Information Security Policy

Review frequency:	3 Years
Last reviewed:	Nov 22
Agreed by Trustees	5/12/22
Next review date:	Nov 25

Information Security

Objective

The information security objective is to ensure that the Academy's information base is protected against identified risks so that it may continue to deliver its services and obligations to the community. It also seeks to ensure that any security incidents have a minimal effect on its business and academic operations.

Responsibilities

The CEO of the Trust has direct responsibility for maintaining the Information Security policy and for ensuring that the staff of the trust adheres to it.

General Security

It is important that unauthorised people are not permitted access to trust information and that we protect against theft of both equipment and information. This means that we must pay attention to protecting our buildings against unauthorised access. Staff must:

- Not reveal pin numbers or building entry codes to people that you do not know or who cannot prove themselves to be employees;
- Beware of people tailgating you into the building or through a security door;
- If you don't know who someone is and they are not wearing some form of identification, ask them why they are in the building;
- Not position screens on reception desks where members of the public could see them;
- Lock secure areas when you are not in the office;
- Not let anyone remove equipment or records unless you are certain who they are;

Visitors and contractors in trust buildings should always sign in using the visitor management system in use in each school.

Security of Paper Records

- Paper documents should always be filed with care in the correct files and placed in the correct place in the storage facility.
- Records that contain personal data, particularly if the information is sensitive should be locked away when not in use and should not be left open or on desks overnight or when you are not in the office;
- Always keep track of files and who has them;
- Do not leave files out where others may find them;
- Where a file contains confidential or sensitive information, do not give it to someone else to look after.

Security of Electronic Data

Most of our data and information is collected, processed, stored, analysed and reported electronically. It is essential that our systems, hardware, software and data files are kept secure from damage and unauthorised access.

A safe and secure username / password system is essential and must apply to all school technical systems, including networks, devices, email and websites.

- All school / academy networks and systems will be protected by secure passwords that are regularly changed.
- The “master / administrator” passwords for the academy systems, used by the technical staff must also be available to the Headteacher or other nominated senior leader and kept in a secure place eg. school safe.
- All users (adults and young people) will have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security. Users must ensure all passwords are securely stored and not visible to others. It is recommended that usernames and passwords are stored separately.
- Passwords for new users, and replacement passwords for existing users will be allocated by the Network manager / ICT TA.
- Users must change their passwords at regular intervals.
- If a user has forgotten their password a request must be made in person to the Network Manager/ ICT TA, who will issue a temporary password. This will ensure that the new password can only be passed to the genuine user.

Staff passwords:

- All passwords should be a minimum of 8 characters long and must include three of – uppercase character, lowercase character, number, special characters
- Temporary passwords e.g. used with new user accounts or when users have forgotten their passwords, will be enforced to change immediately upon the next log on.
- Passwords shall not be displayed on screen, and shall be securely hashed.
- Passwords should be different for different accounts, to ensure that other systems are not put at risk if one is compromised and should be different for systems used inside and outside of school.
- Passwords should be changed at least every 30 days.
- Passwords should not be re-used for 6 months and be significantly different from previous passwords created by the same user. The last four passwords must not be reused.
- Passcodes for IOS devices (iPhone, iPad, iPod, etc.) must be a minimum of 4 digits.

Two factor authentication (2FA):

- Google Chrome must be used by staff and pupils for school purposes.
- When members of staff are accessing sites containing private/ confidential information two factor authentication must be enabled e.g. Arbor, PSF.
- Details on how to enable two factor authentication can be obtained from the Network Manager.

Student / pupil passwords

All users will be provided with a QR code to log in to Trust Chromebooks. Any other passwords required will be supplied by the Network Manager, who will an up to date record of usernames and passwords.

Pupils will be taught the importance of password security during computing lessons.

Use of E-Mail and Internet

The use of the trust's e-mail system and wider Internet use is for the professional work of the trust and its schools. Reasonable personal use of the system in a member of staff's own time is permitted but professional standards of conduct and compliance with the trust's wider policies are a requirement whenever the e-mail or Internet system is being used. The trust uses a filtered and monitored broadband service to protect our pupils. Deliberate attempts to access web sites that contain unlawful, pornographic, offensive or gambling content are strictly prohibited. Staff discovering such sites on the system must report this to their line manager immediately. The Network Manger will ensure that the sites are reported to the broadband provider for filtering.

- To avoid a computer virus arriving over the Internet, do not open any flashing boxes or visit personal websites;
- Do not send highly confidential or sensitive personal information via e-mail;
- Save important e-mails straight away;
- Unimportant e-mails should be deleted straight away;
- Do not send information by e-mail, which breaches the Data Protection Act. Do not write anything in an e-mail which could be considered inaccurate or offensive, and cannot be substantiated.
- Confidential data must be sent by encrypted email. Venture MAT uses Egress for this.

Electronic Hardware

- All hardware held within the trust should be included on the asset register;
- When an item is replaced, the register should be updated with the new equipment removed or replaced;
- Do not let anyone remove equipment unless you are sure that they are authorised to do so;
- In non-secure areas, consider using clamps or other security devices to secure laptops and other portable equipment to desktops (Eg. The iPad in the reception area used for signing in)..

Homeworking Guidance

If staff must work outside of the trust premises or at home, all of the 'Information Security' policy principles still apply. However, working outside of the trust premises presents increased risks for securing information. The following additional requirements apply:

- Do not access confidential information when you are in a public place, such as a train and may be overlooked;
- Do not have conversations about personal or confidential information on your mobile when in a public place. Ensure that, if urgent, you have your conversation in a separate room or away from other people;

If you use a laptop or tablet or smart phone:

- Ensure that it is locked and password protected to prevent unauthorised access;
- Make sure that you don't leave your device anywhere it could be stolen. Keep it with you at all times and secure it when you are in the school;
- Any portable device or memory stick that contains personal data must be encrypted. Personal data may not be taken off the school site or put onto a portable device without the express permission of the Headteacher/Head of School. Taking personal data off-site on a device or media that is not encrypted would be a disciplinary matter.

The Headteacher/Head of School will maintain a register of protected data that has been authorised for use on a portable device; the fixed period of time that the authorization relates to; the reason why it is necessary to place it on the device; the person who is responsible for the security of the device and its data; the nature of encryption software used on the device; confirmation of the date that the data is removed from the device.

When working on confidential documents at home do not leave them lying around where others may see them; dispose of documents using a cross-cut shredder.

If you are using your own computer, ensure that others cannot access documents. When you have completed working on them, transfer them back to the school's system and delete them from your computer. It is forbidden to use a computer owned by you to hold personal data about pupils or staff in the trust.

Audit of Data Access

Where possible our software specifications will include the function to audit access to confidential data and attribute access, including breaches of security, to specific users.

Data Backup

The trust will arrange for all critical and personal data to be backed up and secured remotely. If the school is physically damaged critical data backups will allow the Trust to continue its business at another location with secure data.

Disposal of Information

Paper records should be disposed of with care. If papers contain confidential or sensitive information shred them before disposing of them. Particular care must be taken when selecting papers to be placed in a recycling bin.

Computers and hardware to be disposed of must be completely 'cleaned' before disposal. It is not enough just to delete all the files.

It cannot be assumed that simply deleting a file will prevent it being recovered from electronic media. Electronic memory containing personal information or sensitive personal information must be electronically scrubbed or physically destroyed.

Where a third party contractor holds personal information on behalf of the trust, for example a payroll provider, the trust will seek reassurance from the contractor regarding their data protection policies and procedures.