ICT Security Policy

Approved by:	Trust Board		
Responsible department:	Core MAT Team		
Last review date:	30.01.23	**Last reviewed by:**	The DP Advice Service
Last updated:	July 23	**Last updated by:**	Jayne Firth, COO
Next review due :	July 25		

1. Introduction

1.1 It is a necessary part of everyday working life within the Academy Trust to allow staff and pupils to access desktop computers, laptops and/or tablets to carry out work and research. It is necessary to ensure that such use is carried out in a safe and secure manner having regard for the need to protect any personal information contained on such systems.

This policy sets out the following information:

- The purpose and scope of the policy,
- Definitions of key terms used in the policy,
- Roles and responsibilities,
- Management of the policy,
- Physical security,
- Legitimate use,
- Security breaches,
- Implications of non-compliance with the policy.

2. Purpose and scope of the policy

2.1 The purpose of this policy is to protect the Academy Trust's information stored electronically from all threats (internal and external), deliberate or accidental.

2.2 In order to carry out the purpose at 2.1 above, it is imperative that all staff are aware of the need for ICT and data security to be an integral part of the day-to-day operation of the Academy Trust.

2.3 The Academy Trust will ensure that:

2.3.1 ICT and information stored electronically will be protected against unauthorised access.
2.3.2 Information, in particular personal data, is kept confidential.
2.3.3 Integrity of information will be assured.
2.3.4 Regulatory and legislative requirements are complied with.
2.3.5 ICT security or data protection training is made available to all staff.

2.4 All staff must ensure that the equipment and any data is adequately protected against action that could adversely impact the Academy Trust.

2.5 All staff should be made aware of, and fully comply with, all relevant legislation relating to information and ICT security.

2.6 This policy is for all staff members, trustees, governors and volunteers who have access to, or supervise pupils' use of, ICT equipment belonging to the Academy Trust. Pupil's using Academy Trust ICT systems will be covered by the Academy Trust's 'Use of Digital Technology Policy' or other such equivalent policy.

3. Relationship with existing policies

3.1 This policy should be read in conjunction with the following policies:

3.1.1 The Trust's Use of Digital Technology Policy,

3.1.2 Data Protection policy,
3.1.3 Records Management and Retention policy.

Definitions

ICT/ICT Systems	any device or combination of devices used for the storage or processing of data, including: desktop computer, laptop computer, netbook, notebook, IPad, tablet, mobile phone or any other similar device.
ICT data	any information stored and processed within the ICT system including documents, programmes, text, pictures and sound.
ICT User	applies to any Trust employee, trustee, governor, volunteer, pupil or other authorised person who uses the Academy Trust's ICT systems.
Authorised Personnel	As above.

4. Roles and Responsibilities

4.1 The ICT security policy should be followed by all staff but it is the responsibility of the Trustees, governing body and the Principal to ensure that the policy is complied with.

4.2 The Trustees/governing body has the ultimate responsibility for ensuring that the Academy Trust complies with the legislative requirements relating to the use of ICT systems and data security.

4.3 The Principal is responsible for the day-to-day implementation and compliance with the policy.

4.4 The Principal is responsible for ensuring that users of the systems are familiar with this policy and adhere to the requirements under this (and associated) policies.

4.5 The day-to-day functions relating to ICT security are delegated to the internal IT Team and are managed by the ICT Manager.

4.6 The ICT manager is responsible for the practical aspects of ICT protection such as maintaining the integrity of the data, producing the requisite backup copies of data and protection of the physical access to systems and data.

4.7 The ICT manager will be the point of contact for ICT security issues and is responsible for notifying the Principal or Trustees and Data Protection Officer of any suspected or actual breach of the ICT security. Further information about breaches is set out in section 7 of this policy.

4.8 The ICT manager is responsible for maintaining, repairing and proactively supporting the ICT System so that the requirements of this policy are met. The ICT manager will also monitor the ICT system for breaches of security.

