MERTON COLLEGE MOBILE DEVICE SECURITY REGULATIONS

1. Approval and binding effect

1.1. These Regulations were **approved** by the Governing Body of Merton College ("the College") on Wednesday 3 October 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" includes both Fellows and Junior Members.

2. Definitions

2.1. "DPO" means the College's Data Protection Officer.

2.2. "PIN" means a personal identification number.

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. Information is critical to the College's operations and failure to protect information increases the risk of financial and reputational losses and failure to comply with obligations imposed by legislation. The College is committed to protecting information, in all its forms, from loss of confidentiality, integrity and availability.

3.2. Mobile devices represent a significant risk to information security and data security. If the appropriate security applications and procedures are not applied they can be a conduit for unauthorised access to data controlled by the College ("the College's data") and IT infrastructure.

3.3. These Regulations are intended to ensure that Merton College's security objectives are met in relation to the use of mobile devices such as (but not limited to) smartphones, tablets, and computer laptops.

3.4. These Regulations are applicable across the College and individually apply to:

3.4.1. all individuals who have access to Merton College information and technologies;

3.4.2. any mobile hardware that is used to access or store College information-resources, whether the device is owned by the College or not.

4. Mobile Device Security

4.1. Any mobile device that is used to access the College's data **must** have the remote-wipe capability of the device turned on to protect against potential loss or theft.

4.2. Any mobile device that is used to access the College's data **must** be protected from unauthorised access by for example a PIN of at least 4 digits, a pass-phrase, or the use of biometric security, and be configured to ensure an automatic lock after a period of inactivity.

4.3. Applications installed on any mobile device that is used to access the College's data **must** be trustworthy applications from reputable sources.

4.4. Any mobile device that is used to access the College's data **must** be configured to receive software updates from the manufacturer and other relevant third-parties, and updates should be installed within one week of being released. Mobile device firmware **must** be kept up to date using the manufacturer's website or, for installed software, that of the relevant provider (e.g. Apple in the case of iTunes). Patches **must** be checked regularly and applied when available.

4.5. A mobile device that has undergone a 'jailbreak' procedure **must not** be used to access the College's data; i.e., software/firmware which is designed to gain access to any unintended functionality should not be installed. (For the avoidance of doubt, to 'jailbreak' a mobile device is to remove the limitations imposed by the manufacturer. This gives access to the operating system, thereby unlocking all its features and enabling the installation of unauthorised software.)

4.6. Devices **must not** be connected to any host computer which does not have up-to-date anti-virus software and enabled anti-malware protection.

4.7. Mobile devices **must not** be used to carry special category personal data (as defined by Article 9(1) of the UK General Data Protection Regulation) for longer than necessary.

4.8. Mobile devices **must** be encrypted to protect any data that is on the device.

4.9. Any mobile device that is owned by the College **should** be security-marked and a record of all serial numbers and identifying information **must** be made.

4.10. Devices **must** store any user-saved passwords in an encrypted password store.

4.11. A mobile device **must not** be left unlocked when unattended.

4.12. Mobile devices left in locked vehicles **must** be kept out of sight.

4.13. Where it is not practicable to comply with any of the requirements set out above, exceptions shall be documented to justify the deviation and appropriate compensating controls should be put in place on the advice of the IT Department.

4.14. When the loss or theft of any mobile device which has access to College data is identified or suspected the College's **Data Protection Breach Regulations** apply and **must** be followed.

5. Responsibilities

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

5.1. 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.

5.2. 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.

5.3. 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.

5.4. 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.

5.5. 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.

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

6. 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.

7. 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.

8. 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**, **Network Acceptable Use Regulations**, and the **Data Protection Breach Regulations**.