MAGDALENE COLLEGE - POLICY AND PROCEDURES ON DATA PROTECTION

Introduction

1. The information and guidelines within this policy are important and apply to all members and staff of the College who shall in this policy be collectively referred to as the "College" in the paragraphs below. Non-compliance may result in disciplinary action in accordance with the College's procedures.

2. Like all educational establishments, the College holds and processes information about its members, employees, applicants, students, alumni and other individuals for various purposes, for alumni, please refer to the data protection statement at https://www.magdalenecambridge.com/data-protection. Examples of such purposes are: 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 and certificates. To comply with data protection law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully.

Notification to the Information Commissioner

3. The College has an obligation as a Data Controller to notify the Information Commissioner of the purposes for which it processes personal data. Individual data subjects can obtain full details of the College's data protection registration notification with the Information Commissioner from the College Data Protection Officer or from the Information Commissioner's website (https://ico.org.uk).

The Data Protection Principles

4. The College, as a Data Controller, must comply with the Data Protection Principles that are set out in the 1998 Data Protection Act. In summary these state that personal data, whether held in electronic form on a computer or on paper in a manual file, shall:

- Be obtained and processed fairly and lawfully and shall not be obtained or processed unless certain conditions are met.
- Be obtained for specified and lawful purposes and shall not be processed in any manner incompatible with those purposes.
- Be adequate, relevant and not excessive for those purposes.
- Be accurate and kept up to date.
- Not be kept for longer than is necessary for those purposes.
- Be processed in accordance with the data subject's rights under the 1998 Act.
- Be kept safe from unauthorised access, accidental loss or destruction.
- Not be transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data.

The Destruction of Personal Data

5. When personal data is no longer required for the purposes for which it was obtained it should be destroyed. Guidance on the retention of records containing personal data is provided at Annexe A.

Sensitive Personal Data

6. The College may from time to time process "sensitive personal data" relating to admissions candidates, members and staff of the College. "Sensitive personal data" would include information about a data subject's racial or ethnic origin, religious beliefs or beliefs of a similar nature, trade union membership, physical or mental health or condition, sexual life, offences or alleged offences, and information relating to any proceedings for offences committed or allegedly committed by the data subject, including the outcome of those proceedings. Currently, the College envisages the need to process sensitive personal data of the types specified in the consent forms set out in Annex B to this policy for the purposes specified. For example, data relating to the ethnic origin of members or staff of the College may be processed for the purposes of equal opportunities monitoring or to identify any necessary dietary requirements, or possible sources of financial assistance. Medical records need to be processed for the provision of healthcare and general welfare, to identify any necessary dietary and accommodation requirements and to assist in meeting the needs of members of the College with disabilities. In exceptional circumstances, the College may need to process information regarding criminal convictions or alleged offences in connection, for example, with any disciplinary proceedings or other legal obligations. In other circumstances, where sensitive personal data is to be held or processed, the College will seek the explicit consent of the member of the College in question unless one of the limited exemptions provided in the DPA applies (such as to perform a legal duty regarding employees or to protect the data subject's or a third party's vital interests).

Data Security and Disclosure

7. All persons within the College are responsible for ensuring that:

- Personal data that they hold is kept securely.
- Personal data is not disclosed either orally or in writing or otherwise to any unauthorised third party, and that every reasonable effort is be made to see that data is not disclosed accidentally.
- Unauthorised disclosure is a disciplinary matter and may be considered gross misconduct. If in any doubt, consult the College Data Protection Officer.
- Personal data must be kept securely and examples of how this may be done will include keeping the data locked in a filing cabinet, drawer or room.
- Data stored on a computer is password protected or kept on a disk which is itself kept securely. Where data is held on a laptop, this must be properly safeguarded. Laptops are valuable, attractive, portable, and much sought after by thieves.
- Any other appropriate security measures are taken.

Candidates' and Students' Obligations

8. Candidates and students must ensure that any personal data provided to the College is accurate and up to date. They must ensure that any changes of address or other personal details are promptly notified to the Admissions Tutor or his staff in the case of candidates, or the Senior Tutor or his staff in the case of resident students. Students must also comply with the College's policy concerning the security of personal data held on computers (see paragraph 6 above).

