Information Security Policy

1 Introduction

1.1 Summary

Information security is a concern for any organisation reliant on technology and data to operate, and a breach of information security should be considered a core business risk.

The education sector is facing an increased information security threat and has in recent years rapidly adopted new technologies into core operations, leading to even greater risk.

The Heart of Mercia Multi-Academy Trust acknowledges the significance of this risk and by way of this policy commits to understanding, identifying, and mitigating the risks it faces.

The requirements of this policy are based around three information security frameworks:

- The *Centre for Internet Security*'s (CIS) *Critical Security Controls - Version 8.1*–a list of 153 security safeguards, grouped within 18 overarching Controls. This policy adopts most of the safeguards within the framework. Exact coverage is detailed in Appendix A.1.1.
- The *National Cyber Security Centre's* (NCSC) *Cyber Essentials* – a framework and associated certification that all ESFA funded providers are expected to be working towards. This policy covers all the requirements of the scheme.
- The *Department for Education's* (DfE) *Meeting digital and technology standards in schools and colleges* – a list of 45 standards that all schools and colleges should aim to meet. 7 of these standards are categorised under Cyber Security, and several others deal with security-related issues.

The policy also aims to support the actions and assurances detailed in the NCSC's Cyber Governance Code of Practice.

The requirements of this policy reflect the current membership of the Trust, including the current age range of its learners. This policy will be reviewed in the future to incorporate primary learners and academies with high proportions of SEN learners. An exception statement regarding accessibility is detailed in section 1.4.

1.2 Definitions

For the purposes of this policy, the following definitions apply:

Trust

The Heart of Mercia Multi-Academy Trust including its academies.

Data

Any data or documents that are created, collected, processed, or stored to support the operation of the Trust and its academies, for which the Trust is the owner or has an obligation or organisational need to handle securely. Examples include learner records, staff records, financial records, policy document, process documentation, learning resources.

Device

Physical or virtual devices with the potential to collect, process or store data including:

- Mobile phones and tablets,
- Desktops and laptop PCs
- Physical and virtual servers
- Switches, firewalls, and other network hardware
- Any other device connected to a network or the public internet.

Software

An application or service that is installed on executes on a device and for which the Trust is responsible for installing updates and licencing. For the purposes of this policy, vendor-managed cloud platforms should not be considered software. Examples of software include:

- Device firmware
- Operating systems
- Background services and tools
- End-user software
- Extensions installed in web browsers, email clients and other software.
- Libraries
- Scripts

Cloud Platform

Any service, satisfying the following requirements:

- The service is hosted in third-party data centres and usually accessible over the public internet.
- The vendor is solely responsible for the hosting, maintenance and security of the underlying platform and physical infrastructure.
- It is used to collect, process or stored organisational data. Including data that is not considered personally identifiable information (PII).
- The Trust is responsible for some security configuration of the service, such as adding and removing users.

Infrastructure-as-a-service platforms should be considered cloud platforms, but for the purposes of this policy the resources provisioned within them should be considered devices or software.

System

Any device, cloud platform or software that collects, transmits, processes, or stores data or supports or facilitates the operation of the Trust. For the purposes of this policy most systems including networks, desktop and laptop PCs, web applications are comprised of other smaller sub-systems. Unless otherwise stated, the requirements of this policy apply to all systems at all degrees of granularity.

Control

Any process or technical measure that can be introduced to improve the security of a system.

Staff

Any individual that carries out an employee-like role in the Trust and has need to access any Trust system or work with data. This includes all contracted employees and, depending on exact working practices, may include:

- Local Governing Board members
- Trustees
- Members
- Exam Invigilators
- Other individuals paid on ad-hoc or flexible contracts
- Contractors or individuals from third-party organisations
- Volunteers

Administrator and Administrator Permissions

Any user or system that has widespread or unrestricted permissions to access or modify a system.

1.3 Audience

The intended audiences for this policy are:

- Senior leaders within the Trust and its academies.
- Staff working in information-technology roles.
- Staff working in data management roles.
- Staff responsible for data protection.

1.4 Obligations

Although the Trust is responsible for ensuring the obligations of this policy are met, unless otherwise stated, these obligations may be met by academies on an individual basis.

This policy is not intended to govern the general behaviour of staff and learners within Trust systems, only to impose some requirements around how they must access systems. Staff and learners' obligations within this policy, as well as expectations regarding their usage of systems, must be set out in an Acceptable Use policy or equivalent document that all staff and learners

should review. All obligations for staff and learners set out in this policy are collated in Appendix A.3.

Where requirements of this policy impact how staff and leaners interact with systems, exceptions can be made to ensure systems remain accessible. These exceptions should be limited to individual staff or learners, or where appropriate, whole learner cohorts.

Legislation relevant to this policy and the use or configuration of systems includes:

- Computer Misuse Act 1990
- Data Protection Act 2018
- Privacy and Electronic Communications (EC Directive) Regulations 2003

1.5 External References

Where this or another Heart of Mercia policy does not cover a particular aspect of information security, the Trust is assumed to adopt the position of the following external sources, in order of preference:

- Any legislation or statutory guidance
- The latest version of the DfE's *Meeting digital and technology standards in schools and colleges*.
- Other guidance issued by the DfE
- The latest requirements of Cyber Essentials
- Other guidance issued by the NCSC
- Guidance issued by Jisc
- The latest version the CIS Controls

1.6 Roles and Responsibilities

Most individuals with the Trust have some role in supporting the management of information security risk:

- **The Trust Board**
  - ensure the Trust executive are adequately managing information security risk.
  - challenge and assure the approach of the Trust in alignment with the NCSC's Cyber Governance Code of Practice and with reference to the DfE's Meeting digital and technology standards in schools and colleges.
- **Trust CEO**
  - ensure adequate resources are available centrally to manage security risk.
  - understand the Trust's security risk posture and hold the CDTO accountable for its reduction.

  - ensure engagement from the Trust board and academy heads in the management of security risk.
  - assist the CDTO in the introduction of Trust-wide security initiatives.
- **Trust Chief Data & Technology Officer**
  - act as the senior owner of information security risk in the organisation
  - set information security policy.
  - support academies to improve their security posture.
  - hold academies accountable for policy implementation.
  - ensure the Trust executive and the Trust Board are kept informed of information security risk across the organisation.
  - define and lead Trust-wide initiatives to reduce security risk.
  - liaise with academy heads, IT strategy leads and IT managers to ensure academy security risk is managed adequately
  - act as an escalation point for academy information security issues
- **Academy Heads**
  - ensure appropriate resources are available in the academy to support the reduction of security risk.
  - understand their academy's information security risk posture and hold their IT strategy lead and IT managers accountable for its reduction
  - support with implementation of security initiatives within the academy
  - when necessary, escalate academy information security issues to the CDTO
- **Academy IT Strategy Leads (or equivalent)**
  - in collaboration with the academy IT manager, assess and monitor the information security risk of the academy
  - coordinate academy implementation of this policy
  - own and oversee academy security policy when required (e.g. AUP)
  - hold the IT manager accountable for the technical aspects of this policy and other academy risk reduction initiatives
  - when necessary, escalate academy security issues to the academy head or CDTO

- **IT Managers (or equivalent)**
  - implement and maintain the technical requirements of this policy.
  - work with the academy IT strategy lead to assess the risk of the academy
  - ensure the academy IT strategy lead and CDTO are aware of emerging issues
  - ensuring the whole IT team is aware of the requirements of this policy
  - support system administrators/owners in other operational areas (e.g. safeguarding) with securing their systems.
  - When necessary, escalate academy security issues to the academy IT strategy lead or CDTO.
- **Other System Administrators / Owners**
  - be aware of the requirements of this policy and ensure relevant requirements are applied to systems not managed by the IT team.

- when needed, seek support from IT teams in implementing security measures
- make IT managers or academy IT strategic leads aware of security issues related to systems they own.

