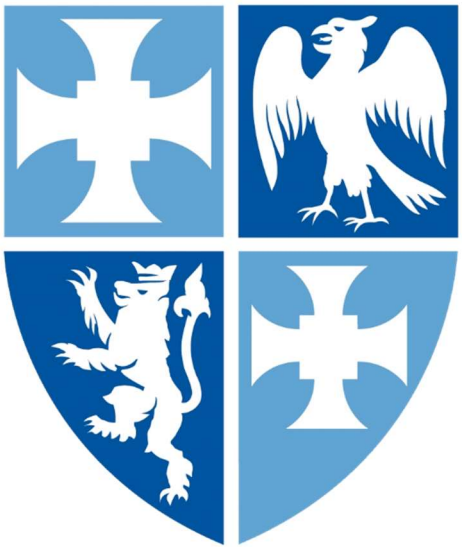
St. John's College, Durham

Data Protection Policy



Document Control

Version	Date of publication	Revisions	Date of next review
1.0	22.03.2024	n/a - first draft of policy	01.01.2025
1.1	31.03.2025	Removal of Research: GATBB, move to 2 yearly review.	01.02.2027

Policy approved by College Officers	14/02/2025
Policy approved by Audit & Risk Committee	04/03/2025
Policy approved by College Council	28/03/2025

Circulation

This Policy is made available to all staff and students via the St John's College website. An email notification will be sent following any update and provision of a hard copy will be made available to those without email access. All new employees are provided with a copy during their induction, and this is recorded on the induction checklist.

Contents

Introduction

In order for St John's College, Durham (the College) to deliver its core functions as a provider of teaching, learning and residential accommodation, to operate effectively as a business and to meet its legal obligations, the College needs to process personal data. The College, therefore, is a data controller.

Purpose

This policy provides a framework for compliance with data protection legislation.

Scope

This policy applies to all those individuals and organisations that are part of the College or that process personal data on behalf of the College, including but not limited to:

- Employees, consultants, contractors and temporary workers
- Students undertaking a programme of study and also students performing paid or voluntary work for the College
- Arms' length organisations associated with, and officially recognised by, the College
- Third parties associated with the College, such as research collaborators

Policy Statement

Lawful processing of personal data is vital to the successful operation and reputation of St John's College, and for maintaining the trust of our students, employees and other stakeholders. The College is committed to protecting the rights and freedoms of individuals in accordance with the provisions of data protection legislation. In order to achieve this, the College shall ensure that personal data is handled appropriately and consistently.

St John's College shall ensure that personal data is processed in accordance with the following principles:

1. lawful, fairness and transparency, by

- making public information about how we process data e.g., through *privacy notices*
- ensuring any consents to collect data are freely given, specific, informed, and unambiguous
- keeping records of what personal data is processed e.g., through *records of processing*
- enabling data subjects to exercise their rights to access, rectify, erase, or move their data
- enabling data subjects to exercise their right to object to processing or not be subject to automated decision-making including profiling

2. purpose limitation, by

- collecting personal data for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes

- allowing processing for archiving purposes in the public interest, scientific or historic research purposes or statistical purposes which is not incompatible with the purpose of collection
- only collecting data where there is a lawful purpose and only, collecting special category data where there is a lawful basis.

3. data minimisation, by

- collecting only the information that is required for the purpose
- anonymising data where possible at the earliest opportunity

4. accuracy, by

- taking reasonable steps to ensure that personal data is accurate
- keeping data up to date where necessary
- ensuring data can be corrected or erased without delay where appropriate

5. storage limitation, by

- keeping data in a form which permits identification of data subjects for no longer than is necessary
- personal data shall be stored for longer periods for archiving purposed in the public interest, scientific or historical research purposes or statistical purposes

6. integrity and confidentiality, by

- ensuring appropriate security measures are in place to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage including providing for arrangements to report data breaches
- using appropriate technical or organisational measures assessed according to the risk
- following policies on information security, IT regulations and guidance from Durham University Computer and Information Services (CIS) as amended from time to time

7. accountability, by

- acknowledging that St John's College, as a data controller, is responsible for compliance
- providing for responsibility to be assigned to the highest level of management with specific responsibilities being delegated as appropriate as set out below under roles and responsibilities
- providing for training in relation to individuals obligations under this policy
- providing for appointment of a Data Protection Officer to oversee compliance
- providing for reporting and assessments so that the College demonstrates compliance with the principles of data protection legislation
- ensuring third party processes agree to appropriate contractual obligations before processing data, see contractual arrangements for sharing data
- ensuring any data exports are subject to appropriate safeguards e.g., standard contractual clauses, see contractual arrangements for sharing data

Roles and responsibilities

College Council and Audit Committee
The College is the data controller and/or data processor as defined in the UK GDPR. The College's governing body, the **College Council**, has overall responsibility for the College's control and processing of data and also ensuring the development and encouragement of good information handling practices across the College. Governance level oversight of the college's responsibilities with regards GDPR is delegated to **Audit Committee**.

