EMMANUEL COLLEGE

DATA PROTECTION POLICY

(Personal information, its processing and privacy)

Purpose and scope

1. The purpose of this policy is to ensure compliance with **data protection law** in the UK (the General Data Protection Regulation and related EU and national legislation). Data protection law applies to the **processing** (collection, storage, use and transfer) of **personal information** (data and other personal identifiers) about **data subjects (**living identifiable individuals).

2. Under data protection law, the College is identified as a **data controller** and as such is subject to a range of legal obligations. For clarity, the University of Cambridge and the other colleges in Cambridge are separate data controllers, with their own policies and procedures. Sharing of personal information between the University and the Colleges is covered by a formal data sharing protocol.

3. This policy applies to all **staff** and **members** of the college, except when they are acting in a private or external capacity. For clarity, the term **staff** means anyone working in any context for the College, including employees, retired but active members and staff, workers, trainees, interns, seconded staff, agency staff, agents, and volunteers. Equally, the term **member** includes senior members (Fellows) and junior members (students), and alumni of the College when they are handling or processing personal information on behalf of the College, except when they are acting in a private or external capacity.

4. This policy should be read in conjunction with:

- College Statutes;
- policies, procedures and terms of conditions of the College and, where relevant, similar documents of the University of Cambridge with regard to:
  - information security;
  - acceptable use of IT facilities (including use of personal devices);

5. This policy has been reviewed and approved by the College Council. It is reviewed at least once every five years. The College Council remains responsible for ensuring appropriate resources are in place to achieve compliance with data protection law in line with an appropriate overall risk profile.

Obligations of the College

6. The College upholds data protection law as part of everyday working practices, through:

a) ensuring all **personal information** (see Annex) is managed appropriately through this policy;
b) understanding, and applying as necessary, the **data protection principles** (see Annex) when processing personal information;
c) understanding, and fulfilling as necessary, the **rights given to data subjects** (see Annex) under data protection law;
d) understanding, and implementing as necessary, the College's **accountability obligations** (see Annex) under data protection law; and
e) the publication of **data protection statements** outlining the details of its personal data processing in a clear and transparent manner.

7. The College shall appoint a statutory data protection officer, who will be responsible for:

a) monitoring and auditing the College's compliance with its obligations data protection law, especially its overall risk profile, and reporting on such annually to the College;
b) advising the College on all aspects of its compliance with data protection law;
c) acting as the College's standard point of contact with the Information Commissioner's Office with regard to data protection law, including in the case of personal data breaches; and
d) acting as an available point of contact for complaints from data subjects.

8. The College shall otherwise ensure all members and staff are aware of this policy and any associated procedures and notes of guidance relating to data protection compliance, provide training as appropriate, and review regularly its procedures and processes to ensure they are fit for purpose.

9. Individual members and staff are responsible for:

a) completing relevant data protection training, as advised by the College;
b) following relevant College policies, procedures and notes of guidance;
c) only accessing and using personal information as necessary for their duties and/or other College roles;
d) ensuring personal information they have access to is not disclosed unnecessarily or inappropriately;
e) where identified, reporting personal data breaches, and co-operating with College authorities to address them; and
f) only deleting, copying or removing personal information when leaving the College as agreed with the College and as appropriate.

Non-observance of the responsibilities in paragraph 9 may result in disciplinary action against individual members or staff.

10. The obligations outlined above do not waive any personal liability for individual criminal offences for the wilful misuse of personal data under data protection legislation.

May 2018

Annex

1. Legal Definition of personal information

Personal information is defined as data or other information about a living person who may be identified from it or combined with other data or information held. Some "special category data" (formerly sensitive personal data) are defined as information regarding an individual's racial or ethnic origin; political opinion; religious or other beliefs; trade union membership; physical or mental health or condition; sexual life; or criminal proceedings or convictions, as well as their genetic or biometric information.

