St Edmund's College
University of Cambridge

Data Protection Policy

Policy Statement

St Edmund's College is committed to protecting personal data and handling it lawfully, fairly, securely and transparently. This policy explains the College's overarching approach to compliance with applicable data protection and privacy legislation, including the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, the Privacy and Electronic Communications Regulations 2003 and, where relevant, amendments made by the Data (Use and Access) Act 2025. Where EU data protection law applies to a particular activity, the College will take appropriate steps to identify and comply with those obligations. It applies to the College's general processing of personal data and should be read alongside the College's privacy notices (also referred to as Data Protection Statements), records retention arrangements, information security requirements, complaints handling arrangements, and any more detailed procedures issued by the College from time to time.

Scope

This policy applies to all personal data processed by or on behalf of the College, whether held electronically, on paper, in image or audio form, or in any other format. It applies to all officers, employees, workers, agency staff, consultants, contractors, volunteers, committee members, Fellows, students, alumni or other members of the College community, whenever they process personal data on behalf of the College or in connection with College business.

For data protection purposes, the College is a separate legal entity and acts as a data controller in relation to the personal data it processes for its own purposes. The University of Cambridge and the other Cambridge colleges are separate controllers in their own right unless a specific arrangement provides otherwise. Where personal data is shared between the College and another organisation, the parties' respective roles and responsibilities must be identified and documented appropriately.

Related Documents

This policy should be read together with the College's more detailed documents and procedures, including as applicable:

- College Statutes and Ordinances;
- College Privacy Notices (also referred to as Data Protection Statements);
- Staff employment contracts and comparable documents (which outline confidentiality obligations when processing information of the College);
- Policies, procedures and terms and 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;
- Data breach reporting, DPIA screening, data sharing and procurement procedures or guidance;
- Any other contractual obligations on the College or the individual which impose confidentiality or information management obligations.

Core Commitments

The College will comply with the data protection principles and will ensure that personal data is:

- Processed lawfully, fairly and transparently;
- Collected for specified, explicit and legitimate purposes and not used in a way that is incompatible with those purposes;
- Adequate, relevant and limited to what is necessary;
- Accurate and, where necessary, kept up to date;
- Kept for no longer than is necessary;
- Protected by appropriate technical and organisational security measures; and
- Processed in a way that enables the College to demonstrate compliance with the above requirements.

The College will provide individuals with clear privacy information about how their personal data is used, including the purposes of processing, lawful basis, retention, recipients, rights, and complaint routes.

The College will identify and document an appropriate lawful basis for each processing activity. Where the College processes special category data, it will identify both an Article 6 lawful basis and an Article 9 condition. Where it processes criminal offence data, it will ensure that the processing is carried out under official authority or is authorised by domestic law, including by meeting an applicable Schedule 1 condition under the DPA 2018, and it will maintain an Appropriate Policy Document where required.

Where the College relies on legitimate interests, it will document its assessment of purpose, necessity and balance. Where the College relies on a recognised legitimate interest under the amended UK GDPR, it will document the relevant recognised legitimate interest condition, why the processing is necessary for that purpose, and how the processing remains fair, transparent and proportionate.

The College will embed data protection by design and by default into new projects, systems, procurement activity, data sharing arrangements, and operational changes.

Roles and Responsibilities

The Council has overall responsibility for ensuring that the College has an appropriate governance framework, sufficient resources, and appropriate oversight arrangements for data protection compliance.

The Senior Information Risk Owner ("SIRO"), the Bursar, is accountable for the College's overall information risk posture and for ensuring that information risk is properly escalated and managed.

The College Data Protection Lead ("CDPL"), the Governance, Risk & Compliance Manager, is responsible for the day-to-day coordination of data protection compliance, including policy implementation, advice, incident coordination, support on rights requests and complaints, maintenance of relevant registers, and liaison with key internal stakeholders.
The Data Protection Officer ("DPO") for the College is Intercollegiate Services Limited (ISL). The DPO is responsible for carrying out the functions required by data protection law, including informing and advising the College on its obligations, monitoring compliance, advising on Data Protection Impact Assessments, and acting as a point of contact for the Information Commission and for data subjects.

Managers and Heads of Department are responsible for ensuring that personal data within their area is handled in accordance with this policy, related procedures, and the principle of least privilege / need-to-know access. They must also ensure that staff in their areas can recognise and promptly escalate data protection complaints, rights requests, breaches and significant information risks.

All individuals in scope of this policy must:

- Complete training required by the College;
- Access and use personal data only where necessary for legitimate College purposes;
- Follow College rules on confidentiality, information security, retention and deletion;
- Keep personal data secure and avoid inappropriate disclosure;
- Report suspected or actual personal data breaches, losses, security incidents, data protection complaints or rights requests promptly through the College's reporting arrangements; and
- Return or securely delete College personal data when their role or engagement ends, in accordance with College instructions and retention requirements.

