SOUTH WEST ESSEX
COMMUNITY EDUCATION TRUST

Data and Cyber-Security Breach Prevention and Management Plan

Policy approved by Finance, HR & Audit Committee

Next review June 2027

Contents

1. Statement of Intent
2. Legal framework
3. Types of security breach and causes
4. Roles and responsibilities
5. Secure configuration
6. Network security
7. Malware prevention
8. User privileges and passwords
9. Monitoring usage
10. Removable media controls
11. Home working and remote learning
12. Backing up data
13. Avoiding phishing attacks
14. User training and awareness
15. Data security breach incidents
16. Assessment of risks
17. Consideration of further notification
18. Evaluation
19. Monitoring and review

Statement of intent

SWECET (South West Essex Community Education Trust) is committed to maintaining the confidentiality, integrity and availability of its information and ensuring that the details of the finances, operations and individuals within the Trust are only accessible to the appropriate individuals. It is, therefore, important to implement appropriate levels of access, uphold high standards of security, take suitable precautions, and have systems and procedures in place that support this.

The Trust recognises, however, that breaches in security can occur. Most breaches are caused by human error, so the Trust will ensure all staff are aware of how to minimise this risk. In addition, because most information is stored online or on electronic devices that can be vulnerable to cyber-attacks, the Trust will ensure there are procedures in place to prevent attacks occurring. To minimise both risks, 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.

1. Legal framework

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

- Computer Misuse Act 1990
- The UK General Data Protection Regulation (UK GDPR (General Data Protection Regulations))
- Data Protection Act 2018
- National Cyber Security Centre (2018) 'Small Business Guide: Cyber Security'
- National Cyber Security Centre (N.D.) 'Cyber Essentials'
- ICO (2021) 'Guide to the UK General Data Protection Regulation (UK GDPR)'
- ESFA (Education and Skills Funding Agency) (2021) 'Academy Trust Handbook 2021'

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

- E-Safety Policy
- Data Protection Policy
- Acceptable Use Agreement
- Disciplinary Policy and Procedure
- Behavioural Policy

2. Types of security breach and causes

Unauthorised use without damage to data – involves unauthorised persons accessing data on the Trust system, e.g., 'hackers,' who may read the data or copy it, but who do not actually damage the data in terms of altering or deleting it. This includes unauthorised people within our schools, e.g., where pupils access systems that staff have left open and/or logged in, or where staff access data beyond their authorisation, as can occur in schools where all staff are given admin-level access for ease.

Unauthorised removal of data – involves an authorised person accessing data, who removes the data to pass it on to another person who is not authorised to view it, e.g., a staff member with authorised access who passes the data on to a friend without authorised access. This is also known as data theft. The data may be forwarded or deleted altogether.

Damage to physical systems – involves damage to the hardware in the Trust IT system, which may result in data being inaccessible to the Trust and/or becoming accessible to unauthorised persons.

Unauthorised damage to data – involves an unauthorised person causing damage to data, either by altering or deleting it. Data may also be damaged by a virus attack, rather than a specific individual.

Breaches in security may be caused by the actions of individuals, and may be accidental, malicious or the result of negligence:

- Accidental breaches can occur because of human error or insufficient training for staff, so they are unaware of the procedures to follow

- Malicious breaches can occur because of a hacker wishing to cause damage to the Trust through accessing and altering, sharing, or removing data
  Breaches caused by negligence can occur because of a staff member knowingly disregarding Trust policies and procedures or allowing pupils to access data without authorisation and/or supervision

Breaches in security may also be caused by system issues, which could involve incorrect installation, configuration problems or operational errors:

- The incorrect installation of antivirus software and/or use of outdated software can make the Trust software more vulnerable to a virus
- Incorrect firewall settings being applied, e.g., unrestricted access to the Trust network, can allow unauthorised individuals to access our system
- Operational errors, such as confusion between back-up copies of data, can cause the most recent data to be overwritten

3. Roles and responsibilities

The Trust IT Team is responsible for:

- Maintaining an inventory of all IT hardware and software currently in use in our Trust.
- Ensuring any out-of-date software is removed from the Trust's systems.
- Implementing effective firewalls to enhance network security and ensuring that these are monitored regularly.
- Installing, monitoring and reviewing filtering systems for the Trust network.
- Setting up user privileges in line with recommendations from the Executive Headteachers.
- Maintaining an up-to-date and secure inventory of all usernames and passwords.
- Removing any inactive users from the Trust's system and ensuring that this is always up-to-date.
- Installing appropriate security software on staff members' personal devices where the Trust has permitted for them to be used for work purposes, in line with the Trust's Working from Home and Overtime Policy.
- Performing a back-up of all electronic data held by the Trust, ensuring detailed records of findings are kept.
- Ensuring all Trust-owned devices have secure malware protection and are regularly updated.
- Recording any alerts for access to inappropriate content and notifying the Chief Operating Officer and Headteachers.
- Acting as the named point of contact within the Trust on all online safety issues.

The Chief Operating Officer is responsible for:

- Organising training and resources for Trust staff on online safeguarding risks and preventative measures.
- Liaising with the LA (Local Authority) where appropriate.
- Ensuring the relevant policies and procedures are in place to protect pupils and staff from harm, including the Online Safety Policy.

- Monitoring online safety incidents which could result in data breaches and reporting these to the Data Protection administrator to be logged.
- Liaising with relevant members of staff on online safety matters.
- The overall monitoring and management of data security.
- Deciding which strategies are required for managing the risks posed by internet use.
- Leading on the Trust's response to incidents of data security breaches.
- Assessing the risks to the Trust in the event of a data security breach.
- Producing a comprehensive report following a full investigation if a significant data security breach occurs.
- Determining which organisations and individuals need to be notified following a data security breach, and ensuring they are notified.
- Working with the IT department and Chief Operating Officer after a data security breach to determine where weaknesses lie and improve security measures.
- Monitoring and reviewing the effectiveness of this policy, alongside the Chief Operating Officer, and communicating any changes they recommend.

Head Teachers are responsible for:

- Ensuring all staff members and pupils are aware of their responsibilities in relation to this policy.
- Establishing any new user profiles and defining users' access rights for both staff and pupils, communicating these to the IT technician and maintaining a written record of privileges.
- Responding to alerts for access to inappropriate content in line with the Online Safety Policy.
- Informing the IT department of staff members who are permitted to use their personal devices for work purposes so that appropriate security methods can be applied.
- Overseeing any necessary disciplinary actions in response to a data security breach.
- Taking responsibility for online safety within the school and promoting online safety measures to parents.
- Coordinating the Schools participation in local and national online safety events, e.g., Safer Internet Day.

The Trust Board is responsible for:

- Supporting the Chief Operating Officer and other relevant staff in the delivery of this policy.

All staff members are responsible for:

- Understanding their responsibilities regarding this policy.
- Undertaking the appropriate training.
- Ensuring they are aware of when new updates become available and how to safely install them.

4. Secure configuration

An inventory will be kept of all IT hardware and software currently in use at the Trust, including mobile phones and other personal devices provided by the Trust. The inventory will be stored in a secure cloud account and will be audited annually to ensure it is up-to-date. Any changes to the IT hardware or software will be documented using the inventory and will be authorised by the IT department before use.

All systems will be audited on a termly basis by the IT department to ensure the software is up-to-date. Any new versions of software or new security patches will be added to systems, ensuring that they do not affect network security, and will be recorded in the inventory. Any software that is out-of-date or reaches its 'end of life' will be removed from systems, e.g., when suppliers end their support for outdated products, meaning that the product is not able to fulfil its purpose anymore.

All hardware, software and operating systems will require passwords from individual users. Passwords will be changed on an annual basis to prevent access to facilities which could compromise network security. The Trust believes that locking down hardware, such as using strong passwords, is an effective way to prevent access to facilities by unauthorised users. Passwords will need to adhere to a specific character length, use special characters, and not be obvious or easy to guess, in line with the Trust's policy on passwords.

