MERTON COLLEGE NETWORK ACCEPTABLE USE REGULATIONS

1. Approval and binding effect

1.1. These Regulations were **approved** by the Governing Body of Merton College (“the College”) on Monday 3 December 2018.

1.2. Any amendments to these Regulations 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, all employees or other staff of the College, and all other Users (as defined below) 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” shall include both Fellows and Junior Members.

2. Definitions

2.1. “College network” means a physical or virtual data network service where the configuration and gateway are within the control of Merton College or a suitably connected third party.

2.2. “DPO” means the College’s Data Protection Officer.

2.3. "Users" are Fellows, employees, students, consultants, contractors, agents and other authorised users accessing Merton College IT systems and applications.

2.4. ‘MUST’ and ‘SHALL’ mean that the item is an absolute requirement.

‘MUST NOT’ and ‘SHALL NOT’ mean that the item is absolutely prohibited.

‘SHOULD’ means that there may exist valid reasons in particular circumstances not to comply with a particular item, but the full implications must be understood and carefully weighed before choosing a different course.

‘SHOULD NOT’ means that there may exist valid reasons in particular circumstances when particular behaviour is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behaviour described with this label.

3. Scope and purpose

3.1. These Regulations outline the College’s approach to the acceptable use of the College and University networks to ensure that the College’s security objectives are met. Anyone who connects a computer or other device to the College network must abide by the Regulations provided here.

3.2. These Regulations are applicable across the College and individually apply to all individuals who connect their computers and other devices to the College network.

4. Use of the College Network

4.1. Anyone who connects a computer or other device to the College network **must** comply with the University's Regulations Relating to the use of Information Technology Facilities (IT Regulations 1 of 2002) as amended from time to time.[1]

4.2. In particular, Users **must not** use College network facilities or IT for any of the following:

4.2.1. any unlawful activity;

4.2.2. the creation, transmission, storage, downloading, or display of any offensive, obscene, indecent, or menacing images, data, or other material, or any data capable of being resolved into such images or material unless specifically approved for academic related reasons;

4.2.3. the creation, transmission, or display of material which is designed or likely to harass another person in breach of the University's Harassment Policy;

4.2.4. the creation or transmission of defamatory material about any individual or organisation;

4.2.5. the sending of any e-mail that does not correctly identify the sender of that e-mail or attempts to disguise the identity of the computer from which it was sent;

4.2.6. the sending of any message appearing to originate from another legal or natural person, or otherwise attempting to impersonate another person;

4.2.7. the transmission, without proper authorisation, of e-mail to a large number of recipients, unless those recipients have indicated an interest in receiving such e-mail, or the sending or forwarding of e-mail which is intended to encourage the propagation of copies of itself;

4.2.8. automatic forwarding of emails received at any email address within the ox.ac.uk domain to any email address outside that domain;

4.2.9. the creation or transmission of or access to material in such a way as to infringe a copyright, moral right, trade mark, or other intellectual property right;

4.2.10. private profit, except to the extent authorised under the user's conditions of employment or other agreement with the University or a college; or commercial purposes without specific authorisation;

4.2.11. gaining or attempting to gain unauthorised access to any facility or service within or outside the University, or making any attempt to disrupt or impair such a service;

[1] https://governance.admin.ox.ac.uk/legislation/it-regulations-1-of-2002

4.2.12. the deliberate or reckless undertaking of activities such as may result in any of the following: (a) the waste of staff effort or network resources, including time on any system accessible via the university network; (b) the corruption or disruption of other Users' data; (c) the violation of the privacy of other Users; (d) the disruption of the work of other Users; (e) the introduction or transmission of a virus into the network.

4.3. Any password, authorisation code, etc. given to a user shall be for that user's use only, and must be kept secure and not disclosed to or used by any other person.

4.4. Distributed file sharing programs which are commonly used to distribute copyrighted material must not be used, including but not limited to BitTorrent, Kazaa, eMule, uTorrent, Limewire, Thunder, Vuze, and Ares.

5. Mobile Devices

5.1. The security of mobile devices shall be the responsibility of the user. If purchased by the College the responsibility shall be that of the assigned user.

5.2. The College shall not be responsible for the payment of any mobile fines (roaming, data charges) incurred, which shall be the responsibility of the user.

5.3. Users of mobile devices connected to the College network or used to access College data shall comply with the College's Mobile Device Security Policy.

6. Responsibilities

The following bodies and individuals have specific information security responsibilities as provided in the College's Information Security Policy and Data Protection Policy:

6.1. 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.

6.2. 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.

6.3. 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.

6.4. 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.

6.5. The **DPO** is (as set out in more detail in the Data Protection Policy) 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.

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

7. Compliance

The College regards any breach of data privacy legislation, of these Regulations 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.

8. Review and development

These Regulations **shall** be reviewed and updated annually by the Finance Bursar and the Data Protection Officer to take account of guidance from the Information Commissioner's Office and national legislation and **shall** be approved by the Governing Body after review by the Finance Committee and the Statutes and Bylaws Committee.

9. Related policies and regulations

These Regulations should be read in conjunction with related policies and regulations, including the **Information Security Policy**, the **Data Protection Policy**, the **IT Password Policy**, **Mobile Device Security Regulations**, and the **Data Protection Breach Regulations**.