THE HONG KONG POLYTECHNIC UNIVERSITY
香港理工大學

Student Affairs Office
學生事務處

Guidelines on Handling of Personal Data

This set of guidelines on handling of personal data prepared by the Student Affairs Office should be read in conjunction with the prevailing "**Personal Data Compliance Manual**" issued by the Legal, Risk and Compliance Unit of the Office of the Executive Vice President and accessible via myPolyU - "Administration > Personal Data Privacy" on the University Homepage.

Table of Contents

(A) Foreword

The Personal Data (Privacy) Ordinance places a legal duty on all departments, units and staff of the University to properly handle personal data. An individual staff member may be held liable for any unauthorised act or omission relating to personal data that is controlled, held, processed or used by the University. Staff members of the Student Affairs Office ("SAO") should read and observe the Guidelines contained in this document and be mindful of their individual responsibility and accountability in handling personal data.

According to the Personal Data (Privacy) Ordinance, "personal data" means information which relates to a living individual and can be used to identify that individual. It must also exist in a form which access to or processing of is practicable. In the context of the records of students, employers and staff members kept at The Hong Kong Polytechnic University ("PolyU"), "personal data" include, but not limited to the following:

Source of Personal Data	**Description**
Students	Personal information: Name, date of birth, student number, photo, marital status, email address, address, telephone number, Hong Kong identity card number, health and medical information, bank account number, resume and job application for career advising, counselling advice, emergency contact information Academic and registration information at PolyU: Programme studied, subject registration details, PolyU and public examination results, internship records, disciplinary records, payment status
Employers	Name, title, telephone number, fax number, email address, copy of Business Registration certificate, company name and address
Staff members	Personnel record, photo, staff identity card, staff appraisal record, medical record, payroll record, counselling record, employer's reference

The main requirements of the Privacy Ordinance are set out in six data protection principles ("the DPPs") (Detailed description of the principles could refer to "***Personal Data Compliance Manual***" which is accessible via myPolyU - "Administration" on the University Homepage. The DPPs may be summarised as follows:

DPP1: Rules applying to the collection of staff personal data

DPP2: Accuracy requirement and duration of retention of staff personal data

DPP3: Rules governing use of staff personal data

DPP4: Security requirements in handling staff personal data

DPP5: Openness requirement relating to staff personal data policies and practices

DPP6: Compliance with requests for access and correction of staff personal data

Staff members who controls the collection, holding, processing, or use of personal data ("Data User"), should always comply with the six DPPs when handling personal data. A flowchart of general procedures for personal data handling is shown in **Appendix A**.

(B) <u>Guidelines for Data Collection, Use and Transparency</u> <u>*(reference DPP1, DPP3 and DPP5)*</u>

1. Personal data shall only be collected in a lawful and fair manner, for the purposes directly related to the functions/ activities of SAO. The collected personal data shall be necessary but not excessive.

2. When collecting personal data from a data Subject, SAO shall provide them 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, or 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 the data access requests may be made.

3. Data users must take all practicable steps to make personal data policies known to the public regarding the types of personal data we hold and how the data is used. In light of this, the following measures should be taken by SAO:

   a) Hyperlink of the University’s Privacy Policies Statement (“PPS”) shall be provided in the website of SAO and its sections’ webpages.

   b) All the application forms and surveys/ questionnaires, etc. used by SAO (in online or paper format) should be incorporated with a printed version or a hyperlink of online version of the Personal Information Collection Statement ("PICS"). Such documents should be reviewed and revised regularly to ensure that they meet the prevailing policies requirements.

4. Currently, the personal data provided to SAO of PolyU will be collected, retained, processed, used and transferred (within or outside of Hong Kong) for the following purposes:

   a) Processing inquiries, application, registration or request for services, activities and facilities:

Source of Personal Data	Examples of Application and Service
Students	▪ Group programmes and events, internship opportunities, training and workshops, talks and courses, scholarship/ financial assistance schemes, funding and reimbursement, academic advising service, counselling service, provision of locker services and sports facilities, hall residency, etc., for individual students and student organisations; ▪ Administration and maintenance of student records including attendance record of activities, internship and co-curricular achievement records for issuance of related transcripts
Employers	Promotion for recruitment talks, career fairs and other activities

   b) Facilitating communications and liaisons;

   c) Facilitating implementation of PolyU’s and SAO’s policies and procedures, and monitoring compliance with the same;

   d) Enabling PolyU/ SAO 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;

e) Conducting quality assurance, surveys and review, statistical analysis, and research; and

f) Other purposes directly relating to any of the above.

5. The Ordinance requires a data user to inform the data subject the ultimate use of the information collected and stipulates that unless the data subject gives consent, personal data should be used for the purpose for which they were collected or a directly related purpose.