Failure to comply with this policy may result in disciplinary or other appropriate action. Nothing in this policy removes any personal liability that may arise under data protection or other law.

Documentation, Retention and Accountability

The College will maintain appropriate records of processing activities and other documentation necessary to demonstrate compliance, including, where relevant, privacy notices, retention information, processor contracts, data sharing arrangements, DPIAs, records of consent where consent is used, and records of personal data breaches. Documentation must be meaningful, sufficiently granular and kept up to date.

Personal data must be retained only for as long as necessary for the relevant purpose or as required by law, regulation, contractual obligation, safeguarding need, or legitimate archival or research requirements. Secure deletion or destruction must take place when data is no longer required, in accordance with the College's Confidential Destruction of Records Procedure. Retention periods are set out in the College's Retention Schedule.

Routine deletion or destruction must be suspended where records are reasonably required for a live or reasonably anticipated subject access request, freedom of information request, complaint, investigation, grievance, disciplinary process, safeguarding matter, insurance claim, legal claim or regulatory enquiry. Any such suspension should be proportionate, documented and lifted when no longer required.

Data Sharing, Processors and International Transfers

Personal data must only be shared where there is a lawful basis, the sharing is necessary and proportionate, and any wider legal or confidentiality duties have been considered. Where the College shares data regularly, on a large scale, or in a high-risk context, it should put in place an appropriate data sharing agreement, information sharing agreement, protocol or equivalent document setting out purpose, roles, standards, security and retention. This is particularly important in higher education contexts involving recurring student welfare, safeguarding or support-related data sharing.

Where a third party processes personal data on the College's behalf, the College must carry out appropriate due diligence and ensure that a compliant written contract is in place meeting Article 28 requirements, including confidentiality, security, support with rights requests and breaches, restrictions on sub-processing, audit / assurance provisions, and return or deletion at the end of the arrangement.

Where personal data is transferred outside the UK and the transfer rules apply, the College will ensure that an appropriate transfer mechanism and any supplementary measures required by law are in place before the transfer takes place.

Information Risk Management and Security

The College adopts a risk-based approach to the protection of personal data. Appropriate technical and organisational measures must be used to protect personal data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure, unauthorised access, or other misuse. Measures may include access controls, least-privilege permissions, multifactor authentication, encryption, secure disposal, supplier assurance, staff training, and incident response arrangements.

All personal data breaches, near misses, control failures and significant information risks must be reported promptly through the College's internal reporting mechanism so that they can be assessed, contained, investigated and documented. The College will keep a record of all personal data breaches, whether or not they are reportable to the Information Commission. Where a breach is likely to result in a risk to individuals' rights and freedoms, the College will notify the Information Commission without undue delay and, where feasible, within 72 hours. Where the risk is high, the College will also inform affected individuals without undue delay unless an exemption applies.

Data Protection Impact Assessments

The College will carry out a DPIA where a type of processing is likely to result in a high risk to individuals' rights and freedoms. DPIAs are an essential accountability tool and a key part of data protection by design. They must be considered at the earliest practical stage of any relevant project or change.

A DPIA screening exercise should be undertaken for new systems, technologies, projects, services, procurement activity or material changes involving personal data. A full DPIA will normally be required where, for example, the College is proposing large-scale processing of special category or criminal offence data, significant or systematic monitoring (including public area surveillance), new technologies or automated decision-making with significant effects, matching or combining datasets, or processing that materially affects vulnerable individuals such as students in crisis, children or vulnerable adults.

The College Data Protection Lead will maintain a central register of DPIAs. The DPO must be consulted on DPIAs and where a DPIA shows that the processing would still present a high risk that cannot be sufficiently mitigated, the College will consult the Information Commission before commencing the processing. DPIAs must be kept under review and updated if the project, risk profile or processing changes.

Individual Rights

The College will respect and facilitate individuals' rights under data protection law, subject to applicable qualifications and exemptions. These include the right to be informed, the right of access, the right to rectification, the right to erasure, the right to restriction, the right to data portability, and the right to object in the circumstances set out in law.

The College will also comply with the current rules on significant automated decisions. Where the College makes a significant decision based solely on automated processing, it must ensure appropriate safeguards are in place, including measures enabling the individual to receive information about the decision, make representations, obtain human intervention, and contest the decision. Significant solely automated decisions involving special category data are further restricted.

Requests to exercise data protection rights may be made verbally or in writing. The College will take proportionate steps to verify identity where necessary. Subject access requests will be handled without undue delay and normally within one month, subject to any lawful extension or pause permitted by law.

The College will maintain procedures for recognising, logging and coordinating rights requests, including requests made verbally, by email, through solicitors or other third parties, or to staff who do not normally handle such requests. Where a request is made by a third party, the College will take reasonable steps to verify authority to act. Searches will be reasonable and proportionate, and disclosures will be made securely, subject to applicable exemptions, restrictions and third-party rights.

