



MAGDALENE COLLEGE

Policy and procedures on Data Protection

Introduction

1. The purpose of the College's Data Protection Policy is to ensure compliance with data protection law (the UK GDPR and related legislation). Data protection law applies to the storing or handling ('processing') of information ('personal data') about living identifiable individuals ('data subjects').
2. 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. The terms "members" and "staff" means anyone working in any context within the College whether permanent, fixed term or temporary, including but not limited to employees, retired but active members, visiting researchers, volunteers, and external members of committees. Non-compliance may result in disciplinary action in accordance with the College's procedures.
3. Like all educational establishments, the College holds and processes information about its members, employees, applicants, students, alumni and other individuals for various purposes. Privacy notices (statements informing data subjects how their personal data is used by the College) can be found at <https://www.magd.cam.ac.uk/administration/policies-and-procedures>.

Data Breaches

4. One of the most important accountability obligations concerns personal data breaches - that is, personal data held by the College is lost, stolen, inadvertently disclosed to an external party, or accidentally published. If a personal data breach occurs, this should be reported immediately to a Head of Department, who should then inform:
 - A. The person responsible for College Data Protection, the Assistant Bursar. The Assistant Bursar will then contact relevant senior members of the College to determine what action is to be taken.
 - B. If the breach is IT-related in any way, the Head of IT.
 - C. The Colleges' Data Protection Officer (DPO) via the online reporting form found at <https://app.casc.cam.ac.uk/pdir>.

Remedial work can then be done so that the breach can be contained. On occasion, we need to report breaches to relevant external authorities, including the ICO, within a short timeframe.

The Data Protection Principles

5. The College is committed to complying with data protection law as part of everyday working practices. Complying with data protection law may be summarised as but is not limited to:

- A. Understanding and applying as necessary, the data protection principles when processing personal data:
The principles in relation to personal data are: lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, and integrity and confidentiality.
- B. Understanding, and fulfilling as necessary, the rights given to data subjects under data protection law:
The data subject rights are: access, rectification, erasure, restriction, data portability, and objection (including in relation to automated decision-making).
- C. Understanding, and implementing as necessary, the College's accountability obligations under data protection law:
The accountability obligations include: implementing appropriate data protection policies, holding relevant records about personal data processing, implementing appropriate technical and organisational security measures to protect personal data, reporting certain personal data breaches to the Information Commissioner's Office.

The Destruction of Personal Data

- 6. 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 Annex A.

Data Security and Disclosure

- 7. All persons within the College, as appropriate to their role and in order to enable the College to comply with data protection law, are responsible for:
 - A. completing relevant data protection training
 - B. when processing personal data on behalf of the College, only using it as necessary for their duties and/or other College roles and not disclosing it unnecessarily or inappropriately
 - C. ensuring that all personal data that they hold is kept securely
 - D. recognising that data held on disk, laptop, or other portable medium are particularly vulnerable and must be properly safeguarded
 - E. ensuring that data stored on a computer is password protected as appropriate and secure methods of transmission are used
 - F. ensuring any other appropriate security measures are taken
 - G. recognising, reporting internally, and cooperating with any remedial work arising from personal data breaches
 - H. recognising, reporting internally, and cooperating with the fulfilment of data subject rights access
 - I. only deleting, copying or removing personal data when leaving the College as agreed with the College Data Controller or other appropriate person

Non-observance of the responsibilities noted above is a disciplinary matter and may be considered gross misconduct. If in any doubt, consult the person responsible for Data Protection in the College, the Assistant Bursar.

Data Subject Access Rights

8. A data subject has the right: to ask us for access to, rectification or erasure of their data; to restrict processing (pending correction or deletion); to object to communications or direct marketing; and to ask for the transfer of their data electronically to a third party (data portability). Some of these rights are not automatic, and the College reserves the right to discuss with the data subject why the College might not comply with a request from a data subject to exercise them. See Annex B.