6. **Disclosure and Transfer of Personal Data**

a) The data should be used by authorised persons within SAO and not be disclosed to any organisations except for the purposes stated below. Disclosure includes making printed copies, viewing on screens, sending electronic copies, or passing data during conversations. The staff member who is able to access personal data should be reminded of the obligation to use the data only for the purposes for which the information has been given to them and to adhere to the guidelines on handling the data.

Examples of personal data disclosure and transfer in SAO operations:

- Students' personal data and examination results used for outside student activities may be released to the engaged outside organisers and contractors within or outside Hong Kong solely for the purposes as set out in Paragraph 4 above;
- Students' personal data and examination results used for scholarship/ financial assistance schemes may be released to the Government and various scholarship/ bursary donors for providing additional support/ services;
- Students' personal data and medical information may be released to University Health Services, hospitals and Hong Kong Police under emergent situations;
- Students' personal data and disciplinary records may be released to Student Discipline Committee and respective academic departments in case of violation of rule of conduct.
- Students' personal data used for the purpose of handling enquiries and provision of special services may be released to relevant resource person/ party.

b) Unless it is required by Law, organisations (such as the Hong Kong Immigration Department, the Student Financial Assistance Agency, educational institutions, prospective employers or employers which require applicant/ student data from the PolyU including the provision of references on a student's general performance, character, potential, etc.) must have obtained the written consent from the data subject concerned before SAO will release any data.

c) Provided there is the need to transfer the personal data to a Third Party outside SAO, the staff-in-charge must inform the Section/ Team Head who will then obtain written consent from the Dean of Students or his/ her delegate before taking any further action.

7. **Direct Marketing**

When data users use personal data for direct marketing purposes, they must inform the data subject of his/her right to opt-out at any time. The following "unsubscribe" statement and link as the opt-out channel into the email content must be included in the electronic direct marketing material via Mailing List Management System (MLM) each time. No Direct Marketing information shall be sent to data subjects who have submitted the opt-out request.

- Unsubscribe statement for students:

"If you do not wish to receive further marketing information from Student Affairs Office of The Hong Kong Polytechnic University, please click here to go to the eStudent System to unsubscribe (including research students admitted in 2018 or after). For research students admitted in 2017 or before, please click here to go to the Research Student Portal to unsubscribe."

- Unsubscribe statement for non-PolyU students:
  "If you do not wish to receive the information from the Student Affairs Office of The Hong Kong Polytechnic University, please click here to unsubscribe.

  To manage your subscription of marketing information from PolyU, please click here."

(C) Guidelines for Data Retention and Security *(reference DPP2 and DPP4)*

8. Upon the expiry of the retention periods or no longer required, the personal data shall be securely destroyed and disposed. All documents containing personal identifiers should not be kept unnecessarily. Care must be taken so as not to overlook e-mail records kept. Disposal record should be kept for future reference by completing the form attached in **Appendix B**.

9. All Sections/ Teams shall review the duration of retention of personal data periodically. A set of guidelines on retention period should be introduced to their staff members in order to ensure that the personal data are kept no longer than necessary. The current retention periods of personal data adapted by individual Sections are listed in **Appendix C**.

10. To ensure data security, all Sections/ Teams should regularly review their security arrangements with reference to the requirement of the Ordinance and the following guidelines:-

    a) Access to personal data is restricted to authorised data users assigned by the Dean of Students or his/ her delegate. Staff who are involved in the handling and processing of personal data must be reminded of their responsibilities in using the data and given clear instructions on the need to and how to ensure security and protection of records/ data and of the necessity to avoid unauthorised disclosure.

    b) Care must be exercised in transmitting records/data so as to ensure safe delivery of such to the intended recipient. Electronic files containing personal data MUST be encrypted. Password of the document should not be sent in the same email with the file attached.

    c) Any temporary staff including student assistants employed should as far as possible not be allowed to have access to the personal data. If this is unavoidable, they should be supervised by a non-temporary staff during the operation. All temporary staff having access to personal data should be asked to sign an undertaking form (**Appendix D**). It is also a good practice for regular staff to sign a similar undertaking.

    d) All student records printed on paper must be properly kept and should not be left unattended in public-accessible areas. Unwanted materials should be properly destroyed.

    e) Remote access of computer terminals using software is not allowed. The terminals should not be placed in areas where unauthorised persons might be able to read the screens. Passwords must be kept confidential and be changed at regular intervals to avoid unauthorised users tampering with the computer database.

    f) Data should be stored securely and kept away from people not entitled to see them. Unwanted files should be properly destroyed.

    g) Personal data should not be stored in removable storage devices. If it is absolutely necessary to do so, this should consult and seek prior permission from the Section/ Team Head before taking action.