- **Staff**
  - report potential security issues
  - engage with training and awareness materials
  - meet their individual obligations within this policy (e.g. password use) and other security-related agreements/policies.
- **Learners**
  - report potential security issues to staff
  - engage with security awareness delivered through the curriculum
  - meet their individual obligations within this policy (e.g. password use) and other security-related agreements/policies.

1.7 Policy Breaches

At the discretion of the roles outlined in section 1.6, where the Trust, operational Trust teams, or individual academies, persistently fail to meet, or work towards meeting, the requirements of this policy these issues may be raised in the Risk Register.

1.8 Point of Contact

Questions about this policy and general information security questions or concerns can be raised by contacting: information.security@heartofmercia.org.uk

2 Aims & Objectives

2.1 Aims

The aim of this policy is to lay a foundation for a good information security culture across the Trust and to support four fundamental goals and obligations of the Trust and its academies:

Teaching, Learning and Learner Outcomes

Teaching and learning across the Trust is inextricably reliant on information and technology systems. By creating a good security culture, the Trust can ensure staff and learner access to systems is not disrupted and ultimately supports the best learning and outcomes for learners.

Safeguarding

A solid foundation of information security ensures the Trust can perform its safeguarding duty by protecting the confidential data held about learners and staff and ensuring the systems that protect learners and staff from online harms are in place and remain relevant.

Funding and Audit

To maintain funding, the Trust has a duty to ensure statutory returns are timely and accurate. A strong security posture ensures the relevant data is not altered or systems disrupted around essential funding deadlines.

Data Protection

Under data protection legislation, the Trust has a legal duty to ensure that all personal data is held securely. Encouraging good security practice across the Trust will support this endeavour in line with the Trust's Data Protection Policy.

2.2 Objectives

The Trust aims to fulfil the purpose of this policy, by developing and maintaining an information security culture that works to achieves five core objectives:

Confidentiality

All systems and data should be accessible only to those who have an operational need to access them in accordance with their role within, or in cooperation with, the Trust, and the legal basis on which the Trust holds any relevant data.

Integrity

All data held by the Trust should be trusted not to have been modified, accidentally or maliciously, to no longer represent the truth, and systems can be trusted to operate as intended.

Availability

All systems and data should be available, within the bounds of confidentiality, to all applicable users when required by an operational need.

Resilience

The Trust should be able to mitigate information security risks or where mitigation is not possible and an attack or breach is successful, the Trust should be able to recover back to normal operation without undue disruption or cost.

Sustainability

The Trust should continuously improve its security culture to ensure all other aims are met as the risk and threat landscape changes over time.

3 Risk Management

3.1 Risk Acknowledgement

- The Trust shall treat information security risk as a significant risk and relevant its core function of delivering teaching and learning.

- Leadership teams across the Trust shall be briefed regularly on and acknowledge the information security risk faced by the Trust.
- Information security risks shall be managed in accordance with the Trust Risk Management Policy and all information security risks should be captured in the central risk platform. As of June 2025, the central risk platform is available at: https://portal.heartofmercia.org.uk
- The Trust and each Academy shall maintain strategic information security items on the Risk Register ensuring adequate coverage and assessment of:
    - the five objectives of this policy (as in 2.2)
    - possible staff and learner behaviours that could cause an information security incident
    - access and permissions of staff

3.2 Risk Appetite

Due to the role of secure systems and a good security culture in fulfilling core aims of the organisation (as in 2.1), the reliance of some of these systems for fulfilling the organisation's duty of care to staff and learners, as well as the sensitivity of the data the Trust holds – the Trust's information security risk appetite is low. This means that the Trust aims to continuously reduce its information security risk posture and is cautious when embarking on initiatives that introduce additional security risk to the organisation.

