Cyber Security Policy

Date revised: June 2024
Review date: June 2026

The Pioneer Vision

We put children first, pioneering excellence and championing each and every child.

Contents

Statement of intent

The Pioneer Academy is committed to maintaining the confidentiality, integrity and availability of its information and ensuring that the details of the finances, operations and individuals within its schools 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 Pioneer Academy recognises, however, that breaches in security can occur. In schools, most breaches are caused by human error, so the schools 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 schools 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.

Legal framework

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

- The UK General Data Protection Regulation (UK GDPR)
- The Data Protection Act 2018
- The Computer Misuse Act 1990
- National Cyber Security Centre (2018) 'Small Business Guide: Cyber Security'
- National Cyber Security Centre 'Cyber Essentials'
- ICO (2022) 'Guide to the UK General Data Protection Regulation (UK GDPR)'
- ESFA (2024) 'Academy Trust Handbook 2024
- DfE (2023) 'Meeting digital and technology standards in schools and colleges'

The Pioneer Academy will implement this policy in conjunction with our:

- GDPR Data Protection Policy
- Acceptable Use Agreements
- E-safety Policy (appendix 6)
- Cloud Computing Policy (appendix 7)
- Protection of Biometric Information (appendix 8)

Types of attack

Unauthorised use without damage to data – involves unauthorised persons accessing data on the 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 the 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 the 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 the 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 the school network, can allow unauthorised individuals to access the school system
- Operational errors, such as confusion between back-up copies of data, can cause the most recent data to be overwritten

Roles and responsibilities

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 school's response to incidents of data security breaches.
- Assessing the risks to the school 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 Head of IT, Computing Lead and Head Teacher 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 Head Teacher, and communicating any changes to staff members.

The Head of IT is responsible for:

- Maintaining an inventory of all ICT hardware and software currently in use at the school.
- Ensuring any out-of-date software is removed from the school systems.
- Implementing effective firewalls to enhance network security and ensuring that these are monitored regularly.
- Installing, monitoring and reviewing filtering systems for the school network.
- Setting up user privileges in line with recommendations from the Head Teacher.
- Maintaining an up-to-date and secure inventory of all usernames .

- Removing any inactive users from the school system and ensuring that this is always up-to-date.
- Installing appropriate security software on staff members' personal devices where the Head Teacher has permitted for them to be used for work purposes, in line with the school's Working from Home Policy.
- Performing a back-up of all electronic data held by the school, ensuring detailed records of findings are kept.
- Ensuring all school-owned devices have secure malware protection and are regularly updated.
- Recording any alerts for access to inappropriate content and notifying the Head Teacher.
- Ensuring a log of cyber-security incidents is maintained

The Computing Lead is responsible for:

- Organising training and resources for staff on online safeguarding risks and preventative measures.
- Taking responsibility for online safety within the school and promoting online safety measures to parents.
- Liaising with the LA where appropriate.
- Ensuring the relevant policies and procedures are in place to protect pupils from harm, including the E-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 on all online safety issues.
- Liaising with relevant members of staff on online safety matters, e.g. the DPO and Head of IT.
- Coordinating the school's participation in local and national online safety events, e.g. Safer Internet Day.

The Head Teacher is 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 Head of IT and maintaining a written record of privileges.
- Responding to alerts for access to inappropriate content in line with the E-Safety Policy.
- Informing the Head of IT 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 online safety officer and DPO.
- Appointing a cyber recovery team who is responsible for implementing the school's procedures in the event of a cyber-security incident

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

The governing board is responsible for:

- Supporting the Head Teacher and other relevant staff in the delivery of this policy.

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.

Secure configuration

An inventory will be kept of all IT hardware currently in use within The Pioneer Academy, including mobile phones and other personal devices provided by the schools. This will be audited on an annual basis 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 Head of IT before use.

Any new versions of software or new security patches will be added to systems, ensuring that they do not affect network security.

Any software that is out-of-date or reaches 'end of life' will be removed from systems, i.e. when suppliers end their support for outdated products, such that any security issues will not be rectified by suppliers.

All hardware, software and operating systems will require passwords for individual users before use. Passwords will be changed on a termly basis to prevent access to facilities which could compromise network security.

The Pioneer Academy believes that locking down hardware, such as through strong passwords, is an effective way to prevent access to facilities by unauthorised users. This is detailed in this policy.

