MERTON COLLEGE IT ADMINISTRATOR USAGE POLICY

1. Approval and binding effect

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

1.5. Failure to comply with this Policy may result in disciplinary action being taken as appropriate.

2. Definitions

2.1. "Administrator Access" is to be understood for the purposes of this Policy as a level of access above that of a normal user. This definition is intentionally vague to allow the flexibility to accommodate varying systems and authentication mechanisms.

2.2. "Access Control" is the process that limits and controls access to resources of a computer system.

2.3. "Access Privileges" are systems permissions associated with an account, including permissions to access or change data, to process transactions, create or change settings, etc.

2.4. "Administrator Account" is a use account with privileges that have advanced permissions on an IT system that are necessary for the administration of this system.

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

2.6. "Privileged Accounts" are system or application accounts that have advanced permissions (as compared to regular user account permissions) on such systems or applications. Examples of user accounts with privileges include: administrative and super user accounts.

2.7. "Service or Application Accounts" are user ID's created on IT systems or applications, which are associated with specific access privileges on such systems and applications. These accounts are not associated with a person but an IT system, an application (or a specific part of an application) or a network service.

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

2.9. '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. This Policy outlines the approach of Merton College to the granting of Administrator Access, the usage of Administrator Accounts, Administrator Account restrictions, Administrator Account review and the revocation of Administrator Accounts. It is intended for use by all Users employed by Merton College with Administrator Access. It is intended to provide a single point of access for all IT Administrators who require information and guidance on this subject.

3.2. In a traditional Microsoft Windows environment, members of the Power Users, Local Administrators, Domain Administrators and Enterprise Administrators groups would all be considered to have Administrator Access.

3.3. In a traditional UNIX or Linux environment, Users with root level access or the ability to sudo would be considered to have Administrator Access.

3.4. In an application environment, Users with 'super-user' or system administrator roles and responsibilities would be considered to have Administrator Access.

3.5. This Policy applies to any User account in that utilisation of access privileges is reserved solely for the intended business purpose.

4. Policy

4.1. Granting of Administrator Access.

4.1.1. The College will provide access privileges to internal systems (including networks, systems, applications, computers and mobile devices) based on the following principles:

4.1.1.1. Requests for Administrator Accounts and access privileges **must** be formally documented and appropriately approved.

4.1.1.2. Requests for privileged accounts (such as vendor accounts, application and service accounts, system administration accounts, shared / generic accounts, test accounts and remote access) **must** be formally documented and approved by the system owner.

4.1.1.3. Administrator Accounts **must** be uniquely identifiable accounts linked to individual Users and **must** be authenticated every time privileged access is granted on a system.

4.2. Administrator Accounts usage.

4.2.1. Administrator Accounts **must** only be used when performing administrative duties in an official capacity.

4.2.2. Accounts **must** be logged out once the task is complete.

4.2.3. Administrator Accounts **must not** be shared with any other User other than the delegated Administrator.

4.2.4. Separate accounts for normal day to day activities **must** be provided alongside Administrator Accounts.

4.3. Administrator Account restrictions.

4.3.1. Administrator Accounts **must not** be used to access any online resources.

4.3.2. An email account **must not** be associated with Administrator Accounts.

4.4. Administrator Account review.

Should an Administrator's job-role change, the Administrator Access privileges **must** be reviewed to ensure that the Administrator has only the lowest level of privileges necessary to carry out their day-to-day role.

4.5. Revocation of Administrator Accounts.

When an Administrative member of staff leaves the company, the Administrator Account **must** be disabled for a period of 6 months and then deleted.

5. Implementation and Review

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

5.2. 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.

5.3. 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

6. 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)