       - The storage device should be provided by SAO with encryption by ITS suggested software. i.e. “BitLocker”.

- The documents containing personal data must be encrypted and should be removed from the removable storage device as soon as possible after completion of work.

h) Data stored in the hard disk of obsolete PC’s should be properly removed before disposal of the PC’s. Detaching the hard disk from the PC should be avoided unless absolutely necessary and, in such case, the hard disk should be kept securely.

11. A detailed data handling guideline extracted from “***Data Governance Framework***” is reproduced in **<u>Appendix E</u>**. Staff member should comply with the practical procedures mentioned in the appendix when handling personal data throughout the its lifecycle.

(D) <u>Guidelines for Access and Correction of Data *(reference DPP6)*</u>

12. A data subject must be given access to his/ her personal data and allowed to make corrections if it is inaccurate. A data user is required to comply with a data access request within 40 days after receiving the request.

13. If a student/ employer/ staff member wishes to access to, and/ or make correction of their personal data kept by SAO, he/ she should write to the Dean of Students, Student Affairs Office, The Hong Kong Polytechnic University, Hung Hom, Kowloon.

14. Detailed guidelines and procedures for handling data access and correction requests could refer to Part 6 *“Data Access and Correction Requests”* in the “***Personal Data Compliance Manual***” which is accessible via myPolyU - “Administration” on the University Homepage.

