Policy Number	FEIT 009
Level	3
Issue	1
Issue date	13/05/2021
Review Date	04/02/2023
Author	Gordon Hope
SMT approval	04/02/2021

Edinburgh College

For the future you want

User Access Control Policy

Estates Services & IT

1. INTRODUCTION

Information is a valuable asset and access to it must be managed with care to ensure that confidentiality, integrity and availability are maintained.

Edinburgh College provides access to information assets, accounts, systems and resources based on the principle of least privilege. The College implements physical and logical access controls across its network, IT systems and services in order to provide authorised and appropriate user access, and to ensure appropriate data confidentiality, integrity and availability in accordance with the Information Security Policy.

This policy is to provide a framework for how user accounts and privileges are created, managed and removed.

This policy outlines the rules relating to authorising, monitoring and controlling access to College accounts and privileges, including how new users are authorised and granted appropriate privileges, as well as how these are reviewed and revoked as required.

2. SCOPE

This policy applies to any person that is granted access to Edinburgh College networks, accounts, information systems, data, and authorised users. Some roles and privilege levels require stronger access controls than those for standard users.

This policy does not apply to Subject Access Requests under the GDPR Regulations or Data Protection Act 2018. These requests are managed separately by the DPO.

3. OBJECTIVES

Compliance with this policy enables consistent controls to be applied throughout the College, minimising exposure to security breaches, whilst allowing systems and information and IT technical staff to conduct their activities within the framework of the law.

This policy ensures that by having the appropriate access controls in place, the right information is accessible to the right people at the right time, and that access to information is appropriately managed and periodically audited.

4. PRINCIPLES

All personnel (e.g employees, students, contractors, and third parties) at the College must abide by relevant information security and access control policies and procedures.

LEAST PRIVILEGE

Access controls must be allocated on the basis of business need and 'least privilege'. Users must only be provided with the absolute minimum access rights, permissions to systems, services, information and resources that they need to fulfil their business role.

ACCOUNT MANAGEMENT

User account management procedures must be implemented for user registration, modification and de-registration on all College information systems. These procedures must also include processes for monitoring redundant and inactive accounts.

5. RESPONSIBILITIES

Information System Owners

Information system owners are responsible for assessing compliance and ensuring their systems comply with this User Access Control policy.

All Account Holders

- Must only use their account and access in accordance with the College's IT Code of Practice.
- Secure their credentials in line with the College's Password Guidance.
- Be responsible for the systems, services and data within their control.
- Transfer services and data prior to vacating a role and closing an account.

Management
Management are responsible for ensuring that members of their team have the minimum levels of access to systems they need to perform their job and they, or information system owners, must authorise the appropriate level of access rights for each individual team member.

Management should only sponsor access requests that are documented, adequate and justified based on a requester's business need.
Managers should ensure that the access rights of people who have a change of duties or job roles or that leave the organisation are revoked immediately and that any access tokens (e.g. smartcards) are recovered.

All managers should review the access levels of their staff to ensure they are appropriate.

Application Support teams
Technical support teams (such as IT, MIS and the Development team) are responsible for granting access to systems in accordance with the User Access Control Policy.

IT Infrastructure team
The IT Infrastructure team has a particular responsibility in assisting system owners with secure management of privileged service accounts. Guidance should be sought from Account Users and/or Management if in doubt over the College policy.

Users
Users must only use College systems for legitimate College use as required by their job and in accordance with the policy and procedures for those systems.

6. ACCESS CONTROL IMPLEMENTATION

Identity Management
Formal user registration and de-registration processes are implemented to enable the assignment of identities and accounts on an individual basis. This ensures accountability for all actions taken by employees, student and associate account users.

Refer to Section 7 for User Registration.

Authentication Management

All account, service and platform access is managed through secure authentication controls.

For more information please refer to the College's password guidance.

Access Governance

A formal user access provisioning process is implemented to assign or revoke access rights for all user types to systems and information assets under the control of the College. The access provisioning is based on the following principles:

- All extra requests for, or changes to, access are documented and tracked.
- All access requests or changes require documented justification.
- Justification will be based on simple risk assessment and the business need, confirmed by the request sponsor.
- Appropriate authorisation and approval required and documented for all access requests and changes.
- All access changes granted are documented and tracked.
- Reviews of access are performed by relevant asset owners periodically.
- These principles are based on least privilege for account, service, application or systems.

