the enquire learning trust

Access Control Policy

Contents

Access Control Policy

This policy covers the use of electronic systems to store and use information that could be deemed as personal or confidential.

1. Introduction

Access to all personal information should be based on restricted privileges – based on job functions and a clear process for defining the level of access. Access should be overseen and managed by Information Owners.

In addition, access to your electronic personal information, systems and applications should be strictly controlled by ICT and Information Owners. This should include, as a minimum:

- Use of unique Users IDs, traceable to each individual user – to enable accountability for Users actions.
- Restricted privileges – based on job functions and a clear process for defining the level of access.
- Secure password management – applying the measures outlined below and the Password Policy.

It applies to all types of systems and accounts, for example:

- User network
- Domain administration
- Cloud Systems
- Shared
- Operating System
- Application

2. Providing Access

Each user should be allocated access rights and permissions to personal information and computer systems that:

- Are commensurate with the tasks they are expected to perform.
- Have a unique login that is not shared with or disclosed to any other user.
- Have an associated unique password that is requested at each new login.

This includes, where enabled by the security features of the software application, separation of duties and/or access into clearly defined roles.

The following software application security features should be adopted where enabled by the software:

- Unable to override access controls (e.g. the admin settings removed or hidden from the user).
- Free from alteration by rights inherited from the operating system i.e. that could allow unauthorised higher levels of access.
- Logging functions i.e. to enable auditing and accountability of actions.

System administration accounts should only be provided to users that are required to perform system administration tasks. They should have individual administrator accounts, and they should be logged and audited. The administrator account should not be used by Systems Administrators for normal day to day activities.

Formal user access control procedures and processes should be documented, implemented and kept up to date for each application and information system to ensure authorised user access and to prevent unauthorised access. Decisions on the appropriate level of access to information or information systems for a particular User should be made by the relevant Information Owner.

3. Responsibilites

Managers should be responsible for:

- Ensuring that users have completed any mandatory or other training before being given access.
- Informing ICT of alterations in a user's role that require a change in access rights. This includes:
  - Users whose role has changed.
  - Users who change roles within a team; a department etc...
  - Users who change roles within your Academy.

Users should follow the Information Security Policy at all times – keeping their passwords confidential at all times and not disclosing their passwords to anyone, including ICT staff and their managers