notification Form.) <input type="checkbox"/> No (Please explain.) <hr/>
PART C – POST-INCIDENT REVIEW	
<b>C1. How and when was the Data Incident solved?</b>	
<b>C2. List all of the recommended changes identified as a result of the post-incident review:</b>	
ENDORSEMENT BY HEAD OF DEPARTMENT	
Name: Post Title and Department:  Date:	Signature: