Information Security Policy

Policy Owner:	Lighthouse Multi Academy Trust
Approved/ Ratified:	Pat Hunt 10.11.26
Review Dates:	November 2027

Document Version Control Log

Version	Modification Date	Synopsis of Changes
1.0	October 2025	
2.0	November 2026	Updated and reviewed policy to update procedures adding to strengthen cyber security, use of passwords and Artificial intelligence.

Contents Page

Introduction and Scope
Roles and Responsibilities
Access Control
Physical Security
Environmental Security
Systems and Cyber Security
Communications Security
Data Breaches
Business Continuity

Appendix 1- Data Breach procedure
Appendix 2- Remote working policy

Introduction and Scope

The Information Security policy outlines **The Lighthouse Multi Academy Trust**'s organisational security processes and standards. The Information Security Policy is based on the UK GDPR's integrity and confidentiality principle (Article 5(1)(f)) and supports the Trust's obligations under Article 32 concerning the security of processing.

To ensure we meet our legal obligations, personal data should be protected by the security model known as the 'CIA' triad. These are three key elements of information security:

- **Confidentiality** – only authorised people should have access to information.
- **Integrity** – information should be accurate and trustworthy.
- **Availability** – authorised people should have access to the information and systems they need to carry out their job.

This policy and its appendices apply to our entire workforce. This includes employees, governors or trustees, contractors, agents and representatives, volunteers and temporary staff working for, or on behalf of, the academies. Individuals who are found to knowingly or recklessly infringe this policy may face disciplinary action.

The Information Security policy applies to all personal data, regardless of whether it is in paper or electronic format. It should be read alongside the other policies within our information governance policy framework, including data protection, records management, and acceptable use of systems.

This policy supports the Trust's obligations under the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and relevant Department for Education (DfE) cyber security standards.

The Trust will implement appropriate technical and organisational measures to protect the confidentiality, integrity and availability of information and systems, taking account of the nature and sensitivity of the information held, the risks associated with its processing and the potential impact of a security incident.

The Trust will regularly assess, monitor and review the effectiveness of its information security arrangements and maintain appropriate evidence of compliance.

Roles and Responsibilities

Trust Board

The Trust Board is responsible for overseeing the Trust's information security arrangements and ensuring that information security risks are appropriately managed. The Board shall receive assurance regarding significant risks, incidents, compliance and the effectiveness of security controls.

Chief Executive Officer and Trust Central Team

The Chief Executive Officer and Trust Central Team are responsible for ensuring that appropriate information security arrangements are implemented across the Trust, sufficient resources are available and significant information security risks are managed effectively.

Headteachers and Senior Leaders

Headteachers and Senior Leaders are responsible for implementing this policy within their academy, ensuring staff understand their responsibilities and reporting information security incidents, risks and concerns in accordance with Trust procedures.

Data Protection Officer (DPO)

The Data Protection Officer shall provide advice on data protection and privacy matters, support compliance with UK GDPR and the Data Protection Act 2018, advise on Data Protection Impact Assessments (DPIAs) and support the management of personal data breaches.

IT Service Providers and Technical Support Staff

IT service providers and technical support staff are responsible for maintaining technical security controls, monitoring systems, managing user access, maintaining backup and recovery arrangements, implementing security updates and supporting incident response activities.

Staff, Volunteers, Trustees and Contractors
All users of Trust information, systems and devices are responsible for:

- Complying with this policy and associated procedures.
- Protecting information and information assets from unauthorised access, disclosure, alteration or loss.
- Completing required information security and cyber security training.
- Reporting information security incidents, suspected breaches and cyber security concerns promptly.
- Using Trust systems and information in a secure and appropriate manner.

Where responsibilities are assigned to academy-based roles, including Headteachers and designated Single Points of Contact (SPOCs), these responsibilities operate within the Trust's wider governance framework. Trust leaders, academy leaders and relevant central services shall work collaboratively to ensure cyber security risks, incidents and compliance requirements are managed consistently across all Trust operations.

Access Control
We will maintain control over access to the personal data that we process.

