`

The Societas Trust

Information Security Policy

Date of Policy	2025
Reviewed and Agreed by	The Directors' Board
Review Date	9 July 2025
Next Review Date	Summer 2026

Contents:

1. Statement of Purpose
2. Legal Framework
3. Roles and Responsibilities
4. Security Breaches and Security Breach Incident Reporting
5. Password Security, Access Control and User Privileges
6. Monitoring Usage
7. Malware Prevention including Firewalls
8. E Mail Security and Secure Data Transfer
9. Mobile Device/Removable Media
10. Working from Home and Remote Access
11. Backing Up Information
12. Personal Network and Cloud Storage
13. CCTV Systems, Printer Scanner and Copier Security
14. Data Information Assets
15. IT requirements in Termination of Staff Contracts
16. Business Continuity and Disaster Recovery Plans
17. Personal Device Procedures
18. Avoiding Phishing Attacks
19. User Training and Awareness
20. Assessment of Risks
21. Data Disposal
22. Video Conferencing
23. Monitoring and Review

1. Statement of Purpose

The Societas Trust in recognising that information is one of the Trust's most important Assets, is committed to the preservation of high standards of **confidentiality, integrity and availability** of data and the assets and processes that support and enable the acquisition, storage, use, protection and disposal of information. This policy strives to achieve a sensible balance of securing the information held by the Trust and academies therein, while making it accessible to those who need the information. The Academy will always however favour security over accessibility where there is any doubt as to the security of information.

It is essential that the Trust's information systems and data networks are adequately protected from events which may compromise the information held or the operational activities of any of the Academies within the Societas Trust and to this end, the Academy is committed to developing and maintaining an information systems structure which has an appropriate level of security in compliance with Principle 6 of the UK General Data Protection Regulation. (UKGDPR)

"*data should be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and accidental loss, destruction or damage using appropriate technical or organisational measures"*

The Societas Trust acknowledges that failure to ensure adequate security and protection of information held by the Trust or any of the Academies therein, may lead to legal action against the Academy/Trust and/or the individual responsible for any breach. Such legal action could include an investigation by the Information Commissioner's Office ("ICO") who can impose significant financial penalties and/or a claim for damages for breach of the UK GDPR and the Data Protection Act 2018

In addition, the Trust is aware that there is a reputational risk if the information held by the Academy or Trust is not kept safe, and as such confidence in the Academy and the Trust held by pupils, parents, guardians, volunteers, the Board of Governors, members of staff and the public at large could be irreparably damaged.

The Trust recognises, however, that breaches in security can occur, particularly as most information is stored online or on electronic devices which are increasingly vulnerable to cyber-attacks. This being the case, it is necessary to have a contingency plan containing a procedure to minimise the potential negative impacts of any security breach, to alert the relevant authorities, and to take steps to help prevent a repeat occurrence.

Much of the information held by the Trust is confidential and sensitive in nature. Therefore, it is necessary for all information systems to have appropriate protection against adverse events (accidental or malicious) which may put at risk the activities of the Academy or protection of the information held. Our processing activities are based on the following principles:

1. **Confidentiality** – access to Data must be confined to those with specific authority to view the Data in question;
2. **Integrity** – information should be complete and accurate. All systems, assets and applicable networks must operate correctly and according to any designated specification;

3. **Availability** – information must be available and delivered to the right person at the time when it is needed and in accordance with the relevant statutory provisions

The Trust will maintain the security and confidentiality of Data held by it, its information security systems and relevant applications and networks for which it is directly responsible by:

4. Ensuring appropriate technical and organisational measures are in place to prevent unauthorised access, damage or interference to and/or with information, IT assets and network services

5. Ensuring that it is aware of, and complies with, the relevant legislation as described in this and the other information governance and IT Policies;

6. Describing the principles of Information Security to Members of Staff, pupils, governors and volunteers and explaining how they will be implemented by the Academy

7. Creating and maintaining a level of awareness of the need for information security to be an integral part of the conducting of Academy/Trust business and ensuring that everyone understands their individual and collective responsibilities in this respect

8. Protecting Data and other information held by and/or on behalf of the Academy/Trust

9. Ensuring that the third party contractors classed as data processors are compliant with data protection legislation.

10. Ensuring that organisations that provide third party software and the processes used for uploading/downloading data are compliant with data protection legislation.