Data Subjects' Consent

9. Certain types of personal data may be processed for particular purposes without the consent of individual data subjects. However, it is the College's policy to seek express consent whenever practicable from individual data subjects for the main ways in which the College may hold and

process personal data concerning them. This is to allow individuals an opportunity to raise any objections to any intended processing of personal data. The College will consider any such objections but reserves the right to process personal data in order to carry out its functions as permitted by law. Therefore, all prospective Fellows, staff, admissions candidates and students will be asked to sign a consent form regarding particular types of information which the College may in due course hold/process about them. Existing Fellows, staff and students will also be asked to sign a consent form. (Magdalene College Data Protection Form attached at Annexe B).

The Right to Access Personal Data

10. Staff, students and other individuals have the right under the 1998 Act to access any personal data that is being held about them either in an "automatically processable form" (mainly computer records) or in a "relevant filing system" (i.e. any set of information structured in such a way that specific information relating to a particular individual is readily accessible) and to request the correction of such data where they are incorrect. An individual who wishes to exercise his/her right of access is asked to complete the College "Subject Access Request" form (DP Form C – attached at Annexe C) which is available from the Assistant Bursar's Secretary and should be completed and returned to the Data Protection Officer. Any inaccuracies in data disclosed in this way should be communicated immediately to the Data Protection Officer who shall take appropriate steps to make the necessary amendments. The College will make a charge of £10 (or such other charge as is permitted from time to time by the Data Protection Act) on each occasion that access is requested and this fee should accompany the Subject Access Request form. In accordance with Data Protection Act, the College reserves the right to refuse repeated requests where a reasonable period has not elapsed between requests. The College will normally respond to the request for access to personal data within 40 days (including bank holidays and weekends) of the request or payment of the fee, whichever is the later. The Freedom of Information Act 2000 gives individuals extended rights of access in certain circumstances to information which is not held on computer or in a relevant filing system. Please contact the Data Protection Officer for further information.

The Processing of Data

11. Processing in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including:

- Organisation, adaptation or alteration of the information or data.
- Retrieval, consultation or use of the information or data.
- Disclosure of the information or data by transmission, or dissemination.
- Alignment, combination, blocking, erasure or destruction of the information or data.

Data Protection Officer

12. The College Data Protection Officer is the Assistant Bursar. All queries about the College policy and procedures and all requests for access to personal data should be addressed to the Data Protection Officer.

Responsibilities of Individual Data Users

13. All members of the College who record and/or process personal data in any form (called "Data Users" in this policy) must ensure that they comply with the requirements of the 1998 Act (including the Data Protection Principles) and with the College's data protection policy (including any procedures and guidelines which may be issued from time to time). A breach of the 1998 Act and/or the College's data protection policy may result in disciplinary proceedings. All Data Users must complete a Data Protection Survey Sheet and register their data holdings with the Data Protection Officer (Data Protection Form D at Annexe D).

14. In particular members of the College must not, without the prior written authorisation of the Data

Protection Officer:

- Develop a new computer system for processing personal data.
- Use an existing computer system for processing personal data for a different purpose.
- Create a new manual filing system containing personal data.
- Use an existing manual filing system containing personal data for a different purpose.

The above rules do not apply to databases which are maintained by individual Data Users within the College for their private domestic use, i.e. private address books. Individual data users, however, should consider if their private use falls within the scope of the 1998 Act.

Data Controllers

15. The Data Protection Officer may from time to time designate Data Controllers for particular types of data within the College. Their responsibilities will include:

- Informing the Data Protection Officer of proposed processing of personal data within the College that may need to be notified to the Office of the Information Commissioner, because it is not already covered by the College's existing registration;
- Providing personal data on a particular subject to the Data Protection Officer in response to a subject access request when requested to do so by the Data Protection Officer.
- Maintaining the security of, and access to, personal data within their designated areas of responsibility.

The principle data sets and the associated Access Controllers within Magdalene College are listed below (paragraphs 16 to 32) as follows:

Student Records

16. **Tutorial files** are maintained in respect of students' academic progress, welfare and financial arrangements. Directors of Studies files contain mostly academic data and are maintained separately by the individual student's Director of Studies. Both sets of files may contain financial and medical data. The purposes for which they are maintained include the relevant student's applications for employment, professional training or admission to other educational establishments. Current Tutorial and DoS files are to be kept by the relevant Tutors and Directors of Studies, respectively. All files may be consulted on a day-to-day basis by the Senior Tutor and, where appropriate, the Admissions Tutors, Dean, the student's individual Director of Studies or Tutor, and/or their related administrative staff.

All other requests for access to a Tutorial file or other related records must be authorised by the Senior Tutor who is the Access Controller.

