THE
ISLAMIC COLLEGE

INFORMATION RETENTION POLICY

September 2024

To be reviewed in September 2025

Table of Contents

1 Information Retention Policy

1.01 Introduction:

1.1 The Islamic College acknowledges that appropriate retention periods must be set for all information processed by the College to ensure effective administration and to meet its strategic aims and objectives. The proper management of this process will enable the College to provide evidence of its transactions and activities and enable it to comply with its legal and regulatory obligations.

1.2 This policy applies to all Information processed by the College including information created, received or maintained by the College while carrying out its business.

1.3 A small proportion of the College's records may be selected for permanent preservation in the College archives to be available for historical research and/or to give a lasting record of the College's business.

1.02 Responsibilities

The Islamic College is the 'Data Protection Officer' and the Trustees of the College are ultimately responsible for compliance with current data protection legislation.

1.03 Information Users

All members of the College are responsible for complying with all relevant data protection legislation and this policy. All members of the College must also ensure that they are aware of the retention periods set for the data they work with and informing the relevant parties should those periods be unclear.

1.04 Data Protection Officer (DPO)

The Data Protection Officer has the responsibility of overseeing compliance and developing good data protection practice within all designated areas.

1.05 Managers and Supervisory Roles

Managers and all employees in supervisory roles should ensure that regular reviews are in place in their areas to ensure that the set retention periods are met and retention reviews are carried out in a timely manner.

1.06 Information Asset Owners (IAO)

Individual personal directly involved with data is called an Information Asset Owners and is responsible for ensuring retention periods for the information is identified as part of the responsibilities more broadly. The IAO need to ensure that through the Managers and Supervisors that information to which the IAO is associated with is included on the College's Information Retention Schedule. The IAO must also ensure that information is either securely disposed of in line with the College's Information Retention Schedule or appropriately archived.

1.07 Retention periods

1.4 Information should be kept for as long as it is needed to meet the operational needs of the College, together with legal and regulatory requirements. Through the information audit conducted by the Data Protection Officer, The Islamic College determines the value and processing conditions for each of the Information Asset, assesses their importance as relating to their support for business activities and decisions, establishes whether there are any legal or regulatory retention requirements.

1.08 Retention Schedule

1.5 The College's Information Retention Schedule is a vital document for the management of information at the College. It aligns the College Information Asset Register with its record collections and informs information users of existing agreed retention periods.

1.6 Retention periods are set by Information Asset Owners to ensure that they meet the business and legal requirements for the data being processed. The Data Protection Officer is responsible for advising on setting retention periods as well as collating approved retention periods and publishing them in the College's Information Retention Schedule. The document will be closely related to the Information Asset Register but will be published as a separate resource.

1.09 Information disposal

1.10 Paper Documents

1.6.1 Physical documents containing no sensitive data may be recycled using standard recycling facilities.

1.6.2 Physical documents containing sensitive information including but not limited to commercially sensitive data, IP data and Personally Identifiable Information must be disposed of in confidential waste bins.

1.11 Digital Documents

1.6.3 Digitally created documents stored on the College shared drives and personal U drive can be deleted using your computer's recycle bin function as normal. They will be retained in the College's rolling backup which provides resilience and recovery options; this is purged regularly.

1.6.4 Where data is held in a system rather than a drive, processes for deletion of files and data will vary. Users should refer to existing guidance specific to the system in question or contact the system owner.

1.12 Archival Transfer

1.6.5 Physical documents with long retention periods and low access requirements may be considered for transfer to an archival facility. A limited amount of long term storage is managed internally by the Data Protection Officer, who is also able to advise on other possible options on an ad hoc basis.

1.13 Using copies of data owned by other departments

1.7 Sharing information internally is vital to the efficient management of the College. In cases where you are called upon to use a copy of data where a master copy is held by another department, your own retention requirements should be considered separate to theirs.

1.8 For example, during the enrolment process of a student would require the interviews to access to Registry's data. Once the enrolment exercise is over that data is updated and returned to the Registry, the interviewing team Chair person would no longer have a reason to process it.

1.14 Relationship to existing policies

1.9 This policy should be used in conjunction with other relevant College policies

1.10 Data Protection Officer should also ensure the records comply with any external guidelines, policies or legislation,

1.15 Implementation and resources

1.11 Data Protection Officer will implement practices to ensure compliance with this policy and review them regularly. It is the responsibility of the information asset owner to ensure that good housekeeping practices are undertaken to ensure the accuracy and relevance of information assets that reside on the College servers.

1.12 It is strongly advised that any personal or residual information or data that has no value or is no longer required for College purposes should be removed from the relevant drives and servers on a regular basis, at least annually.

1.13 Retention and disposal of records will be governed by the College's Information Assets Register and the Information Retention Schedule. The register and schedule provide a list of the types of records produced by the College, and details of the length of time that they should be retained to meet operational and regulatory requirements.

1.16 Contacts

1.14 Any queries or proposed amendments should be referred to the Data Protection Officer.