Data Controller

9. The controller for your personal information is the Magdalene College, Cambridge CB3 0AG. The Data Protection Officer for the College is the Office of Intercollegiate Services Ltd [12B King's Parade, Cambridge; 01223 768745; college.dpo@ois.cam.ac.uk]: OIS Ltd. should be contacted if you have any concerns about how the College is managing your personal information, or if you require advice on how to exercise your rights as outlined in this statement. The person within the College otherwise responsible for data protection at the time of issue, and the person who is responsible for monitoring compliance with relevant legislation in relation to the protection of personal information, is the Assistant Bursar assistant.bursar@magd.cam.ac.uk.
10. The College may from time to time designate responsibility for particular types of data within the College, these are listed below:

Student Records

11. **Tutorial files** are maintained in respect of students' academic progress, welfare and financial arrangements. 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 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 Academic Office staff.

All other requests for access to a Tutorial file or other related records must be authorised by the Senior Tutor. For more detail on how student information is used see <https://www.magd.cam.ac.uk/data-protection-students>.

12. **Student admissions files** are maintained in respect of candidates, and potential candidates, for both undergraduate and postgraduate admissions purposes. During the admissions process such files are maintained and kept by the Admissions Tutors and Academic Office 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 in accordance with the College retention policy (annex A). 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, or the Admissions Tutors. For more detail on how student applicant information is used see <https://www.magd.cam.ac.uk/data-protection-applicants-students>.

13. **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 Postgraduate Tutor, the Bursars and their respective secretaries.

All other requests for access to a student financial file must be authorised by the College

Accountant.

14. **Files relating to disciplinary matters involving students** are maintained and kept by the Dean. Sensitive information may be placed in the student's Tutorial File.

All other requests for access must be authorised by the Dean or Senior Tutor.

15. **Medical notes in respect of students** are 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 may be placed 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 PA.

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

16. **Medical files in respect of the day to day health and welfare of Fellows, staff and students** may be maintained if required by the Health and Wellbeing service.

All requests for access to medical files must be authorised by the Head of Student Wellbeing.

Fellows' and Staff Records

17. **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, the Senior Bursar, the College Accountant and those members of the College Office with specific responsibility for payroll functions or Human Resources.

All other requests for access must be authorised by the Senior Bursar or the Senior Tutor. For more information on how Fellows and Senior Members is used please see

<https://www.magd.cam.ac.uk/data-protection-senior-members>.

18. **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.

All other requests for access to these files must be authorised the Master, President or Senior Tutor. For more detail on how Fellowship application information is used please see

<https://www.magd.cam.ac.uk/data-protection-applicants-senior-members>.

19. **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 and those members of the College Office with specific responsibility for payroll functions or Human Resources.

All other requests for access to these files must be authorised by the Assistant Bursar. For more information on how staff and staff applicants are used please see

<https://www.magd.cam.ac.uk/data-protection-staff> and <https://www.magd.cam.ac.uk/data-protection-applicants-staff>.

20. **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.

Library Records

21. **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.

Other Tenancy Records

22. **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/College Accountant. These files may be consulted on a day-to-day basis by the Senior Bursar, the Assistant Bursar, the Bursars' Secretaries, and appropriate College Office staff.

All other requests for access must be authorised by the Senior Bursar or the Assistant Bursar.

Alumni Records

23. **Alumni.** For information on how the College handles and uses alumni data, please refer to <https://www.magd.cam.ac.uk/alumni-data-protection>.

The Role of the Head of IT in Data Protection

24. When files/information is stored electronically on a computer the Head of IT 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

25. The important role played by the IT Department 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:
- A. access to computer files should be restricted using privilege levels and passwords
 - B. strong passwords should be used (further advice on what is deemed a strong password can be obtained from the Head of IT) and the number of attempted logins limited
 - C. 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
 - D. terminals should be locked (Ctrl-Alt-Del) when left unattended and logged off when finished with or at the end of the day
 - E. redundant data should be wiped or overwritten

- F. appropriate backup and storage should be observed
- G. removable disks should be locked up after use
- H. for large amounts of sensitive data, it might be necessary to keep a copy in a fireproof safe at a separate location.
- I. network systems can be accessed by experienced persons. Whenever possible, personal data should be encrypted to prevent unauthorised access
- J. computer printout containing personal information should be shredded before disposal; it should not be used as scrap paper.
- K. special care must be taken over the security of laptops as these are often targeted by thieves.

The use of CCTV within the College

26. The College operates a number of CCTV cameras within the College in order to provide a safe and secure environment for members of the College, its employees and visitors, and to protect the College's property. Please see <https://www.magd.cam.ac.uk/cctv-code-of-practice> for the Magdalene College CCTV code of practice.

Photography and Videography

27. The College uses photography and videography as part of its legitimate interests to document, promote, and communicate College life, events, and activities. This includes capturing images and videos during events and other College activities, as well as general College life in public spaces. These images and videos may be used for promotional purposes, including on the College website, social media channels, publications, and other marketing materials.

Under the UK GDPR, the College relies on Legitimate Interests as the legal basis for this processing. This approach is proportionate, respects individual privacy rights, and aligns with the College's educational and communication goals. We take reasonable steps to ensure that individual privacy is protected, including providing clear signage when filming is taking place. Individuals who wish to opt out of having their image or video included in such documentation may contact communications@magd.cam.ac.uk.

Email

28. 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.
29. All those working within the College need to be aware that the data protection law 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).
30. 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 UK

31. We may transfer personal data that we collect from you to third-party data processors in other countries, but we will only do so if appropriate data protection agreements and safeguards have been put in place, or it is otherwise lawful to transfer the data.

Complaints Procedure

32. Data subjects wishing to complain about the College's handling of data protection issues should do so in writing to the person responsible for College Data Protection, the Assistant Bursar. The Assistant Bursar will seek to resolve any issue to the satisfaction of the data subject. You retain the right at all times to lodge a complaint about our management of your personal data with the Information Commissioner's Office at <https://ico.org.uk/concerns/> .

Annex A – Retention of Records Containing Personal Data

Annex B – Data Subject Access Request Form

Annex A

Magdalene College Personal Data Retention Schedule

1. Governance and Strategy

Entry	Record	Retention period	Action at end of retention period	Reason for retention period	Information from
1.1	Committee membership records, list of fellows	Indefinitely		Permanent archive	Senior Bursar's Office
1.2	Registers of interests	As long as required for those connected with decision making plus six years	Destroy		Senior Bursar's Office
1.3	Agendas, minutes and papers of the Governing body and standing committees	Indefinitely		Permanent archive	Senior Bursar's Office
1.4	Agendas, minutes and papers of all other committees and working groups	Indefinitely as part of permanent archive Connected notes as required to form papers	Review whether to archive or destroy		Committee Chairs College Archivist
1.5	Fraud and whistle-blowing case files	Last action on case plus six years	Destroy		Senior Bursar's Office
1.6	Records regarding the College's notifications under the GDPR	End of current academic year plus six years	Destroy		Assistant Bursar
1.7	Data access requests	Last action on request plus six years	Destroy		Assistant Bursar
1.8	Requests for information under the Freedom of Information Act	Indefinitely for requests and responses. Any personal data used to compile responses deleted annually if over one year old.	Shred paper and delete electronic information containing personal data over one year from request		FOI Officer
1.9	Contracts and legal agreements, including supporting documentation and advice	End of contract plus six years (under signature) for operational contracts Contracts under seal retained indefinitely	Destroy	Permanent archive	Head of Department Senior Bursar's Office
1.10	Leases and lease agreements	Indefinitely		Permanent archive	Senior Bursar's Office
1.11	Claims by or against the College that do not proceed to litigation	Indefinitely		Permanent archive	Senior Bursar's Office
1.12	Litigation with third parties	Indefinitely		Permanent archive	Senior Bursar's Office
1.13	Records relating to Trusts	Indefinitely		Permanent archive	Senior Bursar's Office

2. Student Administration and Teaching (including admissions)

See also student data protection statement

Entry	Record	Retention period	Action at end of retention period	Reason for retention period	Information from
2.1	Individual student applications: unsuccessful candidates	Up to 3 months following the completion of the admissions process	Destroy hard copy records Electronic records held by University on CAMSIS	Allows for review of offers if required	Academic Office
2.2	Individual student records (tutorial files), including applications, matriculation, academic achievements	Full data set - during student's studies. Subset – non-sensitive personal data held in perpetuity.	Destroy sensitive personal information; remainder of file to College archive	Sensitive personal, health and academic data required during studies	Academic Office
2.3	Records relating to a student's visa status	As part of full data set - At least 6 years from the date that the student leaves the College or approved by the Home Office (whichever is the longer)	Destroy		Academic Office
2.3	CCTV footage	31 Days unless required for investigation, and then until investigation is complete	Destroy / overwrite	Equipment records on 31 day cycle	Head Porter see CCTV Code of Practice
2.4	Accommodation licences Accommodation files: OTR forms, rebate forms and ballot orders Database (spreadsheet) of which students occupied which rooms	End of the current year plus six years – paper and electronic Four years or until student has left College, whichever is longer – paper and electronic Four years or until student has left College, whichever is longer	Destroy	Legal agreements (see 1.9) Provision of references For billing queries	Assistant Bursar

Entry	Record	Retention period	Action at end of retention period	Reason for retention period	Information from
2.5	Student complaint and academic appeal files*	At least 6 years from the date that the student leaves the College	Destroy	Limitation period for negligence.	Academic Office
2.6	Student disciplinary and academic misconduct files*	At least 6 years from the date that the student leaves the College	Destroy	Limitation period for negligence.	Academic Office
2.7	Student fitness to practice files	At least 6 years from the date that the student leaves the College	Destroy	Limitation period for negligence.	Academic Office
2.8	Records of financial aid, scholarships and bursaries*	At least 6 years from the date that the student leaves the College	Destroy	Required retention period for financial records	Academic Office
2.9	Student information on forum including room details for maintenance, housekeeping and other purposes	<i>See IT policy</i>			IT Department
2.10	Outreach residential event: Personal details of children attending the event including parental and medical information	Hard copy – one week after event	Destroy		Academic Office

* summaries may be placed in the tutorial files, 2.2

3. Finance

Entry	Record	Retention period	Action at end of retention period	Reason for retention period	Information from
3.1	Purchase orders, purchase invoices, sales invoices, credit card records, expenses payments, petty cash handling, retail sales transactions and other transaction records	Current financial year plus six years thereafter	Destroy	Required retention period for financial records	Senior Bursar's Office
3.2	Student accounts (for scholarships, bursaries and awards see 2.8)	Seven years after completion of studies	Destroy paper and electronic records	Required retention period for financial records	Academic Office/ Senior Bursar's Office
3.3	Fellows' accounts	Current financial year plus six years thereafter	Destroy	Required retention period for financial records	Senior Bursar's Office
3.4	May Ball information and accounts	Current financial year plus six years thereafter	Destroy	Required retention period for financial records	Senior Bursar's Office
3.5	Insurance disclosures (budget holders and F&GP members)	One year – until following year's disclosures have been received	Destroy	Insurance requirement	Senior Bursar's Office
3.6	Credit card details for payment	Maximum 1 hour	Destroy	Legal requirement	Senior Bursar's Office

4. Human Resources

Entry	Record	Retention period	Action at end of retention period	Reason for retention period	Information from
4.1	Personnel files, including applications, training records, appraisals.	Duration of employment plus no more than 12 months, unless there is a specific need to retain for longer. Subset retained for up to 7 years after the end of relationship with College. Basic data retained in a permanent archive.	Destroy	References and potential litigation Permanent Archive	HR Manager
4.2	Unsuccessful job applications	Six months after the end of the closing date of the application process	Destroy	Time limit on litigation	HR Manager
4.3	See 6.2 donors and supporters				
4.4	Assessments and reviews of workforce requirements	Indefinitely, see 1.4			
4.5	Management succession plans	Indefinitely, see 1.4			
4.6	Wages and salary records	Current financial year plus six years thereafter	Destroy	As part of financial records	Payroll
4.7	PAYE and NI records	Current financial year plus six years thereafter	Destroy	As part of financial records	Payroll
4.8	Pension records – employer and employee contributions	Current financial year plus six years thereafter Subset – pensions preferences retained indefinitely	Destroy	As part of financial records	Payroll
4.9	Disciplinary and grievance records	Up to seven years from the end of employment by the College	Destroy	References and potential litigation	HR Manager
4.10	Facts relating to redundancies where less than 20 redundancies	Up to seven years from the date of the redundancy (see also 1.3 and 1.4 for committee reports)	Destroy	Time limit on litigation	Senior Bursar's Office

