Cambridge Muslim College
Data Protection Policy

1. Purpose

During the course of its activities, the College collects and uses data about a range of individuals, including staff, students, applicants, and visitors. Recognising that Data Protection Law regulates how Personal Data must only be processed in such a way that protects an individual's privacy, this document sets out the College's policy, and associated procedures, for handling personal data in line with the Data Protection Act 2018 and the implementation of the General Data Protection Regulations 2016.

2. Scope

The provisions of this Policy must be followed by all Data Users when processing personal data on behalf of the College, including all service contractors, employees, and students associated with the College. It applies to all types of Personal Data**,** covering current, past and prospective students and members of staff, as well as people who work with and support the College. This Policy applies to all Personal Data processed by the College in any media or format.

3. Data Protection Principles

3.1 When processing personal data, there are 7 data protection principles that the College must follow:

- Lawfulness, Fairness and Transparency
- Purpose Limitation
- Data Minimisation
- Accuracy
- Storage Limitation
- Security
- Accountability
-

3.1.1 **Lawfulness, Fairness and Transparency:** Personal Data should be processed

lawfully, fairly and in a transparent manner. Individuals must be given sufficient information before their Personal Data is collected to enable them to understand how and why their Personal Data is to be used, allowing them to make an informed decision as to whether to provide the requested data. For the processing to be lawful, one of the legal bases set out in Data Protection Law must apply (see below).

3.1.2` Purpose Limitation: Personal Data should only be collected for specified, explicit and legitimate purposes. It should not be re-used for new or different purposes.

3.1.3 Data Minimisation: Personal Data processed should be adequate, relevant and limited to what is necessary in relation to the specified purposes for which they are processed.

3.1.4 Accuracy: Every effort should be made to ensure that all Personal Data collected by the College is accurate and it should be kept up to date.

3.1.5. Storage Limitation: Personal Data should only be kept in a form that allows the identification of individuals for as long as is necessary for the purposes for which the Personal Data are being processed. When no longer needed for the purpose for which it was collected, and if there is no lawful basis for continuing to keep it, the data should be anonymised or deleted.

3.1.6. Security: Personal Data must be processed in a way that ensures security of the data, including protection against unauthorised or unlawful processing and against accidental loss or damage.

3.1.7. Accountability: The Data Controller is responsible for ensuring compliance with the above principles

3.2 **Legal Bases for Processing Personal Data**

The processing of Personal Data is lawful if one or more of the following apply: (a) the data subject has given their consent for their data to be processed, (b) the processing is necessary for the performance of a contract to which the data subject is party, (c) processing is necessary for compliance with a legal obligation, (d) processing is necessary to protect the interests of the data subject, (e) processing is necessary for the performance of a task carried out in the public interest, and (f) processing is necessary in the legitimate interests of the data controller.

3.3 The following tasks are performed in the **"public interest**" of the College: **teaching, research, the conferral of awards, and museums and cultural collections.**

3.4 The following tasks are within the "legitimate interests" of the College: fundraising, alumni relations, events hosted by the College, and services provided for third-party organisations and members of the public.

3.5 The GDPR enshrines further restrictions on the transfer of Personal Data outside of the European Union, to third countries or to international organisations in order to ensure that the level of protection afforded by the GDPR is not weakened.

4. References

- IT Policy
- Data Retention Policy

- Data Backup and Recovery Policy
- Confidentiality Policy
- Academic Appeals and Complaints Policy
- Data Protection Act 2018
- Information Commissioner's Office

5. Responsibilities

5.1 The Board of Trustees is ultimately accountable for ensuring the College meets its legal obligations with regard to data protection compliance.

5.2 The Data Protection Officer is responsible for ensuring that day-to-day operations comply with the Data Protection Policy, working in collaboration with the assigned representatives from the IT and Operations department.

5.3 The Data Protection Officer is required to monitor, evaluate, and review the effectiveness of this policy according to the College's policy review timetable, considering current good practice and having regard to any applicable law.