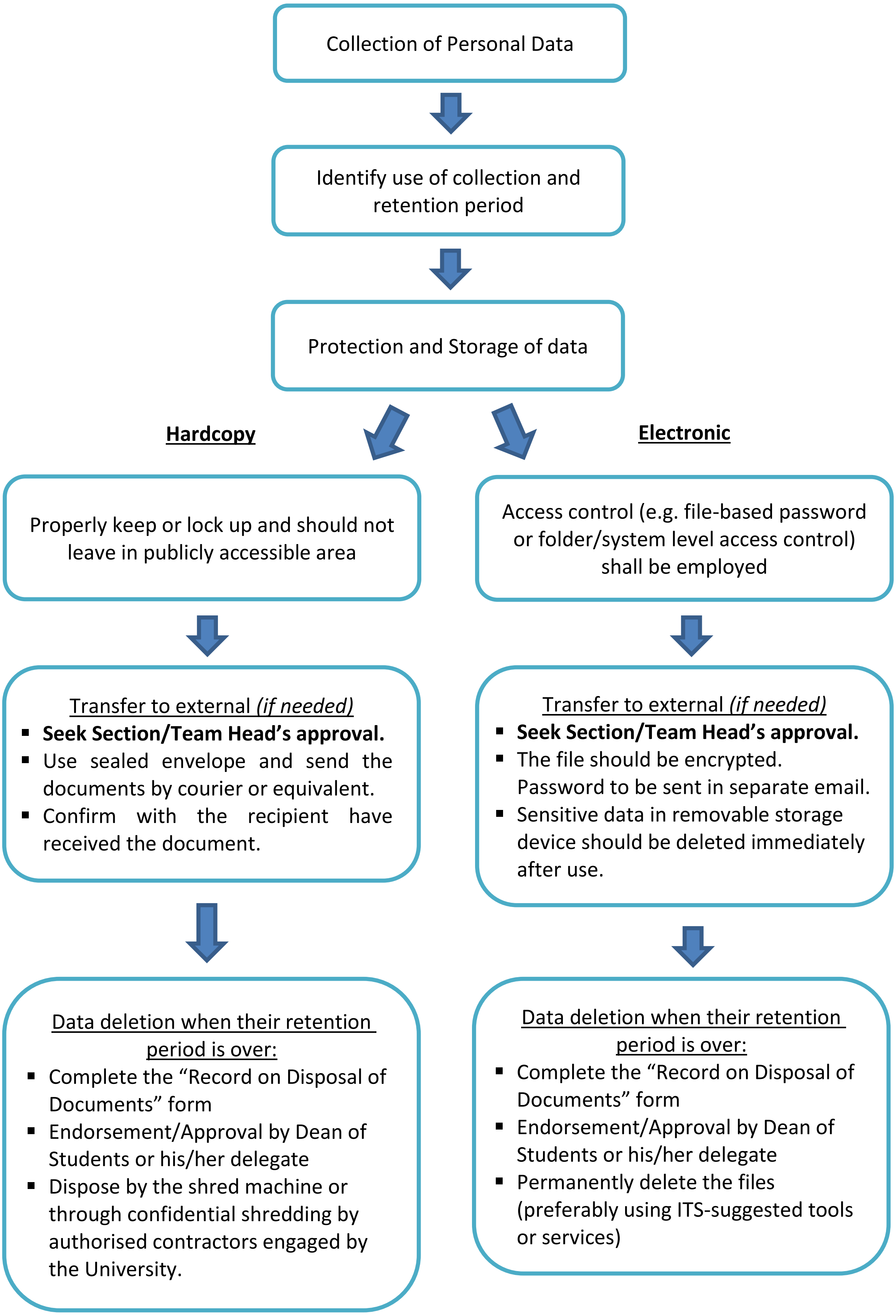
(E) <u>Data Incident</u>

15. Any suspected breach of data security of personal data, such as loss, unauthorised or accidental access, processing, erasure or use, should be reported immediately to the Section/ Team Heads and Dean of Students who should then liaise with the Academic Registry (students’ personal data) or Director of Human Resources (staff members’ personal data) immediately for seeking appropriate guidance from the Management/relevant Committee, as appropriate, for necessary and timely follow-up. Detailed guidelines and procedures for handling data incidents could refer to Part 8 “*Data Incidents*” in the “***Personal Data Compliance Manual***” which is accessible via myPolyU - “Administration” on the University Homepage.

<u>Updated in April 2021</u>

Appendix A

Flowchart of General Procedures for Personal Data Handling



Collection of Personal Data

Identify use of collection and retention period

Protection and Storage of data

Hardcopy

Properly keep or lock up and should not leave in publicly accessible area

Transfer to external *(if needed)*

- **Seek Section/Team Head's approval.**
- Use sealed envelope and send the documents by courier or equivalent.
- Confirm with the recipient have received the document.

Data deletion when their retention period is over:

- Complete the "Record on Disposal of Documents" form
- Endorsement/Approval by Dean of Students or his/her delegate
- Dispose by the shred machine or through confidential shredding by authorised contractors engaged by the University.

Electronic

Access control (e.g. file-based password or folder/system level access control) shall be employed

Transfer to external *(if needed)*

- **Seek Section/Team Head's approval.**
- The file should be encrypted. Password to be sent in separate email.
- Sensitive data in removable storage device should be deleted immediately after use.

Data deletion when their retention period is over:

- Complete the "Record on Disposal of Documents" form
- Endorsement/Approval by Dean of Students or his/her delegate
- Permanently delete the files (preferably using ITS-suggested tools or services)

Appendix B

The Hong Kong Polytechnic University
Student Affairs Office
RECORDS OF DISPOSAL OF DOCUMENTS

Section/Team : ______________________ Date of Disposal : __________________

Description of Documents to be Disposed	
Document Name	
Document Period	
Brief Description	
Document Type	Hardcopy*/Disk*/Other*(please specify)
Sheet	No. of Pages(s): ________attached*/not attached*

Method of Disposal : To be collected by PolyU assigned outside contractor for confidential recycling* / Dispose by own*

**Delete as appropriate*

Staff responsible for the disposal:

Name : ______________________ Position : ______________________

Signature : ______________________ Date : ______________________

Approved By:

Name : ______________________ Position : ______________________

Signature : ______________________ Date : ______________________

Appendix C

Retention Period of Personal Data in SAO

a) Administration Team and Student Development Unit (SDU)

Type of Document	Retention Period
Human Resources	
Former staff member	7 years after departure of staff
Appointment letter of part-time instructors	3 years
Other staff categories (e.g. Cantonese workshop instructors, Student helpers, Peer mentors, Mentors, Open talk speakers, etc.)	2 years, electronic copies ≤3 years
Salary payment record - Part-time instructors - Part-time student helpers	 3 years 2 years
Safety induction sheet of part-time instructors	3 years
Student Programmes and Activities	
Nominations/Recommendations	≤ 4 years
Registration forms/Application forms	≤ 4 years
Interview records	≤ 4 years
Attendance records	≤ 4 years
Students' activity reports / Learning journals	≤ 4 years
Psychological test/Assessment questionnaires (e.g. Personality Dimensions Test)	≤ 4 years
Undertaking form	≤ 1 year
Travel document copy	≤ 1 year
Co-curricular Achievement Transcript (CAT)	Permanent
Survey	
Proceedings, feedback forms and evaluation reports of group and EXCELL programmes	≤ 4 years
Internal assessment on student performance	≤ 4 years
Funds, Grants, Subsidies and Awards	
Application forms	≤ 4 years
Application results	≤ 4 years
Acceptance forms	≤ 4 years
Reports	≤ 4 years
Reimbursement forms	≤ 4 years
Connection with HKPUSU Student Bodies & Non-local Student Associations	
Venue booking records	≤ 2 years (hardcopy), POSS (in line with SAO central system archive schedule)
Locker allocation records	≤ 2 years
Minutes of meetings	≤ 7 years
Student Membership List	≤ 7 years
Undertaking form	≤ 2 years
Evaluation form of programmes	≤ 2 years
List of office-bearers (for CAT)	Permanent
Finance Record	
Student fee and reimbursement	≤ 4 years
Staff reimbursement	≤ 4 years
List of part-time instructors for insurance purchasing	2 years
Group Medical and Public Liability	
Application form	electronic copies ≤ 4 years
Medical claim form	1 year, electronic copies ≤ 4 years
Medical card	≤ 2 years