2. Data Protection Principles

The data protection principles state that personal data shall be:

- processed (i.e. collected, handled, stored, disclosed and destroyed) fairly, lawfully and transparently. As part of this, the College must have a 'legal basis' for processing an individual's personal data (most commonly, the processing is necessary for the College to operate a contract with them, the processing is necessary to fulfil a legal obligation, the processing is in the legitimate interests of the College and does not override their privacy considerations, or they have consented to the processing);
- processed only for specified, explicit and legitimate purposes;
- adequate, relevant and limited;
- accurate (and rectified if inaccurate);
- not kept for longer than necessary;
- processed securely.

3. Data Subject Rights

An individual's rights (all of which are qualified in different ways) are as follows:

- the right to be informed of how their personal data are being used. This right is usually fulfilled by the provision of 'data protection statements' which set out how an organisation plans to use an individual's personal data, who it will be shared with, ways to complain, and so on;
- the right of access to their personal data;
- the right to have their inaccurate personal data rectified;
- the right to have their personal data erased (right to be forgotten);
- the right to restrict the processing of their personal data pending its verification or correction;
- the right to receive copies of their personal data in a machine-readable and commonly-used format (right to data portability);
- the right to object: to processing (including profiling) of their data that proceeds under particular legal bases; to direct marketing; and to processing of their data for research purposes where that research is not in the public interest;
- the right not to be subject to a decision based solely on automated decision-making using their personal data.

4. Accountability

The College is required under law to:

- comply with data protection law and hold records demonstrating this;
- implement policies, procedures, processes and training to promote "data protection by design and by default";

- have appropriate contracts in place when outsourcing functions that involve the processing of personal data;
- maintain records of the data processing that is carried out across the College;
- record and report personal data breaches;
- carry out, where relevant, data protection impact assessment on high risk processing activities;
- cooperate with the Information Commissioner's Office (ICO) as the UK regulator of data protection law;
- respond to regulatory/court action and pay administrative levies and fines issued by the ICO.

5. Review of data used in College departments

Data requirements and the purposes for which data is held vary between College departments.

In order to ensure that data is held and used in a fair, accurate, and secure manner it is necessary for each relevant department to draw up a statement detailing the arrangements which will apply in that department. The policy statement should be produced by the Head of Department, in consultation with the relevant College Officer, and should cover the following:

- What types of Personal Data are held or processed in the department and for what purpose.
- For which categories of Data Subjects is Personal Data held.
- Which members of staff within the department have access to Personal Data.
- Are there any department-specific variations upon the College's general security provisions
- What is the policy operating within the department relating to the retention and deletion of Personal Data? The policy should ensure that no data is held longer than necessary, and that when it is retained there is a sound reason for its retention. It should state the arrangements for reviewing data at certain significant dates (for example, graduation or the completion of the admissions round), and the policy for weeding or destroying data at that point.

6. Security

All reasonable steps must be taken to ensure that personal data is stored and processed securely. This includes the following:

- Access to computer files containing Personal Data will be restricted using privilege levels and passwords.
- Administrative computer equipment will be sited in a secure location where access can be controlled.
- Computer screens will be sited so that they cannot be viewed by members of the public.
- Computer terminals will not be left unattended and should be logged-off at the end of a session.
- Redundant electronic data will be regularly wiped in accordance with the policy applying in each College department.
- Data will be backed up and stored securely.
- Where computer systems containing personal data are connected to an external network, a recognised firewall will be installed.
- All manual Files will be stored securely. It is the responsibility of each Head of Department to ensure that appropriate secure storage arrangements operate in each department.

7. Disclosure of Information to Third Parties

Personal Data will not be disclosed to third parties without the Data Subject's consent. This will apply even when an inquiry is made by a member of the person's family, their friends, local authorities, government bodies, and the police, and applies even when the request is for basic

information such as their address or telephone number in College. However, there are circumstances in which the College has a statutory duty to disclose information to public bodies.

The following are examples of ways in which requests for information from third parties should be handled:

1. If a telephone caller or visitor is trying to contact a student, the student's room number, address or telephone number should not be disclosed. An offer to pass a message to the student informing them of the inquiry is the appropriate response.

2. If a request for an e-mail address for an individual is received, the enquirer should first be referred to the e-mail search facility on the University web site. If the person cannot be identified there a message should be forwarded instead.

3. An e-mail address should only be provided following an enquiry relating to a member of staff if that address is already the published contact.