2. Legal Framework

This policy has due regard to statutory legislation and advisory guidance including, but not limited to, the following:

- The Computer Misuse Act 1990
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- National Cyber Security Centre (2018) 'Cyber Security: Small Business Guide'
- ESFA (2023) Academy Trust Handbook 2023
- ICO (2022) Guide to the General Protection Regulation (GDPR)

- DFE (2023) “Meeting digital and technology standards in schools and colleges”

This policy has due regard to the academy’s policies and procedures including, but not limited to, the following:

- Online Safety Policy
- Data Protection Policy
- Social Media Policy
- Mobile Phone and Photography Policy
- Risk Management Policy
- GDPR ICT Guide
- Disciplinary Policy and Procedure
- Cyber Crime Response Plan

3. Roles and Responsibilities

The Board of Directors have ultimately responsibility for the security of information, however this is delegated to the CEO, Jon Lovatt. The Data Protection Officer (DPO) for the Trust is SBM Services (uk) Ltd. Their contact details are Unit 12 Park Lane Business Centre, Park Lane, Langham, Colchester. CO4 5WR Tel 01206 671103 info@sbmservices.co.uk They will provide advice and guidance relating to Information Security. The CEO will ensure that there is day to day monitoring and management of data security at each Academy through the Headteachers (DPO Representatives) and the specialist IT Professionals at each Academy.

4. Security Breaches and Security Incident Breach Reporting – (Please refer to the Data Protection Policy Section23)

The Academy will have and maintain a separate register (where all Information Security incidents are logged. This log as a minimum will include:

1. the nature of the breach;
2. The number of Information Assets compromised;
3. How the Information Asset(s) has/have been compromised;
4. Whether any Special Category Personal Data was compromised;
5. Whether the incident needs to be reported in accordance with the breach management section 23 of the Data Protection Policy.
6. Examples of an Information Security Breach include but are not limited to:

a. Password(s) written down or stored, in an accessible, plain text or otherwise visible, manner to persons other than the Authorised User

b. Using another person's password

c. Divulging of a password

d. Making use of Personal Data for personal gain

e. Accessing Data for personal knowledge

f. Attempting to gain access under false pretences

g. Unauthorised release of Data;

h. Knowingly entering inaccurate Data

i. Deleting Data prior to the retention period or any other period set out in the Data Retention Policy

j. Changing permissions that allows access to, or sharing information (including Data) with, persons not authorised to access the information

k. Unauthorised removal of Data,

l. Malicious breaches, e.g. as a result of a hacker wishing to cause damage to the academy through accessing and altering, sharing or removing data.

m. Negligence, e.g. as a result of an employee that is aware of academy policies and procedures, but disregards these.

Breaches in security may also be caused as a result of system issues, which could involve:

- Incorrect installation of anti-virus software and/or use of software which is not the most up-to-date version, meaning the academy software is more vulnerable to a virus
- Incorrect firewall settings are applied, e.g. access to the academy network, meaning individuals other than those required could access the system
- Confusion between backup copies of data, meaning the most recent data could be overwritten. The academy will employ firewalls in order to prevent unauthorised access to the systems.

Reporting of Security Breach Incidents

Any individual that discovers a security data breach will report this immediately to the headteacher who will liaise with the IT Representative to identify and record the following:

1. Name of the individual who has raised the incident
2. Description and date of the incident
3. Description of any perceived impact
4. Description and identification codes of any devices involved, e.g. academy-owned laptop
5. Location of the equipment involved

6. Contact details for the individual who discovered the incident
7. The headteacher will take the lead in investigating the breach and will be allocated the appropriate time and resources to conduct this.
8. The severity of the breach will be ascertained as quickly as reasonably possible and what personal data is involved and if and how it has been compromised.
9. The cause of the breach and whether or not it has been contained, will be identified, ensuring that the possibility of further loss/jeopardising of data is restricted as much as possible or eliminated.
10. The headteacher will oversee a full investigation and produce a comprehensive report and advise the DPO and CEO accordingly
11. In the event of an internal breach, the incident is recorded using an incident log, and by identifying the user and the website or service they were trying to access.
12. The headteacher, CEO and Data Protection Link Governor will decide if any disciplinary sanctions to the pupil or member of staff in accordance with the processes outlined in the to the e-safety policy and disciplinary policy respectively
13. In the event of any external or internal breach in liaison with the IT Representative agreed action such as updating the firewall, changing usernames and passwords, updating filtered websites or creating further back-ups of information will be arranged.
14. In the event of external breaches, the Headteacher will work with any third party providers to implement an appropriate response to the attack, including any in-house changes.
15. Any further action which could be taken to recover lost or compromised data through the use of back-ups or updating of systems may be necessary at the individual academy concerned or across The Trust. The Headteacher of the Academy (s) concerned and the CEO/DPO will decide on the what action is to be instigated which include:
    - Informing relevant staff of their roles and responsibilities in areas of the containment process.
    - Taking systems offline.
    - Retrieving any lost, stolen or otherwise unaccounted for data.
    - Restricting access to systems entirely or to a small group.
    - Backing up all existing data and storing it in a safe location.
    - Reviewing basic security, including:
        - Changing passwords and login details on electronic equipment.
        - Ensuring access to places where electronic or hard data is kept is monitored and requires authorisation.
16. Where appropriate, e.g. if offences have been committed under the Computer Misuse Act 1990, the CEO/DPO will inform the police of the security breach.
17. Where the academy has been subject to online fraud, scams or extortion the DPO will also report this using the Action Fraud Website

