Kingdom of Saudi Arabia

Arab Open University

Data Management Policy

Reference No.	SS-P2
Version	1/2019
Approval	UC ../../20
Date	../../ 2019

Contents

Article (1): Title

The present policy shall be called "Data Management Policy at Arab Open University" and shall include within its articles the "Maintain Provision Data".

Article (2): Definitions

The following words and expressions shall have the meanings specified hereunder unless the context indicates otherwise:

University	The Arab Open University (AOU)
Rector	The Rector of the University
Personal Data	Data in any format that relates to any AOU stakeholder who can be identified from that data or other information held by the university, its partners, agents and other third parties.
Records	Information, in any format, which must be retained and represents academic or non-academic actions or decisions related to the services and interactions between AOU and the stakeholders.
Student File	The personal data and the records which have been filed together in electronic or paper format.

Article (3): Student's Record Items

Records about the applicants, current and former students across all campuses and modes of study are maintained secured and protected from unauthorized access and the records are auditable standards for the management of records relating to applicants, enrolled and former students and the university ensures their confidentiality, integrity and availability to authorized users for as long as required by the University. These records include the following items:

- Enrolment and module selection
- Examined and assessment.
- Attendance and attainment.
- Progression and transfers
- Withdrawals and suspensions
- Student schedule, grades, or GPA
- Total number of credits completed or anticipated graduation date
- Non-class room academic and non-academic activities.
- Appeals and complaints
- Received advice and support services.
- Fees and payments

- Disciplinary proceedings

Article (4): Personal Data Items

The personal data requested by the university for the purpose of the admission services and other related services offered for the all applicants, students, and alumni are maintained secured and protected from unauthorized access and the records are auditable. The data include the following components:

- Address, date and place of birth and marital status.
- Phone number.
- Personal photo.
- Nationality, race and religion.
- Family information.
- financial aid or billing information.
- Medical condition and history

Article (5): Principles of Data and Records Management

Data in AOU included all records, personal data and students files, and the data is managed according to a set of principles that must guide all data management procedures, these principles are:

1. The university, rather than any individual or faculty or administrative department, owns all data, included in the records, personal data and student files.
2. Data, regards its type and source, must have a defined custodian in a specific faculty/department, who has overall responsibility for the accuracy, integrity, and security of those data.
3. Data must be protected from unauthorized access and modification.
4. Data should be defined consistently across the University.
5. Data should be updated periodically and the consistency of the data should be maintained at all times, and the student records should always be accurate, up to date and comprehensive for each applicant, enrolled and former student.
6. Student file shall be maintained an accurate audit trail of the service provided to each student and applicant as evidence of fair and consistent practice.
7. Records should be maintained to promote consistency and reduce duplication of information across systems.
8. Student files and all related data shall be maintained with control access to and use of confidential personal information on a "need to know" basis, to protect the privacy of individuals and manage institutional risk.
9. Records shall be maintained in a format and structure appropriate to the University's operational, legal admissibility and preservation requirements.

10. Records shall be maintained to be retrieved readily to meet the University's needs, to facilitate the individuals' rights of access to their own personal information and to comply with the privacy requirements.

Article (6): Information Security

The university shall maintain appropriate technical and organizational measures to comply with the privacy laws maintained in this policy and complies with the regulations in the kingdom of Saudi Arabia. These laws set out specific obligations for the University and all agents, contractors and partners who process personal data and records on its behalf to:

1. The university shall protect student and applicant records and personal data from unauthorized or unlawful access, use or disclosure, and against accidental loss or destruction
2. The university shall process information about students and applicants in accordance with their rights as data subjects under the privacy constraints set in this policy.
3. The authorized employees are permitted to access only to data, applicants and students records and related personal data as is necessary for them to fulfil their duties
4. The authorized employees shall follow the security standards for the management of student and applicant personal data set out in the procedures supporting this policy and the university's information security policies and procedures.
5. Records, personal data and student files should not be revealed to any unauthorized individual, department, or agent, unless it is required for a university services (academic or non-academic), this shall include preparing reports of the services provided, conduct a benchmarking based on analyzed/ statistical data, provide information to the accreditation agencies, provide required information for ministries and legal authorities, under which AOU is licensed and so on.
6. The authorized employees shall not reveal any information to any individual or agent without signed request from those who have the right to grant permissions, including the university rector, the ministry of education and the official agencies.