17. **Student admissions files.** Admissions files are maintained in respect of candidates, and potential candidates, for both undergraduate and graduate admissions purposes. During the admissions process such files are maintained and kept by the Admissions Tutors, including the Tutor for Graduate Admissions and their staff. For successful candidates, the admissions documentation is then included in a tutorial file and passed to the relevant Tutor. For unsuccessful candidates, the admissions documentation is retained for one year and then destroyed. During the admissions process, Admissions files may be consulted by the Tutors (as appropriate) the Admissions Tutors (as appropriate), the Director of Studies and any other interviewers.

All other requests for access to Admissions files must be authorised either by the Senior Tutor, the Admissions Tutors, including the Tutor for Graduate Admissions, who are the Access Controllers.

18. **Files relating to student financial matters** are maintained by the College Accountant. These files

may be consulted on a day-to-day basis by the Senior Tutor, the Graduate Tutor, the Bursars and their respective secretaries.

All other requests for access to a student financial file must be authorised by the College Accountant who is the Access Controller.

19. **Files relating to disciplinary matters involving students** are to be maintained and kept by the Dean. Sensitive information is to be placed in a sealed envelope in the student's Tutorial File.

    All other requests for access must be authorised by the Dean or Senior Tutor who are the Access Controllers.

20. **Medical notes in respect of students** are to be maintained by the Senior Tutor for health and safety reasons to assist in meeting the needs of students with disabilities, or for reasons connected with absences from College, poor performance, and applications to the University or to charities etc. Sensitive information is to be placed in a sealed envelope in the student's Tutorial File. The notes may be consulted on a day-to-day basis by the Senior Tutor and the Senior Tutor's secretary.

    All other requests for access to these notes must be authorised by the Senior Tutor who is the Access Controller.

21. **Medical files in respect of the day to day health and welfare of Fellows, staff and students** may be maintained if required by the College Nurse**.**

    All requests for access to medical files must be authorised by the College Nurse who is the Access Controller.

Fellows and Staff Records

22. **Files relating to Fellows** are maintained and kept by the College Office. These files may be consulted on a day-to-day basis by the Master, the President, the Senior Tutor and the Senior Bursar.

    All other requests for access must be authorised by the Senior Bursar or the Senior Tutor who are the Access Controllers.

23. **Files relating to staff of the College** are maintained and kept by the College Office. These files may be consulted on a day-to-day basis by the Bursars.

    All other requests for access to these files must be authorised by the Assistant Bursar who is the Access Controller.

24. **Files in respect of teaching officers.** The Senior Tutor maintains payment data concerning supervisions. Other wages-related files are maintained and kept by the College Accountant and College Office staff with specific responsibility for payroll functions. These files may be consulted on a day-to-day basis by the Bursars, the College Accountant and those members of College Office staff with specific responsibility for payroll functions.

    All other requests for access to these files must be authorised by the Senior Tutor, Senior Bursar or College Accountant, who are the Access Controllers.

25. **Files relating to Fellows and students maintained by the College Librarian.** These are maintained and kept by the College Librarian to record the whereabouts of library books. These files may be consulted on a day-to-day basis by the College Librarian and the library staff.

All other requests for access must be authorised by the College Librarian who is the Access Controller.

26. **Files relating to tenancies of College properties, suppliers of goods and services to the College, and other third parties not otherwise dealt with in this policy document.** These are maintained and kept by the Senior Bursar, the Assistant Bursar and the College Accountant. These files may be consulted on a day-to-day basis by the Senior Bursar, the Assistant Bursar, the Bursars' Secretaries, the College Accountant, and appropriate College Office staff.

    All other requests for access must be authorised by the Senior Bursar, the Assistant Bursar or the College Accountant who are the Access Controllers.

27. **Alumni.** For information on how the College handles and uses alumni data, please refer to https://www.magdalenecambridge.com/data-protection.

28. **Fellowship Issues.** Matters pertaining to the election of Fellows are conducted by the Fellowship Committee and overseen by the Master, the President and the Senior Tutor who is Secretary. Files relating to this process may be consulted on a day-to-day basis by the Master and the President, the Senior Tutor and their secretaries. Fellowship files are to be kept in a locked filing cabinet and the cabinet shall be stored in the Master's Secretary's office. That office is to be locked at all times when the room is not occupied.

    All other requests for access to these files must be authorised the Master, President or Senior Tutor who are the Access Controllers.

The Role of the Computer Officer in Data Protection

29. When files/information is stored electronically on a computer the College Computer Officer is to ensure that the computer software includes protection against computer viruses. The information held is to be backed-up regularly and protected against unauthorised access, with the back-up system stored separately. The computer is to be password protected and is to be stored in a locked office whenever unattended.

