Name of Policy: Data Protection Policy

RESPONSIBLE COMMITTEE: General Purposes Committee

RESPONSIBLE OFFICER: Principal Bursar

LINKED DOCUMENTS: Information Security Policy, Regulations relating to the use of Information Technology Facilities, Privacy Notice

Annual Review date: Hilary Term

1. Purpose and scope

This policy provides a framework for ensuring that the College meets its obligations under the UK General Data Protection Regulation (GDPR) and associated legislation ('data privacy legislation').[1]

It applies to all processing of personal data carried out for a College purpose, irrespective of whether the data is processed on non-college equipment or by third parties.

'Personal data' means any information relating to an identifiable living individual who can be identified from that data or from that data and other data. 'Processing' means anything that is done with personal data, including collection, storage, use, disclosure and deletion.

More stringent conditions apply to the processing of special category personal data.

'Special category' means 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 an individual, data concerning health or data concerning an individual's sex life or sexual orientation.

This policy should be read in conjunction with the accompanying guidance, which provides further detail and advice on practical application, as well as any other documents that impose confidentiality or data management obligations in respect of information held by the College.

This policy does not cover the use of personal data by members of the College when acting in a private or non-College capacity.

[1] This includes all legislation enacted in the UK in respect of the protection of personal data as well as the Privacy and Electronic Communications Regulations (PECR).

2. Background

The processing of personal data underpins almost everything the College does. Without it, students cannot be admitted and taught; staff cannot be recruited; living individuals cannot be researched; and events cannot be organised for alumni or visitors.

We are responsible for handling people's most personal information. By not handling personal data properly, we could put individuals at risk.

There are also legal, financial and reputational risks for the College. For example:

- If we are not able to demonstrate that we have robust systems and processes in place to ensure we use personal data properly we might lose our ability to carry out research projects requiring access to personal data, particularly in the medical field.
- Reputational damage from a breach may affect public confidence in our ability to handle personal information.
- The Information Commissioners Office (ICO), which enforces data privacy legislation, has the power to fine organisations for serious breaches.

3. Principles

The processing of personal data must comply with data privacy legislation and, in particular, the six data privacy principles.

In summary, they require that personal data is:

- processed fairly, lawfully and in a transparent manner;
- used only for limited, specified stated purposes and not used or disclosed in any way incompatible with those purposes;
- adequate, relevant and limited to what is necessary;
- accurate and, where necessary, up-to-date;
- not kept for longer than necessary; and
- kept safe and secure.

In addition, a new accountability principle requires us to be able to evidence compliance with these principles.

4. Aims and commitments

The College handles a large amount of personal data and takes seriously its responsibilities under data privacy legislation. It recognises that the mishandling of an individual's personal data may cause them distress or put them at risk of identity fraud. As a result, it is committed to:

- complying fully with data privacy legislation;

- where practicable, adhering to good practice, as issued by the ICO or other appropriate bodies; and
- handling an individual's personal data in a careful and considerate manner that recognises the importance of such information to their privacy and welfare.

The College seeks to achieve these aims by:

- ensuring that staff, students and other individuals who process data for College purposes are made aware of their individual responsibilities under data privacy legislation and how these apply to their areas of work. For example, employment contracts include a clause drawing the attention of the employee to data privacy legislation and the College's data protection policy;
- providing suitable training, guidance and advice. The College requires any member of staff who uses a computer for work to complete the University's online training course on data privacy and information security. The online course will be supplemented by bespoke on-site training, where appropriate, together with regular talks and presentations organised by the University or Conference of Colleges.
- incorporating data privacy requirements into administrative procedures where these involve the processing of personal data, particularly in relation to major information systems (the concept of 'privacy by design');
- operating a centrally coordinated procedure (in order to ensure consistency) for the processing of subject access and other rights-based requests made by individuals; and
- investigating promptly any suspected breach of data privacy legislation; reporting it, where necessary, to the ICO; and seeking to learn any lessons from the incident in order to reduce the risk of reoccurrence.

5. Roles and responsibilities

The College is a data controller and a data processor under the GDPR.

The Data Protection Officer (DPO) is responsible for:

- monitoring internal compliance,
- advising on the College's data protection obligations
- acting as a point of contact for individuals and the ICO
- supporting privacy by design and privacy impact assessments;
- coordinating the regular completion and updating of Records of Processing Activity (ROPAs) and privacy notices;
- complying with subject access and other rights-based requests made by individuals for copies of their personal data;
- investigating and responding to complaints regarding data privacy (including requests to cease the processing of personal data); and
- keeping records of personal data breaches, notifying the ICO of any significant breaches and responding to any requests that it may make for further information.

In fulfilling these responsibilities, the DPO will involve, and draw on support from, College Officers and Heads of Department.