4.9 The Data Protection Officer (DPO) is responsible for ensuring that the policy is being adhered to in order to comply with the data security requirements and current data protection laws.

4.10 Users are those employees, trustees, governors, pupils, volunteers or other authorised personnel of the Academy Trust who make use of the ICT system to support them in their work. All users of the Academy Trust's ICT systems and data must comply with this policy. The Academy Trust also have an acceptable use policy which sets out the responsibilities of the users of the Trust's ICT systems.

4.11 Users are responsible for notifying the Principal or other appointed person and DPO of any suspected or actual breach of the ICT security.

4.12 Users are responsible for the equipment they use and should ensure the physical security, data security, their password security and that their work is always protected/backed up.

5. Management of the Policy

5.1 Sufficient resources should be allocated each year to ensure the security of the Academy Trust's ICT systems and to enable users to comply fully with the legal requirements and other matters covered in this policy. If insufficient resources are available to fully implement this policy, then this, and the potential risks associated with it, must be documented and reported to Trustees/Governors by the Principal or other appointed person.

5.2 Suitable training for all ICT users and documentation to promote the proper use of ICT systems will be provided. Users will also be given adequate information on the policies, procedures and facilities to help safeguard these systems and related data. A record should be kept of the training provided through the Academy Trust to each individual user.

5.3 Users will be made aware of the value and importance of such ICT systems and data, particularly data of a confidential or sensitive nature, and be made aware of their personal responsibilities for ICT security.

5.4 The Principal should be responsible for ensuring that any new members of staff are aware of the requirements of this policy and that they have read and signed the staff ICT Acceptable Use policy.

5.5 The Principal should liaise with the IT team to set up the individual user and manage the access rights that the user has, including any necessary limitations of access/use of data.

5.6 The Principal is responsible for ensuring that any staff member who leaves a post, returns any ICT equipment provided to them for their time in post.

6. Physical Security

6.1 The Academy Trust should ensure that adequate security measures are put in place to protect rooms containing ICT equipment (including the server and any cabling). If possible, only authorised personnel should be allowed access to rooms containing servers; if this is not possible then adequate security measures need to be in place to protect servers. The server room should be locked when unattended.

6.2 The ICT Manager or other appointed person shall be responsible for ensuring the safe and secure removal of any ICT equipment. If the ICT equipment is to be destroyed this shall be done in a safe and secure manner, safeguarding any data.

6.3 The location/positioning of laptops, computers or other ICT devices that are used to access and process personal data should be considered to avoid screens being viewed by anyone who is not authorised to have sight or access to that personal data.

6.4 As part of the Acceptable Use Policy, staff members should lock laptops or computers when leaving these unattended.

6.5 Any hard copies of personal data should not be left out on desks when the desk is unattended.

6.6 The Principal, in accordance with the Academy Trust's financial regulations, shall ensure that an inventory of all ICT equipment is maintained and that all items are accounted for; this review should take place at least once in the academic year.

6.7 Any ICT equipment taken off site must always be kept secure.

7. Legitimate Use

7.1 All staff members must ensure that ICT facilities are not used in any way that breaks the law or breaches the Academy Trust's Acceptable Use policy.

7.2 It is important to note that risks can occur from the use of unlicensed or unprotected software. The user should ensure that any software used within the Academy Trust buildings and on the Academy Trust's systems should be authorised by the Principal or other appointed person and checked for GDPR compliance by the DPO.

7.3 Only authorised personnel who have agreed to use ICT systems in compliance with the Academy Trust's ICT policies should be allowed access to the ICT systems. If a staff member, volunteer or other authorised person has failed to sign the Acceptable Use policy then they should not be permitted to use the ICT systems until they have read and signed to agree that they will comply with that policy.

7.4 All ICT systems should be secured by password. The ICT Manager or equivalent should be responsible for the level of password control required depending on the nature of the system and the data used/stored on that system.