The security of personal data held on computers

30. The important role played by the Computer Office in Data Protection does not absolve other computer users from personal responsibility. All reasonable steps should be taken to ensure that personal data held on computers is secure and necessary. The following guidelines are to be followed:

- Access to computer files should be restricted using privilege levels and passwords.
- Regular password changes should be enforced and the number of attempted logins limited.
- Equipment should be sited in a secure location where access can be restricted to authorised persons. Members of the public should not be able to view terminal screens.
- Terminals should not be left unattended and should be logged off at the end of the session.
- Redundant data should be wiped or overwritten.
- Appropriate backup and storage should be observed.
- Removable disks should be locked up after use.
- For large amounts of sensitive data, it might be necessary to keep a copy in a fireproof safe at a separate location.
- Network systems can be accessed by experienced persons. Whenever possible, personal data should be encrypted to prevent unauthorised access.

- Computer printout containing personal information should be shredded before disposal; it should not be used as scrap paper.
- Special care must be taken over the security of laptops as these are often targeted by thieves.

The use of CCTV within the College

31. The College operates a number of CCTV cameras in order to assist with the security of the College and protect property and individuals. If any individual has any queries regarding the operation of the CCTV system, they should contact the College Marshal. The tapes are held in secure conditions for 28 days, and on the 29th day they are erased. If anyone wishes to access any personal data about themselves on the CCTV system within 28 days of the occurrence, they should complete and return a Subject Access Request form (with the requisite £10 fee) with as much information as possible to enable the data to be located (including, if possible, details of the relevant camera, date and time).

Email

32. It is permissible and appropriate for the College to keep records of internal communications which are relevant to an individual's ongoing relationship with the College, whether as a Fellow, member of staff or student, including information concerning performance and conduct issues, provided such records comply with the Data Protection principles. It is recognised that email is used for such communications and that such emails should form part of the College's records.

33. All those working within the College need to be aware that the Data Protection Act applies to emails which contain personal data about individuals which are sent or received by members of the College (other than for their own private purposes).

34. Subject to certain exceptions, individual data subjects will be entitled to make a data Subject Access Request and have access to emails which contain personal data concerning them, provided that the individual data subject can provide sufficient information for the College to locate the personal data in the emails. The legislation applies to all emails from and to members of the College which are sent and received for College purposes, whether or not the emails are sent through the College email system or on an individual's own email account.

Disclosure outside of the European Economic Area (EEA)

35. The College may, from time to time, desire to transfer personal data to countries outside of the EEA in accordance with purposes made known to individual data subjects. For example, the names and contact details at the College of members of staff on a website may constitute a transfer of personal data worldwide. Accordingly, the consent form signifies an individual's consent to the inclusion of such data on an authorised College website. If an individual wishes to raise an objection to this disclosure then written notice should be given to the Data Protection Officer. Other personal data, even if it would otherwise constitute fair processing, must not, unless certain exemptions apply or protective measures taken, be disclosed or transferred outside the EEA to a country or territory which does not ensure an adequate level of protection for the rights and freedoms of data subjects.

Complaints Procedure

36. Data subjects wishing to complain about the College's handling of data protection issues should do so in writing to the College's Data Protection Officer (the Assistant Bursar). The Data Protection Officer will seek to resolve any issue to the satisfaction of the data subject. There is also the right to complain to the Information Commissioner.

Magdalene Data Protection Forms:

Annexe A – Retention of Records Containing Personal Data
Annexe B – Consent Form
Annexe C – Subject Access Request Form
Annexe D – Data Protection Survey Sheet

Annexe A
Magdalene Data Protection Form A
Magdalene College
Data Protection Act 1998

Retention of Records Containing Personal Data

Type of Record	Retention Period	Reason for Period
Personnel Files including training records and notes of disciplinary and grievance hearings	6 years from the end of the employment by the College	References and potential litigation
Application forms/interview notes	At least 6 months from the date of interviews	Time limit on litigation
Facts relating to redundancies where less than 20 redundancies	6 years from the date of the redundancy	Time limit on litigation
Facts relating to redundancies where 20 or more redundancies	12 years from the date of redundancies	Limitation Act 1980
Income tax and NI returns, including correspondence with tax office	At least 3 years after the end of the financial year to which the records relate	Income Tax (Employment) Regulations 1986
Statutory maternity Pay records and calculations	At least 3 years after the end of the financial rear to which the records relate	Statutory Maternity Pay (general) Regulations 1986
Statutory Sick Pay records and calculations	At least 3 years after the end of the financial year to which the records relate	Statutory Sick Pay (general) Regulations 1986
Wages and salary records	6 years	Taxes Management Act 1970
Accident books, records and reports of accidents	3 years after the date of the last entry	Social Security (Claims and Payments) Regulations 1979 RIDDOR 1985
Health Records	During employment	Management of Health and Safety at Work Regulations
Health records where reason for termination of employment is connected with health, including stress related illness	3 years	Limitation period for personal injury claims
Medical records kept by reason of the Control of Substances Hazardous to Health Regulations	40 years	Control of Substances Hazardous to Health Regulations 1985

