AOU Data Protection Policy

Policy Title:	**AOU Data Protection Policy** (Data Protection Code of Practice and Data Retention Schedule)
Version No:	4.0
Approving Committee:	IT Steering Committee
Highest Approving Authority:	University Council 75, March 2022
Executive Owner:	Chief Information Officer
Policy Author/Reviewers:	IT Policy Review committee *and* CIO
Policy Implementation:	All the University Branches and AOU HQ
Policy Monitoring and Compliance:	IT Committee, IT Managers Quality Assurance and Accreditation Department/units
Next Review Date	November 2022

Introduction

The University collects and processes data about its applicants, students, employees and other individuals for many purposes such as admissions, payroll, recording of students' academic progress, monitoring attendance, graduation, promotion, and medical insurance.

There may also be occasions where the University is required to process sensitive personal data. The University is committed to protecting the privacy of Individuals' personal data by ensuring fair, responsible and transparent use of all personal information that it holds, including compliance with the safeguards of the Data Protection and GDPR on the processing of Personal identifiable Information. This Policy and its associated Code of Practice define the minimum standards with which all the University branches and departments would seek to comply in order to satisfy this commitment.

Definitions of 'personal data' and 'sensitive personal data' can be found in this policy. Further special categories of personal data in the GDPR can be found here.

Objective

The objective of this Policy is to ensure that gathering and processing of University Information including personal information of students and staff is conducted in fair and responsible manner and with full consideration for the confidentiality and privacy of each individual covered by the policy.

Responsibilities

The University takes responsibility to process personal information with due regard to the rights and freedoms of individuals. A Data Protection Coordinator/Officer should be nominated in each branch to be responsible for running the day-to-day operations related to data protection matters and encouraging good information handling practices within the University.

Each University department head must take part to ensure that the activities and processes within their departments are compliant with this Policy, and that their staff have a sufficient awareness and knowledge of relevant requirements.

1. **Staff Responsibilities:**
    1.1. All staff must comply with the requirements of this Policy and the accompanying Code of Practice.
    1.2. Staff may only process personal data to the extent to which they have been specifically authorized according to their role within the University.
    1.3. Staff must ensure that existing and new business processes, activities and IT systems are compliant with the requirements of this Policy. Changes to systems or activities entailing a change on the captured personal data shall be reviewed

for conformance with this Policy.

1.4. Academic staff are responsible for ensuring that their students are fully aware about their responsibilities under this policy with regard to coursework or research, which involves gathering or processing of personal information.

1.5. The University staff shall make sure that any information that they provide to the University in connection with their employment is accurate and up to date and that changes to these data will be communicated in a timely manner. The University shall not be held responsible for any data processing errors arising from inaccurate employee information.

1.6. The University staff acting as a custodian of any personal data shall keep such data secure, either physically; for example, in a locked filing cabinet, in a locked drawer, or electronically by means of password protection and secure storage.

1.7. Personal information is not disclosed either orally or in writing or accidentally or otherwise to any unauthorized third party.

1.8. Any deliberate breach of the University data protection policy may be considered a miss-conduct leading to disciplinary action being taken, or access to the University facilities being withdrawn, or even a legal proceeding being enacted

1.9. Lawful processing: All individual data needs to be processed in line with the lawful bases set out in the GDPR. Further information is available from https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/.

1.10. When special category data is processed, it is necessary to identify both a lawful basis for processing and a special category condition for processing in compliance with Article 9 (UK GDPR).

2. Students Responsibilities:

2.1 Students during the course of their research work have the following responsibilities:

2.1.1 to notify their tutors, for their intention to process information about identifiable individuals as part of their academic studies/research;

2.1.2 to take authorization from their tutor for processing personal information intended for their academic studies/research.

2.1.3 to comply with any regulations or requirements implemented by the University order to facilitate compliance with the University Data Protection Policy.

2.2 Students must ensure that all personal data provided to the University is accurate and up to date and that any change related to their data stored at The University side including,

but not limited to contact details are duly updated in their electronic and physical places. The University shall not be held responsible for any data processingerrors arising from inaccurate student information.

