MERTON COLLEGE IT PASSWORD POLICY

1. Approval and binding effect

1.1. The following Policy was **approved** by the Governing Body of Merton College ("the College") on 19 April 2023.

1.2. Any amendments to this Policy require the Governing Body's approval.

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

1.4. All members of the College, all employees of the College, all departments within the College, and all other Users (as defined below) are bound by this Policy and are required to comply with it.

2. Definitions

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

2.2. "Passphrase" is a series of unrelated words that can be used as a password. Three words are much easier to remember than a series of random characters, letters and numbers, yet they are much harder to hack.

"Password" is a secret series of characters that enables a User to access a system, computer, file or application.

"Phishing" is a cybercrime in which a target or targets are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords.

"National Cyber Security Centre" The NCSC is the UK's technical authority for cyber threats. It is part of the Government Communications Headquarters (GCHQ) and has several roles in NIS.

"NIS" is intended to establish a common level of security for network and information systems. These systems play a vital role in the economy and wider society, and NIS aims to address the threats posed to them from a range of areas, most notably cyber-attacks.

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

2.3. ‘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. The Scope and Purpose of this Policy

3.1. This Policy outlines the approach of Merton College to Password management and provides the guiding principles and responsibilities to ensure the College's security objectives are met. It is intended to provide a single point of access for all Users who require information and guidance on this subject.

3.2. All Users access a variety of IT resources, including computers and other hardware devices, data storage systems, and other accounts. Passwords are a key part of IT's strategy to make sure only authorised people can access those resources and data.

3.3. All Users who have access to any of those resources are responsible for choosing strong Passwords and protecting their log-in information from unauthorised people.

3.4. The purpose of this Policy is to make sure all College resources and data receive adequate Password protection. This Policy covers all Users who are responsible for one or more accounts or have access to any resource that requires a Password.

3.5. The importance of constantly updating system Passwords and the responsibility each individual User has for their log-in details are addressed in this Policy and the implications of other Users accessing another's account are made clear.

3.6. If a computer system or data held within a drive are misused, altered or deleted the User logged on will be held solely responsible.

3.7. Support and guidance for departments is offered by the College's IT Department which in turn is supported by the central University of Oxford Information Security team, "InfoSec".

4. Password creation

4.1. All Passwords **should** be reasonably complex and difficult for unauthorised humans or computers to guess. Users **must** use multi-factor authentication (two-step verification) wherever supported.

4.2. Users **should** choose Passwords that are at least sixteen characters long and contain a combination of upper- and lower-case letters, numbers, punctuation marks and other special characters.

4.3. In addition to meeting those requirements, users **should** also use common sense when choosing Passwords. They **must not** reuse old Passwords and basic combinations that are easy to crack. For instance, choices like "password," "password1" and "Pa$$w0rd" are equally bad from a security perspective.

4.4. A Password **should** consist of a memorable passphrase that is easy for the user to remember. For example "Surfing-Housing-Kittens1!" is a Passphrase that satisfies complexity requirements but is easier to remember than random characters.

4.5. Users **must** choose unique Passwords for all their College accounts and **must not** use a Password they already use for a personal account.

4.6. Default Passwords — such as those created for new users when they start or those that protect new systems when they're initially set up — **must** be changed as quickly as possible.

4.7. If the security of a Password is in doubt– for example, if it appears that an unauthorised person has logged in to the account — the Password **must** be changed immediately and the incident **must** be treated as an actual or suspected data breach and reported in accordance with College's Data Protection Breach Regulations.[1]

5. Protecting Passwords

5.1. Users **must not** share their Passwords with anyone else, including co-workers, managers, administrative assistants, IT staff members, etc. Everyone needing access to a system will be given their unique Password.

5.2. Users **must not** share their Passwords with any outside parties, including those claiming to be representatives of a business partner with a legitimate need to access a system.

5.3. Users **should** take steps to avoid phishing scams and other attempts by hackers to steal Passwords and other sensitive information. All Users will receive training on how to recognise these attacks.

5.4. Users **must not** put Passwords into writing and keep them at their workstations or anywhere where they could readily be connected with their accounts. See 4.4 for advice on creating memorable but secure Passphrases.

5.5. Users **must** report any suspicious account activity or if they suspect that their account may have been compromised to the Merton IT Department immediately. An actual or suspected data breach **must** be reported in accordance with the College's Data Protection Breach Regulations (see also 4.7).

6. Implementation, Review, and Amendment

6.1. All Heads of Department **must** ensure that their staff are aware of this Policy. This should be undertaken as part of induction and supervision.

6.2. The DPO in co-operation with the Finance Bursar, the Sub-Warden, and the Senior Tutor **must** ensure that the Fellows and Junior Members of the College are aware of these Regulations and their requirements.

6.3. This Policy **shall** be reviewed and updated annually by the Finance Bursar and the DPO and approved by the Governing Body after review by the Finance Committee and the Statutes and Bylaws Committee

---

[1] Any member of the College who discovers, suspects or receives a report of a breach (or suspected breach) **must** inform the DPO (or if the DPO is not available the Finance Bursar or the Domestic Bursar) and the Head of IT immediately.

Any member of the College's staff who discovers, suspects or receives a report of a breach (or suspected breach) **must** their Head of Department and the Head of IT immediately. They **must** also inform the DPO.

7. References

National Cyber Security Centre advice for system owners responsible for determining Password policies and identity management within their organisations : https://www.ncsc.gov.uk/collection/passwords/updating-your-approach

8. Useful Contacts

Data Protection Officer: dpo@merton.ox.ac.uk - 01865 276310 (College Lodge)

IT Department: it-support@merton.ox.ac.uk - 01865 276310 (College Lodge)

Head of IT: head.of.it@merton.ox.ac.uk - 01865 276310 (College Lodge)