

## **Data Protection - Overview**

In carrying out its statutory duties, King's College needs to hold personal data for a variety of reasons. It strives to ensure that such data is held securely, and that it is used only in appropriate ways. To that end, the College Council has produced the following Data Protection Policy. In addition there are more detailed policies for particular groups of people, available through the links below. Please note that you may be included in more than one group.

The student unions (King's College Students Union and King's College Graduate Union) are independent charities and have their own Data Protection policies. Any data that is shared with the student unions is in accordance with our policies and is covered by a data sharing agreement.

All those acting on behalf of the College are required to observe and enforce these policies.

The controller for your personal data is King's College, King's Parade, Cambridge, CB2 1ST. 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](mailto: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 data, is the Freedom of Information Officer, who can be contacted via [foi@kings.cam.ac.uk](mailto:foi@kings.cam.ac.uk)

### **Purpose and Scope**

The purpose of this policy is to ensure compliance with data protection law in the UK (the UK Data Protection Act 2018 and the General Data Protection Regulation (Regulation (EU) 2016/679, 'GDPR'), as amended by the UK Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 and incorporated into UK law by section 3 of the European Union (Withdrawal) Act 2018). 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).

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.

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.

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).

This policy is reviewed by the College's Governing Body and approved by College Council. It is reviewed at least once every 2 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**

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

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

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

- 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;
- advising the College on all aspects of its compliance with data protection law;
- 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
- acting as an available point of contact for complaints from data subjects.

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.

Individual members and staff are responsible for:

- completing relevant data protection training, as advised by the College;
- following relevant College policies, procedures and notes of guidance;

- only accessing and using personal information as necessary for their contractual duties and/or other College roles;
- ensuring personal information they have access to is not disclosed unnecessarily or inappropriately;
- where identified, reporting personal data breaches, and co-operating with College authorities to address them; and
- only deleting, copying or removing personal information when leaving the College as agreed with the College and as appropriate.

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

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 information that relates to an identified or identifiable individual. Some types of personal data are considered likely to be more sensitive. These types of data are referred to as “special category data”). Special category personal data includes information regarding an individual’s racial or ethnic origin; political opinion; religious or philosophical beliefs; trade union membership; genetic data; health; sex life or sexual orientation.

### **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 is 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 (and in specified other circumstances);
- 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 regulator of data protection law;
- respond to regulatory/court action and pay administrative levies and fines issued by the ICO.

Document Details		
Responsible Officer	First Bursar	
Original Date	15.05.2018	
Next Review Date	April 2026	
Version Control		
Version No.	Approval Date	Change Description
1	2018/05/15	First approval
2	2019/01/21	Minor wording and formatting changes; alterations to the way data protection legislation is referenced. Approved by the First Bursar on behalf of Council.
3	2024/04/30	Minor wording and formatting changes; further alterations to the way data protection legislation is referenced; transfer of existing policy to pro-forma; removal of King's College School.