Type of Document	Retention Period
Immigration	
List of endorsed part-time on campus employment	1 year, electronic copies ≤ 4 years
Warning letter to students who work over 20 hours on part-time on campus	1 year, electronic copies ≤ 4 years
Bank Account Opening	
Address proof	≤ 2 years
Worldwide Emergency Assistance Service	
Claimant record	3 years

b) Careers and Placement Section (CPS)

Type of Document	Retention Period
Student Assistant Appointment	
Appointment letter	3 years
Safety induction sheet	3 years
Undertaking in respect of personal data privacy confidentiality and pirated software	3 years
Work-Integrated Education / Internships	
Application form	3 years
Offer acceptance form	3 years
Report to HAB on internship funding scheme	7 years
WIE transcript	3 years
WIE interview form	3 years
OWS & HA student charter form	7 years
Student feedback form on WIE learning experience	3 years
Attendance timesheet	3 years
Student list of buying air tickets	3 years
Application form of territory leader scheme	3 years
Unsuccessful applications	1 year
Career Advising	
CV and cover letter	3 years
Feedback form	3 years
Online resume template	3 years
Graduate Employment Survey	
Survey	1 year
Training Programme	
Online application form (POSS)	3 years
Training feedback form	3 years
Mentorship Programme	
Mentee's survey form	3 years
Mentee's self-evaluation form	3 years
PolyU Job Board	
Application form	3 years
Recruitment Talk / Senior Executive Sharing / Career Event	
Online application form (POSS)	3 years
Career Fair – Student Survey	
Online application form	3 years
General inquiry	
Online inquiry form	3 years

c) Counselling and Wellness Section (CWS)

Type of Document	Retention Period
Student Counselling	
Registration form and individual case record	3 years upon students' graduation
Online surveys (e.g. DASS, LASSI, Counselling Feedback)	3 years
Student Programmes and Activities	
Enrolment form/undertaking for activities inside and outside campus	1 year or upon completion of programme
Application form and supporting documents of subsidies of student activities	2 years
Registration forms for groups/programmes	Dispose upon completion of programme
Proceedings and evaluation reports of group programmes	1 year
Survey (e.g. DASS, LASSI, Feedback Survey)	1 year
Sports Team	
OSRS application Form & supporting documents: 1. Successful applicants 2. Unsuccessful applicants	 3 years dispose immediately
Team data 1. Office records 2. Individual Coach/Manager	 5 years 2 years (previous and current year)
Academic report	1 year
Team brief report	5 year
Team survey	3 years
Offshore training application form	1 year
Student list for buying air tickets	3 years
Insurance claim form	3 years
Application form: Assistant Coach/ Sports Team Trainer/ Outstanding Athlete/ Best Athlete	3 years
PETeam04a (Team Recruitment Fortnight Reply Form)	Dispose immediately after recruitment
PETeam08 (Team lockers allocation)	1 year
PETeam11a&b (Declaration form for Chinese & Overseas function)	Dispose immediately after trip
Academic Advising	
Consent forms, information worksheets and academic advising records	3 years upon students' graduation
Workshops/ Training/ Activities registration forms	1 year
Online survey (e.g. Evaluation forms (Advising sessions/ Workshops/ Trainings/ Activities))	3 years
Scholarships and Prizes	
Application/Nomination form for various merit-based scholarships and prizes	≤ 4 years, or within 1 year upon awardee's graduation/departure from PolyU (successful applicants) 1 year (unsuccessful applicants)
Human Resources	
Former staff member	7 years after departure of staff
Appointment letter 1. Part-time instructor 2. Student helper	 2 years 2 years