3.3 Operational Information Security Risks

- This policy requires that where certain categories of risk are identified, introduced, or not mitigated these are captured in the Risk Register.
- These risks must be captured as Operational Risks in the Risk Register, with an appropriate senior leader set as the Senior Risk Owner, and the applicable IT manager or equivalent set as the Assignee.
- The there are five categories of risk where a decision has been taken to introduce or not mitigate risk:
    - Externally accessible firewall configuration, according to section 6.3.
    - Openings in firewalls, according to sections 6.3 and 6.4.
    - Systems without enforceable multi-factor authentication, according to section 7.4
    - Granting of administration access, according to section 7.5
    - Vulnerable, unpatched and out of support systems, according to section 8.4
- When documenting these decisions in the central risk platform, the description must include the following:
    - Category of decision
    - Details of the decision being made e.g. the related vulnerability, firewall rule
    - Operational justification for the decision
- Findings from External Security Assessments must also be captured, according to section 8.3.
- Operational Risks should be reviewed periodically according to the timelines set out in the Trust Risk Management Policy.

4 Asset Management

4.1 Device Register

- The Trust must maintain a register of all devices provisioned and managed by the Trust.
- For each device the following must be recorded:
    - Technical details of the device including make/model/vendor/operating system type/operating system version.
    - What is the operational purpose of the device.
    - Where is the device located?
    - How are software and firmware updates applied?
    - If not applied automatically, how *often* are software and firmware updates applied?
    - Who is responsible for monitoring and applying available updates, or in the case of automatically applied updates, who is responsible for monitoring this process?
    - Does the device or its software have known vulnerabilities that cannot be resolved, is unable to receive further updates or is out support from the vendor?
    - If the device is known to be vulnerable or out of support, what steps have been taken to mitigate this risk?
    - Whether there a software firewall enabled on the device and if not, why?
- Where devices are configured and managed uniformly, these may be listed as a single entry in the register, with the number of devices clearly indicated.
- The register must be reviewed and updated annually, when significant numbers of devices are provisioned, or when significant numbers of devices are decommissioned.
- The register must be held in the Trust asset management tool (see 4.6).

4.2 Device Provision and Monitoring

- Provision and management of devices must be centrally managed.
- Networks must be monitored for new or unrecognised devices. New devices should be investigated and removed where undesirable.

4.3 Software Register

- The Trust must maintain a register of all software running on all devices listed in section 4.1 of this policy.
- For each item the following must be recorded:
    - Software title
    - Software vendor/publisher
    - Current utilised versions
    - Where is the software installed?
    - How is the software installed on new devices?
    - How is the software licenced?
    - When does the licence expire?
    - Initial use date
    - The operational purpose of the software

  - How are updates applied?
  - Where applicable, is this software approved for use by learners and staff?
  - If not applied automatically, how *often* are updates applied?
  - Who is responsible for monitoring and applying available updates, or in the case of automatically applied updates, who is responsible for monitoring this process?
  - Does the software have known vulnerabilities that cannot be resolved, is unable to receive further updates or is out support from the vendor?
  - If the software is known to be vulnerable or out of support, what steps have been taken to mitigate this risk?
- The register must be reviewed annually.
- This register must be held in the Trust asset management tool (see 4.6).

4.4 Software Provision and Monitoring

- All software, libraries and scripts must be provisioned on an approval basis, with the installation or use of unauthorised software prevented.
- A process for requesting new software must be documented, followed, and reviewed annually.
- All utilised software must be supported by the vendor and receiving security updates according to section 8.1 of this policy.
- All software must be licenced appropriately for its use within the Trust.
- Devices must be regularly audited, and any unauthorised installed software removed.
- Approved software must be regularly audited and any software that is no longer required removed from the approved list.
- Automated tooling could be used to aid in the discovery and maintenance of the Software Register.

4.5 Cloud Platform Register

- The Trust must maintain a list of all utilised cloud platforms.
- This list must include the name of the platform, the purpose or functionality of the platform, the internal owner of the platform, the staff or team responsible for administering the platform (where different to the owner), the data processing location of the service, and details relating to licencing.
- This list must be reviewed annually.
- This register must be held in the Trust asset management tool (see 4.6).