These controls will differ depending on the format of the data and the status of the individual accessing the data. We will maintain an audit log detailing which individuals have access to which systems (both electronic and manual). This log will be maintained by the **SPOC - Headteacher or appropriate delegate (DHT, AHT)** of each academy, who may delegate to a member of their team.

Access rights must be based on the principle of least privilege, ensuring that individuals are only provided with the access necessary to perform their authorised duties.

Access rights must be reviewed regularly, at least termly for critical systems and whenever an individual changes role, responsibilities or employment status. Any unnecessary or inappropriate access must be removed promptly.

The Trust and its academies must maintain appropriate procedures to ensure that access is removed or amended promptly when staff leave, change roles or no longer require access. This includes notifying the relevant IT support provider and checking that access to all relevant systems, applications, accounts and physical premises has been addressed.

When a Lighthouse Multi Academy Trust employee leaves the employment of the Lighthouse Multi Academy Trust or Governance changes, the IT Support Team must be informed by emailing the helpdesk; user access will then be removed from any IT systems, including the network, Sharepoint, CPOMS, and Arbor, and physical access to the building. At the end of employment with the MAT, all IT equipment that has been issued including laptops, tablets and any other electronic device must be returned in a condition consistent with fair wear and tear.

MAT Issued IT Equipment
A key principle of the DfE Cyber Security Standards and UK GDPR is for organisations to implement appropriate technical and organisational measures in order to ensure data security. The Lighthouse Multi Academy Trust is committed to securing data at all times. All Lighthouse Multi Academy Trust employees and Trustees /Governors with company equipment are responsible for ensuring that the following guidelines are followed at all times:

- All portable computers have appropriate access protection ensuring passwords meet the minimum password complexity policy, as set out in section 10 of this policy.
- Portable computers must not be left unattended in public places.
- Computer equipment is vulnerable to theft, loss or unauthorised access.
- Always secure laptops and other electronic equipment when leaving an office unattended and lock
- equipment away when you are leaving the office.
- When leaving a computer/laptop unattended ensure that the screen is locked, turned off or has been logged out.
- Portable computers must never be left unattended in cars.
- Do not leave any devices (personal or Lighthouse Multi Academy Trust-owned) exposed or unattended

outside the Lighthouse Multi Academy Trust premises.

- Users of portable computing equipment are responsible for the security of the hardware and the information it holds at all times. The equipment must only be used by the individual to which it is issued, be maintained, and batteries recharged as required.
- Staff working from home must ensure appropriate security is in place to protect Lighthouse Multi Academy Trust equipment or information. This will include physical security measures to prevent unauthorised entry to the home, and ensuring Lighthouse Multi Academy Trust equipment and information is kept out of sight.
- Lighthouse Multi Academy Trust issued equipment must not be used by non- Lighthouse Multi Academy Trust employees.

The IT Support Team are responsible for ensuring the following:

- That all users have the means to update their password, enforcing password policies to ensure they meet the minimum password requirements. The password complexity policy is detailed in section 10 of this policy.
- All data carried on portable computers is encrypted.
- All portable computers have an adequate level of antivirus protection.

The use of personal IT Equipment

The use of personal IT equipment is strictly prohibited for accessing Lighthouse Multi Academy Trust systems, with the exception of Email access as outlined in this policy.

Outlook Email Addresses

Employees, Trustees and Governors of the Lighthouse Multi Academy Trust can use the Outlook App (available for IOS and Android) to access emails for Outlook. The Lighthouse Multi Academy Trust has implemented appropriate technical measures in order to protect data using the aforementioned apps.

Access on mobile devices is only permitted in accordance with the following terms:

- The Outlook app is the only permitted route of access to emails for the Outlook/Sharepoint.

The Trust has appropriate mobile application management, remote sign-out, MFA and controls for lost devices.

Suspicious Emails and Content

Lighthouse Multi Academy Trust owned laptops are secured with the latest endpoint protection suite of products, they actively monitor for suspicious files and activity. Emails can host scams, which are undetectable by endpoint protection suites, and malicious software.

To avoid virus infection (or similar) or data theft employees should:

- Avoid opening attachments and clicking on the links when the content is not
- adequately explained (e.g. "watch this video, it's amazing.")
- Be suspicious of 'clickbait' titles (e.g. offering prizes or advice.)
- Be suspicious of incorrectly spelt attachments.
- Look for inconsistencies (e.g. spelling/grammar mistakes, capital letters and/or
- excessive use of punctuation.)
- Check the email address of the sender is spelt correctly.
- Be suspicious of urgent calls to action ("Please make this payment within the hour" or
- I can't talk now, can you send this money to X")
- Be suspicious of threats ("act within 1 hour to claim a reward")

Regard any email the meet the following criteria with particular suspicion:

- If they come from someone you don't know, who has no legitimate reason to send them to you
- If an attachment arrives with an empty message
- If there is some text in the message, but it doesn't mention the attachment
- If there is a message, but it seems uncharacteristic of the sender
- If the message doesn't include any personal references at all
- If it has a filename with a 'double extension', like FILENAME.JPG.vbs or FILENAME.TXT.scr, that may be extremely suspicious.

If you are unsure if an email is legitimate, you must refer to the IT Team immediately by emailing the helpdesk.

Newly appointed staff, directors and governors will be provided with access to cybersecurity awareness training, including email security. This training is mandatory and must be completed annually. Academies will complete training log record which is shared with the Trust. See Cyber Security Policy and Risk Assessment Appendix 7. Access to Trust systems will only be provided once the required training has been completed.

The Trust will provide periodic cybersecurity awareness updates and may undertake phishing awareness exercises where appropriate. Additional or enhanced training will be provided to users with privileged system access or those handling high-risk or sensitive information.

The Trust and its academies will maintain a cyber awareness programme for staff and pupils. Staff will receive appropriate cybersecurity and data protection training, with enhanced or more frequent training where required by role or risk.

Pupil cyber awareness will be addressed through the Trust's curriculum, acceptable use, online safety and safeguarding arrangements, appropriate to pupils' age and stage of development.

These arrangements will be reviewed regularly and following significant cyber incidents or emerging risks.

Password and Authentication Requirements
The Trust will implement authentication arrangements that reflect current cyber security guidance and the risks associated with the systems being accessed.

- Passwords must be sufficiently long, unique and difficult to guess. The Trust will use technical controls to prevent the use of common, weak or compromised passwords wherever possible.
- Multi-factor authentication (MFA) must be enabled for all staff accounts with access to cloud services or remote access to on-site systems, and for all IT administrative accounts. MFA must also be used for systems containing confidential, personal or sensitive personal data where required following risk assessment and DPO advice.
- MFA shall be mandatory for the Trust's core systems, including **Microsoft 365, Arbor and CPOMS**, and for any other system containing confidential, personal or special category personal data where this is required following risk assessment and advice from the Data Protection Officer (DPO).
- Passwords must not be shared, reused across different services where avoidable, or disclosed to other individuals.
- Staff must not be required to change passwords routinely unless there is evidence of compromise, a specific security risk or a system requirement that has been assessed as appropriate.
- Default passwords must be changed before systems and devices are placed into service.
- Systems must use appropriate protections against repeated unsuccessful login attempts, including rate limiting, monitoring or account lockout where suitable.
- Privileged accounts must be restricted to authorised individuals and must not be used for routine activities where a separate standard account is available.

Any suspected compromise of login credentials must be reported immediately to the IT Support Team.

Artificial Intelligence
Please refer to the **Trust Artificial Intelligence policy** for full usage guidelines.

- The Lighthouse Multi Academy Trust recognises the importance of equipping learners and staff with the knowledge, skills and strategies to engage responsibly with AI tools.
- Where used, staff should use AI tools responsibly, ensuring the protection of both personal and sensitive data. Personally identifiable or sensitive information should never be input into AI tools.
- Only AI technologies approved through the Trust's approved process may be used.
- Staff must not input sensitive information, such as pupil information or internal documents, into AI tools. Staff must always recognise and safeguard sensitive data.
- Staff must ensure that when AI is used, it does not infringe copyright or intellectual property conventions – care must be taken to protect intellectual property, including that of the learners, being used to train generative AI models without appropriate consent.
- AI incidents must be reported promptly. Staff must report any incidents involving AI misuse, data breaches,

or inappropriate outputs immediately to the nominated DPO. Quick reporting helps mitigate risks and facilitates a prompt response.

The Trust will maintain and regularly review its Artificial Intelligence (AI) Policy to ensure it remains aligned with emerging technologies, cyber security risks, legal requirements, safeguarding expectations and Department for Education (DfE) guidance. Significant developments in AI, changes in legislation or regulatory guidance, or identified risks arising from the use of AI technologies shall trigger an earlier review where appropriate. The Trust Board, or delegated committee, will receive periodic updates on significant AI-related risks, incidents and developments where these may affect Trust operations, information security or compliance arrangements.

Manual Filing Systems

Access to manual filing systems (i.e. non-electronic systems) will be controlled by a key management system. All files that contain personal data will be locked away in lockable storage units, such as a filing cabinet or a document safe, when not in use.

Keys to storage units will be stored securely. The **SPOC** will be responsible for giving individuals access to the safe place. Access will only be given to individuals who require it to carry out legitimate business functions. Where a PIN is used, the password will be changed every term or whenever a member of staff leaves the organisation, whichever is sooner.

Software and System Audit Logs and Monitoring

The Trust will ensure that appropriate audit logging and monitoring are in place for critical systems to support information security, identify unauthorised access and investigate potential security incidents.

The Trust will ensure that:

- **Logging:** Critical systems, including network infrastructure, user accounts and key information systems, maintain appropriate logs of access, significant activities and security events.
- **Retention:** Audit logs are retained for an appropriate period, based on legal requirements, security risks and the Trust's data retention arrangements.
- **Monitoring:** Logs are reviewed regularly and monitored for suspicious activity, unauthorised access or unusual system behaviour.
- **Responsibility:** The Trust's IT team or designated IT provider is responsible for monitoring and reviewing system logs, escalating concerns to the appropriate Trust lead.
- **Incident reporting:** Suspected security incidents identified through monitoring must be reported and managed in line with the Trust's Data Breach and Incident Reporting Procedures.
- **Protection:** Audit logs must be protected from unauthorised access, alteration or deletion.

Logging and monitoring arrangements must be proportionate to the risks and reviewed periodically.

Data Shielding

We do not allow our workforce to access the personal data of family members or close friends. Users should declare upon employment whether they are aware of any family members or friends who are registered with us in line with

Trust Managing Personal Relationships at Work Policy.

We will then keep paper files in a separate location (with access restricted to minimal employees) and where possible any electronic files will be locked down so that the declaring user cannot access that data.

All staff must declare any relevant personal relationships or conflicts of interest that could create a risk of inappropriate access to personal information.

The Trust will implement proportionate safeguards, including restricted access to relevant records, where necessary to prevent inappropriate access or conflicts of interest.

Failure to comply with these requirements may result in disciplinary action and, where applicable, further action in accordance with relevant legislation.

External Access
On occasions our **academies** will need to allow individuals who are not part of our workforce to have access to systems. This could be, for example, for audit purposes, to fulfil an inspection, when agency staff have been brought in, or because of a partnership arrangement with another educational establishment. The **SPOC - Headteacher or appropriate delegate (DHT, AHT, SBM)**, is required to authorise all instances of third parties having access to systems.

We will maintain an access log, detailing who has been given access to what systems and who authorised the access.

External IT Support and Third-Party Access
External IT support providers and third parties must meet the Trust's data protection and information security requirements before accessing Trust systems, networks or information.

The Trust will ensure that:

- Appropriate security and data protection checks are completed before appointing external providers.
- Contracts clearly define information security, confidentiality and data protection responsibilities.
- Data processing agreements are in place where required under UK GDPR Article 28.
- External access is authorised, restricted to what is necessary and removed when no longer required.
- Secure methods are used for remote access and information sharing.
- Providers report suspected or actual security incidents and data breaches to the Trust immediately.
- Third-party access and security arrangements are reviewed periodically.
- Trust information is securely returned or deleted, and access withdrawn when contracts end.