College Officers and Heads of Department and all those in managerial or supervisory roles throughout the College are responsible for ensuring that the processing of personal data in their department conforms to the requirements of data privacy legislation and this policy. In particular, they must ensure that:

- new and existing staff, visitors or third parties associated with the College who are likely to process personal data are aware of their responsibilities under data privacy legislation. This includes drawing the attention of staff to the requirements of this policy, ensuring that staff who have responsibility for handling personal data are provided with adequate training and, where appropriate, ensuring that job descriptions for members of staff or agreements with relevant third parties reference data privacy responsibilities.
- adequate Records of Processing Activities are kept;
- data protection requirements are embedded into systems and processes by adopting a 'privacy by design' approach and undertaking privacy impact assessments where appropriate;
- privacy notices are provided where data is collected directly from individuals or where data is used in non-standard ways;
- data sharing is conducted in accordance with College guidance;
- requests from the DPO for information are complied with promptly; and
- data privacy risks are included in the College's risk management framework and considered by senior management on a regular basis.

Anyone who processes personal data for a College purpose – including staff, students and volunteers – is individually responsible for complying with data privacy legislation, this policy and any other policy, guidance, procedures, and/or training introduced by the College to comply with data privacy legislation. For detailed guidance, they should refer to the University's Guidance on Data Protection. In summary, they must ensure that they:

- only use personal data in ways people would expect and for the purposes for which it was collected;
- use a minimum amount of personal data and only hold it for as long as is strictly necessary;
- keep personal data up-to-date;
- keep personal data secure, in accordance with the College's Information Security Policy;
- do not disclose personal data to unauthorised persons, whether inside or outside the College;
- complete relevant training as required;
- report promptly any suspected breaches of data privacy legislation, in accordance with the procedure in section 6 below, and following any recommended next steps;

- seek advice from the DPO where they are unsure how to comply with data privacy legislation; and
- promptly respond to any requests from the DPO in connection with subject access and other rights-based requests and complaints (and forward any such requests that are received directly to the DPO promptly).

6. Breaches of data privacy legislation

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. Breaches (including suspected breaches) are to be immediately reported to the DPO and College's IT Office.

7. Compliance

The College regards any breach of data privacy legislation, this policy or any other policy and/or training introduced by the College from time to time to comply with data privacy legislation as a serious matter, which may result in disciplinary action. Depending on the nature of the breach, an individual may also find that they are personally liable (for example, it can be a criminal offence for a member of the College to disclose personal information unlawfully).

8. Complaints

You have the right to make a data protection complaint to us. All complaints will be acknowledged within 30 days of receiving them, handled without undue delays and you will be informed of the outcome of your complaint.

Complaints should be directed to the DPO at: data.protection@sjc.ox.ac.uk or by post to:
Data Protection Officer
St John's College
St Giles
Oxford OX1 3JP

9. Further information

Questions about this policy and data privacy matters in general should be directed to the DPO at: data.protection@sjc.ox.ac.uk or by post to:
Data Protection Officer
St John's College
St Giles
Oxford OX1 3JP

10. Data Protection Legislation

Any law, statute, declaration, decree, directive, legislative enactment, order, ordinance, regulation, rule or other binding restriction (as amended, consolidated or re-enacted from time to time) which relates to the protection of individuals with regards to the processing of personal data to which a party is subject, including the Data Protection Act 2018 and retained EU law version of the General Data Protection Regulation ((EU) (2016/679)) ("GDPR") and any successor legislation to the Data Protection Act 2018 and the GDPR.

10. Related policies

This policy should be read in conjunction with related policies and regulations, including the:

- Information Security Policy
- Privacy Notice; and
- Regulations relating to the use of Information Technology Facilities.

POLICY HISTORY

Date of GB approval	*Brief summary of changes*	*Confirmation that linked documents have been updated if necessary*	*Date College policy register updated*
May 2018	Original document approved by GB	Yes	Yes (Sandra Campbell)
Jan 2019	Document reviewed by Committee and subsequently approved by GB	Confirmed	Yes (Sandra Campbell)
Jan 2020	Section 9 updated to reflect legal changes. Document reviewed by Committee and subsequently approved by GB.	Confirmed	Yes (Kate Doornik)
Jan 2021	Document approved by Committee and subsequently approved by GB	Confirmed	Yes (Sandra Campbell)
Jan 2022	Document approved by Committee and subsequently approved by GB	Confirmed	Yes (Iris Burke)
Jan 2023	Inserted link to University guidance; changed policy owner to Principal Bursar; included postal address for DPO. Approved by GB	Confirmed	Yes (Iris Burke)
HT 2024	Policy reviewed by GB, linked to Privacy Notice	Confirmed	Yes (Iris Burke)
HT 2025	Policy reviewed, updated data protection legislations (clause 9); agreed by GB	Confirmed	Yes (Iris Burke)
HT 2026	Policy reviewed, no amendments; agreed by GB	Confirmed	Yes (Iris Burke)
TT 2026	Added para 8 on Complaints; agreed by GB	Confirmed	Yes (Iris Burke)