Cyber-security Policy

Key Document Details:			
Author:	Data Protection Officer	**Department:**	Central Services
Reviewer:	Head of Primary Education	**Version No:**	1.3
Last Review:	September 2023	**Next Review:**	September 2024
Approver:	Executive Team	**Date Ratified:**	September 2023

Contents

Document Change History

Date:	Version:	Description of Changes:
08/22	1.2	Updated ‘Roles and responsibilities’, ‘Secure configuration’, ‘Removable media controls’ and ‘Backing up data’. Added ‘Home working and remote learning’ and ‘Avoiding phishing attacks’.
09/23	1.3	Renamed to ‘Cyber-security Policy’ and updated in line with the DfE's 'Meeting digital and technology standards in schools and colleges' guidance.

Mission Statement

"To nurture and develop all people in our Trust so that they reach their full potential academically, vocationally, and personally, including being positive role models for future generations in the community. We will achieve this by providing high quality values-based education that cultivates employability and life skills making our schools the first choice for young people, parents, carers, staff and employers."

Values

The values of Respect, Excellence, Collaboration, Independence, Perseverance, Enjoyment, Leadership, Integrity and Care are central to everything we do at the Skills for Life Trust.

Statement of Equality

We have carefully considered and analysed the impact of this policy on equality and the possible implications for pupils with protected characteristics, as part of our commitment to meet the Public Sector Equality Duty (PSED) requirement to have due regard to the need to eliminate discrimination, advance equality of opportunity and foster good relations.

Purpose

The Skills for Life 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. In Trusts and schools, 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

1.1. This policy has due regard to statutory legislation and regulations including, but not limited to, the following:

- Computer Misuse Act 1990
- The UK General Data Protection Regulation (UK GDPR)
- 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 (2022) 'Academy Trust Handbook 2022'
- (DfE) 'Meeting digital and technology standards in schools and colleges'

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

- Data Protection Policy
- E-Safety Policy
- Acceptable Use Policy/Agreement
- Working from Home and Overtime Policy
- Disciplinary Policy and Procedure
- Cloud Computing Policy
- Behaviour Policy
- Social Media Policy

2. Types of security breach and causes

2.1. **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 the Trust, e.g. where pupils access systems that staff have left open and/or logged in, or where staff access data beyond their authorisation.

2.2. **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.

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

2.4. **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 by a specific individual.

2.5. Breaches in security may be caused as a result of actions by individuals, which may be accidental, malicious or the result of negligence:

- Accidental breaches can occur as a result of human error or insufficient training for staff, so they are unaware of the procedures to follow
- Malicious breaches can occur as a result of a hacker wishing to cause damage to the Trust through accessing and altering, sharing or removing data
- Breaches caused by negligence can occur as a result of a staff member knowingly disregarding Trust policies and procedures or allowing pupils to access data without authorisation and/or supervision

2.6. Breaches in security may also be caused as a result of system issues, which could involve incorrect installation, configuration problems or an operational error:

- Incorrect installation of anti-virus software and/or use of software which is not the most up-to-date version, meaning the trust software is more vulnerable to a virus
- Incorrect firewall settings are applied, e.g. access to the trust 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

3. Roles and responsibilities

3.1. The trust board and school governing boards are responsible for:

- Ensuring the school has appropriate cyber-security measures in place.
- Ensuring the school has an appropriate approach to managing data breaches in place.
- Supporting headteachers and other relevant staff in the delivery of this policy.
- Ensuring the school meets the relevant cyber-security standards.

3.2. Headteachers are responsible for:

- Ensuring all staff members and pupils are aware of their responsibilities in relation to this policy.
- Responding to alerts for access to inappropriate content in line with the Online Safety Policy.
- Informing the IT technicians 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.
- Organising training for staff members in conjunction with the Trust IT Manager.

3.3. The DPO is responsible for:

- 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 of a data security breach.
- Determining which organisations and individuals need to be notified following a data security breach, and ensuring they are notified.
- Working with the Trust IT Manager, online safety officer and headteacher after a data security breach to determine where weaknesses lie and improve security measures.
- Monitoring and reviewing the effectiveness of this policy.

