Information Security Policy

Document number:	33
Review frequency:	Biennial
Last reviewed:	May 18
Agreed by Trustees	22/5/18
Next review date:	May 20

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 Principal of the Academy has direct responsibility for maintaining the Information Security policy and for ensuring that the staff of the academy adheres to it.

General Security

It is important that unauthorised people are not permitted access to Academy 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 Academy buildings should always sign in using the visitor management system.

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. Academy staff must:

- Prevent access to unauthorised people and to those who don't know how to use an item of software properly. It could result in loss of information;

- Keep suppliers CDs containing software safe and locked away. Always label the CDs so you do not lose them in case they need to be re-loaded;
- When we buy a license for software, it usually only covers a certain number of machines. Make sure that you do not exceed this number, as you will be breaking the terms of the contract.
- Passwords are a critical element of electronic information security. All staff must manage their passwords in a responsible fashion:
    - Don't write it down;
    - Don't give anyone your password;
    - Your password should be at least 8 characters;

The essential rules your password is something that you can remember but not anything obvious (such as password) or anything that people could guess easily such as your name;

- You can be held responsible for any malicious acts by anyone to whom you have given your password;
- Include numbers as well as letters in the password;
- Take care that no-one can see you type in your password;
- Change your password regularly, and certainly when prompted. Also change it if you think that someone may know what it is.
- Many database systems, particularly those containing personal data should only allow a level of access appropriate to each staff member. The level may change over time.

Use of E-Mail and Internet

The use of the academy's e-mail system and wider Internet use is for the professional work of the academy. 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 Academy's wider policies are a requirement whenever the e-mail or Internet system is being used. The academy 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 Principal 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.

Electronic Hardware

- All hardware held within Academy 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.

Homeworking Guidance

If staff must work outside of the academy or at home, all of the 'Information Security' policy principles still apply. However, working outside of the academy 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 Academy;
- Any portable device or memory stick that contains personal data must be encrypted. Personal data may not be taking off the academy's site or put onto a portable device without the express permission of the Principal/Head of School. Taking personal data off-site on a device or media that is not encrypted would be a disciplinary matter.

The Principal/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 Academy'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 at the academy.

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 academy will arrange that all critical and personal data is backed up to secure on-line (off physical site) storage. If the academy is physically damaged critical data backups will allow the Trust to continue its business at another location with secure data.

Data backup should routinely be managed on a rolling daily process to secure off-site areas.

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 academy, for example a payroll provider, the academy will seek reassurance from the contractor regarding their data protection policies and procedures.