Type of Document	Retention Period
Payment Record 1. Part-time instructor 2. Student helper	 2 years 2 years
Sports Facilities	
Inquiry and complaints	3 years
Sports facilities survey	3 years
PESF04 (Advance Booking)	2 years
PESF05 (Loan of Equipment)	Dispose immediately after return
PESF06 (Banner Display)	Dispose immediately after event date
PESF07 (Equipment Loan List)	1 year
PESF10 (Guest Coach)	1 year
PESF11a (Guest Team)	1 year
PESF11b (Guest Team - PolyU Only)	1 year
PESF12 (Spectators)	Dispose immediately after event date
PESF13 (CCTV Reviewing application form)	1 year
PESF15a (Violation)	4 year
PESF15b (Violation - Abuse Use of ID)	4 year
PESF16 (Violation - Chinese)	4 year
PESF17 (Bad weather)	1 year
PESF17c (Children entering Sports Centre)	1 year
PESF18 (Re-apply for Fitness)	1 year
PESF19 (Deposit Refund)	1 year
PESF21b (Sports User Card - Application Form)	1 year
PESF22 (Sports User Card - Approved Users)	1 year
PESF23 (Sports User Card - Special Approved Users)	1 year
PESF24 (Comment Form)	3 years
PESF25 (Undertaking - Use of Fitness Room)	1 year
PESF26 (Call of Ambulance)	5 years
PESF27 (Injury Record)	3 years
PESF28 (Incident Report)	5 years
PESF30 (Checking of ID)	1-2 years
Healthy Lifestyle Programme	
Roll call list	3 years
Par & Q (PAR-Q)	Dispose upon completion of programme
Medical supporting document	5 years
Exemption of Fitness Training Course	1 year
Sports participation record form	5 years
Fitness assessment record form	5 years
SFQ of Sports Skill Training Course	3 years
Lecture Registration/Attendance Record	2 years
Lecture Sign in/out sheet	2 years
Lecture Online Assessment Submission	2 years
Wellness Centre and EIM-OC Programme	
Roll call list (short courses, workshops, talks)	1 year
Par & Q (PAR-Q)	Dispose upon completion of programme
Wellness Centre consultation data form	Dispose immediately after graduation
Medical supporting document	Dispose immediately after graduation
Ambassador Programme personal data	Dispose immediately after graduation

d) Student Resources and Support Section (SRSS)

Type of Document	Retention Period
Staff Personal Data	
Former staff member	7 years after departure of staff
Other staff categories (e.g. Student Assistants/ Helpers, Hall Tutors)	7 years
Student helpers through Work-on-campus (WOC) Scheme	3 years
Programmes and Activities	
Attendance records/proceedings/enrolment form/undertaking/evaluation for programmes and activities inside and outside campus (here we refer to non-system based enrolment)	1 year or upon completion of programme
Co-curricular Achievement Transcript (CAT) *(to be phased out in 2025)*	8 years
Student Finance	
Application form for PolyU Financial Assistance Scheme and Emergency Financial Assistance Scheme	1 year upon applicant's graduation/departure from PolyU
Application form for deferred tuition fee payment	1 year after applicant's last application
Enquiry correspondence, reimbursement application form, support letter, hard copies of applicant/result/graduate list related to various government's financial assistance schemes	7 years
Government financial assistance record	7 years
Bursary and loan recipient lists kept in individual donation file and Network Shared Drive	7 years upon termination of donation
PolyU financial assistance records kept in Scholarship and Financial Assistance Systems (SFAS)	7 years
Marking sheet of bursary application	7 years
Deferred tuition payment records	5 years
Scholarships and Prizes	
Application/Nomination form for various merit based scholarships and prizes	Successful applicants/nominees: 4 years, or within 1 year upon awardee's graduation/departure from PolyU Unsuccessful applicants/nominees: 1 year
Marking sheet of scholarship application	7 years
Scholarship recipient lists	Permanent, complete recipient lists in or before 1998/1999 academic year subject to availability
Donor Records - Scholarships and Financial Assistance	
Donor personal data, including Name, Title, Position and Contact Information of Contact Person	7 years upon termination of donation
Payment Records - Scholarships and Financial Assistance	
Recipient's bank account information	7 years upon release of payment to the recipients
Student Halls of Residence	
Resident records	
Application record	6 years
Resident record	6 years
Change hall/room application	6 years
Early withdrawal application	2 years
Overnight application	2 years
Hall access record and Visitor registration & pair up record	2 years

Type of Document	Retention Period
Disciplinary record	8 years
Participation and Contribution record	2 years
Inventory check form	2 years
Hall education (enrolment/attendance)	5 years
Survey	
Survey on the profile of new students	3 years upon completion of report
Hall resident survey	2 years
Hall education evaluation survey	2 years
Bursary recipient survey on service delivery	2 years
Financial assistance briefing participant survey	2 years
Scholarship awardee survey on service delivery	2 years
Counter satisfaction survey	2 years
Communal facilities satisfaction survey	
Ad-hoc survey (e.g. RPG Off-campus Living Condition Survey)	2 years
Minor	
Departure form for non-local minors	≤ 4 years
List of minors	≤ 4 years
Record of Amenities Centre / Communal Facilities	
Booking record of Amenities Centre and communal facilities	3 years
Attendance records	1 year
Records of warning cases and disciplinary records	7 years
Student Locker	
Locker application & user record within locker system	4 years
Application record of locker services	2 years
Records of misuse of lockers	7 years
SPECIAL ePortfolio *(phased out in 2017)*	
Student ePortfolio including profile, plan, journals, artifacts, resume and showcase	7 years
Others	
Individual case record of students with disability	9 years