18. The IT Representative will test all systems to ensure they are functioning normally and the incident will only be deemed "resolved" when it has been assured that the academy's systems are safe to use.

19. The DPO is required to report the data breach to the ICO if there is a risk to people's rights and freedoms. If the DPO decides that is risk is unlikely, the breach does not need to be reported; however, the school will need to justify this decision and document the breach.

5. Password Security, Access Control and User Privileges

The Trust/Academy understands that controlling what users have access to is important for promoting network security. User privileges will be differentiated, i.e. pupils will have different access to data and the network than members of staff, whose access will also be role-based.

1. Access to Data stored electronically is controlled through the use of Strong Passwords
2. All hardware, software, and operating systems will require passwords from individual users before use.
3. Access to authorised user accounts must have passwords that are not less than 6 ASCII characters in length and will use upper and lower case letters as well as numbers. Members of staff ensure that they have a strong password for all authorised user accounts and the same password not re-used across different systems
4. Authorised Users are responsible for keeping their assigned password(s) secure and must ensure their password(s) is neither disclosed to, nor used by, anyone else under any circumstances;
5. Users will be required to change their passwords in the event they become known to other individuals.
6. Use of another person's username or password will constitute an Information Security Breach and must be reported in accordance with the procedures set out in this policy or any other relevant policy from time to time in force;
7. Authorised Users are responsible for ensuring that all Academy and/or Client Devices used to access Data or other confidential information, are logged off, switched off or otherwise controlled by a Strong Password when unattended or not in use, at all times
8. Authorised Users with access to the Academy network or a Client Device which is used for, or in connection with Academy business is responsible for any actions carried out under their username and password.
9. Where available, Members of Staff using critical systems or accessing Personal or Special Category Personal Data should use Two-Factor Authentication.
10. Passwords will be changed on a frequent basis (at least every 3 months) to prevent access to facilities which could compromise network security.
11. Setting up of user privileges is in line with recommendations from the headteacher and IT Representative and maintaining a written record of those privileges. (Please see ICT GDPR Guide reference ICT Platform Contacts) Each Academy to complete a

Register of who is responsible for the different platforms to be included in their own ICT GDPR Guide)

12. The IT Lead Representative will ensure that user accounts are set to allow users access to the facilities required, whilst minimising the potential for deliberate or accidental attacks on the network. A 2 factor authentication is utilised for all staff. Conditional access based on location (Geolocation) can be used to bypass 2 factor authentication for teachers in the classroom However this should be used in combination device checks i.e encryption and antivirus..
13. The Broadband Provider utilises an active filter and Internet content is monitored and filtered real time by the provider. If there is anything that appears that is inappropriate this is noted by the member of staff who would notify IT Support for manual filtering.
14. Any member of staff or pupil that has accessed inappropriate or malicious content will be recorded in accordance with the monitoring process
15. The Academy maintains an up-to-date inventory of all usernames and passwords, removing any inactive users from the academy's system, ensuring that this is always up-to-date. This record is encrypted.
16. The IT Lead will be able to reset passwords when necessary.
17. Where pupils have individual logins the teacher/IT lead will set up their individual user account, ensuring appropriate access and that the username and password is recorded.
18. Defining users' access rights for both staff and pupils in accordance with the E, Safety Policy and ensuring of procedures for accessing the Academy/Trust network
19. The "master user" or administrator password will be made available to the headteacher, IT Lead and the DPO and will be kept in the academy safe.
20. Recording any alerts for access to inappropriate content and notifying the headteacher
21. Confidential paper records will be kept in a locked filing cabinet, drawer or safe with restricted access and will not be left unattended or in clear view anywhere with general access.
22. The IT lead will ensure pupil user access rights and email accounts are deleted once they leave the Academy

6. Monitoring Usage

Monitoring user activity is important for the early detection of attacks and incidents, as well as inappropriate usage by pupils or staff. The academy will inform all pupils and staff that their usage will be monitored, in accordance with the Academy's Online Safety Policy.

