Corpus Christi College
University of Cambridge

DATA PROTECTION POLICY

Personal Information, its processing, and privacy

Purpose	To ensure compliance with data protection law in the UK (the General Data Protection Regulations (GDPR) and related EU and national legislation		
Author	JNER	Date	09.05.2018
Replaces	Data Protection Policy (due to GDPR updates)		
Approved by	Governing Body	Date	21.05.2018
Next Review date	Currently under review		

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 at any level or grade (whether permanent, fixed term, temporary or casual) and including employees, retired but active members and staff, visiting Fellows, supervisors, workers, trainees, interns, seconded staff, contracted staff, agency staff, work experience students, 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:

a) College Statutes, Ordinances and Regulations and Rules;
b) staff employment contracts and comparable documents (which outline confidentiality obligations when processing information of the College);

c) policies, procedures and terms of conditions of the College and, where relevant, similar documents of the University of Cambridge with regard to:

i. information security;
ii. acceptable use of IT facilities (including use of personal devices);
iii. records management and retention;
iv. 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. This policy is reviewed and approved by the Executive Body. It is reviewed regularly, with an initial review one year after the introduction of the GDPR. The Executive Body remains responsible for ensuring appropriate resources are in place to achieve compliance with data protection law in line with an appropriate overall risk profile.

6. When changes are made to this policy we will publish the updated version on our website and use other communications channels as we deem appropriate or necessary.

Obligations of the College

7. 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.

8. The College shall (jointly with other Colleges) appoint a statutory data protection officer (sDPO) based within the Office for Intercollegiate Services, who will be responsible for:

a) provision of advice in complex cases of data protection;
b) provision of support in the case of a data breach;
i. assessing whether a data breach is reported to the ICO, managing a breach with the ICO, including all communications and risk assessments, and maintaining records of all breaches for reporting to the individual College;
ii. supporting a College in reporting a data breach crime to the police;
iii. reviewing breaches across all Colleges to identify risks and trends;
c) provision of training support
i. provision of face to face data protection awareness training to College staff, supplementing online training available from the University and internal training by the College;

ii. provision of face to face data protection awareness guidance to governing bodies;
iii. the annual development and review of training and awareness courses;

d) undertaking paper based audit of College documentation and procedures, reviewing governance risk rating, and producing an appropriate report for the College;

e) undertaking audit visits for Colleges with identified high risks, involving attendance the College, interviewing appropriate personnel and producing an appropriate report; and

f) advising on data protection impact statements.

In addition the College shall nominate a Data Protection Coordinator, who will be responsible for:

g) managing **subject data access requests** and managing all **data subject rights requests**;

h) reporting all data breaches to the sDPO;
i. managing the impact of a data breach within the College;
ii. implementing any internal or external recommendations;
iii. liaising with the police if there is determined to be a crime; and
iv. determining and implementing risk measures to reduce the likelihood of breaches occurring.

i) ensuring that staff are appropriately and proportionally trained, depending on their roles, including advising the sDPO on the nature of training gaps;

j) assisting the sDPO in the provision of information;

k) creating, updating, and maintaining appropriate records, including but not limited to Data Protection Statements, asset registers and risk registers;

l) facilitating any audit visits of the sDPO; and

m) acting as the internal point of contact for advice on compliance with data protection law.

9. 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. It shall also maintain records of its information assets.

10. 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 contractual 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 this paragraph may result in disciplinary action against individual members or staff.

11. 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.

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 opinions; 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' or, especially in the context of websites, 'privacy policies') 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.