Aspirational Futures Multi Academy Trust

Cyber Security Policy

Aspirational Futures Multi Academy Trust Wide Policy

September 2023

Document Control

Reviewed by:	**Aspirational Futures Multi-Academy Trust Board**	**Date: Sept 2023**
Approved by:	**Name: Steve Mitchell, A Dowsing** **Signed by: Delegated authority given by Chair of Board, Keith Fielding**	**Date: Sept 2023**
Adopted by Academies:	**Sept 2023**	
Review:	**Annually**	
Next review due by	**Date: Sept 2024**	

Document Information

	Information
Document Name	**Aspirational Futures Multi-Academy Trust Cyber Security Policy**
Document Author	**S Mitchell, A Dowsing**
Document Approval	**Board of Trustees**
Document Status	**Version 1.0**
Publication Date	**Sept 2023**
Review Date	**Sept 2024**
Distribution	**Website**

Version Control

Version	**Issue Date**	**Amended By**	**Comments**
1.0	**Sept 2023**	**S Mitchell, A Dowsing**	**New trust policy**

Contents

Statement of intent

Aspirational Futures Multi Academy 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 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

This policy has due regard to all relevant legislation and guidance 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'

This policy operates in conjunction with the following school policies:

- Online Safety Policy
- Data Protection Policy
- Disciplinary Procedure
- Code of Conduct Policy
- Acceptable Use Policy
- E-Safety policies

2. Types of security breach and causes

Unauthorised use without damage to data – involves unauthorised persons accessing data on a school 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 a school, e.g. schools 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 a school's ICT system, which may result in data being inaccessible to the school 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 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 a school through accessing and altering, sharing or removing data

Breaches caused by negligence can occur as a result of a staff member knowingly disregarding school 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 school software more vulnerable to a virus
- Incorrect firewall settings being applied, e.g. unrestricted access to a school network, can allow unauthorised individuals to access a school 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 Board of Trustees will be responsible for:

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

The headteacher/principal will be responsible for:

- Ensuring all staff members and pupils are aware of their responsibilities in relation to this policy.
- Ensuring appropriate user access procedures are in place.
- Responding to alerts for access to inappropriate content in line with the Online Safety Policy.
- Organising training for staff members in conjunction with the online safety officer and DPO.
- Ensuring a log of cyber-security incidents is maintained.
- Appointing a cyber recovery team who is responsible for implementing the school's procedures in the event of a cyber-security incident.

The DPO will be 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, including leading the cyber recovery team.
- Assessing the risks to the trust in the event of a cyber-security breach.
- Determining which organisations and individuals need to be notified following a data security breach, and ensuring they are notified.

- Working with the Network Manager, online safety officer and headteacher/principal after a data security breach to determine where weaknesses lie and improve security measures.
- Organising training for staff members on data security, network security and preventing breaches.
- Monitoring and reviewing the effectiveness of this policy, alongside the headteacher/principal, and communicating any changes to staff members.

The Network Manager will be responsible for:

- Maintaining an inventory of all ICT hardware and software currently in use in the trust.
- Ensuring any out-of-date software is removed from school 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/principal.
- Maintaining an up-to-date and secure inventory of all usernames and passwords.
- Removing any inactive users from a school system and ensuring that this is always up-to-date.
- Installing appropriate security software on staff members' personal devices where the headteacher/principal has permitted them to be used for work purposes.
- 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 headteacher/principal.

The Network Manager/DSL will be responsible for:

- Organising training and resources for staff on online safeguarding risks and preventative measures.
- Taking responsibility for online safety within a school and promoting online safety measures to parents.
- Ensuring the relevant policies and procedures are in place to protect pupils from harm, including the Online Safety Policy.
- 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 school/trust on all online safety issues.
- Liaising with relevant members of staff on online safety matters, e.g. the DPO and Network Manager.

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.

All staff members will be 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

An inventory will be kept of all ICT hardware and software currently in use in the trust, including mobile phones and other personal devices provided by the trust. The inventory will be stored digitally on the trust's network, and will be audited on a termly basis to ensure it is up-to-date. Any changes to the ICT hardware or software will be documented using the inventory and will be authorised by the Network Manager before use.

All systems will be audited on a termly basis by the Network Manager 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. 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. Passwords will need to adhere to a specific character length, 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 time frame in which vulnerabilities can be exploited. If the manufacturer

stops offering support for the software, the school will replace it with a more up-to-date alternative.

The Network 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.

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

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

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 termly basis to ensure these measures remain effective.

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

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 trust premises, as either discrete technology or a component of another system.

As the trust's firewall is managed on the premises, it is the responsibility of the Network Manager to effectively manage the firewall. The Network Manager will ensure that:

- The firewall is checked monthly 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 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 DPO. The Network Manager will react appropriately to security threats to find new ways of managing the firewall.

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

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

The trust will agree with the Network Manager a system for recording and reviewing decisions made about network security features.

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.

All unpatched or unsupported hardware or software will be replaced by the Network Manager. 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

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 Network Manager will ensure that all trust devices have secure malware protection and undergo regular malware scans in line with specific requirements. The Network Manager will ensure that automated malware protection updates are being carried out on a daily 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 Network Manager.