Data Protection Officer
The *Finance & Operations Director* is the statutory Data Protection Officer, who will:

- monitor and audit the College's compliance with its obligations under data protection law, especially its overall risk profile, and report on such annually to the College;
- in consultation with Durham University's Information Governance Unit (IGU), advise the College on all aspects of its compliance with data protection law;
- act 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;
- have oversight of procedures relating to data management including Data Subject Access Requests; and
- act as an available point of contact for complaints from data subjects or requests for further information about the College's approach to data handling.

Managerial and Supervisory Roles
All those who manage personal data or supervise / line manage roles who manage personal data will:

- ensure the development and encouragement of good information handling practices within their respective areas of responsibility;
- ensure direct reports undertake relevant data protection training required for their role;
- maintain and update the relevant section of the privacy notices that relate to their specific area of responsibility;
- maintain and update the relevant sections of the *Record of Processing Activities*.

All Members of Staff
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.

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 listed responsibilities by members of staff may result in disciplinary action against individual members or staff.

Privacy Notices

Privacy Notices inform data subjects about how the College processes their personal data. A list of Privacy Notices by categories of data subjects are held in *Appendix 2* of this policy. This list is reviewed as a minimum annually, by Audit Committee, and more frequently if there is significant change.

Those in **Managerial and Supervisory Roles** shall consider the need to provide additional notifications such as specialist privacy notices or specific signage (e.g. for CCTV capture) on a case by case basis and seeking advice from the **DPO** where necessary.

Records of Processing

The **DPO** will oversee the compilation of records of processing relying on information provided by those in **managerial and supervisory roles**. Records of processing will be updated from time to time. Those with direct responsibility for the management of personal data must verify the content of the *Records of Processing Activities* for their data when requested from time to time and as minimum, annually.

Data Subject Rights

Data subjects have the following rights regarding data processing, and the data that is recorded about them:

- Right to be informed – Article 12
- Right of access – Article 15
- Right to rectification – Article 16
- Right to erasure (right to be forgotten) – Article 17
- Right to restrict processing – Article 18
- Right to data portability – Article 20
- Right to object – Article 21
- Rights in relation to automated decision making and profiling – Article 22

The College is mandated under Article 12 of the UK GDPR to facilitate the rights of data subjects, for instance, responding to subject access requests (SAR). Subject Access Requests will be processed in line with ICO guidelines, seeking support from Durham University Information Governance Unit where necessary.

Basis of Processing

The College will determine the appropriate lawful basis of processing for all personal data obtained directly or indirectly from data subjects, including students.

Data subjects will be informed of the purpose for processing using the 'Privacy Notice' published on the College's website or by similar means.

Where personal data is obtained from third parties, the data subject will be sent a notice in compliance with Article 14 of the UK GDPR.

Where a special category of personal data, as defined by Article 9 of the UK GDPR, is processed, this shall be for one of the defined 10 exceptions as defined in Article 9.

Security

All staff and students are responsible for ensuring that any personal data which the College holds, and for which it is responsible, is kept secure and is not, under any conditions, disclosed to any third party unless that third party has been specifically authorised to receive the personal data and, where required, signed an NDA.

Disclosure

The College is under a lawful obligation to ensure that personal data is not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, the police, without a legitimate purpose for doing so.

All staff and students should exercise caution when asked to disclose personal data, held on another individual, to a third party, and will be required to attend specific training that enables them to deal effectively with the risk associated with any such disclosure of personal data.

Notwithstanding the foregoing it should be borne in mind that the disclosure of information is relevant to, and necessary for, the conduct of normal College business.

Requests to provide data for one of these reasons must be supported by appropriate paperwork and all such disclosures must be specifically authorised by the DPO.