3.4. The Trust IT Manager is responsible for:

- Maintaining an inventory of all IT hardware and software currently in use at the Trust.
- Ensuring any out-of-date software is removed from the Trust 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 headteacher.
- Maintaining an up-to-date and secure inventory of all usernames and passwords.
- Removing any inactive users from the Trust system and ensuring that this is always up-to-date.
- Installing appropriate security software on staff members' personal devices where the

headteacher 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.
- Organising training for staff members on data security, network security and preventing breaches.
- Recording any alerts for access to inappropriate content and notifying the headteacher.

3.5. The online safety officer is responsible for:

- Organising training and resources for staff on online safeguarding risks and preventative measures.
- Taking responsibility for online safety within the Trust and promoting online safety measures to parents.
- Monitoring online safety incidents which could result in data breaches and reporting these to the DPO.
- Acting as the named point of contact within the Trust on all online safety issues.
- Liaising with relevant members of staff on online safety matters, e.g. the DPO and IT technicians.
- Coordinating the Trust's participation in local and national online safety events, e.g. Safer Internet Day.

3.6. The DSL will be responsible for:

- Assessing whether there is a safeguarding aspect to any cyber-security incident and considering whether any referrals need to be made.

3.7. All staff members are responsible for:

- Understanding their responsibilities in regard to 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

4.1. An inventory will be kept of all IT hardware and software currently in use at the trust, including mobile phones and other mobile devices provided by the trust. This will be stored on a secure server and audited on a termly basis to ensure it is up-to-date.

4.2. Any changes to the IT hardware or software will be documented using the inventory, and will be authorised by the IT technicians before use.

4.3. All systems will be audited on a termly basis to ensure the software is up-to-date and 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 on the inventory.

4.4. 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 out-dated products such that any security issues will not be rectified.

4.5. All hardware, software and operating systems will require passwords for individual users before use. Users are forced to change their password annually to prevent access to facilities, which could compromise network security.

4.6. The trust believes that locking down hardware, such as through the use of strong passwords, is an effective way to prevent access to facilities by unauthorised users.

4.7. Passwords will need to adhere to a specific character length, use special characters, and not be obvious or easy to guess.

4.8. 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 time frame 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.

4.9. The Trust IT manager will:

- Protect every device with a correctly configured boundary, or software firewall, or a device that performs the same function.
- Change the default administrator password, or disable remote access on each firewall.
- Protect access to the firewall's administrative interface with multi-factor authentication (MFA), or a small, specified IP-allow list combined with a managed password, or prevent access from the internet entirely.
- Keep firewall firmware up to date.
- Check monitoring logs as they can be useful in detecting suspicious activity.
- Block inbound unauthenticated connections by default.
- Document reasons why particular inbound traffic has been permitted through the firewall.
- Review reasons why particular inbound traffic has been permitted through the firewall often, change the rules when access is no longer needed.
- Enable a software firewall for devices used on untrusted networks, like public wi-fi.

4.10. All devices will be set up in a way that meets the standards described in the technical requirements.

4.11. The Trust IT Manager will devise a system for monitoring logs and documenting decisions made on inbound traffic.

5. Network security

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

5.2. The trust will employ firewalls in order to prevent unauthorised access to the systems.

5.3. The trust's firewall and network security are deployed as both centralised and localised deployments.

5.4. The trust's main firewall is managed locally by a third party and the firewall management service will be thoroughly investigated by the Trust IT Manager to ensure that:

- Any changes and updates that are logged by authorised users within the trust are undertaken efficiently by the provider to maintain operational effectiveness.
- Patches and fixes are applied quickly to ensure that the network security is not compromised.

5.5. A second level of security is also managed on the premises; it is the responsibility of the Trust IT Manager to effectively manage this internal system and will ensure that:

- Software is checked termly for any changes and/or updates, and that these are recorded.
- 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.
- Any compromise of security through the internal system is recorded using an incident log and is reported to the Trust IT Manager, who will react to security threats to find new ways to improve network security.

5.6. The trust will be aware that security standards may change over time with changing cyber threats.

5.7. The trust will ensure that the security of every device on its network is reviewed regularly.

5.8. The trust will agree with the ICT technician a system for recording and reviewing decisions made about network security features.

5.9. To ensure that the network is as secure as possible, the trust will:

- Keep a register, list, or diagram of all the network devices.
- Avoid leaving network devices in unlocked or unattended locations.
- Remove or disable unused user accounts, including guest and unused administrator accounts.
- Change default device passwords.
- Require authentication for users to access sensitive school data or network data.
- Remove or disable all unnecessary software according to your organisational need.
- Disable any auto-run features that allow file execution.
- Set up filtering and monitoring services to work with the network's security features enabled.