5.4 The Data Protection Officer is responsible for carrying out necessary Data Protection Impact Assessments (DPIA), as an essential part of the College's Accountability obligations (see Data Protection Principles above) and as a way to identify and minimise data protection risks. A DPIA will be carried out if there are to be any changes to how or why personal data is to be processed or any changes to the amount or type of data collected or any changes to the (technical) systems used to process data. It will be carried out before any such changes are made so that it can inform the design and implementation of the process. The DPIA form is at Appendix A to this policy.

5.5 Students are responsible for ensuring that the personal data they have provided to the College is accurate and up to date and notifying a member of the College administrative staff of any changes or corrections.

5.6 Staff are responsible for handling personal data related to their job responsibilities in compliance with the College's Data Protection Policy, Confidentiality Policy, and IT Policy.

5.7 Staff are responsible for ensuring that the personal data they have provided in relation to their employment is accurate and up to date and notifying Human Resources of any changes or corrections.

5.8 Workers engaged in a service contract must comply with this policy.

5.9 Any breaches of Personal Data must be reported to the Data Protection Officer as soon as they become apparent. In some circumstances (if the data breach will result in a risk to the rights and freedoms of any data subjects) it will be necessary to report the breach to the Information Commissioner's Office within 72 hours of the breach. It is necessary to inform data subjects if there is a high risk to their rights and freedoms.

5.10 A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data and thus could include any of the following: access by an unauthorised third party; deliberate action (or inaction) by a processor; sending personal data to the wrong recipient; computing devices containing personal data being lost or stolen; alteration of personal data without permission; and loss of availability of personal data.

5.11 All breaches of personal data will be recorded by the Data protection Officer, irrespective of whether it was necessary to inform either the data subjects or the Office of the Information Commissioner.

5.12 The Human Resources team will be responsible keeping records of and, ensuring all staff receive data protection training annually delivered online by an external provider. Data Protection officers will receive training specific to Data Officers by external providers**.**

5.13 Onboarding/induction training will include data security training and staff responsibilities listed in clause 9 below.

6 Use of Staff Data

6.1 The College, per the Data Protection Act 2018, collects, stores, and transmits staff personal information in paper and electronic formats for a range of administrative purposes.

6.2 Access to personal information is limited to staff who require this information to carry out their contractual responsibilities.

6.3 A structure for access privileges for the IT system, linked to the job descriptions for each person to support the claim for access, is managed by the IT Officer. This ensures that personal data is only shared with staff who need it to do their work.

6.4. Staff personal information and related sensitive data may be needed for any of the following purposes:

- To create an employment record.
- To administer a range of processes related to Human Resources.
- To manage employment services provided by the College.
- To administer salary and pension.
- To establish communication.
- To establish, monitor, and support staff professional development.
- To monitor and support staff health, safety, and welfare
- To put in place reasonable adjustments to comply with Disability and Equal Opportunities and Equality and Diversity legislation.

7 Use of Student Data

7.1 The College, per the Data Protection Act 2018, collects, stores, and transmits student personal information in paper and electronic formats for a range of administrative and academic purposes.

7.2 Access to student personal information is limited to staff who require this information to carry out their contractual responsibilities.

7.3 A structure for access privileges for the IT system, linked to the job descriptions for each person to support the claim for access, is managed by the College IT Officer. This ensures that personal data is only shared with staff who need it to do their work.

7.4 Student personal information and related sensitive data may be needed for any of the following purposes:

- To process student applications
- To create an academic record.
- To administer funds relating to students' academic programmes.
- To manage student use of services provided by the College.
- To establish communication with students.
- To monitor and support student health, safety and welfare.
- To put in place reasonable adjustments to comply with Disability and Equal Opportunities and Equality and Diversity legislation.

8 Use of Non-Employee and Non-Student Data

8.1 The College collects, stores, and transmits personal information of individuals other than students and employees, associated with the College, such as trustees, donors, marketing distribution lists, suppliers.

8.2 Personal information of other individuals associated with the College is handled according to the principles outlined above, and in line with the Confidentiality Policy.