The school 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 school 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 school 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 school 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 school 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 Head of IT will:

- Protect all devices on every network 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 to help detect 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.

Network security

The Pioneer Academy will employ firewalls in order to prevent unauthorised access to the systems. The Pioneer Academy's firewall will be deployed as a:

- **Centralised deployment**: the broadband service connects to a firewall that is located within a data centre or other major network location.

As The Pioneer Academy's firewall is managed locally by a third party, the firewall management service will be thoroughly investigated by the Head of IT, to ensure that:

- Any changes and updates that are logged by authorised users within The Pioneer Academy, 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.
- Any changes and/or updates that are added to servers, including access to new services and applications, do not compromise the overall network security.
- The firewall is checked regularly to ensure that a high level of security is maintained and there is effective protection from external threats.

Malware prevention

The school 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 Head of IT will ensure that all school devices have secure malware protection and undergo regular malware scans in line with specific requirements. The ICT technician will update malware protection on a ongoing 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 school's hardware and software.

Staff will follow procedures for filtering and monitoring to keep pupils safe as set out in the Online Safety Policy. The school's filtering provider will be:

- A member of Internet Watch Foundation (IWF)
- Signed up to Counter-Terrorism Internet Referral Unit list (CTIRU)
- Effective at blocking access to illegal content

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

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

The school 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 Head of IT will review the mail security technology on an ongoing 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 online safety officer. Where apps are installed, the ICT technician will keep up-to-date with any updates, ensuring staff are informed of when updates are ready and how to install them.

The school 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.

Managing user privileges

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

The Head Teacher will clearly define what users have access to and will communicate this to the Head of IT, ensuring that a written record is kept.

The Head of IT will ensure that user accounts are set up appropriately such that users can access the facilities required, in line with the Head Teacher's instructions, whilst minimising the potential for deliberate or accidental attacks on the network.

All users will be required to change their passwords on a termly basis 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 this becomes known to other individuals.

Pupils are responsible for remembering their passwords; however, the Head of IT will be able to reset them if necessary.

Pupils in key stage 1 will not have individual logins and class logins will be used instead. If it is appropriate for a pupil to have their individual login, the Head of IT will set up their individual user account, ensuring appropriate access and that their username and password is recorded.

The 'administrator' password used by the Head of IT will be made available to the CFOO, or any other nominated senior leader, and will be kept in a secure place.

The Head of IT will liaise with individual schools to delete inactive users or users who have left The Pioneer Academy.

Monitoring usage

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

The Pioneer Academy will inform all pupils and staff that their usage will be monitored, in accordance with The Pioneer Academy's Acceptable Use Policy and E-safety Policy.

An alert will be sent to the Head of IT when monitoring usage, if the user accesses inappropriate content or a threat is detected. Alerts will also be sent for unauthorised and accidental usage.

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

The Head of IT will record any alerts using an incident log and will report this to the Head Teacher. All incidents will be responded to in accordance with this policy, and as outlined in the E-safety Policy.

All data gathered by monitoring usage will be kept in a secure location, 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.

Removable media controls

The Pioneer Academy understands that staff may need to access the school 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.

The Head of IT will encrypt all school-owned devices for personal use, such as laptops and tablets, to ensure that they are password protected. If any portable devices are lost, this will prevent unauthorised access to personal data.

Staff are not permitted to use their personal devices where The Pioneer Academy shall provide alternatives, such as work laptops and tablets. Staff are not permitted to use personal USB sticks.

When using laptops, tablets and other portable devices, the Head Teacher will determine the limitations for access to the network, as described in this policy.

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

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

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

The Wi-Fi network at The Pioneer Academy will be password protected and will only be given out as required. Staff are not permitted to use the Wi-Fi for their personal devices, such as mobile phones or tablets, unless instructed otherwise.

Home working and remote learning

Staff and pupils will adhere to data protection legislation and the school'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 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 school system through a proxy, e.g. VPN. 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 school 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 school 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 Head Teacher, and it will be ensured that the appropriate security measures are in place by the Head of IT 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. School devices will automatically lock after a period 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 the school premises to allow staff to work from home, it will be transported in a lockable bag or container. The school's procedures for taking data off the school premises will apply to both paper-based and electronic data.