1. If a user accesses inappropriate content or a threat is detected, an alert will be sent to the headteacher. Alerts will also be sent for unauthorised and accidental usage
2. Alerts will identify, the user, the activity that prompted the alert and the information, service, website that the user was attempting to access. Where the software does not send alerts the user will be required to log in to check user activity

3. Any alerts will be recorded in the incident log and reported to the headteacher and Data Protection Link Governor for the Academy as outlined in the Online Safety policy.
4. All data gathered by monitoring usage will be kept electronically. This data be accessible by the Data Protection Link Governor and DPO. This data may be used as a method of evidence for supporting a potential breach of network security. The data may be used as evidence to ensure the academy is protected and all software up to date
5. Internet Use - Alerts serve as a warning to ensure individuals do not ignore, turn off, bypass any information security controls that have been put in place by the Trust/Academy

7. Malware Prevention including Firewall

The Trust/Academy understands that malware can be damaging for network security and may enter the network through a variety of means, such as email attachments, social media, malicious websites or removable media controls.

1. The IT Representative will ensure that all academy devices have secure malware protection and undergo regular malware scans in line with specific requirements.
2. The Academy's firewall is managed locally /the broadband service connects to a firewall that is located on a system on the academy premises as either discrete technology or a component of another system or it is managed offsite remotely by the Broadband Provider.
3. Patches and fixes are applied quickly to ensure that the network security is not compromised.
4. Firewall is maintained by the Broadband Provider. It is the responsibility of the Broadband Provider under contract to maintain the firewall and broadband connection.
5. Any changes and/or updates that are added to servers, including access to new services and applications, are checked to ensure that they do not compromise the overall network security.
6. The firewall is checked regularly to ensure that a high level of security is maintained and there is effective protection from external threats.
7. Any compromise of security through the firewall is recorded using an incident log and is reported to the Headteacher of the Academy concerned and the DPO. The IT Representative will react to security threats to find new ways of managing the firewall.
8. The academy will consider installing additional firewalls on the servers in addition to the third-party service as a means of extra network protection. This decision will be made by the IT Representative in liaison with the headteacher, taking into account the level of security currently provided and any incidents that have occurred
9. Malware Detection is included in antivirus software and is updated automatically.
10. Malware protection will also be updated in the event of any attacks to the academy's hardware and software.

11. Staff will follow procedures for filtering and monitoring to keep pupils safe as set out in the Online Safety Policy.

12. The filtering system will be able to identify technologies and techniques that allow users to get around the filtering such as VPNs and proxy services and block them and provide alerts when any web content has been blocked.

13. Filtering of websites will ensure that access to websites with known malware are blocked immediately and reported to the IT Representative

14. Encryption is used to limit susceptibility to malware attack when on site

15. The IT Representative will review the mail security technology on a termly basis to ensure it is kept up-to-date and effective.

16. Staff members are only permitted to download apps on any academy-owned device from manufacturer-approved stores and with prior approval from the headteacher and IT Representative.

17. Where apps are installed, the IT Representative will keep up-to-date with any updates, ensuring staff are informed of when updates are ready, how to install them, and that they should do this without delay.

8. E Mail Security and Secure Data Transfer

1. Personal Data, Special Category Personal, confidential and sensitive information sent or transmitted externally using an electronic systems or services must be secured using a process that ensures the Data is encrypted and Users must carefully check the recipient's contact details before sending
2. Data must only be sent or transmitted externally when authorised by job description, Trust policy, applicable legislation, or when specially authorised by the Data Protection Officer
3. The sending or distribution of any Data should only be done in accordance with the applicable statutory provisions, this policy and any other applicable policy of the Academy;
4. The sending of Personal Data and Special Category Personal Data to personal cloud systems or services email accounts is expressly forbidden. Members of staff working remotely are required to access Data through the Trust's authorised systems and services
5. Data must not be sent using any systems or services, including but not limited to, cloud platforms and social media providers or any other type system not owned by the Academy, including text messaging.
6. Personal Data and Special Category Personal Data must be sent to named Users only. Multi-User posting, sending or transmission, including, but not limited to, email

lists, distribution groups, security groups, chat/team-based groups, forums, rooms, and channels is prohibited.

