THE
ISLAMIC COLLEGE

DATA PROTECTION POLICY

Version:	**1.0**
Dated:	**September 2021**
Document Owner:	**Data Protection Officer**

Approval

Version	Approval Board	Date of Approval
V 1.0	Academic Board	September 2021

Review

September 2022

Contents

1. Purpose

The purpose of this Policy is to affirm the Islamic College's commitment to a policy of protecting the rights and freedoms of individuals with respect to the processing of their personal data as per the U.K Data Protection Act 2018 and the General Data Protection Regulation (GDPR) for individuals within the European Union. These ensure that data about individuals are not processed without their knowledge, are processed with their consent wherever possible and offers them the freedom to have access to their personal information if necessary.

2. The Scope of this Policy and Information Held

This policy applies to electronic and paper records held in filing systems containing personal data. Personal data means data which relates to an individual who can be identified by name or in any other way from the data. Like all educational establishments, IC collects a large amount of personal data every year. Apart from demographic information and contact details of students, staff, next of Kin and Alumni, obtained during recruitment, we also keep passport details, DBS certificates, bank statements, educational certificates, sensitive information on ethnicity, religion, sexual orientation, assessment outcomes, student funding applications and outcomes and medical reports. Other data include any expression of opinion about an individual and intentions towards an individual, including reference letters, student meeting forms and any other forms of correspondence with students. This policy also applies to data held visually in photographs or video clips (including CCTV) or as sound recordings. This policy is to be used by all staff who hold personal data on students or other employees.

3. Purpose of Data Collection and Processing

IC, like all educational establishments, holds and processes information about its employees, applicants, students, alumni and other individuals for various purposes (for example the administration of the admissions process, the effective provision of academic and welfare services, to record academic progress, to operate the payroll and to enable correspondence and communications, including the provision of references, certificates and for equal opportunities monitoring purpose.

4. Compliance

To comply with Data Protection legislation, information collected will be obtained with the consent of the individual in question, used fairly, stored safely, retained for the intended period and not disclosed to any unauthorised person. IC will keep a log of all data we hold, where it came from and who we share it with (Information Asset Register) The organisation will regard all personal information relating to students as confidential and will not divulge such information to other persons or organisation without the consent of the student, except as indicated below or as required by law. Students and staff will be informed of their rights under the GDPR, including having access to all personal data held on them.

5. Responsibilities

IC has a legal responsibility to comply with the Act. The College, as a corporate body, is named as the Data Controller under the Act.

IC is required to notify the Information Commissioner of the processing of personal data and is included in a public register of data controllers available on the Information Commissioner's website.

The Data Protection Officer is responsible for drawing up guidance on good data protection practice and promoting compliance with this guidance by advising and training staff on the creation, maintenance, storage and retention of records which contain personal information.

Every member of academic or non-academic staff that holds information about identifiable individuals has to comply with data protection in the management of that information as Individuals can be liable for breaches of the Act.

6. Student Consent

Prospective Students will sign the organisation's application form and give their explicit consent to IC holding and processing, for all relevant purposes, all data relating to them. The applicant will also consent to the college providing their information to other organisations for processing and analysis in connection with student funding, examinations and other assessments, awards, research and

administration. The organisations to which IC may provide data relating to the student as a statutory requirement include, but are not limited to, the Office for Students (OfS), Students Loans Company (SLC), Office of the Independent Adjudicator (OIA), Validation partner (Middlesex University) and awarding organisation (Pearson Education), Higher Educational Statistical Agency (HESA), Quality Assurance Agency (QAA), Home Office, Local Councils and for those in receipt of benefits, the Department for Work and Pensions (DWP), In some cases, personal information is provided to such organisations through agencies acting on their behalf.

Where a student of any age is sponsored, the student will be required to confirm that the organisation can provide details of attendance, progress, achievements and other relevant matters to the sponsor.

7. Access to Information

Students and employees have rights of access to information about themselves in accordance with the provisions of the Data Protection legislation and the right to decline to be contacted by the organisation for marketing purposes.

The organisation will annually confirm the data held with each student and employee and confirm their acceptance to hold and process this data.

Students or staff who want access to their personal data are required to do so in writing. A response will be given within one month of the request at no additional cost to the student or staff.

If IC refuses a request for data, the individual will be informed in writing with reasons why their request cannot be fulfilled within a maximum of one month.

8. Other Individual Rights

Apart from the right to be informed of data and to access information stored about them, our students and employees also have the right to request for data rectification, erasure, restrict processing and object to data processing entirely if you have good reasons to doubt the accuracy of the data and believe it has been unlawfully processed. Individuals also have the right to complain to the Information Commissioners Office if they are not satisfied with the way data is handled in the institution.

9. Data Breaches and Procedures for Security of Personal Data

At IC, data is stored in each department's information management systems designed specifically for the department. It is accessed only by the Data processors and the Data Protection Officer is required, and unauthorised access is highly unlikely. Our hard copy data is stored in locked filing cabinets and in secure rooms with lock and key. Keys to such premises must only be available to the authorised personnel.

Staff who have access to our data are provided with specific guidelines on how to prevent breaches of data as per our procedures on the Security of personal data as follows:

- All keyboards must be locked when leaving the PC.
- If sending personal data by email, ensure this is encrypted before transmission.
- Destroy all paper and electronic records by appropriate means such as shredding and appropriate deletion of electronic files (note that deleting electronic files does not equate to destroying them as they can still be retrieved.
- Ensure any computer equipment that is sold or given to another institution or staff for use at home is cleared of all personal data.

Personal information discussed about students and staff in meeting minutes will not identify students and staff by name. This is important as these meeting minutes may be submitted to a third party for any reasons.

The Organisation only operates within the UK and does not normally transfer data to other EU or non-EU countries. Staff who access information from the College on personal laptops from home ensure that their laptops are password protected and the screens are locked when not in use.

Staff who use student data for research purposes are expected to abide by the department's guidelines. This will include anonymising the data, informed consent from the data subject, use of secure and password protected electronic files and formulating a clear data management plan.

If staff with access to data identifies any reason to suspect that information stored has been accessed by unauthorised persons (stolen computer, sent wrong data to a third party), the information will be reported to the Data Protection Officer.

Depending on the extent of the breach, the Data Protection Officer will make a report to the Information Commissioner's Office and the individual/s involved.

A data subject may apply to the court for compensation if they have suffered damage (financial loss or physical injury, and possibly associated distress) if the College loses, destroys, discloses or allows access to personal data without the data subject's consent. The court will need to consider if the College has taken all reasonable care to prevent the loss, destruction, disclosure or access to this data.

10. Queries

To ensure IC manages personal data effectively, and within Data Protection legislation, the Data Protection Officer (DPO) will undertake the role for the organisation. The DPO will report to the College Board of Trustees and the Academic Board on any matters concerning Data Protection. This Policy will be reviewed annually, and changes will be agreed by the College Board of Trustees before implementation.