These requirements must be followed alongside the **Trust's Data Protection Policy**, Procurement Procedures and Data Breach and Incident Reporting Procedures.

Physical Security
We will maintain high standards of physical security to prevent unauthorised access to personal data. We will maintain the following controls:

Clear Desk Policy
Individuals will not leave personal data on desks, or any other working areas, unattended and will use the lockable storage units provided to secure personal data when not in use.

Alarm System
We will maintain a security alarm system in our premises so that, when the premises are not occupied, an adequate level of security is still in operation.

Building Access
External doors to the premises will be locked when the premises are not occupied. Only authorised individuals will be key holders for the building premises. The **SPOC**, who may delegate to a member of their team, will be responsible for authorising key distribution and will maintain a log of key holders.

Internal Access
Internal areas that are off limits to pupils and parents will be kept locked and only accessed through PIN or keys. PINs will be changed every six months or whenever a member of staff leaves the organisation. Keys will be kept in a secure location and a log of any keys issued to staff maintained.

Visitor Control
Visitors will be required to sign in and provide information necessary to manage site security, identify visitors and support safeguarding and emergency arrangements. This may include their name, organisation, car registration (where applicable) and nature of business. Additional information will only be collected where necessary and proportionate.

Visitor information may be collected in paper or electronic format and will be handled securely. Visitors will be escorted where appropriate and will not be permitted to access restricted areas without authorisation and suitable supervision.

Visitor records will be retained only for as long as necessary for security, safeguarding and legal requirements, in accordance with the **Trust's Records Management (retention) and Data Protection Policies**, and will then be securely disposed of or deleted.

Secure Disposal
We will ensure that all personal data is securely disposed of in line with our **Records Management Policy** and retention schedule https://web.starmat.uk/policies/ Hard copy information will be securely destroyed by shredder or a confidential waste provider.

Electronically held information will be deleted automatically with retention periods built into the system wherever possible. Otherwise, manual review and deletion will take place at least annually.

Redundant computer equipment will be disposed of in accordance with the Waste Electrical and Electronic Equipment (WEEE) Regulations and through secure and auditable means.

Environmental Security
As well as maintaining high standards of physical security to protect against unauthorised access to personal data, we must also protect data against environmental and natural hazards such as power loss, fire, and floods.

It is accepted that these hazards may be beyond our control, but we will implement the following mitigating controls:

Back Ups
We will regularly back up our electronic data and systems and carry out tests to ensure that they restore correctly. These backups will be held in a different location to the main server or held off-site by an external provider. This arrangement will be governed by a data processing agreement. Should our electronic systems be compromised by an environmental or natural hazard then we will be able to reinstate the data from the backup with minimal disruption.

Fire-proof Cabinets
We will aim to only purchase lockable data storage cabinets that can withstand exposure to fires for a short period of time. This will protect paper records held in the cabinets from any minor fires that break out on the building premises.

Fire Doors
Areas of the premises which contain paper records or core electronic equipment such as server boxes, will be fitted with fire doors so that data contained within those areas will be protected, for a period of time, against any fires that break out on the premises. Fire doors must not be propped open unless automatic door releases are installed.

Fire Alarm System
We will maintain a fire alarm system at our premises to alert individuals of potential fires and so the necessary fire protocols can be followed.

Systems and Cyber Security
We will protect against hazards to our IT network and electronic systems. It is recognised that the loss of, or damage to, IT systems could affect our ability to operate and could potentially endanger the safety of our pupils and workforce.

We will implement the following security controls in order to mitigate risks to electronic systems.

Cyber Security Risk Management
The Trust will maintain a cyber security risk assessment covering its digital systems, networks, data, devices, services and third-party dependencies.

The assessment will:

- Be reviewed at least annually and revisited each term.
- Identify key cyber security risks and the potential impact on the Trust, its academies, pupils, staff and other stakeholders.
- Identify appropriate mitigating controls, actions, responsible individuals and review dates.
- Be updated following significant incidents, changes to systems or services, or the identification of significant new risks.

