



**THE AGA KHAN UNIVERSITY**  
(International) in the United Kingdom

Institute for the Study of Muslim Civilisations

# DATA RETENTION POLICY


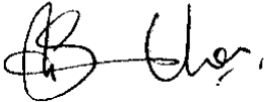


# 2022

## Table of Contents

1. Purpose.....	5
2. Review.....	5
3. Applicability.....	5
4. Records Retention.....	5
5. Guidelines & Procedures.....	5
6. Disposal Schedule.....	6
7. Archiving Digital Data.....	7
8. Retention Period Protocols .....	8
9. Storage and preservation of paper records .....	8
10. Sharing of Information .....	8
11. Audit Trail.....	9
12. Monitoring.....	9

# AKU-UK Data Retention Policy

## Document Approval

Name	Signature	Date
AKU UK Senior Management		October 2022
AKU Global Chief Information Officer (CIO)		September 2022
AKU Global Legal Representative		September 2022
AKU Global Data Protection Officer (DPO)		September 2022

## Version Control

Version	Maintained by	Release date
1.0	Data Protection Team (DPT) as part of Global Data and Analytics Office (GDAO)	July 2020
2.0	Data Protection Officer (DPO)	September 2022

# AKU-UK Data Retention Policy



## Referenced Documents

The following documents support this policy:

<b>Title</b>	<b>Version</b>	<b>Maintained by</b>
AKU-UK Data Retention Schedule	1.0	Data Protection Team (DPT) as part of Global Data and Analytics Office (GDAO)
AKU-UK Data Retention Guide	1.0	Data Protection Team (DPT) as part of Global Data and Analytics Office (GDAO)
AKU-UK Data Retention Guide	2.0	Updated contacts, versions, signatories.

## 1. Purpose

This document represents the Aga Khan University (International) in the United Kingdom (AKU-UK) policy regarding the retention and disposal of records and the retention and disposal of electronic documents. The purpose of this Policy is to ensure that necessary records and documents are adequately protected and maintained and to ensure that records that are no longer needed by ISMC or are of no value are discarded at the proper time. This Policy is also for the purpose of aiding employees of ISMC in understanding their obligations in retaining data of students, donors, employees, vendors, financial and non-financial data, in physical and electronic form.

## 2. Review

Review is the examination of closed records to determine whether they should be destroyed, retained for a further period or transferred to an archive for permanent preservation.

## 3. Applicability

This policy applies to all physical and electronic records as mentioned in AKU-UK Records Retention Schedule, including both original documents and reproductions.

## 4. Records Retention

Records should be kept for as long as they are needed to meet the operational needs of the organization, together with legal and regulatory requirements. We have assessed our records to:

- Determine their value as a source of information about the organization, its operations, relationships and environment.
- Assess their importance as evidence of business activities and decisions.
- Establish whether there are any legal or regulatory retention requirements as per the General Data Protection Regulations 2019.

## 5. Guidelines & Procedures

AKU UK manages records efficiently and systematically, in a manner consistent with the GDPR requirements, and this policy is widely disseminated to ensure a standardized approach to data retention and records management.

## AKU-UK Data Retention Policy

It is our intention to ensure that all records and the information contained therein is:

- **Accurate** - records are always reviewed to ensure that they are a full and accurate representation of the transactions, activities or practices that they document
- **Accessible** - records are always made available and accessible when required (with additional security permissions for select staff where applicable to the document content)
- **Complete** - records have the content, context and structure required to allow the reconstruction of the activities, practices and transactions that they document
- **Compliant** - records always comply with any record keeping legal and regulatory requirements
- **Monitored** - Data Retention Policy is regularly monitored to ensure that the objectives and principles are being complied with at all times and that all legal and regulatory requirements are being adhered to.

## 6. Disposal Schedule

Disposal schedule is a key document in the management of records and information. It is a list of series or collections of records for which predetermined periods of retention have been agreed between the Information Business Owners and Data Protection Officer (DPO).

Records on disposal schedules will fall into three main categories:

- i. Destroy after an agreed period; where the useful life of a series or collection of records can be easily predetermined (for example, destroy after 5 years, destroy 2 years after the end of the financial year etc.)
- ii. Selected for permanent preservation; where certain groups of records can be readily defined as worthy of permanent preservation and transferred to an archive.
- iii. Review – see [section 2](#) above.

Records can be destroyed in the following ways:

- a. Non-sensitive / Public information – can be placed in a rubbish bin.
- b. Internal information – cross cut shredded.
- c. Confidential information – cross cut shredded.
- d. Highly confidential information – cross cut shredded.
- e. Electronic equipment containing information – destroyed an app such as “*kill disk*” etc. Individual folders should be permanently deleted from the system.

Destruction of electronic records should render them non-recoverable even using forensic data recovery techniques.

## 7. Archiving Digital Data

Digital data which is no longer be actively used can be archived in offline storage for long term retention, audit and regularity compliance purpose. Following principles must be considered when archiving digital data:

- Digital data archive must be indexed and searchable so that files can be easily located and retrieved.
- All documents stored in the digital archive are protected against unauthorized access during the whole archiving process. Access to the documents is controlled by relevant document owner. Information within the digital documents must be categorized and properly labelled as per AKU information classification policy.
- Digital archive data must be managed to ensure that they are unaltered, and the original data is preserved.
- There is always a risk of portable media (e.g. USB memory sticks, CDs, DVDs) degrading or becoming corrupted; it is therefore good practice for digital data archive to be held on a central server, so that it will be adequately backed up and safeguarded from hardware failure.
- Records held electronically remain accessible and do not become trapped in obsolete technology.
- Inbound and outbound official email messages must be archived to meet operational needs together with legal and regulatory requirements. The retention period of emails shall be governed by retention schedule mentioned in AKU-UK Records Retention Schedule.
- Once the retention period has elapsed, the digital data archives are either reviewed, re-archived or confidentially destroyed depending on their purpose and action type mentioned in retention schedule.

### 8. Retention Period Protocols

All data and records retained during their specified retention periods are traceable and retrievable. Any file movement, use or access is tracked and logged. Carry out periodical reviews of the data retained, checking purpose, continued validity, accuracy and requirement to retain.

### 9. Storage and preservation of paper records

Documents need to be arranged systematically and labelled helpfully and consistently, so that it will be possible to locate them with ease and respond promptly to enquiries. File covers for paper records should be labelled with disposal dates, so that it is easy to locate material due for destruction. Local storage for paper records should be secure and protect the records from:

- Water damage (from flooding, leaks, or sprinklers)
- Fire damage
- Light damage
- Large fluctuations in temperature/humidity
- Pests

### 10. Sharing of Information

Duplicate records should be destroyed. Where information has been regularly shared between business areas, only the original records should be retained in accordance with the guidelines mentioned above. Care should be taken that seemingly duplicate records have not been annotated.

Where we share information with other bodies, we will ensure that they have adequate procedures for records to ensure that the information is managed in accordance with organization's policies, relevant legislation(s) and regulatory guidance.

Where relevant to do so, we will carry out a Data Privacy Impact assessment and update our Privacy Notices to reflect data sharing.



### 11. Audit Trail

Disposal of records which have been listed on the records retention schedule do not need to be documented. However, documents either disposed of earlier or kept for longer than listed should be recorded for audit purpose. This will provide an audit trail for any inspections conducted by the Information Commissioner Office (ICO) and will aid in addressing Freedom of Information requests, where we no longer hold the material.

### 12. Monitoring

Responsibility of monitoring the disposal policy rests with the Data Protection Officer. The policy will be renewed annually and on as and when required.