The Trust will consider referring to the five security controls outlined in the National Cyber Security Centre's (NCSC's) 'Cyber Essentials.' These are:

- **Firewalls** – Firewalls function as a barrier between internal networks and the internet. They will be installed on any device that can access the internet, particularly where staff are using public or otherwise insecure Wi-Fi.
- **Secure configuration** – The default configurations on devices and software are often as open as possible to ensure ease of use, but they also provide more access points for unauthorised users. The Trust will disable or remove any unnecessary functions and change default passwords to reduce the risk of a security breach.
- **Access control** – The more people have access to data, the larger the chance of a security breach. The Trust will ensure that access is given on a 'need-to-know' basis to help protect data. All accounts will be protected with strong passwords, and where necessary, two-factor authorisation.
- **Malware protection** – The Trust will protect itself from malware by installing antivirus and anti-malware software, and using techniques such as whitelisting (a cyber-security strategy under which a user can only take actions on their computer that an administrator has explicitly allowed in advance) and sandboxes (an isolated virtual machine in which potentially unsafe software code can execute without affecting network resources or local applications).
- **Patch management** – The Trust will install software updates as soon as they are available to minimise the period in which vulnerabilities can be exploited. If the manufacturer stops offering support for the software, the Trust will replace it with a more up-to-date alternative.

5. Network security

In line with the UK GDPR, the Trust will appropriately test, assess, and evaluate any security measures put in place on a yearly basis to ensure these measures remain effective.

The Trust will employ firewalls to prevent unauthorised access to the systems.

Localised firewall deployment

The Trust's firewall will be deployed as a localised deployment, which means the broadband service connects to a firewall that is located on an appliance or system on our school premises, as either discrete technology or a component of another system.

As the Trust firewall is managed on the school premises, it is the responsibility of the IT department to effectively manage the firewall. The IT department will ensure that:

- The firewall is checked weekly for any changes and/or updates, and that these are recorded using the inventory.
- 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.
- The firewall is also checked weekly to ensure that a high level of security is maintained, and there is effective protection from external threats.
- Any compromise of security through the firewall is recorded using an incident log and is reported to the Chief Operating Officer. The IT department will react appropriately to security threats to find new ways of managing the firewall.

6. Malware prevention

The Trust 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.

The IT department will ensure that all Trust devices have secure malware protection and undergo regular malware scans in line with specific requirements. The IT department will update malware protection on a yearly basis to ensure it is up-to-date and can react to changing threats. Malware protection will also be updated in the event of any attacks to the Trust's hardware and software.

Filtering of websites, as detailed in the 'User privileges and passwords' Section of this policy, will ensure that access to websites with known malware are blocked immediately and reported to the IT Department.

The Trust will use mail security technology, which will detect and block any malware that is transmitted by email. This will also detect any spam or other messages which are designed to exploit users. The IT department will review the mail security technology on a yearly basis to ensure it is kept up-to-date and effective.

Staff members are only permitted to download apps on any school-owned device from manufacturer-approved stores and with prior approval from the IT department. Where apps

are installed, the IT Department will keep up-to-date with any updates, ensuring staff are informed of when updates are ready and how to install them.

7. User privileges and passwords

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

The Chief Operating Officer will clearly define what users have access to and will communicate this to the IT department, ensuring that a written record is kept. The IT department will ensure that user accounts are set up to allow users access to the facilities required, in line with the Chief Operating Officer's instructions, whilst minimising the potential for deliberate or accidental attacks on the network.

All users will be required to change their passwords on an annual basis and/or if they become known to other individuals, in line with the 'Secure configuration' Section of this policy. Pupils are responsible for remembering their passwords; however, the IT Department will have an up-to-date record of all usernames and passwords and will be able to reset them if necessary. The record of all usernames and passwords is encrypted. Only the IT department has access to this inventory. Multi-factor authentication (multiple different methods of verifying the user's identity) should be used wherever possible.

The administrator password used by the IT team will be made available to the Headteacher upon request.

