23 October 2017

ELT Information Governance Policy
Section 4.4: Data Security and 5.4: Passwords/Academy ICT Responsibilities

All staff are responsible for ensuring that data security is maintained in line with the following requirements, the wider Information Governance Policy (IGP) and any related Academy policies and procedures.

Section 4.4: Data Security

The Trust and its Academies will ensure that appropriate technical and organisational measures are taken against unlawful or unauthorised processing of personal data and against the accidental loss of, or damage to, personal data as follows:

- All staff will read and sign to state they will comply with the ELT Staff Acceptable Use Policy. This document was circulated to all staff on 04/09/2017 and staff signatures are required to confirm that they have read and understood the contents of the document. This will be reviewed annually, with renewed signatures required.

Organisational measures:

1. Each Academy will define an Access Control Policy, outlining the roles within the school and the systems, applications and information they need to access in order to fulfil their role. This document was circulated to all staff on 23/10/2017 and staff signatures are required to confirm that they have read and understood the contents of the document.

2. Paper records must be kept in a locked filing cabinet, drawer, or safe, and only made available where there is relevant/appropriate purpose to do so.

3. If personal data is held on a laptop, mobile device or other removable storage media, that media must itself be kept in a locked filing cabinet, drawer, or otherwise secured when not in use.

4. Lock laptops and computers/screens if logged in when leaving the computer for any short period of time (a maximum of 5 minutes is advised).

5. Log out the laptop/computer if logged in when leaving it for an extended period of time (more than 30 minutes is advised).

6. When viewing personal information on screen or at your desk, consider who may be able to view the information and use the locked screen function when away from your desk.

Section 5.4.1: Passwords – Policy for all Employees

All Employees must follow the controls below at all times:

- Never reveal passwords or PIN numbers to anyone – including external ICT staff and their managers.
- Never use the “remember password” function on devices other than your own.
- Never write passwords or PIN numbers down or store them where they are open to theft.
- Never store passwords or PIN numbers in a computer system without encryption.

Section 5.4.2: Strong Passwords

All passwords used by staff must:

- Be a minimum of eight characters long.
- Include three of the following:
  - Uppercase character.
  - Lowercase character.
  - Number.
- Special character.
- Not include proper names.
- Not include any part of the employee's username.

Section 5.4.3: Strategic ICT responsibilities

The Strategic ICT Officer of the Trust Leadership will ensure the following measures are enforced by the following Networks, System and Applications:

Measures:

- Passwords must comply with Strong Passwords above.
- Passwords must be changed every 180 days.
- The last three passwords cannot be re-used.
- The account will "locked out" following four successive incorrect log-on attempts.
- Password characters will be hidden by symbols.

Networks, System and Applications:

Active Directory – access to all Trust network data
SIMS
Office 365 – email
Google Apps for Education – all services other than email
Sage
Trust Intranet
Web Filtering and Monitoring applications
MDM solution

Any changes – i.e. due to the functionality of Systems or Applications – will be documented and the potential risk assessed by the Strategic ICT Officer of the Trust Leadership before being implemented:

Section 5.4.4: Academy ICT responsibilities

Where not covered by 5.4.3 Strategic ICT responsibilities above, each academy shall ensure its ICT adheres to the following minimum standards:

- Ensure that log-on procedures are secure and do not provide unnecessary information (i.e. that could enable unauthorised access or detail the level of access that the login ID provides) for example, provide clues about valid User IDs; the operating system version (and therefore its vulnerabilities) or that the person has administration rights.
- Ensure that secure authentication methods are used to access the ICT network and security infrastructure, server and client operating systems and corporate systems such as internet and e-mail.

- Ensure that new accounts are created with a temporary password which the user is required to change at first logon.
- Ensure that the initial password for an employee account will only be given to the new employee.
- Ensure that the login procedure is also protected by:
    - Not displaying any previous login information e.g. username.
    - Limiting the number of unsuccessful attempts and locking the account if exceeded.
    - The password characters being hidden by symbols.
    - Displaying a general warning notice that only authorised employees are allowed.
- Ensure than when leaving your device, it is either locked, or logged out.
- Ensure all successful and unsuccessful log-on attempts should be logged and monitored.
- Ensure System Administration passwords are always available to a senior, nominated officer within Academy who is separate to the System Administrator(s), for example the Principal.
- Ensure Operating System access control should apply to all computers and devices that have an operating system e.g. servers, PCs, laptops, tablets.
- Ensure Operating System and network domain log-on procedures should also include an enforced “User acknowledgement” statement, confirming compliance with the IGP and Acceptable Use Policy.

All staff are required to read this statement in conjunction with the Access Control Policy (attached) following which staff are required to sign to say they have read and understood the contents of both documents.

Access Control Policy

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

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; and
- 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
- Shared
- Domain administration
- Operating System
- Cloud Systems
- Application

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; and
- 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; and
- 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.

Responsibilities

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/department; and
    - 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.