Data Protection Policy

Key contact information:	
The Controller of Personal Data:	Trinity College, Trinity Street, Cambridge, CB2 1TQ
College Data Protection Lead:	Health, Safety and Data Protection Manager data.protection@trin.cam.ac.uk 01223 760027
Senior Information Risk Officer Responsible for Data Protection:	The Junior Bursar Junior.bursar@trin.cam.ac.uk 01223 338400
Data Protection Officer:	Office of Intercollegiate Services Ltd, 64 Bridge Street Cambridge CB2 1UR, College.dpo@ois.cam.ac.uk 01223 768745

If you have any concerns regarding how the College is managing your personal information, or if you require advice on how to exercise your rights within this policy, please contact the College Data Protection Lead in the first instance. If you continue to have concerns, you can contact The Office of Intercollegiate Service (OIS) as our designated Data Protection Officer.

Trinity College Cambridge (Ref: Z6239965) and Trustees of the Trinity College Staff Pension Scheme (Ref: Z5945092) are registered with the Information Commissioner's Office as organisations that processes personal data.

Version:	Date:	Review Date:	Author	Sign off by:
1	May 2018	January 2020	Junior Bursar	JB Office
2	January 2020	January 2021	Health, Safety and Data Protection Manager Review	JB Office
3	October 2020	October 2021	Health, Safety and Data Protection Manager General review	Council 27/11/2020
4	March 2023	March 2025	Health, Safety and Data Protection Manager (Ref to UK GDPR following Brexit)	Council
5	July 2025	July 2027 (or before if new Bill or adequacy changes)	Health, Safety and Data Protection Manager General review – approved by DPO (OIS)	Approved CM25.140(b)

Contents

Summary and Commitment

Trinity College is a Data Controller and Data Processor based on the context of the processes under the Data Protection Act 2018 (DPA) and the General Data Protection Regulations (UK) (GDPR).

The Data Protection Policy confirms Trinity College's commitment to protecting the privacy of the personal data of anyone affected by the undertaking of the College. The policy outlines legal and regulatory requirements under the UK GDPR and the DPA and sets out responsibilities to ensure compliance with relevant obligations. Additionally, information is referenced for providing instruction and guidance for those handling personal data.

Scope

This policy applies to all personnel as defined by the GDPR. In accordance with the regulations, it covers all forms of data storage and processing, regardless of format.

It applies to all Trinity Members and staff acting in an official capacity, including but not limited to:

- College staff (permanent, temporary, and contractors)
- Fellows and students
- Volunteers conducting work on behalf of the College
- Other official third parties

Failure to comply with this policy may result in disciplinary action.

Definitions

Personal data is defined as any information relating to an identified or identifiable natural living person (e.g. name, email address, photographs etc.).

The DPA or UK GDPR do not cover anonymised data if the data cannot be reverse engineered to identify the subject.

Some types of information are considered highly sensitive (Special Category Data) and must be afforded greater protection (e.g. race or ethnic origin, political opinions, biometric data etc.) – see 'Appropriate Policy Document for Special Category Data' for further details.

Roles and Responsibilities

College Master and College Council

Have overall responsibility and accountability for all Data Protection matters and must:

- Appoint a Senior Information Risk Officer (SIRO) to manage decision-making and ensure compliance.
- Ensure adequate resources are made available in the form of personnel, finance, and a forum for discussion.

Senior Information Risk Officer (SIRO)

Provides strategic leadership and oversight for data protection across the College by:

- Embedding data protection as a core consideration in strategic and operational decision-making.
- Ensuring risk management and data protection compliance are prioritised at a senior level.
- Appointing and supporting a College Data Protection Lead (CDPL) to manage day-to-day compliance.
- Appointing a Data Protection Officer (DPO) to provide independent advice and monitoring.
- Chairing the Data Protection Committee and setting direction for the data protection strategy.
- To act as the initial point of contact for data protection related complaints.

- Ensuring that College departments integrate data protection into their processes, with appropriate support.
- Overseeing arrangements for staff training and awareness-raising, in collaboration with the CDPL.
- Ensuring that audits and reviews are commissioned and acted upon, to assess compliance and manage risk.

College Data Protection Lead (CDPL)
Responsible for the implementation of data protection compliance across the College, by:

- Providing advice and guidance to the SIRO in developing a data protection strategy and in the wider discharge of their responsibilities.
- Developing, implementing, and updating data protection policies and procedures.
- Managing and coordinating the College's response to data breaches, including appropriate reporting to the SIRO and DPO.
- Supporting Heads of Department and other responsible persons with Data Protection Impact Assessments (DPIAs), and reporting outcomes to the DPO.
- Coordinating audit activity and ensuring accountability and ongoing compliance in collaboration with departments.
- Providing regular updates and compliance reports to the SIRO.
- Leading staff and College Member training and awareness activities, in consultation with the SIRO and DPO.
- Administering Subject Access Requests (SARs) in collaboration with relevant College personnel.