The master user account is used as the 'administrator' which allows designated users to make changes that will affect other users' accounts in the Trust, such as changing security settings, monitoring usage, and installing software and hardware.

A multi-user account will be created for visitors to our schools, such as volunteers, and access will be filtered as per the headteacher's instructions. Usernames and passwords for this account will be changed on a yearly basis and will be provided as required.

Automated user provisioning systems will be employed to automatically delete inactive users or users who have left the Trust. The IT department will manage this provision to ensure that all users that should be deleted are, and that they do not have access to the system.

The IT department will review the password system on a yearly basis to ensure it is working at the required level.

8. 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 Trust will inform all pupils and staff that their usage will be monitored, as well as how it is being monitored and why, in accordance with the Trust's Acceptable Use Policy and Online Safety Policy.

If a user accesses inappropriate content or a threat is detected, an alert will be sent to the IT department. Alerts will also be sent for unauthorised and accidental access. Alerts will identify

the user, the activity that prompted the alert, and the information or service the user was attempting to access.

The IT department will record any alerts using an incident log and will report this to the Chief Operating Officer. The Chief Operating Officer will then inform the headteacher and others as appropriate. All incidents will be responded to in accordance with the 'Data security breach incidents' Section of this policy, and as outlined in the Online Safety Policy.

The IT department will ensure that websites are filtered on a weekly basis for inappropriate and malicious content. Any member of staff that accesses inappropriate or malicious content will be recorded in accordance with the monitoring process in the 'Data security breach incidents' Section of this policy.

All data gathered by monitoring usage will be kept on a secure shared drive for easy access when required. This data may be used as a method of evidence for supporting a not-yet-discovered breach of network security. In addition, the data may be used to ensure the Trust is protected and all software is up-to-date.

9. Removable media controls

The Trust understands that staff may need to access the network from outside our premises. Effective security management will be established to prevent access to, or leakage of, data, as well as any risk of malware.

The IT department will encrypt all Trust-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.

Before distributing any Trust-owned devices, the IT department 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. The IT department will check Trust-owned devices on a yearly basis to detect any unchanged default passwords.

Staff are not permitted to use their personal devices where the Trust provides alternatives, such as work laptops and tablets unless instructed otherwise by the Chief Operating Officer. If staff are instructed that they can use their personal devices, they will ensure that they have an appropriate level of security and firewall to prevent any compromise of the Trust's network security. This will be checked by the IT department.

Staff who use Trust-owned laptops, tablets and other portable devices will use them for work purposes only, whether on or off our premises. Staff will avoid connecting to unknown Wi-Fi hotspots, such as in coffee shops, when using any Trust -owned laptops, tablets, or other devices, or when accessing the network.

The IT department will use encryption to filter the use of websites on Trust-owned devices to prevent inappropriate use and external threats which may compromise network security when bringing the device back onto the premises. The Trust uses tracking technology where possible to ensure that lost or stolen Trust-owned devices can be retrieved.

All data will be held on systems centrally to reduce the need for the creation of multiple copies, and/or the need to transfer data using removable media controls.

The Wi-Fi network at our school's 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 agreed prior to usage. A separate Wi-Fi network will be established for visitors at our schools to limit their access to the Trust's networks and any other applications which it is not necessary for them to access.

10. Home working and remote learning

Staff will adhere to data protection legislation and the Trust's related policies when working remotely.

Staff will receive annual training regarding what to do if a data protection issue arises from any home working or remote learning.

Wherever possible, personal data will not be taken home by staff members for the purposes of home working, due to the risk of data being lost or the occurrence of a data breach.

Staff may be required to use their own devices for the duration of the remote working or learning period. Any user on a personal device will need to access the Trust network through a proxy, e.g., VPN. Using a shared personal or household device for work purposes should be avoided where possible; however, the Trust understands that this may not always be possible.

Staff are not permitted to let their family members or friends use any Trust equipment, to protect the confidentiality of any personal data held on the device. Any staff member found to have shared personal data without authorisation will be disciplined in line with the Disciplinary Policy and Procedure. This may also result in a data breach that the Trust would need to record and potentially report to the ICO.