3. Data Protection Coordinator/Officer Responsibilities:

Each branch in the University shall assign a Data Protection Coordinator/Officer or Information Compliance Officer with the below responsibilities:

3.1. Liaison with the data owners and custodians/controllers to ensure proper data protection practices are followed.

3.2. Receive, evaluate and respond to inquiries and requests related to personal data access and processing, including requests from police or country legal bodies.

3.3. Ensure compliance of all parties with the policy and code of practice and respond to complaints related to policy violations and data breaches.

3.4. Provide data protection impact assessment whenever required, taking into account the nature of data to be processed and the risk of rights and freedom of processing it.

Scope

a) This Policy applies to all the University staff and students, and any other individuals authorized to access the University information.

b) This Policy applies to all recorded information, which relates to identified or identifiable individuals, irrespective of the format in which that information is held. This includes student and staff photos stored in the University databases as well as data images and videos captured by means of CCTV systems along with any information derived from the analytic part of these systems such as vehicle numbers. The policy also applies to all physical records containing personal information about students, staff including information about family members.

c) This Policy does not apply to information processed by other entities like students' unions or any entity, which is located inside the University premises but is not owned or managed by the University.

Policy Statement:

The University is committed to protecting the privacy of individuals by ensuring fair, responsible and transparent use of all personal information that it holds, including compliance with the safeguards of the Data Protection Act 1998, which defines UK law on the processing of data on identifiable living people and also comply with the Data Protection Act 2018 and the General Data

Protection Regulation ((EU) 2016/679) (GDPR).This Policy and its associated Code of Practice define the minimum standards with which all the University branches and departments would seek to comply in order to satisfy this commitment.

Definitions

The following definitions applies to this Policy and its accompanying Code of Practice:

Personal data/information	Any recorded information relating to an identifiable living individual, including expressions of opinion or intentions.
Sensitive personal data	Any personal data consisting of ethnic origin, political opinions, religious or other beliefs, membership of a trade union, physical or mental health or condition, offences or alleged offences, and proceedings for any offence or alleged offence, etc
Processing	Any action that can be done with personal data, including gathering, using, storing and disclosing it.

Generic Guiding Principles:

The policy is governed by the University Equal Opportunity policy, the University confidentiality policy and the University code of conduct policy.

a) The University does not hold any personal or professional information of staff and students more than what is necessary.

b) All data held by the University will be time marked with a time limit after which it would no more be the responsibility of the University to keep it.

c) All personal and professional data that the University holds of students or staff must be transparent with the stakeholders who should be well aware of the kind of data, the period for which it would be stored and the intended purpose of its use. The University would further take 'informed consent' from the person concerned of the use of these data.

d) The University shall fully assure the staff or students whose data it holds of its information security as per its information security policy and any accidental or incidental breach that happens by the University, it shall take full responsibility.

Data Protection Principles

a) The University will comply with the Data Protection Principles as outlined below:

1. Personal data must be processed fairly and lawfully, and only when specified conditions are satisfied;

2. The individual consent should be taken on the processing of their personal

information.

3. Personal data must be processed for specified purposes only;
4. Personal data must be adequate, relevant and not excessive for the purpose it is obtained for;
5. Personal data must be accurate and up-to-date;
6. Personal data must not be kept for longer than necessary;
7. Personal data must be processed in accordance with the rights of individuals;
8. Personal data must be kept appropriately secure;

b) The accompanying Code of Practice informs the practical application of these Principles to the University activities.

Rights of Individuals

a) The University will comply with the rights given to individuals under the Data Protection Policy as highlighted below:

1. Individuals have a right to access their personal data stored by the University and to request a copy of it.
2. Individuals have the right to request deletion of their personal data if they are no longer required by the University.
3. Individuals have the right to request moving their data to another organization with proper procedure and subject to applicable fees.
4. Individuals can ask the University to provide their data in a more portable format, e.g. csv file whenever necessary and applicable.
5. Individuals have the right to withdraw their consent, which the University has processed their personal information based on it.
6. Individuals can ask the University to limit the processing of their personal data to certain purposes.
7. Individuals can ask the University to cease processing their personal information for a particular purpose, which is likely to cause them substantial and unwarranted damage or distress.
8. Individuals can ask the University to cease processing their personal information for direct marketing purposes.
9. Individuals can seek compensation if they have suffered damage or distress arising from a breach of their privacy.