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 Network Manager will review the mail security technology on a termly basis to ensure it is kept up-to-date and effective.

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**

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

All users will be required to change their passwords 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 Network Manager will be able to reset them if necessary.

The Network Manager will ensure that inactive users or users who have left school, have their account deleted/disabled. The Network 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.

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

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.

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.

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 Online Safety Policy.

If a user accesses inappropriate content or a threat is detected, an alert will be sent to the Network Manager. 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 Network Manager will record any alerts using an incident log and will report this to the DPO. The DPO will then inform the headteacher/principal and online safety officer 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.

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 school is protected and all software is up-to-date.

9. Removable media controls

The trust understands that pupils and staff may need to access their school network from outside the school premises. Effective security management will be established to prevent access to, or leakage of, data, as well as any possible risk of malware.

When using laptops, tablets and other portable devices, the headteacher will determine the limitations for access to the network, as described in the 'Network security' section of this policy.

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

The Wi-Fi network at school 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 the school to limit their access to school networks and any other applications which it is not necessary for them to access.

10. Home working and remote learning

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

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 and pupils may be required to use their own devices for the duration of the remote working or learning period. Using a shared personal or household device for school purposes should be avoided where possible; however, the school understands that this may not always be possible.

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. 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/principal, and it will be ensured that the appropriate security measures are in place by the Network Manager and the DPO, 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. Trust devices will automatically lock after ten minutes of inactivity to avoid an unauthorised person gaining access to the device. 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's procedures for taking data off the premises will apply to both paper-based and electronic data.

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.

Pupils will not alter the passwords or encryptions protecting school 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.

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

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.

Any devices that are used by staff and pupils for remote working and learning will be assessed by the Network Manager 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 school website
- Device security check – the security of the personal device, including any 'bring your own device' systems

The Network Manager will provide staff and pupils with details and instructions for accessing the school network that they will be using throughout the duration of the remote working and learning period.

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

The Network Manager performs a back-up of all electronic data held by the trust on a daily basis. Each back-up is retained for 5 days before being deleted. The Network Manager performs an incremental back-up on a weekly basis of any data that has changed since the previous back-up.

The Network Manager 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.

The number of devices with access to back up data will be kept to an absolute minimum.

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.
- Considering using the Cloud to store backed-up data.
- Referring to the NCSC's Cloud Security Guidance.
- Ensuring that backing up data is regularly practised.

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

The trust's back-up strategy will be tested on a termly basis.

12. Avoiding phishing attacks

The Network Manager will configure all staff accounts using the principle of 'least privilege' – staff members are only provided with as many rights as are required to perform their jobs.

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 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?

The Network Manager 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 Network Manager 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 DPO will ensure the school's social media accounts and websites are reviewed on a termly basis, making sure that only necessary information is shared. The headteacher/principal and DPO 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/principal will ensure parents, pupils, staff and other members of the school community are aware of acceptable use of social media and the information they share about the school/trust and themselves.

13. User training and awareness

The DPO and headteacher/principal will arrange training for pupils and staff on a yearly basis to ensure they are aware of how to use the network appropriately. 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.

The online safety officer will arrange for staff and pupils to undertake the appropriate training relating to online safety issues.

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

members will be arranged by the online safety officer and DPO within two weeks following an attack, breach or significant update.

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. All staff will receive training as part of their induction programme. All pupils will receive training upon joining a trust school.

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 Behaviour Policy and the Disciplinary Policy and Procedure.

14. Cyber-security incidents

All cyber-security incidents will be managed in line with the trust's Cyber Response and Recovery Plan.

Any individual that discovers a cyber-security incident will report this immediately to the headteacher/principal and the DPO.

When an incident is raised, the DPO 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. trust-owned laptop
- Location of the equipment involved
- 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 school's DPO will take the lead in investigating the incident, with assistance from the cyber recovery team, and will be allocated the appropriate time and resources to conduct this. The DPO, as quickly as reasonably possible, will ascertain the severity of the incident and determine if any personal data is involved or has been compromised. The DPO will oversee a full investigation and produce a comprehensive report. The cause of the incident, 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 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, the incident is recorded using an incident log, and by identifying the user and the website or service they were trying to access
- The headteacher/principal will issue disciplinary sanctions to the pupil or member of staff who caused the breach, in accordance with the Behaviour Policy or Disciplinary Policy and Procedure

- In the event of any external or internal breach, the DPO 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 back-ups of information
- The trust will organise updated staff training following a breach
- 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 DPO will establish what steps need to be taken to prevent further data loss, which will require support from various school 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 DPO will inform the police of the security breach.

The trust is 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.

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.

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.

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

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 DPO will notify those concerned directly of the breach without undue delay.

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

The DPO and Network Manager 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 DPO to fully and effectively assess the risks that the cyber-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, 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 school's reputation, or risk to the trust's operations?

- Who could help or advise the school 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?

In the event that the DPO, or other persons involved in assessing the risks to the school, are not confident in the assessment of risk, they will seek advice from the ICO.

16. Consideration of further notification

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

The DPO 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 school 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 DPO 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 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.

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.

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

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