4.6 Additional Considerations

- All registers must be treated as data and protected according to section 5 of this policy.
- The Trust shall maintain a centrally managed asset management tool for technology assets and to support compliance with sections 4.1, 4.3 and 4.5. As of June 2025, this platform is an instance of *Snipe IT* accessible at: https://assets.heartofmercia.org.uk

5 Data Security

5.1 Data Encryption

Data in Transit

- All data must be encrypted in transit, using secure protocols and methodologies.
- Encryption must be applied, regardless of the network conditions.
- Where applicable, systems must be configured to prefer encrypted traffic and redirect or reject unencrypted traffic.
- Where applicable, systems must be configured to use modern encryption schemes and ciphers and reject the use of encryption schemes and ciphers with known weaknesses.

Data at Rest

- Unless technically prohibitive, systems must encrypt all data at rest using a modern encryption method.
- Where devices are issued to individual staff or learners, full disk encryption or an equivalent control must be enabled and enforced. For staff devices, pre-boot authentication must be in place requiring biometric authentication, or a password or PIN that complies with section 12 of this policy.
- Where systems storage sensitive data (e.g. medical, safeguarding, SEND), additional layers of encryption must be applied, allowing only certain processes or users to access plaintext data.
- When allowed according to section 6.4, and utilised by staff, writeable removable storage mediums must be encrypted before any data is transferred.

5.2 Backups

- All long-lived data must be backed up. Exceptions can be made in cases where it would be practical to restore the data using a third-party source.
- At least three backup or redundant copies of data must be in place at any given time.
- It must be possible to restore the data to a state no older than 24 hours, using any of the three backup copies.
- In combination, copies taken must fulfil the following requirements:
    - At least one copy must be logically separated from the original data and at least one other backup copy.
    - At least one copy must be physically separated from the original data and at least one other backup copy.
    - At least one copy must be geographically separated from the original data and at least one other backup copy.
    - At least one copy must be protected from modification by the use of write-once-read-many storage or an ‘air gap’. This copy must also be logically and physically separated from the original data and at least one other backup copy.
- At least one copy must be stored in a cloud-based service.

- At least one copy must fulfil all requirements.
- Incremental backups must be taken as often as is practical and must be retained for at least 7 days.
- Full backups must be taken at least every 7 days and retained for at least 28 days.
- Access to backups must be applied on a strict least-privilege basis according to section 7.5 of this policy.
- The failure of a backup process must trigger an alert to appropriate stakeholders.
- Unless technically prohibitive, the existence of backups should be verified by a system independent of the backup system itself.
- The restoration of backups from all possible copies should be tested termly.
- The restoration of backups without any functioning infrastructure should be planned for and trialled where possible.
- Detailed processes around all aspects of data backups and restoration must be documented centrally, followed, and reviewed annually.

5.3 Additional Considerations

- Access to data must be granted on a least-privilege basis according to section 7.5 of this policy.
- Unless technically prohibitive, access or modification of sensitive data must be logged according to section 9 of this policy.
- Data Loss Prevention solutions or controls must be in place within systems that may be easily used to share or exfiltrate data, including email systems and others that allow arbitrary file sharing.
- Where possible, data storage devices must be securely wiped when undergoing a change of use or before being disposed of. Where secure wiping is not possible, storage devices must be retained within the organisation or securely destroyed.

6 Architecture and Configuration

6.1 General Principles

- A 'secure by default' approach to architecture and configuration must be adopted, ensuring systems are as secure as possible when provisioned, with access and features limited unless clearly indicated by organisational need.
- A 'defence in depth' approach to architecture and configuration must be adopted, ensuring adequate security controls are in place across all layers and sub-systems of a given system.
- Good 'system hygiene' must be practiced, ensuring unused systems are decommissioned and additional access, configuration and features within systems is removed or disabled when no longer required.
- Wherever possible, a ‘cloud first’ approach will be taken to the provision of new systems, adopting software-as-a-service systems whenever possible.
- Where practical, systems must be configured with built-in redundancy, failover capabilities and other configuration to support the availability of the system.

- All systems should be managed and maintained using secure methods and systems.
- All communication between systems and within networks must be transmitted over secure, authenticated, and encrypted protocols in accordance with section 5.1 of this policy.