10. Individuals can ask for incorrect or misleading data to be amended.
11. Individuals may object for processing their personal data for scientific or historic research or statistical purposes, unless the processing is necessary for the performance of a task carried out for reasons of legitimate interest to the University or Public.
12. Individuals have the right to obtain confirmation as to whether their personal information are being processed, and, where that is the case, to have access to the following information:
    - the purposes of processing;
    - the categories of personal data concerned;
    - the recipients to whom the personal data have been or will be disclosed;
    - the period for which the personal data will be stored;
    - the existence of the right to request the erasure of personal data or restriction of processing of personal data or to object to such processing;
13. Individuals have the right to request the communication form through which the requested data shall be provided by the University.
14. Individuals have the right to object to the Data Protection Coordinator/Officer for the conceived misuse of their personal information.

b) Students will be entitled to get information about their marks for both coursework and examinations as part of their tutorial support in line with this policy relating to the release of data. However, the University may withhold certificates, accreditation or references in the event that the full course fees have not been paid.

Data Protection Procedure: Data Access Requests

a) Any individual is entitled to ask for copies of information relating to them, which are held by the University.

b) The University employees send their particular data requests to the HR departments in their respective branches. The University uses templates to ease the data request process. Requestors are encouraged to use the forms from the HR share folder to ensure that sufficient information is provided to enable the University to properly and efficiently process their requests.

c) The University students send their written data requests to the registration department in their respective branch accompanied with the applicable data request fees.

d) Any other internal or external parties must address their requests to the Data Protection Coordinator/Officer.

Internal Processing of a Data Access Request

a) The data processing department will liaise with the Data Protection Coordinator/Officer and

relevant departments to collect all information relevant to the request. The processing will include checking for compliance with Data Protection Policy.

b) Where information cannot be provided without disclosing information relating to another identifiable individual, it may be necessary to withhold or anonymize that information in accordance with Data Protection requirements.

c) Members of staff who have been asked to supply information in conjunction with a Data Access Request should note that: -

   1. Any withholding or releasing of information, which should not be disclosed, will be done prior to disclosure.
   2. The identity of a Data Access Requestor should be considered as confidential information and only disclosed to other individuals where strictly necessary.

Responding to a Data Access Request

a) In response to a Data Access Request, requestors will be provided with the following information as appropriate to each request:

   1. Confirmation that the University processes the subject's personal data;
   2. The personal data of which that individual is the data subject, the purposes for which that data is processed, any information available as to the source of that data, and the categories of recipient to whom that data may be disclosed;
   3. Copies of information constituting personal data of which that individual is the data subject.
   4. Where necessary, the logic involved in any data processing, which evaluates matters relating to the data subject, where such processing is automated and constitutes the sole basis for any decision, which significantly affects the data subject.

b) The disclosure of personal data in response to a Data Access Request will be made either in paper form, electronic form or made viewable in person according to the discretion of the requestor.

Transparent Communication of Data Access Responses

a) Appropriate measures are taken to provide information related to processing personal data in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

b) The University shall not refuse to act on the request of the Individuals for exercising his or her rights mentioned under 'The rights of Individual' article, nor cause undue delay to fulfill the request within a reasonable period of time.

c) The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. If the requestor is the data subject, then information may also be provided orally if the identity of the data subject has been verified.

d) Where the Individual makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the Individual.

e) If no action is taken on the request of the Individual, the individual shall be informed without delay the reasons of not taking action and on the possibility of lodging a complaint to the Data Protection Coordinator/Officer and seeking a remedy.

New or additional processing

a) Employees of the University must not do any of the following, without the proper authorization and approval from their head of department:

1. Develop, purchase or subscribe to a new computer system/platform for processing personal data
2. Use an existing computer system to process personal data for a new purpose
3. Create a new electronic or paper filing system, including spreadsheets' containing personal data
4. Use an existing electronic or paper filing system, including spreadsheets' containing personal data for a new purpose.
5. All new software and systems must be approved and procured through IT Services, who will check for technical, security and data protection compliance. In certain circumstances (for example, the introduction of new technologies, systems or software) a Data Protection Impact Assessment (DPIA) maybe required. ICO guidance on Data Protection Impact Assessments can be found here.