7.5 Encryption passwords unique to individual staff members should be set by the staff member and MUST be a minimum of 8 characters, including a mix of letters (upper and lower case) and numbers

7.6 Laptop/computer passwords should be changed regularly; it is recommended that this takes place termly. The ICT manager or equivalent should set up reminders to ensure that staff are prompted to change passwords at these times. If passwords are of significant length and complexity, there may not be a need to change the password on a termly basis.

7.7 Passwords should be memorised. If a password is written down, it MUST NOT be kept with the device in any form.

7.8 All ICT systems should be protected by passwords and/or screen saver protection.

7.9 If a staff member leaves the Academy Trust, then all centralised passwords must be changed. If an individual suspects that their password has been compromised or that their system has been breached, then their password MUST be changed as soon as possible, and the staff member must notify the DPO.

7.10 Staff members must not give their password out to other people, including other authorised personnel.

7.11 Only devices approved by the ICT Manager or equivalent should be permitted to be connected to the network. Where devices are connected to the network, the wireless network must be secure. Open Access Wireless Access Points must not be connected to the Trust's network.

7.12 Mobile devices may connect to the network but only when permitted and when being used in full compliance with the ICT policy and Acceptable Use policy.

7.13 Access to the internet for pupils should be filtered using an approved system. It is the responsibility of the ICT manager to monitor effectiveness of the filtering system.

7.14 In case of an ICT system failure, back-up copies of stored data will be taken at regular intervals as determined by the ICT Manager/other appointed person.

7.15 Data essential for the day to day running and management of the Academy Trust should be stored on the Trust's network. Unencrypted storage devices must not be used.

7.16 Backups containing data that must be protected, should be clearly marked stating what they are and when they were taken and should be stored securely offsite.

7.17 The Academy Trust must ensure that all ICT systems are protected with the appropriate Anti-virus software and should take precautions to avoid malicious software that may destroy or corrupt data.

7.18 All users need to be aware that any ICT system device suspected of being infected with a virus must be disconnected from the network and reported to the ICT manager/ or other appointed member of staff as soon as possible. The ICT manager or equivalent must then take steps to remove the virus and protect the system.

7.19 Any third-party laptops/mobile devices not normally connected to the Academy Trust's network drive must be checked by the IT Team for viruses and anti-virus software before being allowed to connect to the network.

7.20 All personal data held on ICT systems including USB sticks and other portable ICT equipment must be confidentially and permanently destroyed in line with the Records Management and Retention Policy prior to a device being destroyed.

7.21 If any ICT equipment is no longer in use by the Academy Trust and is to be disposed of in any way, then the ICT Manager/or other appointed member of staff or approved external company must ensure that all personal data has been removed from that system prior to its disposal.

7.22 If any ICT equipment is damaged and repairs are to be carried out by a third party, then the equipment must be assessed to see what, if any, personal data is held on that

equipment. Any personal data should be protected before the equipment is provided to the third party for repair.

7.23 The Academy Trust should avoid duplication of personal data in multiple locations and should therefore avoid saving and storing anything containing personal data on desktops.

8. Security Breaches

8.1 All suspected or actual breaches of ICT security shall be reported to the ICT Manager, the SLT and the Data Protection Officer (in line with Section 4 above).

8.2 Steps must be taken by the ICT Manager or designated person, to ensure that the adequate protections are put in place as soon as a breach is suspected.

8.3 Steps must be taken to identify the cause of the breach and to update any policies and procedures to try and avoid the breach occurring in the future.

8.4 Any risk to personal data caused by the breach must be reported to the Data Protection Officer and the necessary steps under the Data Protection Policy for dealing with breaches, should be followed.

9. Breach of Policy

9.1 The ICT Manager or equivalent appointed person, Principal and the DPO are responsible for reviewing and monitoring compliance with this policy.

9.2 Any reports of staff, trustees, governors or third parties breaching this policy should be reported to the CEO and investigated fully. Any breaches will be taken seriously.

9.3 Any member of staff who fails to comply with the requirements of this policy may be subject to disciplinary action.