In other situations in which a request for information is made the matter should be referred to the Bursar. This is the case even when the inquiry comes from a public body such as a Council or the Police.

8. CCTV

The College's policy relating to the use of CCTV cameras and recording equipment is available at: https://www.emma.cam.ac.uk/about/documents/pdfs/CCTV%20Policy.pdf

9. Staff code of practice for data processing

The College recognises that all staff must have access to appropriate information in order to fulfil their job responsibilities. At the same time, data relating to students, Fellows, staff or others must be processed fairly and lawfully and in accordance with the Data Protection Principles at 2 above. These principles apply to the storage or use of all information about a living person, who can be identified from the data, or identified from the data in conjunction with other information. In order to avoid confusion, it should be assumed that these principles apply to all data stored or processed by the College. In order to comply with these principles, the following arrangements must be observed:

- You must obtain authorisation from your Head of Department before accessing or using administrative information.
- You must clearly label confidential information and ensure that such information is kept securely.
- When an office is left unoccupied it must be locked securely.
- Any password issued to you which gives you access to the College computer systems must be kept securely and kept to yourself.
- Any anti-virus arrangements or the use of anti-virus software, which is notified to you periodically by the College must be applied.
- You must ensure that any stored information is removed before disposing of old equipment.
- You must obtain authorisation before taking data or equipment out of the office in which you work.
- You should be aware that electronic mail is not a secure medium, and you must observe the College's e-mail and internet policy.
- You must not install or use any untested software without authorisation from your Head of department.

10. References

The author of a reference owes a duty of care to the person about whom it is written, and may be liable in damages to that person if loss is caused through negligence. Liability may come about through carelessness either as to matters of fact or in the formulation of opinion. The author of a reference has therefore an obligation to the subject of the reference. The author is also likely to have an obligation to the recipient of the reference.

The College has insurance that covers both itself and individual members of staff (as employees of the College) against claims arising from a reference. This covers references written by a member of staff in the context of his/her employment in the College – ie, references on behalf of students, fellow academics, other members of staff, etc. It does not cover references where the individual is acting in his/her private capacity (eg, a character reference on behalf of a friend or neighbour).

There are two principal aims of a reference:

- To confirm facts – to confirm the accuracy of the statements made in an application;
- To provide opinions – to give the referee's opinion as to the candidate's suitability for the post/course in question, and his/her potential for the future.

A reference relies on both facts and opinions, but these two should be clearly differentiated.

The following recommended guidelines relate specifically to student references, but the principles are equally applicable to all references:

- If you are likely to be asked to give a reference, prepare in advance, you will normally be asked to act as a referee by a student and it is therefore sensible to collect relevant information to make the composition of the reference a relatively easy task
- Try to be fair to both the student and the recipient of the reference.
- Ensure that the reference is factually accurate and complete
- Make sure that your opinions are clearly stated as opinions, are based on fact, and that you are qualified to give such opinions:
- Do not confuse fact and opinion: "on her performance to date, I would be surprised if X did not get a first class degree" is clearly an opinion; "she will get a first class degree" suggests that the matter is beyond doubt.
- Ensure that the opinions you state are honest opinions based on facts known to you. Do not make statements which you are not qualified to make. For example, "I consider X to be well suited to the post for which s/he has applied, and am happy to support his/her application" is better than "X will be a success in the post of…."
- For this reason, particular care should be taken where you are asked for a reference for a student who is not known to you. Do not give an opinion which is not your own, just because the person who knew the student has left. It is preferable to quote someone who has knowledge of the candidate, giving the source of the quote.
- There may be issues on which you are asked to express an opinion on which you have limited knowledge – eg honesty and integrity. Here you may have to say, for example, "…I know nothing that would lead me to question X's honesty…"
- Avoid using ambiguous or 'coded' language.

The same guidelines apply to references given over the telephone: do not be tempted to make incautious statements simply because they are not in writing. Ideally, references should not be given over the telephone and you should resist such requests other than in exceptional circumstances.

A copy of any reference you give should be placed on the relevant student file.

If you are challenged over a reference you have given, refer the matter to the Senior Tutor or Bursar as soon as possible.