Retention

The retention period for each category of personal data will be detailed in *Record of Processing Activities* with the criteria used to determine this period, including any statutory obligations to retain personal data. The principles that inform the retention and deletion schedule are outlined in *Appendix 3*.

Personal data must be disposed of securely in accordance with the sixth data processing principle – processed in an appropriate manner to maintain security, thereby protecting the "rights and freedoms" of data subjects.

Personal Data Breaches

The College will investigate incidents involving a possible breach of data privacy legislation in order to ensure that, where necessary, appropriate action is taken to mitigate the consequences and prevent a repetition of similar incidents in future. Depending on the nature

and severity of the incident, it may also be necessary to notify the individuals affected and/or the ICO. A breach will occur where, for example, personal data is disclosed or made available to unauthorised persons or personal data is used in a way that the individual does not expect.

Incidents involving failures of IT systems or processes must be reported to the Durham University Computer Information Services (CIS) immediately. A subsequent report must then be made to the College's DPO.

All other incidents must be reported directly to the College's DPO at the earliest possible opportunity.

Disciplinary Action

All staff and students are to adhere to this policy and its intent. Failure to do so may result in disciplinary action being taken. Such action might include written or verbal warnings or instant dismissal in circumstances that amount to gross misconduct.

The College reserves the right to take appropriate disciplinary action against contractors and self-employed service providers who fail to comply with this policy. Such actions include, but are not limited to, the termination of any contract with the College.

Contractual arrangements for sharing personal data

Third parties processing personal data on behalf of the College shall comply with this policy alongside any specific terms and conditions agreed contractually. Data Users must ensure that a written agreement between the parties to a data sharing arrangement is in place where personal data is shared on a systematic basis or there is a large-scale transfer of personal data. Such agreements shall, as a minimum, include:

- The classes, or specific items, of personal data to be shared
- The source(s) of the personal data
- The objective(s) of the data sharing arrangement
- The lawful basis for sharing the personal data
- The individuals/groups that will have access to the personal data
- The methods by which the personal data will be transferred, including any controls for protecting the data from loss, destruction or unauthorised access
- The frequency with which the personal data will be shared
- Storage requirements for the personal data, including any controls for protecting the data from loss, destruction or unauthorised access
- The parties' responsibilities for ensuring the accuracy of the personal data
- Retention and disposal requirements
- Arrangements for enabling data subjects to exercise their rights
- Processes and procedures for handling information security incidents.

When a Data User seeks to share data overseas, especially outside of the European Economic Area (EEA), appropriate safeguards such as valid standard contractual clauses and an assessment of equivalence must be made. It should be noted that providing access to data or placing data on a cloud service with access by others in a country outside the EEA would qualify as sharing overseas for this purpose.

Guidance will be sought from Durham University IGU in relation to the content of contracts and export of personal data.

Training

All employees of the College (grades 3 and above) whose work involves accessing personal data, shall:

- be provided by HR with a copy of this Policy alongside their contract of employment and be required to confirm to HR that they have read and understood it
- be required to undertake the University's online *Data Protection and Information Governance* training module (the training) and successfully pass the integral test within 4 weeks of receiving IT access. If an employee declines to undertake the module or repeatedly fails the test, HR will investigate and where the reason for this is deemed unacceptable by the Director of Finance and Operations, the employee's access to the University's IT systems will be removed
- be required to refresh the training on an annual basis.

All employees whose work does not ordinarily involve accessing personal data and all employees who do not have a work email account (this includes employees and casual workers on grades 1 and 2, drivers, cleaners, caretakers, catering assistants, maintenance supervisors and other maintenance workers, plant operatives, security officers and porters) shall:

- be required to watch the ICO video *Data protection explained in three minutes* (https://www.youtube.com/watch?v=YJInlE99vSs)

All casual workers (including students) and agency temps whose work involves accessing personal data, shall:

- be required to undertake the training as soon as possible after receiving IT access. If they are not to receive IT access, then they should receive a paper version of the training module. The onus is on supervisors to ensure that such casual staff and agency temps are aware of their responsibilities.
- be required to refresh the training on an annual basis.

A general data protection training course shall be made available to all employees through Durham University's Oracle training programme.

Appendix 1 – UK GDPR Definitions

Child – in the United Kingdom of Great Britain and Northern Ireland, the processing of personal data of a child under the age 13, in relation to 'Information Society Services', is only lawful if the consent of the person with parental responsibility has been obtained. The controller shall make reasonable efforts to verify that consent is given or authorised by the person who is the holder of parental responsibility over the child.