The Trust will maintain appropriate processes for identifying, prioritising and addressing software vulnerabilities and security updates. Unsupported software and systems must be identified and managed through an appropriate risk-based plan.

The Trust will also monitor and review its cyber security arrangements to ensure that controls remain effective and are consistent with relevant DfE cyber security standards and recognised good practice.

Cyber security risks will be incorporated into the Trust's wider risk management arrangements where appropriate. Significant cyber security risks will be escalated through the Trust's risk management and governance arrangements and reported to the Board of Trustees or relevant committee where appropriate.

The Trust and its academies will maintain a documented cyber incident response plan as part of its business continuity and disaster recovery arrangements. The plan will be tested periodically and updated following significant incidents, exercises or material changes to the Trust's systems or risks.

The Trust and its academies will maintain appropriate registers of its digital technology assets, systems, software and services, including relevant ownership, support arrangements and lifecycle information.

Digital technology will be appropriately licensed, supported and maintained. Unsupported or end-of-life hardware, software or services will be identified and managed through an appropriate risk-based plan.

The Trust require:

- An annual test of the Cyber Response Plan, including simulation of a cyber incident.
- Cyber security risks shall be included within the Trust's Risk Register and reviewed at least termly, with a full annual assessment undertaken to identify emerging threats, vulnerabilities and control effectiveness.
- Regular testing of backup and recovery processes, with evidence retained.
- Annual cyber security awareness training for all staff.
- Periodic phishing simulations and reporting of outcomes.
- Documentation of all testing activities, lessons learned and resulting actions.

Records of testing and review should be reported to the Trust Board or appropriate committee and retained as evidence of compliance with the Trust's cyber security and risk management arrangements.

Software Download Restrictions

Users must request authorisation from our IT provider before downloading software onto our IT systems. Our IT provider will vet software to confirm its security certificate and ensure the software is not malicious. Our IT provider will retain a list of trusted software so that this can be downloaded onto individual desktops without disruption.

Firewalls and Anti-Virus Software

We will ensure that the firewalls and anti-virus software is installed on electronic devices and routers. We will update the firewalls and anti-virus software when updates are made available and when advised to do so by our IT provider.

We will review our firewalls and anti-virus software on an annual basis and decide if they are still fit for purpose. We will ensure that updates and patches are applied when they are available to ensure any security weaknesses are addressed as soon as they are known.

Shared Drives
We maintain a shared drive on our servers. Whilst users are encouraged not to store personal data on the shared drive it is recognised that on occasion there will be a genuine business requirement to do so.

The shared drive will have restricted areas that only authorised users can access. The **SPOC** will be responsible for giving shared drive access rights to users. Information held within the shared drives will still be subject to our retention schedule.

Removable Storage Media
The use of removable storage media, including USB drives and external hard drives, must be limited to legitimate business purposes and must comply with Trust IT security requirements.

Where removable media is permitted, only Trust-approved and appropriately encrypted devices may be used to store Trust information. Personal or unknown removable storage devices must not be connected to Trust equipment unless specifically authorised by the IT Support Team.

Sensitive or personal data must not be transferred using removable media unless there is a genuine business need and appropriate security controls are in place.

Communications Security
The transmission of personal data is a key business need and, when operated securely, is a benefit to us and pupils alike. However, data transmission is extremely susceptible to unauthorised and/or malicious loss or corruption. We have implemented the following transmission security controls to mitigate these risks:

Sending Personal Data by Post
Where personal data is sent by post, staff must use a method appropriate to the sensitivity of the information and the risks associated with its transmission.

Before sending, staff must:

- Check that the recipient's name and address are correct.
- Ensure that only the intended information is enclosed.
- Use appropriate packaging to prevent accidental disclosure.
- Use a tracked or otherwise secure delivery method where required by the sensitivity or volume of the information.

Sending Special Category or Highly Confidential Information
Special category and other highly confidential information must be sent using a method that provides appropriate protection against unauthorised access or disclosure.

Where information is sent by post, staff must use an appropriate secure and tracked delivery method based on the sensitivity of the information and the risk assessment. A second-person check must be completed where required by the Trust's procedures or where the risk warrants an additional safeguard.
Where appropriate, staff should use an approved secure electronic transmission method instead of postal delivery.

