MERTON COLLEGE INFORMATION SECURITY 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 this Policy require the Governing Body's approval. The Governing Body approved amendments to this Policy on 19 June 2023.

1.3. This Policy shall be reviewed **annually** to ensure that 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" include both Fellows and Junior Members.

1.5. This Policy shall be communicated to users and relevant external parties, and a link to it will be provided from the College's website.

1.6. Wilful failure to comply with this Policy and the Baseline will be treated extremely seriously by the College and may result in disciplinary action against a group and/or an individual.

2. Scope and Purpose

2.1. This Policy outlines the approach of the College to information security management and provides the guiding principles and responsibilities to ensure the College's information security objectives are met.

2.2. This Policy is applicable across the College and individually applies to:

2.2.1. all individuals who have access to the College's information and technologies;

2.2.2. all facilities, technologies and services that are used to process the College's information;

2.2.3. information processed, in any format, by the College pursuant to its operational activities;

2.2.4. internal and external processes used to process the College's information; and

2.2.5. external parties who provide information processing services to the College.

2.3. The College's objectives for information security are that :

2.3.1. a culture is embedded to ensure that in all teaching, research and administration activities information security is considered;

2.3.2. individuals are aware and kept informed of their information security responsibilities;

2.3.3. information risks are identified, managed and mitigated to an acceptable level;

2.3.4. authorised users can securely access information to perform their roles;

2.3.5. facilities, technologies and services adequately balance usability and security;

2.3.6. implemented security controls are pragmatic, effective, and measurable;

2.3.7. contractual, regulatory and legal obligations relating to information security are met; and

2.3.8. incidents are effectively managed and resolved, and are learnt from to improve the College's control environment.

2.4. Support and guidance for departments are offered by the Merton IT Department which in turn is supported by the central University of Oxford Information Security team, "InfoSec".

3. Information Security Policy Framework ("ISPF")

3.1. Information is critical to the College's operations and failure to protect information increases the risk of financial and reputational losses. The College is committed to protecting information, in all its forms, from **loss of confidentiality, integrity, and availability**, ensuring that:

3.1.1. all relevant employees and members of the College complete information security awareness training;

3.1.2. information security risk is adequately managed and risk assessments on IT systems and business processes are performed where appropriate;

3.1.3. all relevant information security requirements of the College are covered in agreements with any third-party partners or suppliers, and compliance against these is monitored;

3.1.4. appropriate information security controls are implemented to protect all IT facilities, technologies, and services used to access, process and store the College's information;

3.1.5. all information security incidents are reported in a timely manner via appropriate internal channels, information systems are isolated, and incidents properly investigated and managed;

3.1.6. Information Asset Owners are identified for all the College's information assets, assets are classified according to how critical and sensitive they are, and rules for their use are in place; and

3.1.7. information security controls are monitored to ensure they are adequate and effective.

3.2. To provide the foundation of a pragmatic information security framework, the College will implement a set of minimum information security controls as set out in College regulations and the College's handbooks (to be known as 'the Baseline').

3.3. Where research, regulatory or national requirements exceed the Baseline, controls will be increased at necessary service or project level. Where it is not possible or practicable to meet the Baseline, exceptions will be documented to justify the deviation and appropriate compensating controls will be put in place. The Baseline will support the College in achieving its information security objectives.

4. Responsibilities and Compliance

4.1. The following bodies and individuals have specific information security responsibilities:

4.1.1. The **Finance Bursar** is accountable to the Governing Body for management of the information security risks to the College's Fellows, employees, Junior Members and other members.

4.1.2. The **Finance Committee** has responsibility for overseeing the management of the information security risks to the College's Fellows, employees, Junior Members and other members.

4.1.3. The **Domestic Bursar** is responsible for establishing and maintaining such arrangements as may be necessary to ensure the availability, integrity and confidentiality of the College's information.

4.1.4. The **Data Protection Officer** is (as set out in more detail in the Data Protection Policy) responsible for monitoring internal data protection compliance, advising on the College's data protection obligations and acting as a point of contact for individuals and the ICO.

4.1.5. The **Head of IT** is responsible for the implementation of information security arrangements for the computer and digital information systems operated internally by the College. The Head of IT is responsible for the provision of expert technical advice in relation to computer and digital information security arrangements with any third party partners or suppliers.

4.1.6. **Users** are responsible for making informed decisions to protect the information that they process.

4.2. The College shall conduct information security compliance and assurance activities, facilitated as appropriate by the University's Information Security Team, to ensure information security objectives and the requirements of the ISPF are met.

5. Review and Development

This Policy, and supporting ISPF documentation, shall be reviewed and updated annually by the Finance Bursar, the Domestic Bursar, and the Data Protection Officer and approved by the Governing Body after review by the Finance Committee and the Statutes and Bylaws Committee to ensure that they **remain operationally fit for purpose**; **reflect changes in technologies**; **are aligned to relevant best practice**; **and support continued regulatory, contractual and legal compliance**.