Complaints

Any individual who is concerned that the College has mishandled personal data, failed to comply with data protection law, or failed to respond properly to a rights request may make a data protection complaint to the College.

Complaints should normally be sent to the College Data Protection Lead and may also be raised with the SIRO. However, a data protection complaint may be made by email, in writing, verbally, through a representative, or through any other channel by which it is received, including where it is sent to another College department or member of staff. Staff who receive a data protection complaint must escalate it

promptly in accordance with the College's internal procedures. The College will take reasonable steps to help individuals make complaints and to understand the process. Where necessary, the College may ask for proportionate evidence of identity or authority to act for another person but will not ask for more information than is reasonably necessary.

The College will acknowledge receipt of a complaint within 30 days of receiving it. The College will begin making appropriate enquiries without undue delay and will investigate the complaint fairly, proportionately and by reference to the circumstances of the case. The College will keep the complainant informed where the matter is complex, further enquiries are required, or there is likely to be a delay in providing an outcome.

Once the investigation is complete, the College will tell the complainant the outcome without undue delay. The outcome will explain the College's conclusions, the reasons for those conclusions, and any remedial action taken or proposed. Where appropriate, the response will address each issue raised and provide sufficient information to help the complainant understand how the College reached its view.

The College encourages individuals to raise data protection concerns with the College so that it has an opportunity to consider and, where appropriate, resolve them. Individuals also have the right to complain to the Information Commission and may do so at any point. Where a complainant remains dissatisfied with the College's response, they may complain to the Information Commission via its website.

The College will maintain a confidential record of data protection complaints, including the date received, acknowledgement, relevant communications and documents, outcome, actions taken, key themes, trends and response times. Complaint records will be retained only for as long as necessary and used for accountability, learning and service improvement purposes.

Training, Monitoring and Review

The College will provide training and awareness measures that are proportionate to role and risk. Training and awareness should help staff recognise data protection complaints, rights requests and breaches, and know how to escalate them promptly. Additional role-specific guidance and training may be required for those handling higher-risk data or functions, including HR, student welfare, safeguarding, admissions, governance, fundraising, alumni relations, estates / CCTV, and procurement.

The College will monitor compliance through review, audit, incident learning, complaints handling, and periodic updates to its documentation and controls. Policies and procedures will be reviewed and updated where necessary to reflect legal, operational or technological change.

Ownership and Review

This policy is owned by the SIRO and managed day-to-day by the College Data Protection Lead. It will be reviewed at least every two years, and sooner where there is a significant legal, regulatory, operational or technological change. College Council is responsible for approving the policy and for ensuring that the College has an appropriate compliance framework and resources in place.

Appendix 1: Key Definitions

- Personal data means any information relating to an identified or identifiable living individual. An individual may be identifiable directly or indirectly.
- Special category data means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data used for identification, health data, sex life data, or sexual orientation data. Criminal allegations, proceedings and convictions are not special category data; separate rules apply to them.
- Criminal offence data means personal data relating to criminal convictions and offences, allegations, investigations, proceedings and related security measures.
- Processing means any operation performed on personal data, including collection, recording, organisation, structuring, storage, use, disclosure, retrieval, erasure or destruction.
- Data controller means the person or organisation that determines the purposes and means of processing personal data. Processor means a person or organisation that processes personal data on behalf of a controller.

Appendix 2: Privacy Notice (Data Protection Statement) Log

This log records the College's current Privacy Notices (also referred to as Data Protection Statements) and provides version control for each notice. The Privacy Notices are maintained as linked controlled documents within the College's wider data protection framework and are reviewed alongside the Data Protection Policy on a two-year cycle. Any interim updates to individual notices will be recorded in this log but will not reset the overall scheduled review date, unless the change requires a wider review of the Policy.

Title	Version	Last Updated	Change Type	Next Scheduled Review
Alumni and Supporters	4	18 May 2026	Scheduled review	May 2028
College Members (Other than Students and Alumni)	4	18 May 2026	Scheduled review	May 2028
DBS (Dinner Booking System) Users and their Guests	3	18 May 2026	Scheduled review	May 2028
Health & Wellbeing Records	4	18 May 2026	Scheduled review	May 2028
Job Applicants and Candidates for Election to College (Non-Student) Membership	4	18 May 2026	Scheduled review	May 2028
OSTicket Users	3	18 May 2026	Scheduled review	May 2028
Staff	4	18 May 2026	Scheduled review	May 2028
Students	4	18 May 2026	Scheduled review	May 2028
Users of the College's Websites(s)	4	18 May 2026	Scheduled review	May 2028
Visitors and Guests	4	18 May 2026	Scheduled review	May 2028