Data controller – the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Data subject – any living individual who is the subject of personal data held by an organisation.

Data subject consent - means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data.

Establishment – the main establishment of the controller in the EU will be the place in which the controller makes the main decisions as to the purpose and means of its data processing activities. The main establishment of a processor in the EU will be its administrative centre. If a controller is based outside the EU, it will have to appoint a representative in the jurisdiction in which the controller operates to act on behalf of the controller and deal with supervisory authorities.

Filing system – any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

ICO – Information Commissioner's Office, is the UK's independent body set up to uphold information rights.

Personal data – any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Personal data breach – a breach of security leading to the accidental, or unlawful, destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. There is an obligation on the controller to report personal data breaches to the supervisory authority and where the breach is likely to adversely affect the personal data or privacy of the data subject.

Processing – any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use,

disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Profiling – is any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person, or to analyse or predict that person's performance at work, economic situation, location, health, personal preferences, reliability, or behaviour. This definition is linked to the right of the data subject to object to profiling and a right to be informed about the existence of profiling, of measures based on profiling and the envisaged effects of profiling on the individual.

Special categories of personal data – personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Third party – a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

Appendix 2 – Privacy Notices

Privacy Notices inform data subjects about how the College processes their personal data. Privacy Notices for the following categories of data subjects will be published by College:

- Alumni, Donors and Supporters
- College Library Readers
- College Security and CCTV: Staff, Students and Visitors
- Conference And Events: Attendees, Organisers and Others Involved with Conference and Events
- Governance: Members of College Council & Sub-Committees
- Research Grants: ECLAS
- Staff: Job Applicants/Potential Applicants
- Staff: Office Holders or Employees
- Students: Applicants & Prospective Students
- Students: Current
- Suppliers And Contractors who have a Financial, Administrative or Accounting Connection with the College

Appendix 3 - Retention Schedule

St John's College has determined its retention periods taking account of the following factors:

- The general approach to retention adopted by Durham University
- The College's business needs
- Legislative requirements, such as accounting and employment law
- The operational limitations faced by a college, such as ours, with limited people resources

The adoption of standardised periods allows for review and disposal of data during the summer vacation or other times in the year when staffing can be available more easily to ensure compliance with our retention policies.

Retention periods for specific items of personal data are included in the *Records of Processing Activities* held separately and located here: **S:\Compliance\GDPR & data sharing**. In determining these, the College has had regard for the following general principles:

1. **Sensitive personal data** is retained until **one year** after the end of the academic year following leaving office or the cessation of employment or study, subject to the need to extend this beyond that date for specific circumstances in order to comply with statutory or accounting requirements.

2. **Short term records**, for example relating to the management of events, are retained until the end of the academic year in which the creation of the record took place, subject to the need to extend this beyond that date for specific circumstances in order to comply with statutory or accounting requirements.

3. **Admissions records** for unsuccessful applicants or applicants who do not enrol are retained for one year after the end of the relevant application cycle. Some records for successful applicants are retained permanently as part of the College's archive; the remainder is retained for **six years** after the end of the academic year when they cease to be a registered student.

4. **Records relating to the Principal, College Officers and students** are retained permanently in the College's archive. Related financial information will be deleted one year after the end of the year following departure from office or the cessation of employment or study, except where legislation requires retention for a longer period or where financial information needs to be retained for other specific purposes, such as where any outstanding financial obligation has not been met.

5. **Records relating to all other staff**, are retained until seven years after the end of the year following the cessation of their employment except where legislation requires retention for a longer period or where financial information needs to be retained for other specific purposes, such as where any outstanding financial obligation has not been met.

6. **Other operational data** is retained until the end of the academic/financial year following the end of employment, SCR membership, a period of study or a contract for works, subject

to any need to extend beyond that date in order to comply with statutory or accounting requirements.

7. **Supplier and client records** are retained for the duration of the supplier/client relationship or potential future supplier/client relationship or as required for VAT or other legislative requirements, if longer. Normal requirements are for these records to be retained for a period of **six years** from the date when they were generated for compliance purposes, unless there is compelling justification for the data to be retained for a longer period, for example in connection with legal advice, or in relation to auditing obligations.

8. **Safeguarding information** regarding a concern or allegation relating to a member of staff will be retained for a period of 70 years, according to the College's *Safeguarding Policy for Children, Young People and Vulnerable Adults.*