- Immediately change passwords which have been compromised or suspected of compromise.
- Protect against a brute-force attack on all passwords by allowing no more than 10 guesses in five minutes, or locking devices after no more than 10 unsuccessful attempts.

5.10. Unlicenced hardware or software will never be used by the trust.

5.11. All unpatched or unsupported hardware or software will be replaced by the ICT technician. Where it is not possible to replace these devices, they will have their access to the internet removed so that scanning tools cannot find weaknesses.

6. Malware prevention

6.1. 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.

6.2. The Trust IT Manager will ensure that all trust devices have secure malware protection and undergo regular malware scans.

6.3. The Trust IT Manager will ensure malware protection is updated on a daily basis to ensure it is up-to-date and can react to changing threats.

6.4. Malware protection will also be updated in the event of any attacks to the trust's hardware and software.

6.5. Filtering of websites, as detailed in the 'User privileges and passwords' section of this policy, will ensure that access to websites with known malware is blocked immediately and reported to the Trust IT Manager.

6.6. The Trust IT Manager will ensure that our email provider is applying the appropriate email 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.

6.7. The Trust IT Manager will review the mail security technology provided by our email provider on a termly basis to ensure it is kept up-to-date and effective.

6.8. Staff members are only permitted to download apps on any school-owned device from manufacturer-approved stores and with prior approval from a member of the trust IT team. Where apps are installed, the IT team will keep up-to-date with any updates, ensuring staff are informed of when updates are ready and how to install them.

6.9. The trust will use anti-malware software that:

- Is set up to scan files upon access, when downloaded, opened, or accessed from a network folder.
- Scans web pages as they are accessed.
- Prevents access to potentially malicious websites, unless risk-assessed, authorised and documented against a specific business requirement.

7. User privileges and passwords

7.1. 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 be role-based.

7.2. The Trust IT Manager will ensure that user accounts are set up to allow users access to the facilities required, whilst minimising the potential for deliberate or accidental attacks on the network.

7.3. All staff user accounts are forced to change their passwords annually and must use upper and lowercase letters, as well as numbers, to ensure that passwords are strong. Users will also be required to change their password if it becomes known to other individuals.

7.4. Pupils are responsible for remembering their passwords; however, the Trust IT Manager will have an up-to-date record of all usernames and passwords, and will be able to reset them if necessary.

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

7.6. Password strength will be enforced at a system level – the school will use a deny list for automatic blocking of common passwords and passwords must contain a minimum of eight characters.

7.7. The trust will implement a user account creation, approval and removal process which is part of the trust joining and leaving protocols.

7.8. User accounts and access privileges will be appropriately controlled, and only authorised individuals will have an account which enables them to access, alter, disclose or delete personal data.

7.9. Users will have a separate account for routine business if their main account:

- Is an administrative account.
- Enables the execution of software that makes significant system or security changes.
- Can make changes to the operating system.
- Can create new accounts.
- Can change the privileges of existing accounts

7.10. The trust will consider using multi-factor authentication, particularly for accounts that have access to sensitive or personal data.

7.11. The Trust IT Manager will review the password system on a termly basis to ensure it is working at the required level.

8. Monitoring usage

8.1. Monitoring user activity is important for the early detection of attacks and incidents, as well as inappropriate usage by pupils or staff.

8.2. The trust will inform all pupils and staff that their usage will be monitored, in accordance with the trust's E-Safety Policy and Acceptable Use Policy/Agreement.

8.3. If a user accesses inappropriate content or a threat is detected, an alert will be sent to the Trust IT Manager and/or the school safeguarding team. Alerts will also be sent for unauthorised and accidental usage.

8.4. Alerts will identify: the user, the activity that prompted the alert and the information or service the user was attempting to access.

8.5. The ICT technician will ensure that websites are filtered on a weekly basis for inappropriate and malicious content.

8.6. Any member of staff or pupil 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.

8.7. 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

9.1. The trust understands that pupils and staff may need to access the trust 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.