Article (7): Maintaining Provision Data

The data of the administration, financial, human resources and research and community services are maintained and provision at the different departments and gathered, analyzed and reported at the Quality Assurance and Accreditation Unit (QAAU). The data is managed, provision, centrally maintained according to IT Users and Personal Computer Policy and protected by the Information Security Policy. The Information Technology department follows the implemented mechanism to prevent data hacking, stealing, altered or deleting. The department has the necessary ant-virus and firewalls to protect the data from fraud activities unauthorized access. A statistical reports can be obtained by the periodical analysis that is implemented at the information and statistics

center, which is reporting directly to the Quality Assurance and Accreditation Unit (QAAU). The information and statistics center is enabled to obtain all the data needed to fill the reports about administration, financial, human resources and research, community services and so on.

Figure 1 illustrates the process of maintaining provision of data from students and stakeholders in the university.

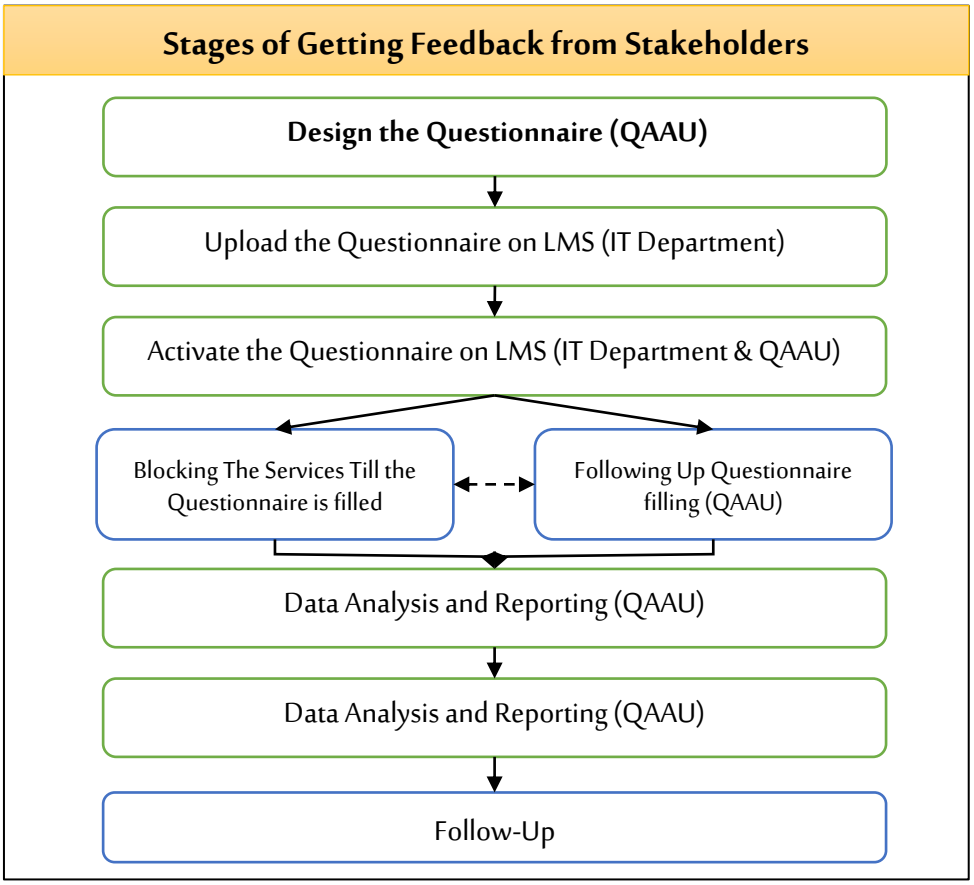

Figure 1: Feedback Attaining and Data Provision

Article (8): Admission Data Verifications

At the admission and registration activities, administrative are responsible for capturing in the official student record file all relevant information including evidential documents submitted in the course of the student's application. Copies of the documents shall be verified by the authorized administrative and all documents relating to enrolled students must be transferred from into the student file after careful verifications. Applicants through the online system are only admitted after the verification is implemented.

Article (9): Unenrolled Applicants

The university will delete the applicant records from the systems in which the applicant was seeking to enter the University. Thus, if someone applies for entry and their application is unsuccessful their record will be due for deletion following the final enrolment deadline.

Article (10): General Provisions

A. The present policy shall abrogate all previous bylaws regulating the data and records.

B. The University Council shall decide on all cases not covered by the provisions of present policies.

Document History

Version	Author / Reviewer	Details of Changes	Date	Approved by	Approved Date/Info
2019/1	QA	Change the name "Maintain Provision Data" and add records management details.	16/12/2019		