Sending personal data by email
We will only send personal data and special category data by email if using a secure email transmission portal. Individuals will always double check the recipient's email address to ensure that the email is being sent to the intended individual(s). Use of autocomplete should be strongly discouraged.

When sending emails to a large number of recipients, such as a mail shot, or when it would not be appropriate for recipients to know each other's email addresses then we will utilise the Blind Copy (BCC) function.

Exceptional Circumstances
In exceptional circumstances we may wish to hand deliver, or use a direct courier, to ensure safe transmission of personal data. This could be because the personal data is so sensitive that the usual transmission methods would not be considered secure, or because the volume of the data that needs to be transmitted is too big for usual transmission methods.

Data Breaches

All actual or suspected personal data breaches and information security incidents must be reported immediately in accordance with the Trust's Data Breach Procedure.

The Trust, as data controller where applicable, will assess each personal data breach to determine the likelihood and severity of the risks to individuals.

Where a breach is likely to result in a risk to the rights and freedoms of individuals, the Information Commissioner's Office (ICO) will be notified without undue delay and, where feasible, within 72 hours of the Trust becoming aware of the breach.

Where a breach is likely to result in a high risk to the rights and freedoms of individuals, affected individuals will be informed without undue delay, unless an applicable legal exception applies.

All personal data breaches must be documented, including those that do not meet the threshold for reporting to the ICO. The records must include the facts relating to the breach, its effects, the action taken and the rationale for any decision not to notify the ICO or affected individuals.

Business Continuity

We will ensure that we have a business continuity plan in place to ensure we can continue normal business in the event of a security incident.

We will ensure that we have a Critical Incident Plan in place to ensure a process is documented for what to do, who to call and what the priorities are in the event of a disaster.

We have a process in place for testing, assessing and evaluating the effectiveness of the measures we have in place. We will obtain appropriate insurance which includes cyber security cover, to ensure we can cover the costs of a serious cyber event.

The Trust will maintain documented backup and recovery arrangements for critical systems and information.

Recovery arrangements will identify:

- Critical systems and services and the order in which they must be restored.
- Appropriate recovery time and recovery point objectives, proportionate to operational needs and risks.
- The individuals responsible for activating and managing recovery arrangements.
- Procedures for restoring data and systems following a cyber incident, system failure or other disruption.

Backups must be appropriately protected against unauthorised access, alteration, deletion and ransomware attacks. Recovery arrangements will be tested periodically, with the results documented and any identified weaknesses addressed.

Business continuity and disaster recovery arrangements will be reviewed at least annually and following a significant incident or material change to critical systems.

Links with other Policies

This policy should be read in conjunction with the following:

Academy Policies	Trust Policies
• Business continuity and disaster recovery planning • Cyber Security Policy and risk assessment • Cyber Security Standards • Digital Standards policy • RPA-Cyber Response Plan	• Artificial Intelligence (AI) Policy • Data protection policy • Information Security Policy • Managing Personal Relationships at work Policy • Online Safety Policy • Records Management Policy • Staff Acceptable Use

Appendix One – Data Breach Procedure **Introduction**

To enable us to report serious incidents to the ICO within 72 hours it is vital that we have a robust system in place to manage, contain, and report such incidents.

This procedure has been written to govern our management of data breaches.

Roles and Responsibilities
Single Point of Contact (SPOC) – Headteacher or appropriate delegate (DHT, AHT, SBM) Senior Information Risk Owner (SIRO) – CEO or appropriate member of the senior leadership team.
Information Asset Owner (IAO) – Headteacher as detailed in the Information Asset Register. Data Protection Officer (DPO) – Veritau.

Immediate Actions (within 24 hours)
If any member of the workforce is made aware of an actual data breach, or an information security event (a 'near-miss'), they must report it to their line manager and the Single Point of Contact (SPOC) within 24 hours. If the SPOC is not at work at the time of the notification, their nominated deputy would need to start the investigation process.

If the breach has the potential to have serious or wide-reaching detriment to data subjects, then the Data Protection Officer must be contacted within this 24-hour period.