Staff who require access to personal data to enable them to work from home will first seek approval from the Headteacher, and it will be ensured that the appropriate security measures are in place by the IT department, e.g., secure passwords and anti-virus software.

Staff will be informed that caution should be exercised while accessing personal data if an unauthorised person is in the same room. If a member of staff needs to leave their device unattended, the device should be locked. Where staff are using a personal device, they will be advised that a similar function should be implemented.

Personal data should only be transferred to a home device if this is necessary for the member of staff to carry out their role. When sending confidential information, staff must never save confidential information to a personal or household device. Data that is transferred from a work to a home device will be encrypted so that if any data is lost, stolen or subject to unauthorised access, it will remain safe until it can be recovered.

To ensure reasonable precautions are taken when managing data, staff will avoid:

- Keeping personal data on unencrypted hard drives.
- Sending work emails to and from personal email addresses.

- Leaving logged-in devices and files unattended.
- Using shared home devices where other household members can access personal data.
- Using an unsecured Wi-Fi network.

Staff working from home will be encouraged and enabled to go paperless, where possible, as paper files cannot be protected digitally and may be misplaced. If sensitive data is taken off Trust premises to allow staff to work from home, it will be transported in a lockable bag or container. The Trust procedures for taking data off the school premises will apply to both paper-based and electronic data.

Any devices that are used by staff for remote working and learning will be assessed by the IT department prior to being taken to the home setting, using the following checks:

- System security check – the security of the network and information systems
- Data security check – the security of the data held within the systems
- Online security check – the security of any online service or system.
- Device security check – the security of the personal device, including any 'bring your own device' systems

The IT department will provide staff with details and instructions for accessing the Trust network that they will be using throughout the duration of the remote working and learning period.

If a staff member decides to leave the Trust permanently, all data in any form will be returned on or before their last day.

11. Backing up data

The IT department performs a back-up of all electronic data held by the Trust daily, and the date of the back-up is recorded using a log. Each back-up is retained for two weeks before being deleted. The IT department performs an offline back-up on a weekly basis of any data that has changed since the previous back-up. The Trust must follow the NCSC's guidance on backing up data where necessary, including:

- Identifying what essential data needs to be backed up.
- Storing backed-up data in a separate location to the original data.
- Consider using the Cloud to store backed-up data.
- Refer to the NCSC's Cloud Security Guidance.
- Ensure that backing up data is regularly practised.

Where possible, back-ups are run overnight and are completed before the beginning of the next day. Upon completion of back-ups, data is stored on the Trust's hardware, which is password protected. Data will be replicated and stored in accordance with the Trust's Cloud Computing Policy. Only authorised personnel will be able to access back-ups of the Trust's data.

The Trust will ensure that offline or 'cold' back-ups are secured. This can be done by only digitally connecting the back-up to live systems when necessary, and never having all offline back-ups connected at the same time.

12. Avoiding phishing attacks

The IT department will configure 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.

Designated individuals who have access to the master user account will avoid browsing the web or checking emails whilst using this account. Two-factor authentication is used on any important accounts, such as the master user account, or any key accounts, such as the headteacher's.

Staff will use the following warning signs when considering whether a communication may be unusual:

- Is it from overseas?
- Is the spelling, grammar, and punctuation poor?
- Is the design and quality what you would expect from a large organisation?
- Is it addressed to a 'valued customer,' 'friend' or 'colleague'?
- Does it contain a veiled threat that asks the staff member to act urgently?
- Is it from a senior member of the Trust asking for a payment?
- Is it from a supplier advising of a change in bank account details for payment?
- Does it sound too good to be true? It is unlikely someone will want to give another individual money or access to another service for free.
- Is it from a generic email address, such as Gmail or Hotmail?

The IT department will ensure that an appropriate email filtering system is used to identify which emails would be classed as junk or spam, applied in accordance with the 'Malware prevention' Section of this policy. The IT department will ensure that the filtering system is neither too strict nor too lenient, to allow the correct emails to be sent to the relevant folders.