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

Pupils are not permitted to use school-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 school 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 school. Pupils will not alter or disable any security measures that are installed on school 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 school devices or software in accordance with this policy will be disciplined in line with the Behavioural 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 IT Team 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 IT Team 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 school permanently, all data in any form will be returned on or before their last day.

Backing up data

The IT Team performs a back-up of all electronic data held by the school on a daily basis.

The school 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.

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

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

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 school's Cloud Computing Policy. Only authorised personnel will be able to access back-ups of the school's data.

The school 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.

Avoiding phishing attacks

The IT Team 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 Head Teacher's or SBM's accounts.

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 IT Team 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 Team 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 Head Teacher 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 Head Teacher and DPO will ensure the school's Social Media Policy includes expectations for sharing of information and determines what is and is not appropriate to share.
The Head Teacher 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 and themselves, in accordance with the school's Acceptable Use Policy.

User training and awareness

The Head Teacher will arrange training for staff on an annual basis to ensure they are aware of how to use the network appropriately in accordance with the Acceptable Use Policy and E-safety Policy.

Training will also be conducted around any attacks that occur and any recent updates in technology or the network.

All staff will receive training as part of their induction programme, as well as any new pupils that join The Pioneer Academy.

Staff with access to the school's IT network will be required to undertake basic cyber-security training upon induction which is refreshed every year. At least one member of the governing board will also take part in this training. The training will focus on the following:

- Phishing
- Password security
- Social engineering
- The dangers of removable storage media

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 E-safety Policy.

Incidents

In the event of an internal attack or any incident which has been reported to the Head of IT, this will be recorded using an incident log and by identifying the user and the website or service they were trying to access.

All incidents will be reported to the Head Teacher, who will 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 attack, the Head of IT will record this using an incident log and will contact the third party provider to ensure the attack does not compromise any other schools' network security.

The Head of IT will work with the third party provider to provide an appropriate response to the attack, including any in-house changes.

If necessary, the management of e-security at The Pioneer Academy will be reviewed to ensure effectiveness and minimise any further incidents.

Security breach incidents

Any individual that discovers a security data breach will report this immediately to the Head Teacher and data controller.

When an incident is raised, the Head Teacher will record the following information:

- Name of the individual who has raised the incident
- Description of the incident
- Description of any perceived impact
- Description and identification codes of any devices involved, e.g. school-owned laptop

- Location of the equipment involved
- Contact details for the individual who discovered the incident

The DPO will take the lead in investigating the breach, 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 breach and determine if any personal data is involved or compromised.

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

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.

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 Head Teacher will issue disciplinary sanctions to the pupil or member of staff, in accordance with the processes outlined in the E-safety Policy.
- The DPO 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 school 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 DPO 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 school’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.

Assessment of risks

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 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/damage to the Academy's reputation, or risk to the school's operations?
- Who could help or advise the school on the breach? Could the LA, external partners, authorities, or others provide effective support?

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

Consideration of further notification

The Academy 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.

The Academy will decide whether notification will help the school meet its security obligations under the seventh data protection principle.

The school 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.

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

The school 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 school is willing to do to help them.
- A way in which they can contact the school for further information or to ask questions about what has occurred.

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

The school 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.

Under the GDPR, the following steps will be taken if a breach of personal data occurs:

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

Where a breach is likely to result in significant risk to the rights and freedoms of individuals, the school will notify those concerned directly with the breach.

Where the breach compromises personal information, the notification will contain:

- The nature of the personal data breach including, where possible:
  - The type(s), e.g. staff, pupils or governors, and approximate number of individuals concerned.
  - The type(s) and approximate number of personal data records concerned.
- The name and contact details of the data controller or other person(s) responsible for handling the school's information.
- A description of the likely consequences of the personal data breach.
- A description of the measures taken, or proposed, to deal with and contain the breach and, where appropriate, of the measures taken to mitigate any possible adverse effects.

Evaluation and response

The DPO will establish the root of the breach, and where any present or future risks lie.

The DPO will consider the data and contexts involved.

The DPO will identify any weak points in existing security measures and procedures.

The DPO and Head Teacher will identify any weak points in levels of security awareness and training.

The DPO will report on findings and, with the approval of the school leadership team, implement the recommendations of the report after analysis and discussion.

Monitoring and review

This policy will be reviewed by the Data Protection Officer on an annual basis or earlier if deemed necessary.

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