Data Protection Policy

Version 4

Arab Open University

Data Protection Policy

Policy Title:	Data Protection Policy
Version Number	4
Approving Body	University Council # 75, March 2022
Executive Owner:	Vice President Planning and Development Affairs
Policy Reviewer & Approval :	Information Technology (IT) Committee
Policy Implementation:	Vice President Planning and Development Affairs Office
Policy Monitoring and Compliance:	Vice President Planning and Development Affairs Office
Next Review Date	2025

Note: *A policy can be reviewed before the designated review date, should there be a need to.*

AOU's Data Protection Policy & Procedures

Introduction

AOU 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.

AOU 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 compliance to the Branch country regulations. This Policy and its associated Code of Practice define the minimum standards with which all AOU branches and departments would seek to comply in order to satisfy this commitment.

1. Scope

1.1 This Policy applies to all AOU staff and students, and any other individual authorized to access AOU information.

1.2 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 photos stored in student information system 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.

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

2. Objectives

The purpose of this Policy is to ensure that personal information gathered and processed by AOU is done fairly, responsibly and transparently, and with full consideration for the confidentiality and privacy of each individual covered by the policy.

3. Generic Guiding Principles

3.1 The AOU data retention policy is governed by the AOU Equal Opportunities policy, AOU Confidentiality Policy and the AOU Code of Conduct Policy.

3.2 The Arab Open University does not hold any personal or professional information of staff and students than what is necessary.

3.3 All data held by AOU will be time marked with a time limit after which it would no more be the responsibility of AOU to hold it.

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

3.5 AOU shall fully assure the staff or students whose data it holds of data security as per its confidentiality policy and any accidental or incidental breach that happens by AOU, it shall take complete responsibility.

4. 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 racial or ethnic origin, political opinions, religious or other beliefs, membership of a trade union, physical or mental health or condition, sexual life, 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.

5. Responsibilities

AOU takes responsibility to process personal information with due regard to the rights and freedoms of individuals. A Data Protection Coordinator 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 AOU.

Each AOU 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.

5.1. Staff Responsibilities

5.1.1. All staff must comply with the requirements of this Policy and the accompanying Code of Practice.

5.1.2. Staff may only process personal data to the extent to which they have been specifically authorized according to their role within AOU.

5.1.3. 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.

5.1.4. 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.

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

5.1.6. AOU 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.

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

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

5.2. Students Responsibilities

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

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

2. to take authorization from their tutor for processing personal information intended for their academic studies/research.
3. to comply with any regulations or requirements implemented by AOU order to facilitate compliance with AOU Data Protection Policy.

5.2.2. Students must ensure that all personal data provided to AOU is accurate and up to date and that any change related to their data stored at AOU side including, but not limited to contact details are duly updated in their electronic and physical places. AOU shall not be held responsible for any data processing errors arising from inaccurate student information.

6. Data Protection Principles

6.1. AOU will comply with the Data Protection Principles as outlined by the Data Protection Act as follows:

1. Personal data must be processed fairly and lawfully, and only when specified conditions are satisfied;
2. Personal data must be processed for specified purposes only;
3. Personal data must be adequate, relevant and not excessive for the purpose;
4. Personal data must be accurate and, where necessary, up-to-date;
5. Personal data must not be kept for longer than necessary;
6. Personal data must be processed in accordance with the rights of individuals;
7. Personal data must be kept appropriately secure;

6.2. The accompanying Code of Practice informs the practical application of these Principles to AOU activities.

7. Rights of Individuals

7.1. AOU will comply with the rights given to individuals under the Data Protection Act, Specifically, this policy states that:

1. Individuals have a right to access their personal data held by AOU.
2. Individuals can ask AOU to cease processing their personal information for a particular purpose, which is likely to cause them substantial and unwarranted damage or distress.
3. Individuals can ask AOU to cease processing their personal information for direct marketing purposes.
4. Individuals can seek compensation if they have suffered damage or distress arising from a breach of their privacy.
5. Individuals can ask for incorrect or misleading data to be amended.

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

8. Data Protection Procedure: Data Access Requests

8.1. Any individual is entitled to ask for copies of information relating to them, which are held by AOU.

8.2. AOU employees send their particular data requests to the HR departments in their respective branches. AOU 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.

8.3. AOU students send their written data requests to the registration department in their respective branch accompanied with the applicable data request fees.

9. Internal Processing of a Data Access Request

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

9.2. 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.

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

a. Any withholding or releasing of information, which should not be disclosed, will be done prior to disclosure.

b. The identity of a Data Access Requestor should be considered as confidential information and only disclosed to other individuals where strictly necessary.

10. Responding to a Data Access Request

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

a. Confirmation that AOU processes the subject's personal data;

b. 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 classes of recipient to whom that data may be disclosed;

c. Copies of information constituting personal data of which that individual is the data subject.

d. 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.

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

11. Complaints relating to Subject Access Requests

11.1. Any AOU employee who is dissatisfied with the way in which AOU has handled a 'Data Access Request' should put their concerns in writing to the Legal department in the corresponding branch.

11.2. Any student who is dissatisfied with the way in which AOU has handled a Data Access Request should put their concerns in writing to the student affairs department in the corresponding branch.

References:

1. Freedom of Information Policy - Teesside University.
2. Data Protection Policy - University of Birmingham.
3. Wikipedia, Data Protection Act 1998, http://en.wikipedia.org/wiki/Data_Protection_Act 1998.
4. http://www.legislation.gov.uk/ukpga/1998/29/contents.
5. ICO: Information Commissioner's Office, http://www.ico.gov.uk/
6. International Data Protection Policy, www.visteon.com/utils/media/privacy.pdf
7. Data Protection Policy, University of Andrews, 2003.
8. Said Almadhoun, fellow, Open Society Justice Initiative Status of Freedom of Information Legislation in the Arab World, February 6, 2010

Data Protection Code of Practice

Contents

Introduction

This Code of Practice accompanies the AOU'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

AOU publishes Data Processing notice/privacy Statements, which provide general information about how AOU 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 fair 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 AOU, 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 AOU, the Legal department in the respective AOU branch must be consulted to ensure legislative compliance.

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 data may only be processed when one of the following criteria is met:

- the individual has given their explicit consent;
- the processing is necessary for a legal obligation in connection with contractual issues with employees or enrollment of students.
- the processing relates to racial or ethnic origins, check for equal opportunities, etc, provided that it is carried out with appropriate safeguards for the rights of the individuals.

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 Controller (i.e. AOU, 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 (appendix 1).

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 AOU's Record Retention Policy 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.

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.

6.2. Personal information can be shared within AOU 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 AOU's processing of personal information must be brought to the attention of the Assistant Director (Legal Services).

9. Contacts and Further Information

Queries relating to the processing of personal information or the Data Protection Policy should be referred either to branch Registration Department or Human Resources as appropriate.