7. Emails containing sensitive or confidential information are password protected if there are unsecure servers between the sender and the recipient. Circular emails are sent BCC (Blind Carbon Copy) to email addresses are not disclosed to other recipients. When sending confidential information staff will always check that the recipient is correct before sending.
8. Before sharing information staff members should check they are allowed to send the information, there is adequate security in place to protect it and those who receive the data have been outlined in a privacy notice

9. Mobile Device/Removable Media Protection

1. Removable Media storing Data must only be used as a last resort, when all other options have been considered, including the need to store or process the data or the secure network service is not available.
2. Only Removable Media provided by the Academy or Trust that has been encrypted should be used for the storing of Data
3. Removable Media should not be used for the storing of Personal Data, Special Category or Sensitive Data unless the device is capable of and has been encrypted.
4. Removable Media must be stored securely
5. If Removable Media used for, or in connection with Academy business is lost or stolen, the loss/theft should be reported to Data Protection Officer and IT Support Team immediately. Where possible the Personal Device should be remotely accessed and the information erased.

10. Working from Home and Remote Access

1. Appropriate security software should be installed on staff members' personal devices where the headteacher has permitted for them to be used for work purposes.
2. Members of staff working remotely are required to access Data through the Trust's authorised systems and services.
3. Data must not be sent using any systems or services, including but not limited to, cloud platforms and social media providers or any other type system not owned by the Academy, including text messaging
4. The academy understands that pupils and staff may need to access the academy network from areas other than on the premises. Effective security management will be established to prevent access to, or leakage of, data, as well as any possible risk of malware.
5. The IT representative will encrypt all academy-owned devices for personal use, such as laptops, USB sticks, mobile phones and tablets, to ensure that they are password protected. If any portable devices are lost, this will prevent unauthorised access to personal data.

6. Before distributing any academy-owned devices, the IT Representative will ensure that manufacturers' default passwords have been changed. A set password will be chosen and the staff member will be prompted to change the password once using the device.
7. The IT Representative will check academy-owned devices on a termly basis to detect any unchanged default passwords.
8. Pupils and staff are not permitted to use their personal devices where the academy provides alternatives, such as work laptops, tablets and USB sticks, unless instructed otherwise by the headteacher.
9. If pupils and staff are instructed that they are able to use their personal devices, they will ensure that they have an appropriate level of security and firewall to prevent any compromise of the academy's network security. This will be checked by the IT Representative.
10. When using laptops, tablets and other portable devices, the headteacher will determine the limitations for access to the network,
11. Staff who use academy-owned laptops, tablets and other portable devices will use them for work purposes only, whether on or off the academy premises.
12. Staff members will avoid connecting to unknown Wi-Fi hotspots, such as in coffee shops, when using any laptops, tablets or other devices.
13. The IT Representative will employ a combination of encryption, antivirus and consistent patching of devices to protect the networks from the release of malware on the premises.
14. The academy uses tracking technology where possible to ensure that lost or stolen devices can be retrieved.
15. All data will be held on systems centrally in order to reduce the need for the creation of multiple copies, and/or the need to transfer data using removable media controls.
16. The Wi-Fi network at the academy will be password protected and will only be given out as required. Staff and pupils are not permitted to use the Wi-Fi for their personal devices, such as mobile phones or tablets, unless instructed otherwise by the headteacher.
17. A separate Wi-Fi network will be established for visitors at the academy to limit their access to printers, shared storage areas and any other applications which are not necessary. As the use of printers is password protected, temporary passwords may be provided.
18. Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of the school containing sensitive information are supervised at all times.
19. The physical security of the school's buildings and storage systems and access to them is reviewed on a weekly basis. If there are increased risks of burglary or vandalism then extra measures relating to secure data storage are implemented.
20. The school will regularly test, assess and evaluate the effectiveness of any and all measures in place for data security.

11 Backing Up Information.

The Trust recognises that it is essential for detailed records to be kept to enable retrieval

1. A back up of all electronic data held by the academy is performed on a daily basis through the onsite servers. These are stored on external hard drives. An additional back up is performed by the IT Representative and the date of the back-up is recorded and given to the Business Manager for secure storage. Each back-up is retained for 1 week before being overwritten.