Removal or Adjustment of Access Rights

The access rights of all employees, students, and associate account users to information and information processing facilities will be removed upon termination of their employment, contract or agreement, or adjusted upon change.

This will be managed by IT staff, the Management information team and the Development team.

Additional access to accounts, assets, systems or services are subject to review and approval on a case-by-case basis, as outlined in the Access Governance section above.

Access Reviews

Access to assets, services and systems will be periodically reviewed. The frequency of reviews will depend on the level of risk surrounding the asset and access.

Access in Special Circumstances

THERE ARE SPECIAL CIRCUMSTANCES WHERE EXTRA OR PRIVILEGED ACCESS IS NEEDED. FOR ALL CASES, ACCESS TO AN ACCOUNT, THE INFORMATION SERVICE CONTAINED WITHIN AN ACCOUNT OR INFORMATION PERTAINING TO THE ACTIVITY OF AN ACCOUNT, IS CAREFULLY RESTRICTED AND MUST ONLY BE CARRIED OUT WITH APPROPRIATE AUTHORISATION AND SAFEGUARD IN PLACE.

7. USER REGISTRATION

User registration should ensure the following:

- Accounts are provided on the basis of valid records in the HR and student information systems. For any user not in either of those systems, access is granted via the appropriate staff form signed by their head of department/faculty.
- Using unique user Identification (IDs) so that users can be linked to and made responsible for their actions. The use of shared IDs is not usually permitted, but dispensation may be made where group permissions are required for the work carried out.
- Checking that the user has authorisation from the system owner for the use of the information system or service. Separate approval for access rights from management may also be appropriate.
- Checking that the level of access granted is appropriate to the business purpose and is consistent with the Security Policy.
- Giving users access to a written statement of their access rights.
- Requiring users accept the conditions of access, such as the Acceptable Use Policy.
- Ensuring service providers do not provide access until authorisation procedures have been completed.
- Maintaining a record of all persons registered to use the service.
- Removing access rights of users who have changed jobs or left.
- Periodically checking for, and removing, redundant user IDs and accounts.

- Ensuring that redundant user IDs are not issued to other users.

8. PRIVILEGE ACCOUNT MANAGEMENT

“Special privileges” are those such as are allowed to the system manager, administrators or system programmers, allowing access to sensitive areas. The allocation of privilege rights shall be restricted and controlled and not provided by default. Authorisation for the use of such accounts shall only be provided explicitly, upon written request from a senior manager or information system owner (such as a head of department) and will be documented by the system owner.

The IT team shall guard against issuing privilege rights to entire teams to prevent potential losses of confidentiality and/or integrity.

Privileged accounts must not be used for standard activities; they are for program installation and system reconfiguration, not for day-to-day program use, unless it is otherwise impossible to operate the program.

9. PASSWORD MANAGEMENT

All new users must be briefed on the importance of passwords and instructed in the manner in which they are to be used.

The College:

- Requires users to agree to the Acceptable Use Policy and the password requirements therein.
- Provides mandatory cyber-security training for all staff to offer essential guidance on password security requirements.

10. SERVICE ACCOUNTS

Service accounts are non-human accounts which run in the background to execute applications and services or to perform particular functions. Such accounts often have high privilege levels to systems and data. Therefore, proper management of service accounts is important to reduce what can otherwise be a significant cyber-security risk.

Service accounts:

- Must not use any shared passwords with other similar accounts.
- Must not be shared across different systems or services where it can be avoided.
- Must not have a fixed password which never changes. In particular, service account passwords should be rotated when an employee with access to those credentials leaves the College.
- Must not be left running with the default or a blank password.
- Should follow a shared naming convention so that service accounts are easily identified.
- Must not be used for interactive login by any users. User accounts must also not be used to run as service accounts.
- Must not be kept active beyond the time they are needed. A decommissioning checklist for systems and services must include steps for the lifecycle of service accounts.

11. POLICY REVIEW

This policy will be reviewed whenever changes effect its content or every two years.