To prevent anyone having access to unnecessary personal information, the IT department will ensure each of our school's social media accounts and websites are reviewed on a termly basis, making sure that only necessary information is shared. The IT department and Chief Operating Officer will ensure the Trust's Social Media Policy includes expectations for sharing of information and determines what is and is not appropriate to share.

The Headteacher will ensure parents, pupils, staff, and other members of our school communities are aware of acceptable use of social media and the information they share about the school/Trust and themselves, in accordance with the Trust's Acceptable Use Policy.

13. User training and awareness

The Chief Operating Officer and HR Director will arrange training for staff on a yearly basis to ensure they are aware of how to use the network appropriately, in accordance with the Acceptable Use Policy. This will cover identifying irregular methods of communication 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. Unusual communications could come in a variety of forms, e.g., emails, phone calls, text messages or social media messages.

The HR department will also arrange training for staff on a yearly basis on maintaining data security, preventing data breaches, and how to respond in the event of a data breach.

Through training, all staff will be aware of who they should inform first if they suspect a security breach, and who they should inform if they suspect someone else is using their passwords. All staff will receive training as part of their induction programme.

All users will be made aware of the disciplinary procedures for the misuse of the network leading to malicious attacks, in accordance with the process detailed in the Behavioural Policy and the Disciplinary Policy and Procedure.

14. Data security breach incidents

Any individual that discovers a data security breach will report this immediately via email to databreach@swecet.org.

When an incident is raised, the Chief Operating Officer will record the following information:

- Name of the individual who has raised the incident
- Description and date of the incident
- Description of any perceived impact
- Description and identification codes of any devices involved, e.g., school-owned laptop
- Contact details for the individual who discovered the incident
- Whether the incident needs to be reported to the relevant authorities, e.g., the ICO or police

The Trust's Chief Operating officer/Data Protection Administrator will take the lead in investigating the breach and will be allocated the appropriate time and resources to conduct this. The as quickly as reasonably possible, will ascertain the severity of the breach and determine if any personal data is involved or has been compromised. The Chief Operating Officer will oversee a full investigation and produce a comprehensive report. The cause of the breach, and whether it has been contained, will be identified – ensuring that the possibility of further loss or jeopardising of data is eliminated or restricted as much as possible.

If the Chief Operating Officer determines that the severity of the security breach is low, the incident will be managed in accordance with the following procedures:

- In the event of an internal breach, the incident is recorded using A Data breach log, and by identifying the user and the website or service they were trying to access
- The headteacher will issue disciplinary sanctions to the pupil or member of staff who caused the breach, in accordance with the Behavioural Policy or Disciplinary Policy and Procedure
- The Trust will work with the third-party provider to provide an appropriate response to the attack, including any in-house changes
- Any further action which could be taken to recover lost or damaged data will be identified – this includes the physical recovery of data, as well as the use of back-ups

Where the security risk is high, the Chief Operating Officer will establish what steps need to be taken to prevent further data loss, which will require support from various Trust departments and staff. This action will 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.

Where appropriate, e.g., if offences have been committed under the Computer Misuse Act 1990, the Headteacher or his/her representative will inform the police of the security breach.

Multi Academy Trusts are required to report personal data breaches to the ICO if there is a likelihood of risk to people's rights and freedoms. If the Chief Operating Officer decides that risk is unlikely, the breach does not need to be reported; however, the Trust will need to justify this decision and document the breach.

The Trust COO will notify the ICO within 72 hours of becoming aware of a breach where it is likely to result in a risk to the rights and freedoms of individuals.

The UK GDPR recognises that it will not always be possible to investigate a breach fully within 72 hours. The information required can be provided in phases if this is done without undue further delay.

In line with the UK GDPR, the following must be provided to the ICO when reporting a personal data breach:

- A description of the nature of the breach, including, where possible:
    - The categories and approximate number of individuals concerned
    - The categories and approximate number of personal data records concerned
- The name and contact details of the DPO
- A description of the consequences of the breach
- A description of the measures taken, or proposed to be taken, to deal with the breach
- A description of the measures taken to mitigate any possible adverse effects, where appropriate

The Trust will report a personal data breach via the ICO website. The Trust will also make use of the ICO's self-assessment tool to determine whether reporting a breach is a necessary next step.