Student Records, including academic achievements and conduct CCTV footage.	At least 6 years from the date that the student leaves the College, in case of litigation for negligence. At least 10 years for personal and academic references. Certain personal data may be held with perpetuity 28 days.	Limitation period for negligence. Permits the College to provide references for a reasonable length of time. While personal and academic references may become 'stale', some data eg. transcripts of student marks, may be required throughout the student's future career. Upon the death of the data subject, data relating to him/her ceases to be personal data. To allow sufficient time for a crime or serious event to be discovered and investigated.

Annexe B

Magdalene Data Protection Form B

Magdalene College
Data Protection Act 1998

Consent Form

To assist the College comply with its legal obligations under the Data Protection Act 1998, you have been given access to the College's policy and procedures on data protection. Whilst this is not strictly necessary in every case, it is the College's policy to seek the consent of members and staff of the College to hold and process personal data about them.

Listed in the Schedule to the College's policy and procedures on data protection are the main categories of data that the College may hold/process, the main purpose(s) for holding/processing such data, the possible disclosures of such data and the likely sources of such data. Full details of the College's data protection/notification with the Information Commissioner can be obtained from the Assistant Bursar who is the Data Protection Officer.

In addition to having a legitimate basis for processing data, the College has a duty only to process that data fairly (for example in accordance with any duty of confidentiality owed to you).

Please sign underneath to confirm your consent. If you have any queries they should be raised with the Data Protection Officer.

I confirm that I have been given access to the College's Policy and Procedures on Data Protection and consent to the College holding and processing the categories of personal data about me, including sensitive personal data, as specified in its registration/notification to the Information Commissioner for the specified purposes (summarised in the College's Policy and Procedures on Data Protection).

Name (please print) ……

Signed ……..

Date …….

Annexe C

Magdalene Data Protection Form C

Magdalene College
Data Protection Act 1998

Subject Access Request Form

Please complete this form (in BLOCK CAPITALS) and return it to:
Data Protection Officer
Magdalene College
Magdalene Street
Cambridge
CB3 OAG

Part 1 – Personal Details

1. Surname (*please include any former names if relevant to request*)

……

2. Full Forenames

……

3. Title

……

4. Date of matriculation / date of admission to Fellowship / dates of employment

……

5. State clearly the information you require, with dates where known

(*if necessary please continue on a separate sheet*)

Magdalene Data Protection Form C

Part 2 – Declaration

Please delete as applicable

I am acting on my own behalf
or
I am acting on behalf of someone who is unable to act for themselves and Part 1 relates to them.

My relationship to the data subject is:

……

Please delete as applicable

Accordingly, I enclose:

the individual's written consent to disclosure of the information stipulated in Part 1
or
a Court Order (eg, Power of Attorney) permitting release of the information stipulated in Part 1 to the individual named in Part 2

To the best of my knowledge, the information I have given on this form is correct.

Name (please print):

……

Signed:

……

Date

……

Full address

……

Telephone number

……

Please enclose verification of identity e.g., a photocopy of your passport or driving licence.
NB: This is not required for current members of College.

Magdalene College will use the information provided for the purpose of locating the information requested and it will be kept securely for 2 years in case of further inquiries from you following which the form will be destroyed.

Date SAR received …….

Date Fee received …….

Date response sent …….

Annexe D

Magdalene Data Protection Form D

Magdalene College Data Protection Act 1998

Data Protection Survey Sheet

Department:	
File Set General Description:	
Custodian's details:	
Telephone number:	
Purpose: *What is the information in this file set used for?*	
Type of Data held: *Delete as appropriate*	Personnel records Pay and pensions Line management supervisory records Academic records Training records Recruiting records Admissions records Welfare records Medical records Disciplinary records Health & safety Other (*specify*):
Data Subjects: *eg. Fellows, staff or students*	
Source: *From whom does the information come?*	
Duration for which file set is retained:	
Any other relevant information:	