Research

The DPA 2018 and GDPR include specific exemptions for the processing of personal data that is necessary for archiving purposes, scientific or historical research purposes or statistical purposes. For further information, see paragraph 620 of the **Explanatory Notes** to the DPA 2018.

Retention of personal data

a) The GDPR sets out the principle that personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

b) Personal data may be stored for longer periods when the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

c) Personal data may be stored for longer periods when the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

d) The University Data Retention Schedule for various information categories is provided in the Code of Practice attached to this policy.

Data Security

Appropriate measures must be in place to ensure appropriate level of protection of Personal data, considering the potential cyber-crimes and impacts of processing systems on the safety and freedom of information. This includes:

a) Securing personal data against accidental or illegal destruction, loss, change, and unauthorized disclosure during store, access, send or processing of personal data.
b) Encryption of Personal data according to the sensitivity of the data as aligned by the University data classification policy and Information Security Policy.
c) Guarding against the risks of intercepting correspondences with personal data during communication or errors in transmission. Recipient address in such correspondences must be carefully selected to avoid disclosing sensitive information to unintended parties. If information is highly sensitive, email attachments can be password protected and/or encrypted.
d) Ensuring confidentiality, integrity, availability and resiliency of the systems processing personal data.
e) Regular testing, assessment, audit and evaluation of the effectiveness of the technical and organizational measures for ensuring the security of data processing.
f) If personal information must be stored at third-party/service provider, or processed off-site then precautions must be taken for the security measures at the service provider/off-site to ensure the confidentiality of the Personal Information.
g) Keeping records of all requests related to Personal data access and processing including but not limited to:

- Requestor details.
- Purpose and if necessary the legal basis for which the processing request of data is made and how the data will be used.
- Category of data being requested.
- Classification of data being requested.
- Data fields requested.
- How the data will be provided.
- Who will have access to the requested data.
- Where and how will the data be stored if it will be sent out of its electronic storage.
- How long the access/processing is needed.
- Procedure for disposing the transferred data once it is no longer needed.

Data Breaches

a) Any unauthorized or accidental disclosure of personal data should be considered a data breach. If any staff member believes a data breach has occurred, they need to report it to the Data Protection Coordinator/Officer or Information Compliance Officer for advice and guidance as

soon as possible. They will work together with the aim of minimizing the effects of the breach. All data breaches will be logged internally.

b) If the breach is judged to be serious, it will need to be reported to the Information Commissioner's Office within 72 hours. It is therefore essential that all breaches are reported immediately.

Complaints relating to Access Requests

a) Any University employee who is dissatisfied with the way in which the University has handled a 'Data Access Request' should put their concerns in writing to the Data Protection Coordinator/Officer in the corresponding branch.

b) Any student who is dissatisfied with the way in which the University has handled a Data Access Request should put their concerns in writing to the student affairs department in the corresponding branch. Escalations can also be made to the Data Protection Coordinator/Officer if no remedy is made to the student complaints.

References:

In preparing this Policy, the international relevant literature on data protection and data protection acts has been consulted including the following references:

1. https://www.open.ac.uk/about/main/strategy-and-policies/policies-and-statements/website-privacy-ou
2. https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/security/ .
3. ICO: Information Commissioner's Office, http://www.ico.gov.uk/
4. https://www.citra.gov.kw/sites/en/LegalReferences/Data_Privacy_Protection_Regulation.pdf
5. https://gdpr-info.eu/

Revision History

Version Control			
Version	Author	Date	Changes
1.0	IT Policy Review committee 2011	June 2011	Approved VC, 2011
2.0	IT Policy Review committee 2016	Aug 2016	Approved VC, 2011UC#57, 2016
3.0	IT Policy Review committee 2017	July 2017	Updated and modified version
4.0	IT Policy Review committee 2021	Nov 2021	Updated and added some of the compliant point of GDPR

Data Protection Code of Practice

Contents

Introduction

This Code of Practice accompanies the University's Data Protection Policy and puts into practical terms the requirements that must be followed in order to fulfil the objectives of the Data Protection Policy.

