St John's College

Data Protection Policy: an elaboration
(Personal information, its processing and privacy)

Purpose and scope

1. **The purpose of this document is to elaborate on College Standing Order J.2: Data Protection Policy**. Our Policy seeks 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 at any level or grade (whether permanent, fixed term or temporary) and including employees, retired but active members and staff, visiting Fellows, workers, trainees, interns, seconded staff, agency staff, agents, volunteers, and external members of College committees. 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, Ordinances and Regulations;
- staff employment contracts and comparable documents (which outline confidentiality obligations when processing information of the College);
- 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);
    - records management and retention;
    - any other contractual obligations on the College or the individual which impose confidentiality or information management obligations (which may at times exceed those of College policies with respect to storage or security requirements – e.g. for funded research).

5. Policy in respect of data protection is reviewed by the Head of Information Services and Systems at least once every two years, through a report to the College's Library and Records Committee. Any change in policy is approved by the College Council on the recommendation of that Committee.

Obligations of the College

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

a) ensuring all **personal information** is managed appropriately through this policy;
b) understanding, and applying as necessary, the **data protection principles** when processing personal information;
c) understanding, and fulfilling as necessary, the **rights given to data subjects** under data protection law;
d) understanding, and implementing as necessary, the College's **accountability obligations** 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. Definitions of these terms are found in the Annex below.

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 under 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 members and staff are aware of this policy and any associated procedures and notes of guidance relating to data protection compliance, and review regularly its procedures and processes to ensure they are fit for purpose.

9. Individual members and staff are responsible for:

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

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.

Last updated: May 2018

Annex

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.

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.

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 'privacy notices' (also known as '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.

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.