2. Weekly back-ups are processed on site through the Academy. The server performs an incremental back-up on a monthly basis of any data that has changed since the previous back-up and will record the date of any incremental back-up, alongside a list of the files that have been included in the back-up.

3. The ICT technician will ensure that there are at least three backup copies of important data, on at least two separate devices – one of which will remain off-site, e.g. cloud backups.

4. The school will keep under review where servers can be replaced with cloud solutions, including accessing files, documents and shared folders. Where cloud solutions are used, the school will confirm its ICT provider ensures that data is portable and allows for:

- Secure encrypted transfer.
- Data export to an open standard or commonly used format.
- Data links through secure, documented application programming interfaces (APIs).
- A timely process for data transfer in an open standard or neutral format if the school ends the contract.
- Easy and secure access from a range of devices.

5. Where possible, back-ups are run overnight and are completed before the beginning of the next academy day.

6. Upon completion of back-ups, data is stored on the academy's hardware which is password protected.

7. Data is also replicated and stored in accordance with the academy's Cloud Procedures.

8. Only authorised personnel are able to access the academy's data.

12. Personal Network Storage and Cloud Storage

The following procedures apply to the use of Personal Network Storage, Cloud Storage:

1. Only cloud computing networks or services, including Social Media commissioned by the Academy, or expressly authorised by the Data Protection Officer, may be used to store and send information concerning or relating to Academy business. Please note that Dropbox Cloud Storage Area is the official channel for Trust electronic storage and is arranged and approved by CEO, who is also the Data Protection Lead for the Trust.
2. The use of personal cloud storage solutions (Skydrive, Onedrive Personal, iCloud, G-Drive etc.) for the transfer of Academy information is only to be used in connection with digital and educational learning. Any cloud solutions should use HTTPS for transmitting data with a check for the padlock icon
3. Personal Data, Special Category Personal, confidential and sensitive information, whether on the Academy network or a Client Device must not be stored on a cloud computing network or service not commissioned by the Academy, or expressly authorised by the Data Protection Officer.
4. If Data or other information concerning or relating to Academy business is to be stored in or on a cloud network, the Academy will take all reasonable steps to find out in which country the Data or other information is being stored, and to ensure that appropriate measures are in place in relation to any Data transferred outside of the EEA to comply with the UK General Data Protection Regulations.
5. If the Academy receives notification that Data in respect of Academy business has been corrupted, lost or otherwise compromised while stored on a cloud network, the Academy should ascertain whether any or all of the information stored in the cloud can be recovered and if this is possible restore that information
6. Any corruption, loss or compromise of information held on a cloud network should be recorded in the risk register and if appropriate reported via the mandatory reporting procedure The sending of Personal Data and Special Category Personal Data to personal cloud systems or services email accounts is expressly forbidden.

13. CCTV Systems, Printer, Scanner and Copier Security

CCTV Systems are subject to stringent security procedures, with restricted access. Please see CCTV policy.

Printers have been adapted so only when a password is input, can staff members print to the copiers/printers preventing confidential information being retrieved by other members of staff

14. Data Information Assets

The Headteacher/Business Manager will be responsible for ensuring the Information Security of all Information Assets held by or on behalf of the Academy. The nominated person will also have and maintain an Information Asset register which should record all Information Assets held by the Academy;

1. A copy of the Information Asset register will be filed with the Compliance and Training Manager /Data Protection Lead at the Trust each year;

2. The Academy will ensure that only authorised individuals are allowed access to restricted areas containing Personal Data or Special Category Personal Data or information systems where there is an identifiable need to access that area
3. Access to Personal Data and/or restricted physical locations will be monitored by the Academies nominated person to ensure authorised access to relevant information and to prevent unauthorised access to Personal Data or Special Category Personal Data;
4. Where an unidentified person or any other person without authorisation to be in a restricted area is found, the individual is to be challenged as to their identity and the purpose for which they are in the restricted area. If the unauthorised individual has no legitimate reason to be in the restricted area, this information is to be logged as an Information Security Breach and the Data Protection Officer should be consulted as to whether the matter requires reporting to the ICO
5. External doors and windows must be locked at the end of each day;
6. Equipment that serves multiple users must be capable of identifying and verifying the identity of each authorised user;
7. Devices or equipment capable of displaying output upon multi-user displays or presentation equipment, including but not limited to, Projectors, Interactive Whiteboards, televisions, video walls, remote computer sessions and desktops, or any other form of presentation equipment, must not be used to access, view or process personal Data in a manner that allows Persons other than the Authorised User to view the Data.
8. Members of staff of the Academy with access to and use of Data must maintain a clear desk and clear screen policy to reduce the risk of unauthorised access to Information Assets such as papers, media and information processing facilities;
9. Academy wireless systems should be secured to industry standard Enterprise security level/appropriate standards suitable for educational use;

