Cambridge Muslim College
Confidentiality Policy

1. Purpose

This document sets out the College's policy and associated procedures, for ensuring appropriate levels of confidentiality within the College, in line with the Data Protection Act 2018 and the implementation of the General Data Protection Regulations 2016.

2. Scope

This policy applies to students, staff, fellows, consultants, trustees, volunteers, and donors.

3. Principles

3.1. Protecting the confidentiality of all members of the College community is a fundamental principle of the College and compliments the data security principles detailed in the College's Data Protection Policy

3.2. This policy restricts an employee from sharing information obtained by merit of their position in the College to outside parties unless permitted by law or with the permission of the Principal

3.3. Cambridge Muslim College will safeguard confidential information concerning students, employees, donors, volunteers, fellows, partners, College operations, faculty research, conflicts within the College, the College's financial details situation (except that which requires disclosure under law) and other matters pertaining to the College.

3.4. Unauthorised accessing and/or disclosure of confidential information is prohibited.

3.5. This policy restricts employess from sharing confidential information internally with colleagues who do not need to see the information

3.6. A breach of confidentiality occurs when information about anyone associated with the College is passed on to a third party without that person's permission, or there is a sharing of information about the College that is regarded as confidential.

3.7. The policy applies whether the information is stored electronically, on paper or communicated verbally.

3.8. Confidentiality covers and goes beyond the data protection standards expected by the Data Protection Act 2018, to encompass, in the broadest sense, an individual's right to privacy regarding any aspect of their personal lives which has been disclosed to the College.

3.9. Employees may not comment on College affairs to representatives of the Media in any country without authorisation from the Principal.

3.10. Confidential Information includes:

3.10.1. Personal information in whatever form (including, without limitation, in written (including email correspondence), oral, visual or electronic form or on any magnetic or optical disk or memory and wherever located) relating to employees, students, lecturers, fellows, trustees, partners, donors and other stakeholders (previous, current or potential). This includes:

- Name, date of birth, age, sex, ethnic origin, sexuality
- Address, email, phone numbers
- Contact details of family members
- Bank details
- Medical history
- Academic records, references
- Incoming or outgoing personal correspondence.
- Employment records.

3.10.2. finances of the College except that which is in the public domain;

3.10.3. relationships and partnerships with the College unless approved by the Head of College;

3.10.4. day to day affairs of the College including corporate governance, negotiations with potential stakeholders, and administrative issues including conflicts between staff members;

3.10.5. Student behaviour and performance.

4. References

- Data Protection Policy
- Complaints Policy
- Staff Disciplinary Policy

5. Responsibility

5.1. The Operations Director is responsible for reviewing the effectiveness of this policy according to current good practice and having regard to any applicable law.

5.2. It is the responsibility of everyone within the scope of this policy to have a practical understanding of what confidentiality means for the operation of the College. This includes

5.2.1 staff ensure they do not discuss cases where they can be overheard by students (or other staff members whose jobs do not need them to know this information) to inadvertently discussing confidential issues with third parties

5.2.2 Ensuring . Physical personal data is kept in a locked, discreetly labelled filing cabinet or drawer.

5.2.3 Physical personal data are not left on desks unattended.

5.2.4 Physical personal data is shredded when no longer needed
5.2.5 Electronic personal data is kept on Microsoft exchange centre, encrypted, password protected and stored on the cloud
5.2.6 Electronic personal data is password protected.
5.2.7 Electronic personal data is never sent by email.
5.2.8 Electronic personal data is never saved to employees' personal laptops or computers.
5.2.9 Office computers are backed onto a network device and password protected
5.2.10 Individual machines are protected with a user password
5.2.11 If work is done at home it is fully password-protected and deleted completely so that it is not stored
5.2.12 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.
5.2.13 Computers are locked when left unattended.
5.2.14 Computers are protected with unique and strong passwords which are not shared with anyone and are changed according to the IT Policy.
5.2.15 Computers are protected by the use of anti-virus software and server firewall.
5.2.16 Back-up procedures are followed as outlined in the Data Backup and Recovery Policy.
5.2.17 Personal information is not disclosed orally or in writing to an unauthorised third party, intentionally or otherwise.

6. Procedure

6.1 Unauthorised Breaches of Confidentiality

6.1.1 Unauthorised breaches must not be ignored even if it appears there are no immediate consequences for the College. Once discovered, unauthorised breaches must be reported to the Operations Manager as soon as the discovery is made, in writing.
6.1.2 If confidential records, either physical or electronic, are lost or stolen, a check should be made by the Operations Manager or a designated individual, as to what information is missing, and the matter reported to the Principal, the Board of Trustees and the police.
6.1.3 Any persons affected by the breach must be notified by HR in writing. Where it can be proved that confidentiality was breached wilfully or maliciously, the matter must be reviewed for disciplinary action according to the College's Disciplinary Policy.
6.1.4 Any persons affected by the breach has the right to make a make a formal complaint according to the College's Complaints Policy.
6.1.5 The Operations Manager must review internal procedures with the person who caused the breach and keep a written record of actions taken. Review internal procedures.

6.2 Authorised Breaches of Confidentiality

6.2.1 A decision to breach confidentiality can only be made with authorisation from the Principal in writing.

6.2.2 A request to access or communicate confidential information must be put in writing to the Operations Manager. The Operations Manager must pass the request to the Principal, keeping a record of any decisions taken.

6.3 Circumstances when confidentiality might need to be breached could include:

6.3.1 When there is danger to the health, safety or wellbeing of any person (including members of the public), and medical or police intervention is needed.

6.3.2 Where there is concern for the immediate safety of anyone in the College, it may be necessary to call the police. If possible, the person should be warned that if a particular behaviour continues, the police may be called and be given their name and address. In these circumstances, there is no breach of confidentiality in calling the police and giving that information. When the police arrive, the policy on confidentiality must be explained, so that they understand that the College will not give details of any other people who were present without their express permission.

6.3.3 When the College reputation is at risk, whereby information relating to someone associated with the College needs to be released to protect the College's reputation (for example, were the College to be wrongly linked to illegal, criminal, or extremist activities). In such situations, the College may need to make the true nature and circumstances public.

6.3.4 When disclosure of information is required by law. For example, under the Terrorism Act 2000, it is an offence for a person holding information about acts of terrorism to fail without reasonable excuse to disclose that information.

6.3.5 Clause 6.3.1 is not exhaustive, and authorised breaches of confidentiality will be determined on a case by case basis.

6.3.6 Disciplinary action may be taken if a member of staff willfully or accidently breaches the provisions of this policy

REVISION HISTORY

Revision Number	Effective Date	Description of Change
00	01/03/2017	New policy
01	05/10/2018	1. Changed formatting to structure 2. Updated responsibility to note new role of HR.
02	18/11/2020	1 Updated HR to Operations Manager 2 Updated Head of College to Principal To reflect to new hires now responsible for each task
03	23 March 2022	1. Clarified scope 2. Imbedded connection with data protection policy and data security