9.2. The Trust IT Manager will ensure that all trust-owned devices for personal use, such as laptops, USB sticks, mobile phones and tablets are encrypted and password protected. If any portable devices are lost, this will prevent unauthorised access to personal data.

9.3. Before distributing any Trust-owned devices, the IT technicians will ensure that manufacturers' default passwords have been changed. A password will be chosen, and the staff member will be prompted to change the password once using the device.

9.4. Pupils and staff are not permitted to use their personal devices where the trust provides an alternative, e.g. work laptops, tablets and USB sticks.

9.5. When using laptops, tablets and other portable devices, the Trust IT Manager will determine the limitations for access to the network.

9.6. Staff who use trust-owned laptops, tablets and other portable devices will use them for work purposes only, whether on or off trust premises.

9.7. 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 Trust networks.

9.8. The Trust IT Manager will use encryption to filter the use of websites on these devices, in order to prevent inappropriate use and external threats which may compromise network security when bringing the device back onto the premises.

9.9. The trust uses tracking technology where possible to ensure that lost or stolen devices can be retrieved.

9.10. Where appropriate, 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.

9.11. The Wi-Fi network at the trust will be password protected and the Trust IT Manager will provide access. Staff and pupils are not permitted to use the Wi-Fi for their personal devices, such as mobile phones or tablets, unless agreed by the Trust IT Manager.

9.12. A separate Wi-Fi network is available for visitors, which limits their access to printers, shared storage areas and any other applications that are not necessary.

10. Home working and remote learning

10.1. Staff and pupils will adhere to data protection legislation and the Trust's related policies

when working remotely.

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

10.3. 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.

10.4. Staff and pupils 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 system 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.

10.5. Staff and pupils are not permitted to let their family members or friends use any Trust equipment, in order 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.

10.6. 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 technicians and the DPO, e.g. secure passwords and anti-virus software.

10.7. 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.

10.8. 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.

10.9. 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.

10.10. 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 the Trust premises to allow staff to work from home, it will be transported in a lockable bag or container. The Trust's procedures for taking data off the premises will apply to both paper-based and electronic data.

10.11. When taking physical copies of data, e.g. paper documents and Trust-owned devices, off the premises, staff will sign out the documents at the school office. The physical data will be signed back in when staff return it.

10.12. Pupils are not permitted to use Trust-owned devices or software for activities that do not pertain to their online education, e.g. use of social media, gaming, streaming or viewing content that is not applicable to their curriculum. Pupils are not permitted to download any software onto Trust devices, unless instructed to and approved by their teacher.

10.13. Pupils will not alter the passwords or encryptions protecting Trust documents and systems put in place by the Trust. Pupils will not alter or disable any security measures that are installed on Trust devices, e.g. firewalls, malware prevention or anti-virus software. Pupils will not share any confidential and/or personal information made accessible to them, e.g. VPN passwords, with anyone who is not authorised to view that information.

10.14. Pupils that do not use Trust devices or software in accordance with this policy will be disciplined in line with the Behaviour Policy.

10.15. Pupils must report any technical issues to their teacher as soon as possible. Parents and pupils will be encouraged to contact the online safety officer if they wish to report any concerns regarding online safety.

10.16. Any devices that are used by staff and pupils for remote working and learning will be assessed by the IT technicians 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, e.g. the website
- Device security check – the security of the personal device, including any 'bring your own device' systems

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

10.18. In the event that a staff member or pupil decides to leave the Trust permanently, all

data in any form will be returned on or before their last day.

11. Backing-up data

11.1. The Trust IT Manager performs a backup of all electronic data held by the trust on a weekly basis, and the date of the backup is recorded using a log. Each backup is retained for 30 days before being deleted.

11.2. The Trust IT Manager performs an incremental backup on a daily basis of any data that has changed since the previous backup. The data controller will record the date of any incremental backup, alongside a list of the files that have been included in the backup.

11.3. 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.

11.4. Where possible, backups are run overnight and are completed before the beginning of the next working day.

11.5. Upon completion of backups, data is stored on the trust's hardware which is password protected

11.6. Admin servers are backed-up remotely by a third party.

11.7. Only authorised personnel are able to access the trust's data.

12. Avoiding phishing attacks

12.1. The IT technicians 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.

12.2. 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.

12.3. 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 or school 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?

12.4. The IT technicians will ensure that an appropriate email filtering system is used to identify which emails would be classed as junk or spam. The IT technicians 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.