6.2 Network Architecture and Configuration

- Network diagrams and other documentation relevant to network architecture must be documented and reviewed annually.
- Standard secure network architecture patterns must be documented and applied to all significant additions or changes to a network. Patterns should be reviewed annually to ensure they still meet security best practices.
- Networks must be configured to isolate systems from each other wherever possible.
- Connections to networks must be limited to known pre-registered devices. A dedicated personal-device network segment may be provisioned but must only allow access to the public internet. Staff and learners must be required to authenticate to utilise this personal-device network. Unauthenticated and 'guest' networks must not be made available.
- Any part of the network required to be exposed to the public internet must route all traffic through an appropriate firewall, and, except for public websites, must authenticate users to allow access.

6.3 Network Internet Boundaries and Firewalls

- The boundary between the internet and any Trust networks must be protected by an appropriate firewall.
- There must be a justifiable operational need for boundary firewalls to be configurable externally and multi-factor authentication must be enabled for all external access to boundary firewalls, in accordance with section 7.4 of this policy.
- If external configuration is required, this must be captured on the Risk Register according to section 3.3 of this policy.

Hardware Firewalls

- The default passwords for all hardware firewalls shall be changed at the point of installation, using a password that complies with section 12.3 of this policy.
- The steps required to change firewall passwords must be documented, followed, and reviewed annually.
- If a hardware firewall password is known or suspected to have been compromised or could have been compromised by a known vulnerability or malware incident, the password must be changed in according with section 12.4 of this policy.

Incoming Traffic

- Firewalls and internet boundaries must be configured to block all incoming traffic by default.
- There must be a justifiable operational need for any allowable incoming traffic.
- Any rules allowing incoming traffic must be captured on the Risk Register according to section 3.3 of this policy.

- Firewalls must be configured to allow as few ports, services, and external sources of traffic as possible to meet this need.

Outgoing Traffic

- Firewalls and internet boundaries must be configured to block all traffic and services for outgoing traffic by default.
- There should be a justifiable operational need for any allowable outgoing traffic.
- Any rules allowing outgoing traffic must be captured on the Risk Register according to section 3.3 of this policy.
- Firewalls must be configured to allow as few ports, services, and external sources as possible to meet this need.
- Outgoing DNS requests to known malicious domains musted be blocked.
- Other traffic, including web traffic, to known or suspected malicious destinations must be blocked.

6.4 Device Configuration

- Unless otherwise stated all devices must comply with all applicable requirements of Cyber Essentials.
- Standard secure configurations for common device types should be documented and applied to all new applicable devices. These configurations should be reviewed annually to ensure they still meet security best practices.
- Where supported, software firewalls must be enabled on all devices. Where not supported, devices must have unused ports closed. Software firewalls must block all traffic by default.
- Any rules allowing inbound or outbound traffic must be captured on the Risk Register according to section 3.3 of this policy.
- All default or built-in accounts on a device must have their password changed as part of the provisioning process using a password that complies with section 12 of this policy.
- Any local account on a device must be deleted or disabled unless there is a technical or operational need for them to remain. Local accounts on devices should be reviewed annually.
- All software on devices must provisioned on an approval basis and fully supported by the vendor according to section 4.4 of this policy and updated according to section 8.1 of this policy.
- Installation of extension into web browsers must be disabled by default. Extensions must be considered software and managed according to sections 4.4 and 8.1 of this policy.
- Wherever possible, devices should be configured with remote-wiping capabilities in place.

Device Locking

- Where technically possible, all devices that a user can interact with, shall ‘lock’ after a period of inactivity of no more than:
    - 10 minutes for laptops, desktops and tablets
    - 2 minutes for smartphones

- Devices that operate in a 'kiosk' mode to provide a single function or other embedded devices, do not need to meet this requirement.
- Once locked, a device shall only be unlocked using one of the following:
    - Biometric mechanisms
    - The password used to originally log into the device.
    - A PIN compliant with section 12 of this policy.
- When a PIN is used, this must only unlock the device. The user must authenticate using biometrics or a password before being able to access data or other systems.
- Devices shall be protected from repeated unlocking attempts by throttling the user's ability to input an attempt.
- This protection shall not allow more than 10 unsuccessful attempts in any 5-minute period.