Appendix D

Date :

To : <<Name of Recipient>> of Student Affairs Office

Dear Sir/Madam

Undertaking in respect of Confidentiality and Pirated Software (for Temporary Staff or Student Helper)

During your appointment with the Student Affairs Office ("SAO") of The Hong Kong Polytechnic University ("PolyU"), you may come across data/information on applicants/students/graduates and may use the workstations in the office. It is of utmost importance that:

- data/information is properly used only for the need of your work at the SAO and is kept strictly confidential. Except in circumstances arising from the normal performance of your duties, you shall not at any time during or after the end of the employment period, make use of, tamper with, divulge or communicate to any person internal or external to the University these confidential data/information.

- installation/use of pirated/illegal software at workstations in the office is strictly forbidden. By virtue of the Intellectual Property (Miscellaneous Amendments) Ordinance of Hong Kong, staff (including temporary staff) using pirated computer software on PolyU PC(s) would render the staff liable to criminal offences.

Please sign the undertaking below and return it to me as soon as possible.

Yours faithfully

<<Name of Staff>>
<<Post Title>>
Student Affairs Office

To : Student Affairs Office

I understand the confidential nature of the data/information on applicants/students/graduates and the details of the Intellectual Property (Miscellaneous Amendments) Ordinance of Hong Kong, and undertake to abide by the above requirements.

Signature : ______________________

Name : ______________________

Date : ______________________

Appendix E

Data Handling Guidelines *(extracted from "Data Governance Framework", January 2020)*

General Principles:

1. Restricted or Confidential data should be (as far as possible) stored within the University's environment/ systems.
2. Restricted or Confidential data should not be stored on removable storage devices. If storing Restricted or Confidential data on removable storage devices is inevitable, the data shall be stored in encrypted format and be limited to the minimal quantity required for conducting business and operations of the University.
3. Restricted or Confidential data should not be stored on non-University managed public cloud services (e.g. Dropbox, iCloud, Google Drive, Box, etc.). If it is inevitable, the data shall be stored in an encrypted format and be limited to the minimal quantity required for conducting business and operations of the University.
4. The circulation of Restricted, Confidential or Internal Use data should not be wider than it is required for the performance of staff's duties and should be limited to those who have authorised access.

Data Lifecycle Stage	**Format**	**Data Classification**			
		Restricted	**Confidential**	**Internal Use**	**Public**
Data Access	-	Access is restricted to authorised users based on their roles and responsibilities.			No access restriction.
Data Storage	**Hardcopy Documents**	Store in a secured location with restricted access (e.g. lockable filing cabinet, drawer or record room).		Reasonable precautions to prevent access by unauthorised staff members or third parties.	Not applicable.
	Electronic Files/ Data	Data should be stored in encrypted format wherever feasible. Procedures for data encryption are available on the *Data Protection Theme Page of IT Security Website*. Access control shall be employed to protect electronic files/ data from unauthorised access. Access controls may be implemented in form of file based password protection or folder/ system level access control. Procedures for setting access control on IT systems are available on the *Data Protection Theme Page of IT Security Website*.		Access control shall be employed to protect electronic files/ data from unauthorised access. Access controls may be implemented in form of file-based password protection or folder/ system level access control. Procedures for setting access control on IT systems are available on the *Data Protection Theme Page of IT Security Website*.	

<table>
<tr><th rowspan="2">Data Lifecycle Stage</th><th rowspan="2">Format</th><th colspan="4">Data Classification</th></tr>
<tr><th>Restricted</th><th>Confidential</th><th>Internal Use</th><th>Public</th></tr>
<tr><td rowspan="4"></td><td rowspan="4"></td><td colspan="3">**IT Equipment Containing the Data (e.g. servers, workstations, etc.)**
The IT equipment shall be hardened and applied with necessary access controls, such as user authentication to prevent unauthorised access. University managed workstations, i.e. Windows workstations joined Enterprise Domain, are hardened and safe for processing such type of data.
Procedures for hardening IT systems are available on the *Data Protection Theme Page of IT Security Website*.</td><td>The IT equipment shall be hardened. University managed workstations, i.e. Windows workstations joined Enterprise Domain, are hardened and safe for processing such type of data.
Procedures for hardening IT systems are available on the *Data Protection Theme Page of IT Security Website*.</td></tr>
<tr><td colspan="3">**Removable Storage Devices (e.g. USB flash drives, external hard drives, memory cards, etc.)**</td><td rowspan="3">Not applicable</td></tr>
<tr><td colspan="2">Data shall be stored in encrypted format on removable storage devices. The encryption may be applied on file level or device level.
Removable storage devices shall be stored in a secured location with restricted access (e.g. lockable filing cabinet, drawer or record room).
Procedures for encrypting data on removable storage devices are available on the *Data Protection Theme Page of IT Security Website*.</td><td>Data shall be stored in encrypted format on removable storage devices. The encryption may be applied on file level or device level.
Reasonable precautions to prevent access of removable storage devices by unauthorised staff members or third parties.
Procedures for encrypting data on removable storage devices are available on the *Data Protection Theme Page of IT Security Website*.</td></tr>
<tr><td colspan="3">**Mobile Devices**
Mobile devices for handling such type of data shall be protected with a password or pin and the device shall not be jailbroken or rooted.
Procedures for setting password/ pin protection on mobile devices are available in the *Data Protection Theme Page of IT Security Website*.</td></tr>
</table>