1. Data Processing Statements

The University publishes Data Processing notice/privacy Statements, which provide general information about how The University processes the personal information of its students and employees. The staff statement is published on the HR share folder and distributed to new staff during induction. The student statement is published on the Student Online Services portal as well as in the student handbook.

2. General requirements when processing personal information:

Personal information must be processed at all times according to the following requirements:

- Being open and transparent about how personal information is used.
- Handling personal information only in the ways that would be reasonably expected by the individuals concerned and avoid processing personal

information in ways, which would have unjustified adverse effects on the individuals concerned.

- Only processing personal information where it is necessary for legitimate purposes.
- Not commit unlawful acts with personal information.

2.1. Personal information may only be processed when one of the following criteria are met:

- The individual has given their consent on the processing of their personal information.
- The processing is necessary to comply with a legal obligation.
- The processing is necessary for legitimate interests pursued by the University, and does not prejudice the rights or interests of the individual.

2.2. Personal information processed for any purpose must be adequate, relevant, not excessive and is not used for further processing that has incompatible intent.

2.3. Reasonable measures should be taken to ensure that personal information is accurate and up-to-date.

2.4. Personal information must be kept appropriately secure at all times, with precautions commensurate with its confidentiality and sensitivity. Particular care must be taken when processing personal information at home or at another off-site location, which can expose personal data to loss, theft or damage.

2.5. When processing information about individuals, a distinction is made between 'professional' and 'private' information. Information related to an individual's professional job like contact details or job title, will be subject to less stringent privacy considerations than information of a more private nature like home contact details.

2.6. In cases where personal information is processed by another organization on behalf of the University, the Legal department in the respective University branch must be consulted to ensure legislative compliance.

2.7. Personal data related to racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a person or revealing data concerning to health condition, sexual orientation shall be prohibited.

3. General requirements when processing sensitive personal information

3.1. Particular care must be taken with the gathering, use, storage, disclosure and destruction of sensitive information.

3.2. Sensitive Personal information must be processed fairly at all times. This requirement includes:

- being open and transparent about how personal information is used;
- handling sensitive personal information only in a reasonable way as expected by the individuals concerned;
- avoiding processing sensitive personal information in ways which are unlawful or would have unjustified adverse effects on the individuals concerned;
- processing sensitive personal information only when it is necessary for legitimate purposes;

3.3. Sensitive personal data may only be processed when one of the below criteria is met:

- the individual has given their explicit consent;
- the processing is necessary for a legal obligation related to employee contractual issues or students enrollment issues.
- the processing is needed to fulfill an obligation requested by police or country legal bodies .
- the processing relates to racial or ethnic origins for the sole purpose of check for equal opportunities, provided that it is carried out with appropriate safeguards for the rights of the individuals.
- the processing is necessary for legitimate interests by the University.

4. Gathering Personal Information

4.1. Only the minimum necessary information should be gathered to satisfy the specific purpose for which the information was gathered for.

4.2. When data is gathered from individuals, the information below must be made clear to them:

- the identity of the Data Protection Coordinator/Officer (i.e. the University, not the particular departments);
- the purpose for which the data will be processed;

4.3. This is achieved in the form of a Privacy Notice/ Fair Processing Notice and is applied when personal information is gathered from individuals, whether via paper forms, online forms, verbal way, or other means, and seeks to ensure that any subsequent processing can be “reasonably expected” by the individual.

4.4. Where a Privacy Notice is supplied to an individual, a record of that Notice should be kept for as long as the personal information is retained.

4.5. Where practicable, a record should be kept of the circumstances in which the personal information was obtained (e.g. when and how).

5. Storing and Disposing of Personal Information

5.1. Personal information must always be kept appropriately secure against damage or unauthorized access, amendment or deletion, with precautions appropriate to its confidentiality and sensitivity.

5.2. Electronic and physical files should have appropriate access restrictions in place so that only authorized individuals can gain access to them.