Data Protection Officer (DPO) – Office of Intercollegiate Services (OIS)
The Data Protection Officer is not a role directly related to, or responsible for, the operational activities of the College. However, their functions include:

- Informing and advising the College, its Fellows, and staff who process personal information of their obligations under the DPA and the UK GDPR.
- Monitoring the College's engagement with the DPA and the UK GDPR, and the extent to which its policies, procedures and practices align with these regulations.
- Undertaking regular audits to monitor compliance with relevant policies, procedures, and practices, and to review and advise on matters, including internal awareness-raising and training of College Members and staff.
- Providing advice, where requested by the College, on any required Data Protection Impact Assessments (DPIAs).
- Acting as the contact point for, and cooperating with, the Information Commissioner's Office (ICO), the UK's statutory supervisory authority for the DPA and the UK GDPR.
- Having due regard, in all of their functions, to the risks associated with personal information processing, considering the nature, scope, context and purposes of processing.

The Data Protection Officer from the Office of Intercollegiate Services also offers a point of relative independence for data subjects to enquire about any issues or concerns related to the processing of their personal data, or for advice on how they can exercise their rights under the DPA or UK GDPR.

Head of IT:
Advises the College in all matters relating to digital security and:

- Ensures this policy is observed within the IT department.
- Collaborates with the CDPL and the SIRO on all matters involving data protection.
- Ensures appropriate resources and support are in place for data protection compliance.

Head Porter:
Advises on all matters relating to the physical security of the site, which may impact the security of personal data.

Heads of Department/Managers and Supervisors
For larger departments with several managers and supervisors, it should be agreed who will carry out the following duties:

- Ensure this policy is observed within their department.
- Collaborates with the CDPL and the SIRO on all matters involving data protection.
- Enable staff within their department to attend relevant training.
- Ensure appropriate resources and support are available for data protection compliance.
- Lead by example and promote good practice on all data protection and information security matters.

All Employees and College Members
All Staff and College Members will:

- Complete relevant data protection training.
- Follow relevant procedures, advice and guidance depending on their role, regardless of whether access to and processing of personal data is through College-owned and managed systems, or through their own or a third party's systems and devices.
- When processing personal data on behalf of the College, staff will only access and use it as necessary for their contractual duties and/or other College roles and not disclose it unnecessarily or inappropriately.
- Recognise, report internally, and cooperate with any remedial work arising from personal data breaches.
- Recognise, report internally, and cooperate with the fulfilment of Subject Access Requests.
- Only delete or copy personal data when leaving the College with prior permissions from CDPL.

Data Protection Principles

The College will ensure that all personal data is:

- Processed lawfully, fairly, and in a transparent manner (lawfulness, fairness, and transparency).
- Collected only for specified, explicit and legitimate purposes (purpose limitation).
- Adequate, relevant, and limited to what is necessary in relation to the purposes for which it is to be processed (data minimisation).
- Accurate and where necessary kept up to date (accuracy).
- Not kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed (storage limitation).
- Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction, or damage (security, integrity, and confidentiality).
- Overseen by the SIRO, Heads of Department will demonstrate compliance with the principles by record keeping (accountability).

Lawfulness, fairness, and transparency

Trinity College shall maintain a Record of Processing Activities (ROPA) for personal data. The ROPA shall be reviewed on an annual basis by the Head of Department or key personnel responsible for the data.

Individuals have the right to access their data. All Subject Access Requests (SARS), and any related requests, shall be handled in line with the UK GDPR via the College Data Protection Lead (or delegated where appropriate)

All data processed by Trinity College must be undertaken on one of the following lawful bases: consent, contract, legal obligation, vital interests, public task, or legitimate interests.

- Heads of Department will record the lawful basis for processing data on the ROPA.
- Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data.
- Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent must be clearly available. The Head of Department or person responsible for the data must ensure such revocations are reflected accurately in the College's systems.

Note: Once consent has been given, it will only be valid for the original purpose for which it was provided.

Data Minimisation and Accuracy

Trinity College shall ensure that personal data are adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed. This should form part of the annual review of the ROPA by the Head of Department and/or responsible person, and as part of any significant change or additional information.

Retention

To ensure that personal data is kept for no longer than necessary, the CDPL shall put in place a Retention Policy. Each Head of Department/responsible person shall review the personal data and why/how it is processed annually.

The Retention Policy shall consider what data should/must be retained, for how long, and why.

Security

The Head of IT will advise the College on issues around data security within the IT system when applicable and shall ensure that personal data is stored securely, recommending modern, up-to-date software. They will ensure appropriate backup and disaster recovery solutions are in place.

The Head Porter will advise regarding the physical security of personal data when applicable and shall recommend reasonable security measures across the site.

Personal Data Breaches

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, the person discovering the data breach shall promptly initiate the Personal Data Breach Procedure.

All College Members who handle personal data must ensure that they observe and comply with the Personal Data Breach Procedure.

The CDPL will advise and assist on the reporting process and ensure that the DPO and the SIRO are alerted via the correct forum.

Monitoring and review

This policy will be reviewed biennially, or sooner if required due to legal/regulatory changes or as a result of any other significant change. It is the responsibility of all College Members to ensure they are familiar with the most up-to-date version of this policy.