MERTON COLLEGE DATA PROTECTION POLICY

1. Approval and binding effect

1.1. The following Policy was **approved** by the Governing Body of Merton College ("the College") on Wednesday, 3rd October 2018.

1.2. Any amendments to the Policy require the Governing Body's approval. The Governing Body approved amendments to this Policy on 21 March 2021 and 19 June 2023.

1.3. This Policy is to be reviewed **annually** to ensure any new developments are covered and protected.

1.4. All members of the College and all employees or other staff of the College are bound by these Regulations and **must** comply with them. For the avoidance of doubt any reference to employees or staff shall include permanent, temporary, contract and other support staff as applicable ; and "members" includes both Fellows and Junior Members.

1.5. The College regards any breach of data privacy legislation, of this Policy or of any other policies or regulations 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).

2. Scope and Purpose

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

2.2. 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.

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

2.4. This Policy should be read in conjunction with the accompanying Regulations, which provide further detail on practical application, as well as any other documents that impose confidentiality or data management obligations in respect of information held by the College.

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

3. Background

[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 (EC Directive) Regulations 2003.

3.1. The processing of personal data underpins almost everything the College does. Without it, students cannot be admitted and taught; employees 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.

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

3.2.1. Reputational damage from a breach may affect public confidence in our ability to handle personal information.

3.2.2. The Information Commissioner's Office ("ICO"), which enforces data privacy legislation, has the power to fine organisations up to £17.5 million or 4% of global annual turnover (whichever is higher) for serious breaches.

4. Principles

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

4.2. In summary, they require that personal data be:

4.2.1. processed fairly, lawfully and in a transparent manner;

4.2.2. used only for limited, specified stated purposes and not used or disclosed in any way incompatible with those purposes;

4.2.3. adequate, relevant and limited to what is necessary;

4.2.4. accurate and, where necessary, up to date;

4.2.5. not kept for longer than necessary; and

4.2.6. kept safe and secure.

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

5. Aims and Commitments

5.1. 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:

5.1.1. complying fully with data privacy legislation;

5.1.2. where practicable, adhering to good practice, as issued by the ICO or other appropriate bodies; and

5.1.3. handling an individual's personal data in a careful and considerate manner that recognises the importance of such information to their privacy and welfare.

5.2. The College seeks to achieve these aims by:

5.2.1. ensuring that employees, 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;

5.2.2. providing suitable training, guidance and advice. The University's online training course on data privacy and information security is available to all members of the University. The online course is supplemented by bespoke on-site training, where appropriate.

5.2.3. 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');

5.2.4. 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

5.2.5. 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 reccurrence.

6. Roles and responsibilities

6.1. The **Finance Bursar** is accountable to the Governing Body for the management of data privacy risks to the College's members and employees.

6.2. The **Finance Committee** has responsibility for overseeing the management of data privacy risks to the College's members and employees.

6.3. The **Data Protection Officer** ("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. In addition, the DPO is responsible for :

6.3.1. developing policies and procedures to facilitate the College's compliance with data privacy legislation;

6.3.2. ensuring the availability of guidance and training materials on data privacy legislation and specific compliance issues;

6.3.3. supporting privacy by design and privacy impact assessments;

6.3.4. responding to requests for advice from members and employees of the College;

6.3.5. coordinating a College-wide register exercise to capture the full range of processing that is carried out;

6.3.6. complying with subject access and other rights-based requests made by individuals for copies of their personal data;

6.3.7. investigating and responding to complaints regarding data privacy (including requests to cease the processing of personal data); and

6.3.8. 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.

6.4. **Supervising College Officers and Heads of Department (or equivalent)** are responsible for ensuring that the processing of personal data in their area of supervision or department conforms to the requirements of data privacy legislation and this policy. In particular, they must ensure that:

6.4.1. employees, visitors or third parties who are likely to process personal data are aware of their responsibilities under data privacy legislation: this includes but is not limited to drawing the attention of employees, visitors, and third parties to the requirements of this policy, ensuring that employees who have responsibility for handling personal data are provided with adequate training and, where appropriate, ensuring that job and role descriptions for employees or agreements with relevant third parties refer to data privacy responsibilities;

6.4.2. adequate records of processing activities are kept (for example, by undertaking register exercises);

6.4.3. data protection requirements are embedded into systems and processes by adopting a 'privacy by design' approach and undertaking privacy impact assessments where appropriate;

6.4.4. privacy notices are provided where data is collected directly from individuals or where data is used in non-standard ways;

6.4.5. data sharing is conducted in accordance with University guidance;

6.4.6. requests from the DPO for information are complied with promptly;

6.4.7. data privacy risks are considered by supervising College Officers and Heads of Department on a regular basis; and

6.4.8. departmental policies and procedures are adopted where appropriate and implemented.

6.5. **Anyone who processes personal data for a College purpose e.g. Fellows, Lecturers, students, other employees and other College members** is individually responsible for complying with data privacy legislation, this policy and any other policy, guidance, procedures, and/or training introduced by the University to comply with data privacy legislation. In summary, they must ensure that they:

6.5.1. only use personal data in ways people would expect and for the purposes for which it was collected;

6.5.2. use a minimum amount of personal data and only hold it for as long as is strictly necessary;

6.5.3. keep personal data up to date;

6.5.4. keep personal data secure, in accordance with the College's Information Security Policy and related regulations;

6.5.5. do not disclose personal data to unauthorised persons, whether inside or outside the College;

6.5.6. complete relevant training as required;

6.5.7. report promptly any suspected breaches of data privacy legislation, in accordance with the procedure in section 6 below and the College's Data Protection Breach Regulations, and following any recommended or required next steps;

6.5.8. seek advice from the DPO where they are unsure how to comply with data privacy legislation; and

6.5.9. 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).

7. Breaches of data privacy legislation

7.1. The College **shall** 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.

7.2. Where a breach is identified or suspected the College's **Data Protection Breach Regulations** apply and **must** be followed.

8. Further information

Questions about this policy and data privacy matters in general should be directed to the DPO at: dpo@merton.ox.ac.uk.

9. Related policies

This policy **should** be read in conjunction with related policies and regulations, including the **Information Security Policy**; **Data Protection Breach Regulations**; and **Regulations relating to the use of Information Technology Facilities**.

10. Review and development

This Policy **shall** be reviewed and updated annually by the Finance Bursar and the DPO to take account of ICO guidance and national legislation and **shall** be approved by the Governing Body after review by the Finance Committee and the Statutes and Bylaws Committee.