Entry	Record	Retention period	Action at end of retention period	Reason for retention period	Information from
4.11	Facts relating to redundancies where 20 or more redundancies	Up to seven years from the date of the redundancy (see also 1.3 and 1.4 for committee reports)	Destroy	Time limit on litigation	HR Manager
4.12	Statutory maternity pay records	At least 3 years after the end of the financial year to which the records relate	Destroy	Regulatory requirement	Payroll
4.13	Statutory sick pay records	At least 3 years after the end of the financial year to which the records relate	Destroy	Regulatory requirement	Payroll
4.14	Holiday and sick leave records, time sheets	At least 3 years after the end of the financial year to which the records relate Summary records included in financial records (see 3.1)	Destroy		Payroll
4.15	General personnel records for interns or casual staff	See 4.1			
4.16	Staff records kept in departments by HODs	Until member of staff leaves	Pass to HR department for destruction	Day to day operational requirements	Head of Department

5. Master, Fellows and other Teaching Staff

Entry	Record	Retention period	Action at end of retention period	Reason for retention period	Information from
5.1	Personal contact details of Master and all Fellows	For the length of their life and spouse's life if applicable	Remove from database	To forward mail and keep informed about events and developments at the college	Master's Office, President's Office and, College Office (restricted access only)
5.2	Unsuccessful JRF applicant information	No more than 12 months after the closing date of the application process. Applicant name on interview schedule kept indefinitely. If relevant personal details may be retained for contact regarding College activities or membership.	Destroy	In case of appeals against decision	President's Office
5.3	Personal files of successful JRF applicants	As for Fellows below. If the post has required a 'resident market test' all application records retained for duration of the sponsored post and 12 months thereafter.	Destroy	Statutory requirement	President's Office
5.4	Personal files of Fellows	Duration of employment or membership plus no more than 12 months, unless there is a specific need to retain for longer. Subset retained for up to 7 years after the end of relationship with College. Basic data retained in a permanent archive.	Destroy	References and potential litigation E.g. major health or personal injury incident Maintenance of benefits and College records of members	President's Office

Entry	Record	Retention period	Action at end of retention period	Reason for retention period	Information from
5.5	Personal information of other teaching staff, including CV	Indefinitely in paper file and as part of Committee papers see 1.3		Potential litigation. Permanent College archive May need to re-employ.	Academic Office
5.6	CVs of prospective Fellows - unelected	Indefinitely as part of papers for Governing Body see 1.3		Potential litigation. Permanent College archive	Senior Bursar's Office

See also other sections for particular types of information

6. Development and Alumni Relations

Entry	Record	Retention period	Action at end of retention period	Reason for retention period	Information from
6.1	Enquiries from the general public and responses	Subject to the nature of the enquiry	Destroy	Answer query and further response requirements	Alumni and Development Office
6.2	Basic records concerning individual alumni, donors and supporters. Kept in Raiser's Edge database.	Indefinitely			Alumni and Development Office
6.3	Records of transactions with donors	Indefinitely			Alumni and Development Office
6.5	Planning and organisation of events and meetings for alumni, donors and supporters	Indefinitely			Alumni and Development Office
6.6	Mailing lists for College publications	Indefinitely (subject to data subject consent)			Alumni and Development Office
6.7	Information about alumni, donors and supporters: previous support, career details, interests/hobbies and philanthropic tendencies	Indefinitely (subject to data subject consent)			Alumni and Development Office
6.8	The College captures and uses images and videos to document and promote College life, events, and achievements, supporting our goal to represent and celebrate our community. These images and videos may be used across various platforms, including on the College website, social media channels, publications, and other marketing materials.	We retain these materials only as long as they serve our promotional and educational purposes effectively. Images and videos are periodically reviewed to ensure that they continue to reflect the College's values, represent our community appropriately, and align with our communication goals. Materials that no longer support these objectives or are no longer			Alumni and Development Office

		relevant may be securely archived or deleted. If an individual opts out of having their image or video used, we will make every reasonable effort to remove or restrict access to any materials where they are identifiable, while maintaining the integrity of our archives and records.			
--	--	---	--	--	--