9 Data Security

All staff members, when handling data for their contractual responsibilities, are responsible for ensuring that personal data is kept securely. Staff must ensure:

- Physical personal data is kept in a locked, discreetly labelled filing cabinet or drawer.
- Physical personal data are not left on desks unattended.
- Physical personal data is shredded when no longer needed.
- Electronic personal data is kept on Microsoft exchange centre, encrypted, password protected and stored on the cloud.
- Electronic personal data is password protected.
- Electronic personal data is never sent by email.
- Electronic personal data is never saved to employees' personal laptops or computers.
- Office computers is backed onto a network device and password protected

- If work is done at home, it is fully password-protected and deleted completely so that it is not stored.
- If any physical or electronic personal data needs to be taken out of the College, every care is taken to ensure that it is not left unattended, is kept securely, and returned to the College as soon as possible.
- Computers are locked when left unattended.
- Computers are protected with unique and strong passwords which are not shared with anyone and are changed according to the IT Policy.
- Computers are protected using anti-virus software and server firewall.
- Back-up procedures are followed as outlined in the Data Backup and Recovery Policy.
- Personal information is not disclosed orally or in writing to an unauthorised third party, intentionally or otherwise.

10 Subject Access Requests

10.1 Under the Data Protection Act 2018 and the GDPR an individual has the right, subject to certain exemptions, to access the personal data about them held by an organisation. This covers the following:

- The right to be informed about how their Personal Data is to be used;
- The right of access to their Personal Data held by the College and other information;
- The right to rectification if their Personal Data is inaccurate or incomplete;
- The right to request the deletion or removal of Personal Data where there is no compelling reason for its continued processing;
- The right to restrict processing in certain circumstances;
- The right to data portability which allows individuals to obtain and reuse their Personal Data for their own purposes across different services;
- The right to object to processing in certain circumstances;
- Rights in relation to automated decision making and profiling.

10.2 Accessing personal data in this way is known as making a 'subject access request'. All individuals who are the subject of personal data held by the College are entitled to access this information by making a subject access request.

10.3 Subject access requests must be made in writing, either by letter or email, to the Data Protection Officer at dataprotection@cambridgemuslimcollege.ac.uk.

10.4 Before the Data Protection Officer can fulfil the request to release personal data, the identity of the subject must be verified, by, for example, passport, driving licence or utility bill.

10.6 On receipt of a completed request, and verification of the subject's identity, the Data Protection Officer is obliged to respond within 14 calendar days. The information will be

supplied subject to any applicable exemptions.

10.7 The College will not disclose personal information to third-party organisations without the consent of the subject unless it is required by law or is in the interest of the student or staff member, as indicated in the College's Confidentiality Policy.

10.8 Students are entitled to receive their assessment marks and feedback from markers. However, the College may withhold certificates, or refuse to supply references if the full programme fees have not been paid.

Revision History

Revision Number	Effective Date	Description of Change
00	March 2017	New Policy
01	July 2021	• Updated to reflect the 2018 Data Protection Act. • Aligned with new document format.
		•
02	23 March 2022	• Updated policy • Amended 7 principles of data protection • Added legal basis for processing data • Added role of data protection officer • Added process for breaches of personal data • Amended clause for subject access request to include areas covered

Signed: Sohaira Siddiqui ……
Position: Chair of the Board of Trustee

Dated…April 12th, 2022……

Appendix A

Cambridge Muslim College
Data Protection Impact Assessment Form

This Template follows the process set out in the Information Commissioners Office DPIA guidance, and should be read alongside that guidance and the Criteria for an acceptable DPIA set out in European guidelines on DPIAs.
You should start to fill out the template at the start of any major project involving the use of personal data, or if you are making a significant change to an existing process. The final outcomes should be integrated back into your project plan.

Submitting controller details	
Name of controller	
Subject/title of DPO	
Name of controller contact /DPO (delete as appropriate)	

Step 1: Identify the need for a DPIA
Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.

Step 2: Describe the processing
Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?
Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?
Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?

Step 3: Consulting Process
Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

Step 4: Assess necessity and proportionality
Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

Step 5: Identify and assess risk			
Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
	Remote, possible or probable	Minimal, significant or severe	Low, medium or high

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5				
Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved**
		Eliminated reduced accepted	Low medium high	Yes/no

Step 7: Sign of and record outcomes		
Item	**Name/position/date**	**Notes**
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:		DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice:		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		