Physical Security

An inventory will be kept of all ICT hardware and software currently in use at the Academy, including mobile phones and other personal devices provided by the academy. This will be stored in the headteacher's office/business manager's office and will be audited on a termly basis to ensure it is up-to-date. Any software that is out-of-date or reaches its 'end of life' will be removed from systems, i.e. when suppliers end their support for outdated products such that any security issues will not be rectified. (Please see Financial Procedures Manual for write off of equipment).

1. All Servers and storage devices should be securely locked in adequately ventilated places.
2. Laptops, cameras, ipads and tablets should be locked away when not in use.
3. Visitor Credentials and identity badges should be checked and any necessary information stored securely.
4. The issue and access to keys should be monitored and checked
5. Data recorded on paper must be kept locked away in a safe, cabinet or other form of secure furniture when not in use
6. Personal Data and Special Category Personal Data, confidential and sensitive information about the Academy whether stored electronically or on paper must be kept locked away in a secure room or in a safe, cabinet or other form of secure furniture when not in use

7. Documents containing Data must not be left unsecured, unattended at mail points or on printers, photocopiers, scanners or fax machines and must be removed immediately when received.

15. IT Requirements relating to Termination of Staff Contracts

Upon leaving the Academy, Members of Staff must return/transfer, in a useable format, all equipment and information, including Data to the Academy, on or before the agreed leaving date (e.g. last day of employment) to their Line Manager, or other Academy representative if their Line Manager is not available. This includes, but is not limited to:

1. All information, including data, used or stored as part of the role, both physical and electronic
2. All information, including files, documents and emails, including any Data, stored within individual Cloud Service accounts
3. Client Devices loaned by the Academy, including PIN numbers, usernames or passwords required to reuse or reset the devices (i.e. mobile phones, tablets, laptops, computers, other devices)
4. Any Removable Devices provided by the Academy
5. Access control, PIN, tokens and ID Cards
6. Keys and PIN numbers used to access physical locations
7. The above is detailed on the Leavers Form.

With Reference to Cloud Computing

Add an additional owner(s) to any Cloud Service Calendars and/or calendar resources that you own. This will ensure that these resources continue to be accessible once your Academy account is closed ¨ Make sure to transfer any important meetings in your Cloud Service Calendar to another owner ¨ Add an additional owner(s) to any Cloud Service Groups and Cloud Service Sites that you own. This will ensure that Cloud Service groups, lists and Sites continue to be accessible once your Academy account is closed

16. Business Continuity and Disaster Recovery

Each Academy within the Trust has developed a managed process to counteract the interruption of Academy business caused by major IT service failure. This is detailed in the business continuity and cyber response plans which includes all IT systems and networks which store and/or Process Data. (Please refer to Business Continuity Plan/Cyber Response Plan)

17. Personal Devices Procedures

See Mobile Phone and Camera Policy

18 Avoiding Phishing Attacks

1. The I T Representative configures all staff accounts using the principle of ‘least privilege’ – staff members are only provided with as much rights as are required to perform their jobs.

2. Designated individuals who have access to the master user account will avoid browsing the web or checking emails whilst using this account.

3. Two-factor authentication is used on any important accounts, such as the master user account.

4. The I T Representative/headteacher/business manager organises regular training for staff members – this will cover identifying irregular emails in order to help staff members spot requests that are out of the ordinary, such as receiving an invoice for a service not used, and who to contact if they notice anything unusual.

5. Staff will use the following warning signs when considering whether an email may be unusual:

    a. Is the email from overseas?

    b. Is the spelling, grammar and punctuation poor?

    c. Is the design and quality what you would expect from a large organisation?

    d. Is the email addressed to a ‘valued customer’, ‘friend’ or ‘colleague’?

    e. Does the email contain a veiled threat that asks the staff member to act urgently?

    f. Is the email from a senior member of the academy asking for a payment?

    g. Does the email sound too good to be true? It is unlikely someone will want to give another individual money or access to another service for free.

    h. Is it from a supplier advising of a change in bank account details for payment?

    i. Is it from a generic email address, such as gmail or Hotmail?