7. Health and Safety

Entry	Record	Retention period	Action at end of retention period	Reason for retention period	Information from
7.1	Student health records (general)	One year after completion of studies, except where as part of tutorial files (2.2) or committee records(1.3,1.4)	Destroy	RCN Guidelines	College Nurse
7.2	Clinical information generated in consultation with the College Nurse	Normally eight years from completion of studies	Destroy	RCN Guidelines	College Nurse
7.3	Staff and Fellows' health records (general)	One year after cessation of relationship with College	Destroy	RCN Guidelines	College Nurse
7.4	Health records where reason for termination of employment or withdrawal from course is connected with mental or physical health	See section 2 – Students Section 4 – staff Section 5 – Senior Members		Limitation period for personal injury claims	
7.5	Medical records kept by reason of the Control of Substances Hazardous to Health Regulations	40 years	Control of Substances Hazardous to Health Regulations 1985	Control of Substances Hazardous to Health Regulations 1985	Senior Bursar's Office
7.6	Health and Safety training records see 4.1				
7.7	Accident reports and incident investigation forms	At least 3 years		Legal requirement	Senior Bursar's Office
7.8	PAT testing records – items in individual rooms with names	Current year plus three years	Destroy	Legal requirement	Maintenance department

8. Dinners, Conferences and Events

Entry	Record	Retention period	Action at end of retention period	Reason for retention period	Information from
8.1	Dietary requirements	Fellows: as long as fellow is associated with the college, Alumni and supporters; as required for each event Students: until academic year following the student leaving College Visitors: as required for each event	Destroy (unless request by data subject to retain)	Potential litigation Serve meals in accordance with dietary requirements	Head of Catering
8.2	Lists of those attending dinners – see also 6.5	Completion of event	Destroy	Catering requirement	Head of Catering
8.3	Contact details of those booking events – students, fellows and external individuals – for planning and organising events	4 years after the completion of the event	Destroyed		Conference Office
8.4	Contracts for events see 1.9				
8.5	Contact details of chapel attendees (where recorded as part of Alumni and Development Office records)	Indefinitely (subject to data subject consent)			Alumni and Development Office
8.6	Room numbers and names of guests at events and otherwise	No longer than necessary for each event. Detail may be included in financial records see 3.1	Destroyed		Conference Office
8.7	Contact details of those making initial enquiries about booking but not leading to a booking	Two years from the last action	Destroy	Potential follow up requirements	Conference Office

9. IT and Library Facilities

Entry	Record	Retention period	Action at end of retention period	Reason for retention period	Information from
9.1	Details of visiting scholars and those requesting images and information (Pepys and Old Libraries, archive)	In perpetuity		Historic record of scholarship, for publication royalties and understanding further enquiries	Pepys Librarian's Office, Archivist
9.2	Visitor's book in the Pepys Library	In perpetuity		Permanent archive	Pepys Librarian's Office, Archivist
9.3	Phone or written enquiries (New Library, archives)	Subject to the nature of the enquiry	Destroy	Answer query and further response requirements	Pepys Librarian's Office, Archivist
9.4	Record of donations (New Library, archive)	In perpetuity			College Librarian's Office/ Alumni and Development Office, Archivist
9.5	Library borrower details, including record of books borrowed, fines	One year after completion of studies	Destroy, delete electronic information		College Librarian's Office
9.6	Student support details (main library)	Academic year after the student leaves College	Destroy, delete electronic information		College Librarian's Office

10. Other

Entry	Record	Retention period	Action at end of retention period	Reason for retention period	Information from
10.1	Baptismal register (Chapel)	Indefinite		Permanent official record	Dean of Chapel

Annex B



Magdalene College

Data Subject Access Request Form

Please complete this form (in BLOCK CAPITALS) and return it to:

Assistant Bursar
Magdalene College
Magdalene Street
Cambridge
CB3 0AG

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)

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 and retained in accordance with the College Data Retention Policy which can be found at <https://www.magd.cam.ac.uk/administration/policies-and-procedures>

Date SAR received

Date response sent