Data Lifecycle Stage	Format	Data Classification			
		Restricted	Confidential	Internal Use	Public
		Public Cloud Service Electronic files/ Data should be stored in the University managed public cloud service with proper access control implemented. If it is technically feasible, the data should be stored in encrypted format. If storing such type of data on public cloud service, which is not managed by the University, is unavoidable, the electronic files/ data shall be stored in encrypted format on these unmanaged public cloud services. Procedures for data encryption are available on the *Data Protection Theme Page of IT Security Website*.			
Data Disclosure/ Transmission	**Hardcopy Documents**	Use of sealed envelope marked as “Private & Confidential” and “To-be Opened by Addressee Only” is required.		Use of sealed envelope is required.	
		Documents delivered by internal mail shall be delivered in person to the recipients. Courier or equivalent methods shall be used for delivering external mail.	Documents delivered by internal mail should be delivered in person to the recipients. Courier or equivalent methods should be used for delivering external mail.		
	Electronic Files/ Data	Electronic files/ Data shall be encrypted in transmission over public networks, such as the Internet. Alternatively, the transmission channel shall be encrypted. Procedures for data encryption are available on the *Data Protection Theme Page of IT Security Website*.		Electronic files/ data should be transmitted in encrypted format. Alternatively, the transmission channel should be encrypted. Procedures for data encryption are available on the *Data Protection Theme Page of IT Security Website*.	

<table>
<tr><th rowspan="2">Data Lifecycle Stage</th><th rowspan="2">Format</th><th colspan="4">Data Classification</th></tr>
<tr><th>Restricted</th><th>Confidential</th><th>Internal Use</th><th>Public</th></tr>
<tr><td rowspan="5"><b>Data Deletion</b></td><td><b>Hardcopy Documents</b></td><td colspan="2">Use shred machine or use confidential shredding by authorised contractors engaged by the University (use cross-cut shredding as far as possible).</td><td>Use shredding machine or use confidential shredding by authorised contractors engaged by the University.</td><td rowspan="5"></td></tr>
<tr><td rowspan="4"><b>Electronic Files/ Data</b></td><td colspan="2">Deletion of electronic files/ data using the ITS suggested software tools is required.
Details on electronic files/ data deletion are available on the <i>Data Protection Theme Page of IT Security Website</i>.</td><td>Electronic files/ data should be deleted using the ITS suggested software tools.
Details on electronic files/ data deletion are available on the <i>Data Protection Theme Page of IT Security Website</i>.</td></tr>
<tr><td colspan="3"><b>IT Equipment Containing the Data (e.g. servers, workstations, etc.)</b>
Use ITS suggested tools/ services to dispose IT equipment containing the data.
Details on the deletion of data on IT equipment for disposal are available on the <i>Data Protection Theme Page of IT Security Website</i>.</td></tr>
<tr><td colspan="3"><b>Magnetic Media (e.g. hard disks, backup tapes, etc.)</b>
Use ITS' Secure Disposal Service to dispose magnetic media.
Details on the deletion of data on magnetic media for disposal are available on the <i>Data Protection Theme Page of IT Security Website</i>.</td></tr>
<tr><td colspan="3"><b>Flash Memory Devices (e.g. USB flash drive, memory cards, etc.)</b>
Manufacturers' built-in commands, which provide effective sanitisation that destroys the entire drive data, shall be used to securely delete the data before disposal or re-use of the devices.
Shred or disintegrate into particles that have nominal edge dimensions of 2 millimeters or less shall be applied for physical destruction of flash memory devices.</td></tr>
</table>

Data Lifecycle Stage	Format	Data Classification			
		Restricted	Confidential	Internal Use	Public
		Mobile Devices Mobile devices shall be securely formatted using the manufacturer’s built-in functions.			
		Public Cloud Service Contractual terms shall be in place to ensure all data is securely deleted, including testing data and backup copy after service engagement.			