If appropriate, the individual who discovered the breach, or their line manager, will make every effort to retrieve the information and/or ensure recipient parties do not possess a copy of the information.

Internal reporting deadlines must not delay the Trust's assessment, containment or notification of a personal data breach. Any incident that may meet the statutory reporting threshold must be escalated to the DPO and the appropriate Trust leadership immediately.

Assigning Investigation (within 48 hours)
Once received, the SPOC will assess the data protection risks and determine the severity rating using the Risk Matrix. An Investigation Report should also be completed.

The SPOC will notify the Senior Information Risk Owner (SIRO) and the relevant Information Asset Owner (IAO) that the breach has taken place. The SPOC will recommend immediate actions that need to take place to contain the incident.

The IAO will assign an officer to investigate any near misses, very low, low and moderate incidents. High or very high incidents will be investigated by the SPOC or SIRO, with assistance from the Data Protection Officer (DPO).

Reporting to the ICO/Data Subjects
The SIRO, in conjunction with the relevant manager, SPOC, IAO and DPO will decide whether the incident needs to be reported to the ICO, and whether any data subjects need to be informed. The relevant member of staff/IAO will be responsible for liaising with data subjects and the DPO for liaising with the ICO.

Investigating and Concluding Incidents
The SPOC will ensure that all investigations have identified all potential information risks and that remedial actions have been implemented.

When the DPO has investigated a data breach, the SIRO must sign off the investigation report and ensure recommendations are implemented.
The SIRO will ensure all investigations have been carried out thoroughly and all highlighted information security risks addressed.

All incidents should be recorded on our Data Breach Log, along with the outcome of the investigation

Appendix Two – Remote Working Policy **Introduction**

On some occasions our workforce may need to work at home or remotely. Where this is the case, the workforce will adhere to the following controls:

Lockable Storage
Individuals will ensure they have lockable storage to keep personal data and our equipment safe from loss or theft. If the individual does not have access to lockable storage, they may apply to the school for assistance in purchasing such storage.

Individuals must not keep personal data or our equipment unsupervised at home for extended periods of time (during periods of annual leave).
Individuals must not keep personal data or our equipment in cars if unsupervised.

Private Working Area
Individuals must not work with personal data in areas where other individuals could potentially view or even copy the personal data (for example on public transport).

Individuals should also take care to ensure that other household members do not have access to personal data and do not use our equipment for their own personal use.

Secure Remote Access and Confidentiality
Staff must only access Trust systems remotely using approved and appropriately secured methods.
When working remotely, staff must:

- Ensure that screens and printed information cannot be viewed by unauthorised individuals.
- Use approved secure remote access arrangements and multi-factor authentication where required.
- Avoid discussing confidential information where conversations may be overheard.
- Use approved platforms for online meetings and ensure that meetings involving confidential information are appropriately secured.
- Avoid downloading or storing personal data locally unless there is a genuine business need and appropriate security measures are in place.
- Report immediately any suspected loss, theft, unauthorised access or disclosure of Trust information or equipment, including incidents occurring while working remotely.

Trusted Wi-Fi Connections
Individuals will only connect their devices to trusted Wi-Fi connections and **will not** use 'free public Wi-Fi' or 'Guest Wi-Fi'. This is because such connections are susceptible to malicious intrusion.
When using home Wi-Fi networks individuals should ensure that they have appropriate anti- virus software and firewalls installed to safeguard against malicious intrusion. If in doubt, assistance should be sought from our IT provider.

Encrypted Devices and Email Accounts
Individuals will only use encrypted devices issued by ourselves to access school data, unless authorised by the SIRO in accordance with the acceptable use policies.
Individuals will not use personal email accounts to access or transmit school related personal data. Individuals must only use school issued, or school authorised, email accounts.

Data Removal and Return
Individuals will only take personal data away from our premises if this is required for a genuine business need.
Individuals will take care to limit the amount of data taken away from the premises and will ensure that all data is returned to our premises either for re- filing or for safe destruction. Individuals will not destroy data away from the premises as safe destruction cannot be guarantee.