6. The IT Representative will ensure that email filtering systems are neither too strict or lenient; filtering that is too strict may lead to legitimate emails becoming lost, and too lenient filters may mean that emails that are spam or junk are not sent to the relevant folder.

7. The Data Protection Representative/Data Protection Officer ensure that the Academy/Trust Websites and Social Media Accounts are reviewed on a termly basis making sure only necessary information is shared

8. The headteacher will ensure parents, pupils, staff and other members of the academy community are aware of acceptable use of social media and the information they share about the academy and themselves, in accordance with the E Safety and Acceptable Use Policy

19. User Training and Awareness

As part of an Induction Training and on an annual basis the headteacher is responsible for ensuring that training for staff members on network security has been organised including Data Protection and Cyber Security. At these training sessions staff are advised that information security is the responsibility of everyone at all levels.

1. The IT Representative and headteacher arrange training for pupils and staff on a annual basis to ensure they are aware of how to use the network appropriately in accordance with the Online Safety Policy and have signed the appropriate declarations.

2. The Data Processing Representative will also arrange training for pupils and staff on anannual basis on maintaining data security, preventing data breaches, and how to respond in the event of a data breach.

3. Training for all staff members will be arranged by the DP Representative/IT Representative and DPO within two weeks following an attack, breach or significant update.

4. Through training, all pupils and staff will be aware of who they should inform first in the event that they suspect a security breach, and who they should inform if they suspect someone else is using their passwords.

5. Any new pupils who join the academy mid-term also receive appropriate training which will covers information regarding passwords, emails and cyberbullying and social media. Parents and pupils both sign an acceptable use agreement as detailed in the Online Safety Policy.

6. All users are made aware of the disciplinary procedures for the misuse of the network leading to malicious attacks, in accordance with the process detailed in the Online Safety Policy.

20. Assessment of Risks

The following questions will be considered by the Headteacher/CEO to fully and effectively assess the risks that the I T security breach has brought, and to help take the next appropriate steps.

1. What type and how much data is involved?

2. How sensitive is the data? Sensitive data is defined in the GDPR; some data is sensitive because of its very personal nature (e.g. health records) while other data types are sensitive because of what might happen if it is misused (e.g. bank account details).

3. Is it possible to identify what has happened to the data – has it been lost, stolen, deleted or tampered with?

4. If the data has been lost or stolen, were there any protective measures in place to prevent this, such as data and device encryption?

5. If the data has been compromised, have there been effective measures in place that have mitigated the impact of this, such as the creation of back-up tapes and spare copies?

6. Has individuals' personal data been compromised – how many individuals are affected?

7. Who are these individuals – are they pupils, staff, governors, volunteers, stakeholders, suppliers?

8. Could their information be misused or manipulated in any way?

9. Are there further implications beyond the risks to individuals? Is there a risk of loss of public confidence/damage to the academy's reputation, or risk to the academy's operations?

10. Who could help or advise the academy on the breach? Could external partners, authorities, or others provide effective support? (In the event that the Headteacher/DP Represenative are not confident in the risk assessment, they will seek advice from the DPO/ICO. (Please see Data Protection Policy Section 23 relating to the Management of Breaches and the Risk Management Policy)

21. Data Disposal

When disposing of data, paper documents will be shredded and digital storage devices will be physically destroyed when they are no longer required. Certificates of safe disposal should be signed for all disposed data, whether it is from a third party contractor or the IT Technicians as confirmation that data has been destroyed and laptops cleansed. This will be reviewed as part of the Internal Scrutiny Process.

22. Video Conferencing

As a Trust we are increasingly using Video Conferencing for our Meetings. We have acknowledged the Staffordshire County Council Research in that their recommendations are as follows:

- Adobe Connect – meets adequate security requirements
- GoToWebinar – meets adequate security requirements
- WhatsApp/FaceTime should be used with caution, when no other alternative available
- Zoom – Avoid does not have adequate security arrangements
- Microsoft Teams – meets adequate security arrangements

It is the recommendation that as a Trust we use Microsoft Teams as the preferred platform as they are the authorised service under the Microsoft Tenancy Agreement.

23. Monitoring and Review

This policy will be reviewed by the headteacher and DP Link Governor in conjunction with IT Representative and CEO and Compliance and Training Manager on an annual basis, together with an external review from the DPO.

The CEO is responsible for monitoring the effectiveness of this policy, amending necessary procedures and communicating changes to staff.