SOMERVILLE
COLLEGE
UNIVERSITY OF OXFORD

Data Protection Policy

1. Purpose and scope

"Data protection is the fair and proper use of information about people. It's part of the fundamental right to privacy – but on a more practical level, it's really about building trust between people and organisations. It's about treating people fairly and openly, recognising their right to have control over their own identity and their interactions with others, and striking a balance with the wider interests of society" *(ICO website accessed 5/6/19)*

Somerville College recognises and respects the rights conferred on individuals and their personal data by the GDPR and the Data Protection Act 2018. These include the right to be informed, to access their data, to have their data rectified, erased, restricted, or extracted, to object to the processing of their data and the right to challenge automatic decision making using their personal data.

This policy provides a framework for ensuring that the Principal and Fellows of Somerville College ('the College') meet their obligations under the General Data Protection Regulation (GDPR) and associated legislation ('data privacy legislation'). Its provisions cover all staff members of college, temporary and permanent, academic and support staff. It should be read in conjunction with other documents and policies that impose confidentiality or data management obligations in respect of information held by the College, including but not limited to, the employee handbook, the information security policy and the college privacy notices. It applies to all processing of personal data carried out for a College purpose, irrespective of whether the data is processed on non-university equipment or by third parties. This policy does not cover the use of personal data by members of the College when acting in a private or non-College capacity. An example of this might be the exchange of private mobile phone numbers and subsequent correspondence about non college matters between employees.

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', or 'sensitive' data 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.

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 and any mishandling of that information could put individuals at risk.

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

- 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 up to 4% of global annual turnover or €20,000,000, whichever is greater, for serious breaches.

3. Principles

The processing of personal data must comply with data privacy legislation and, in particular, the six data privacy principles. These principles are explained in detail in the website of the Information Commissioner

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/

In summary, they require that personal data is:

• processed fairly, lawfully and in a transparent manner;	We must specify our legal basis for collecting personal data and disclose it to our data subjects whenever we ask for their details (this can be done via a link to our privacy notice)
• used only for limited, specified stated purposes and not used or disclosed in any way incompatible with those purposes;	Data collection must have a stated purpose e.g. to enable us to contact a student about college matters and not be used for other purposes e.g. non-college/university-related advertising.
• adequate, relevant and limited to what is necessary;	We should not collect personal data 'just-in-case'. For example if we don't use data concerning race or gender then it should not be collected.
• accurate and, where necessary, up-to-date;	We should actively seek to keep data accurate through mailings, online forms etc
• not kept for longer than necessary; and	For example, photographs from old events should be deleted if not being transferred to the archives.
• kept safe and secure.	For example, data should not be removed from the college on unencrypted data sticks

In addition, we are required 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. This is effected through heads of departments who are required to refresh their data processing documents with the GDPR team on an annual basis and consult with the team when new processes are implemented.
- providing suitable training, guidance and advice. The University's online training course on data privacy and information security is compulsory for all members of the University and the College. The online course is supplemented by bespoke on-site training, where appropriate, along with regular updates in college internal communications and at Governing Body meetings
- 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'). This is most often effected through Data Protection Impact Assessments conducted by the GDPR team. ;
- 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

Governing Body

The Governing Body of Somerville College has executive responsibility for ensuring that the College complies with data privacy legislation.

Data Protection Fellow

This is the member of Governing Body to whom the responsibility of monitoring compliance is delegated. The Data Protection Fellow will ensure that the college appoints a DPO who has the appropriate professional experience and knowledge of data protection law and a data protection team who can implement GDPR within the College. They will ensure that the DPO and the Data Protection team are enabled to work independently and with sufficient resources to undertake the role and that Governing Body considers the college's compliance with GDPR on a termly basis with a regular update from the DPO/GDPR team.

Data Protection Officer (DPO)

The College has appointed IT Governance Ltd to act as their DPO. The DPO is responsible for monitoring internal compliance, advising on the College's data protection obligations and acting as a point of contact for individuals and the ICO.

Data Protection Compliance Team

The Data Protection Compliance team (the Head of Information Services and the Assistant Archivist) is responsible for ensuring policies and procedures within the college are compliant with Data Protection Legislation and for implementing the provisions of relevant legislation. The Data Protection Compliance team is also responsible for responding to DSARs and for investigating Data Breaches and Data Protection complaints. They can be contacted on dpo@some.ox.ac.uk

Information Security Working Group

The Information Security Working Group meets termly and the minutes are submitted to IT Committee. It is responsible for:

- establishing and maintaining policies and procedures at a central level to facilitate the College's compliance with data privacy legislation;
- establishing and maintaining guidance and training materials on data privacy legislation and specific compliance issues;
- supporting privacy by design and privacy impact assessments;
- maintaining Data Protection awareness amongst staff throughout the college

In fulfilling these responsibilities, the team may also involve, and draw on support from, representatives from departments.

Heads of Departments within the College

Heads of Department are responsible for ensuring that the processing of personal data in their department conforms to the requirements of data privacy legislation and this policy. Their departments are reviewed annually during the internal data processing audit by the GDPR team. 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 and ensuring that their staff undergo the University's Online Information Security Training Module when appropriate. This training module is part of staff IT induction and is also required to be refreshed each year. Non-completers are monitored and contacted on an annual basis.
- adequate records of processing activities are kept and reviewed annually and retention policies adhered to. Any new processes are implemented in consultation with the GDPR team
- data protection requirements are embedded into systems and processes by adopting a 'privacy by design' approach in consultation with the GDPR team 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 the University guidance at https://www.infosec.ox.ac.uk/privacy
- any data privacy risks are included in the College's risk management framework and considered by senior management on a regular basis; and
- College policies and procedures are adopted where appropriate.

Others processing personal data for a College purpose eg. staff, students and volunteers

Anyone who processes personal data for a College purpose 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 and any relevant College policies and procedures. 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 e.g. don't use student email addresses for notifications about non-college or university events;

- 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 both College's and the University's Information Security Policy
- do not disclose personal data to unauthorised persons, whether inside or outside the College or University;
- 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;

6. Breaches of data privacy legislation

Data breaches occur when a breach of security leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. Examples might be the theft of a laptop or the accidental sharing of an email with an unintended recipient. 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 Oxford University Computer Emergency Response Team (OxCert) within 4 working hours of discovery. OxCert will liaise, as appropriate, with the Information Compliance Team.

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. Further information

Questions about College policy and data privacy matters in general should be directed to the Data Protection team at: dpo@some.ox.ac.uk. General questions about Information Security within the University should be directed to the Information Security Team at: infosec@it.ox.ac.uk. More information about data protection and channels for complaints may be found at https://ico.org.uk/

9. Review and development

This policy, and supporting guidance, went into effect on 30 June 2019. It will be reviewed annually.