Where a breach is likely to result in a significant risk to the rights and freedoms of individuals, the Trust will notify those concerned directly of the breach without undue delay.

Where the Trust has been subject to online fraud, scams or extortion, the Chief Operating Officer will also report this using the Action Fraud website.

The IT department 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 Trust's systems are safe to use.

The Trust is aware it must seek permission from the ESFA to pay any cyber-ransom demands in the event of a cyber-crime.

15. Assessment of risks

The following questions will be considered by the Chief Operating Officer to fully and effectively assess the risks that the security breach has brought, and to help take the next appropriate steps. All relevant questions will be clearly and fully answered in the report, which should record:

- What type of, and how much, data is involved?
- How sensitive is the data? Sensitive data is defined in the UK 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).
- Is it possible to identify what has happened to the data – has it been lost, stolen, deleted, or tampered with?
- If the data has been lost or stolen, were there any protective measures in place to prevent this, such as data and device encryption?
- 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?
- Has individuals' personal data been compromised – how many individuals are affected?
- Who are these individuals – are they pupils, staff, governors, volunteers, stakeholders, suppliers?
- Could their information be misused or manipulated in any way?
- Could harm come to individuals? This could include risks to the following:
    - Physical safety
    - Emotional wellbeing
    - Reputation
    - Finances
    - Identity
    - Private affairs becoming public.
- Are there further implications beyond the risks to individuals? Is there a risk of loss of public confidence and/or damage to the Trust's reputation, or risk to the Trust's operations?
- Who could help or advise the Trust on the breach? Could the LA, external partners, authorities, or others provide effective support?
- Does the breach need to be reported to the ICO? If so, has it been successfully reported without undue delay?

If the Chief Operating Officer, or other persons involved in assessing the risks to the Trust, are not confident in the assessment of risk, they will seek advice from the ICO.

16. Consideration of further notification

The Chief Operating Officer will consider whether there are any legal, contractual, or regulatory requirements to notify individuals or organisations that may be affected or who will have an interest in data security.

The Chief Operating Officer will assess whether notification could help the individual(s) affected, and whether the individual(s) could act on the information provided to mitigate risks, e.g., by cancelling a credit card or changing a password. In line with the 'Data security breach incidents' Section of this policy, if many people are affected, or there are serious consequences, the ICO will be informed.

The Chief Operating Officer will consider who to notify, what to tell them and how they will communicate the message, which may include:

- A description of how and when the breach occurred and what data was involved.
- Details of what has already been done to respond to the risks posed by the breach.
- Specific and clear advice on the steps they can take to protect themselves, and what the Trust is willing to do to help them.
- A way in which they can contact the Trust for further information or to ask questions about what has occurred.

The Chief Operating Officer will consider, as necessary, the need to notify any third parties, such as the police, insurers, professional bodies, funders, trade unions, website and/or system owners, banks and/or credit card companies, who can assist in helping or mitigating the impact on individuals.

17. Evaluation

The Data Protection Administrator will document all the facts regarding the breach, its effects and the remedial action taken. This should be an evaluation of the breach, and what actions need to be taken forward.

The Chief Operating Officer will consider the data and contexts involved, establish the root of the breach, and where any present or future risks lie, taking into consideration whether the breach is a result of human or systematic error and see how a recurrence can be prevented.

The Chief Operating Officer will identify any weak points in existing security measures and procedures. The Chief Operating Officer will work with the IT department to improve security procedures wherever required. The Chief Operating Officer and IT department will identify any weak points in levels of security awareness and training.

The Chief Operating Officer will report on findings and implement the recommendations of the report after analysis and discussion.

18. Monitoring and review

This plan will be reviewed by the Chief Operating Officer and Trust committee on an annual basis. The next scheduled review date for this plan is June 2027.