5.3. Personal information must not be stored on portable media devices (e.g. memory sticks, DVDs) unless this is essential to serve a particular legitimate short-term purpose. Such devices are particularly susceptible to damage, loss or theft.

5.4. Where personal information needs to be stored on a portable media device, and is particularly sensitive data fined in the Data Protection Policy, or the loss of that information would otherwise cause damage or distress to an individual, that information should be encrypted using facilities provided by the University.

5.5. Personal information must not be kept for longer than is necessary. Be particularly aware of electronic databases building up indefinitely. The University's Retention Schedule in this policy provides guides the retention requirements for records relating to various activities.

5.6. Personal information must be disposed of in a manner appropriate to its sensitivity. Records awaiting destruction must continue to be stored securely.

5.7. The Data Destruction and Sanitization Policy guides the manner by which the Personal data is disposed from paper documents and electronic storage media.

6. Disclosing and Sharing Personal Information

6.1. Personal information may not be disclosed to any third party without the consent of the individual concerned, or authorization from either Registration department or Human Resources as appropriate with close coordination with the University Data Protection Coordinator/Officer.

6.2. Personal information can be shared within the University provided that such sharing is reasonable, necessary, not excessive, and is not incompatible with the original purpose for gathering the data.

6.3. When disclosing or discussing information about individuals, reasonable steps should be taken to verify the identity of the recipient, especially in telephone conversations or email correspondence.

7. Unauthorized Processing

Registration Department must be informed at the earliest opportunity of any situation which involves, or which may involve or give rise to, the unauthorized access, disclosure,

and/or processing of personal information.

8. Complaints

Any complaints, concerns or dissatisfaction regarding the University's processing of personal information must be brought to the attention of the Data Protection Coordinator/Officer or Information Compliance Officer or legal department where appropriate.

9. Contacts and Further Information

Queries relating to the processing of personal information or the Data Protection Policy should be referred to the University Data Protection Coordinator/Officer or Data Compliance Officer.

Arab Open University Data Retention Schedule.

JOB APPLICANT'S INFORMATION

Unsolicited applications (or after deadline) and the University's reply	3 years
Information on e-recruitment	3 years
Applicant information and interview/selection notes	6 month

STAFF INFORMATION

Staff Name, age, date of birth, address, telephone and email contact details	10 years until after termination
Offer letter, contract of employment and any contract amendments	10years until after termination
Documents confirming policies and procedures have been read and understood	10 years until after termination
Relocation Agreement	10years until after termination
Loan and Reimbursement Agreement	10 years until after termination
References (from a third party)	5 years until after termination
References (provided to a third party, such as potential employer, voluntary organization, etc.)	5 years until after termination
Requirements regarding job specific training and Continuing Professional Development together with the training provided to meet these requirements	5 years until after termination
Records documenting job-specific statutory/regulatory training requirements and the training provided to meet these requirements	5 years until after termination

Details of qualifications, skills, experience and employment history, including start and end dates with previous organisations (normally gained from application form/CV)	5 years until after termination
Application form and CV	5 years until after termination
Job Description	5 years until after termination
Record of annual leave and (if applicable) permissions	6 years until after termination
Bank account details	30 years until after termination
Loan and Reimbursement Agreement	6 years until after termination
Salary records, including overtime, allowances, and other payments	30 years until after termination
Information on end of service benefits	6 years until after termination
Qualifications and professional memberships applicable to the role	5 years until after termination
Driving license or any other driving qualification applicable to the role	5 years until after termination
Probation records	5 years until after termination
Induction records	5 years until after termination
Annual appraisals	5 years until after termination
Secondment agreement/Secondment review information	5 years until after termination
Secondment Review information	5 years until after termination
Training records (correspondence relating to training and development needs, training requests and attendance records)	5 years until after termination
Health and Safety training records	5 years until after termination
Financially supported training scheme records, e.g. staff scholarship scheme	5 years until after termination
Unauthorized Leave	10 years until after termination
Information relating to disciplinary, grievance and/or capability proceedings	30 years until after termination
Disciplinary sanctions issued in line with relevant policy	30 years until after termination
Information relating to a potential or actual redundancy	1 year until after termination
Correspondence to and from you concerning your employment	5 years until after termination