12.5. To prevent anyone having access to unnecessary personal information, the DPO will ensure the Trust's social media accounts and websites are reviewed on a termly basis, making sure that only necessary information is shared.

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

13. User training and awareness

13.1. Trust schools will arrange regular training for pupils and staff to ensure they are aware of how to use the network appropriately in accordance with the Acceptable Use Policy.

13.2. This will cover identifying irregular methods of communication 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. Unusual communications could come in a variety of forms, e.g. emails, phone calls, text messages or social media messages.

13.3. 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.

13.4. All staff will receive training as part of their induction programme, as well as any new pupils that join the trust.

13.5. All users will be made aware of the disciplinary procedures for the misuse of the network leading to malicious attacks.

14. Cyber-security incidents

14.1. Any individual that discovers a cyber-security incident will report this immediately to the Trust IT Manager and DPO (DPO).

14.2. When an incident is raised, the DPO will record the information in the trust's data protection management system.

14.3. The DPO will take the lead in investigating the breach with assistance from the Trust IT Manager, and will be allocated the appropriate time and resources to conduct this.

14.4. The DPO will ascertain the severity of the breach as quickly as reasonably possible and determine if any personal data is involved or compromised.

14.5. The DPO will oversee a full investigation and produce a comprehensive report.

14.6. 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 eliminated or restricted as much as possible.

14.7. If the DPO 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, details of the incident are recorded in the trust's data protection management system
- The appropriate senior leader may issue disciplinary sanctions to the pupil or member of staff, in accordance with the processes outlined in the E-safety Policy
- In the event of any external or internal breach, the Trust IT Manager will record this using an incident log and respond appropriately, e.g. by updating the firewall, changing usernames and passwords, updating filtered websites or creating further backups of information
- The Trust IT Manager will also work with the third-party provider to provide an appropriate response to the attack, including any in-house changes.

14.8. Any further action that 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 backups.

14.9. Where the security risk is high, the trust will establish what steps need to be taken to prevent further data loss, which will require support from various 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
- Testing all systems to ensure they are functioning normally

14.10. Where appropriate, e.g. if offences have been committed under the Computer Misuse Act 1990, the DPO will inform the police of the security breach.

14.11. 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 DPO 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.

14.12. The DPO 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.

14.13. 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, as long as this is done without undue further delay.

14.14. 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 likely 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

14.15. 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.

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

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

14.18. The DPO and Trust IT Manager will test all systems to ensure they are functioning normally; the incident will only be deemed 'resolved' when it has been assured that the trust's systems are safe to use.

14.19. 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

15.1. The following questions will be considered by the DPO in order 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 DPO's report and records:

- What type and how much data is involved?
- How sensitive is the data? Sensitive data is defined in the Data Protection Act 1998; 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 backup 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/damage to the trust's reputation, or risk to the trust's operations?
- Who could help or advise the trust on the breach? Could external partners, authorities, or others provide effective support?

15.2. In the event that the DPO, or other persons involved in assessing the risks to the trust, are not confident in the risk assessment, they will seek advice from the Information Commissioner's Office (ICO).

16. Consideration of further notification

16.1. The trust 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 security.

16.2. The trust will assess whether notification could help the individual(s) affected, and whether individuals could act on the information provided to mitigate risks, e.g. by cancelling a credit card or changing a password.

16.3. If a large number of people are affected, or there are very serious consequences, the ICO will be informed.

16.4. The trust 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 will be included.
- 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.

16.5. The trust will consult the ICO for guidance on when and how to notify them about breaches.

16.6. The trust will consider, as necessary, the need to notify any third parties – police,

insurers, professional bodies, funders, trade unions, website/system owners, banks/credit card companies – who can assist in helping or mitigating the impact on individuals.

17. Evaluation and response

17.1. The DPO 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.

17.2. The DPO 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.

17.3. The DPO and headteacher will identify any weak points in existing security measures and procedures. The DPO will work with the Trust IT Manager to improve security procedures wherever required. The DPO and headteacher will identify any weak points in levels of security awareness and training.

17.4. The DPO will report on findings and implement the recommendations of the report after analysis and discussion.

18. Monitoring and review

18.1. This policy will be reviewed by the DPO on an annual basis.

18.2. The next scheduled review for this policy is September 2024.