Last day of employment, records relating to ending of employment and reason for leaving	5 years until after termination
Next of kin Emergency Contact details	5 year until after termination
Marriage or civil status, disability status, and maternity status,	5 years until after termination
Criminal conviction and offence information	50 years until after termination
Maternity, Adoption, Surrogacy, Paternity, Parental, Shared Parental, Parental, Time Off for Dependents Leave, Special Leave, Sabbatical Leave	5 years until after termination
Pregnancy, new mother and breastfeeding risk assessments	5 year until after termination
Sick Absence paperwork	5 years until after termination
Sick Leave and pay records	5 years until after termination
Medical or health information	5 years until after termination
Occupational health records	5 years until after termination
Restricted i.e. sensitive documents that it has been agreed are not for general viewing	6 years until after termination
Records documenting major injuries to staff member arising from accident in the workplace	5 years until after termination
CCTV records	5 years until after termination
Information on relationships (as per the Policy on Disclosure of Intimate Relationships)	5 years until after termination

STUDENT INFORMATION

Admission & Registration

Unsolicited request for application	6 months
Admission and registration fee details	12 + 10years
Student submitted testimonials (marks cards, reference letter etc)	12 + 10years
Confirmation of acceptance for studies	12 + 10 years
E-Mail/Letter to student against rejection	1 year
Correspondence with prospective students which includes specific admission guidance	1 year
Details of people who have enquired about courses or programmers	1 year
Registered students' personal record (full	permanent

name, date of birth, gender, nationality, programme of study, award date and classification)	
Email/letter inviting current students to participate in recruitment events, e.g. student led tours on campus, events and student "shadowing".	1 year
A list of current students working as unpaid volunteers at recruitment events, including Widening Participation events	2 years
Bank account details if any provided by the student	20 years
Relevant documentation, including postgraduate application form, record of an interview with student and identity of supervisor	20 years

Teaching and Learning

Records of progress meetings and correspondence with students	12 + 6 years
Locally held student contact details, eg subject area-specific enrolment form collected from students enrolled on course	permanent
Documentation (including notes of meetings, emails and outcome letter) relating to unsatisfactory progress and measures taken in response to this	12 + 6 years
Student timetables	12 + 6 years
Marking non-assessed coursework - Annotated non-assessed coursework	12 + 6 years
Marking non-assessed coursework -Staff's record of informal evaluations	12 + 6 years
Attendance register	2 years
Record of credit hours completed	12 + 120 years
Mailing list for students enrolled on course	12 + 6 years
Record informing Student Systems of student transfer to different program	12 +20 years
Sample of assessed work for quality assurance purposes	12 + 6 years

Assessed work where the student has lodged an appeal in connection with the assessment	12 + 6 years
Assessed research projects, dissertations or equivalent where the student has not appealed	12 + 6 years
Other assessed coursework and exam scripts where the student has not appealed	12 + 6 years
Mark sheets from all assessed work	12 + 100 years
Record (eg spreadsheet or database) of the individual marks awarded for pieces of work assessed for a single course	12 + 100 years
For undergraduate courses with a graduation date record of total mark and grade awarded for each course studied	12 + 100 years
For certificate and diploma students, record of total mark and grade awarded for each course studied, plus record of qualification for diploma or certificate	12 + 100 years
Correspondence and decision as to whether student can resubmit coursework	12 + 6 years
Record of which scripts have been sent to which examiner and which external examiner	12 + 6 years
External examiners' reports	12 + 6 years
Entry in spreadsheets/database confirming mark has been recorded accurately	12 + 100 years
Record of marks, grades and courses completed for undergraduates who did not complete their degree	12 + 100 years
Record of concessions to which a student is entitled and associated correspondence	12 + 6 years
Papers relevant to special circumstances or potential for special circumstances for individual students' e.g; doctor's notes, correspondence with student about difficulties.	12 + 100 years
Minutes and papers of Special Circumstances Committee	12 + 6 years
Minutes and papers of Board of Examiners meetings	12 + 6 years
Record of which students have submitted coursework for assessment	12 + 100 years
Plagiarism record sheet	12 + 6 years

Record of any concessions to which a student is entitled	12 + 6 years
Minutes of Assessment Board meetings	12 + 100 years
Produced early during the first year, a written plan for the student's research goals, including specific milestones and deadlines (revised periodically)	12 + 6 years
Correspondence and other documentation concerning research and progress meetings	12 + 6 years
Documentation of handling of appeal against outcome of research degree final assessment, including letter from student and letter of outcome.	12 + 6 years
Documentation of handling of complaints	12 + 6 years
Correspondence concerning decision to withdraw	12 + 6 years
Notification to Student Systems of permanent withdrawal of student	12 + 6 years
Application, correspondence, supporting documentation, minutes relating to request for extension/suspension and outcome	20years
Confirmation that student has met all regulations for degree award and listing degree classification	Permanent
Undelivered graduation certificates	permanent
List of graduates	permanent
Letter from accrediting body confirming graduate's accreditation	50 years
Completed course evaluation questionnaires	12 + 6 years
Other student feedback	12 + 6 years
Career guidance/ counselling	12 + 6 years
Student information form and confidentiality agreement	12 + 6 years
Entry on database of student's presenting problems and use of service	15 years
Counselling records, partially anonymized by codes	12 + 6 years
Pastoral-themed correspondence between students and Director of Studies/supervisors/lecturers/tutors/course organizers/ potentially any staff-member anywhere in the University	12 + 6 years
Letters to academic staff involved with the student	12 + 6 years

student request for a reference and letter of reference	12 + 6 years
Information on student disability	12 + 6 years
Information from schools, institutions, doctors, access centers, educational psychologists or other professionals who have assessed this student	12 + 6 years
Documents arranging personal assistance via Disabled Student's Allowance: record of which students successful and unsuccessful	12 + 6 years
Creating user names, login passwords and e-mail accounts. Entry in student database recording personal e-mail address	12 + 6 years

INSTITUTIONAL DOCUMENTS

Entry of University database	Permanent
Auditable log of activity within the management service	Permanent
Letter of contract with the partnering body or any other similar institution.	Permanent
Institutional Self Evaluation Document	Permanent
Branch self-evaluation documents	Permanent
Audit visits by accreditation validating bodies	Permanent
Correspondence between The University and local/OU towards institutional approval an programme validation	Permanent
Honors and awards to The University	Permanent
Correspondence with Ministry of Higher Education in Branch Country	Permanent
Approval letters from Ministry of Higher Education and other local accrediting bodies.	Permanent
The University representation on international platform invitations, acceptance and subsequent proceedings	Permanent
Correspondence related to appointment of senior management	Permanent

Correspondence related to termination ofemployment	Permanent
Institutional policies	Permanent
Approval of amendment to policies	Permanent

Financial and Administrative documents Student's fee status and funding arrangements (Including back history).	50 years
Financial documents consisting of staff salaries/ research grants/professional development costs etc.	50 years
Fees status and funding arrangements in University database	50 years
Tuition fee record	50 years
Record informing Fees Office of fees change ensuing from student transfer to different program	15 years
Update to Finance of fees changes	50 years
Details of student fees sponsor	25 years
Direct debit mandate & payment information	50 years
Record of payment requested	25 years
Record of payments received from student or sponsor	50 years
Record of failure to collect payment, correspondence with student and other parties about recovering the debt	50 years
Record of bad debt written off	50 years
Correspondence with student, completed application form, evidence of financial position, outcome letter	25 years
Minutes of financial aid decision-making committee	50 years
Annual spreadsheet of allocated funds	50 years
Letter to Fees Office doing one of the following: if internal award, instructing them to pay fees with University account; if external award, stating the student will be receiving funding from the external source.	50 years

Letter to the donor, listing the recipient(s) for the year (not always part of the process)	25 years
Reports of the project funded	25 years
All records generated by the appeals process (grant/scholarship/prize), including request for appeal, minutes and papers for whichever committee conducted the appeal process and outcome letter	25 years
Information from Student Loan Institutions detailing their records of what program and what year students are in	25 years