Anti-Malware

- A modern, behaviour-based anti-malware software must be deployed to all applicable devices.
- Anti-malware software must be managed according to sections 4.4 and 8.1 of this policy.
- Anti-malware software must support automatic signature updates. These must be installed within 3 days of becoming available.
- Wherever possible, advanced anti-malware features must be enabled.
- Where possible, anti-malware must be configured to scan webpages and other traffic.

Removable Media

- Anti-malware provisioned as above must be configured to scan removable storage.
- Autorun and autoplay features for removable storage media must be disabled.
- General use of removable media, including USB drives, should be prohibited by default and allowed only in specific use-cases for a defined subset of users.

6.5 Email Configuration

- SPF and/or DKIM records must be configured for all legitimate sources of outgoing email traffic.
- A suitable DMARC policy must be in place that reports traffic appropriately and signals recipients to reject unauthenticated messages.
- MTA-STS and TLS-RPT must configured be to ensure inbound mail is encrypted.
- Email clients must be fully supported by the vendor and managed according to sections 4.4 and 8.1 of this policy.
- Installation of extensions into email clients must be disabled by default. Extensions must be treated as software and managed according to sections 4.4 and 8.1 of this policy.
- Email systems must, wherever possible, scan incoming and outgoing traffic for potential security threats including malware and malicious links.
- Email systems must block the sending or receiving of high-risk file types including executables and scripts.

- Email clients must be configured to support users in reporting messages they believe to be potentially fraudulent or malicious.

7 Account and Access Management

7.1 General Account Management

- Wherever possible, all accounts should be issued within a centralised identity directory.
- Unless technically prohibitive, systems must be configured to only authenticate access against this centralised directory.
- When procuring systems, significant weighting must be given to systems can authenticate access against the centralised directory.

7.2 Staff Accounts

- All staff must be issued an account (their 'main account') within a central identity directory.
- This account must be linked to an organisational email address and inbox, and physical on-site access (where applicable).
- Any additional accounts issued to staff by the Trust, for systems that cannot authenticate staff using their main account, must be linked to their organisational email address.
- Where staff individually create additional work-related accounts in third-party services and systems, these accounts must be linked to their organisational email address.

Management of Staff Accounts

- Staff accounts must be issued no earlier than their formally agreed start date, unless access to systems is required to complete mandatory pre-start training.
- If a staff account is issued earlier for training purposes, steps must be taken to limit access to other systems and services until the formally agreed start date.
- Staff must not be given access to detailed learner data, or detailed data about other staff, prior to their formally agreed start date.
- For contracted staff, the agreed start date must be their contractual start date. For other staff, the formally agreed start date must be the first day they execute an employee-like role in the Trust.
- In all cases, staff accounts must only be issued if appropriate pre-start checks have been completed. These checks must include an enhanced Disclosure and Barring Service (DBS) check.
- Staff accounts must be deactivated or disabled no later than the day after their formally agreed end date.
- For contracted staff, the agreed end date must be their contractual end date. For other staff, the formal agreed end date must be the last day they perform an employee-like role in the Trust.
- Unless technically prohibitive, the management of staff accounts must be automated and based on an appropriate central data source managed by human resources or equivalent role.

- The process for managing all staff accounts, including additional accounts, must be documented, followed, and reviewed annually.
- Actions taken outside of the documented process must only be permitted:
    - At the discretion of an appropriate senior leader or HR
    - Where a staff account is suspected to have been compromised

7.3 Learner Accounts

- All learners must be issued an account (their 'main account') within a central identity directory.
- The main account must be linked to an organisational email address and inbox, and physical on-site access.
- Any additional accounts issued to learners by the Trust, for systems that cannot authenticate learners using their main account, must be linked to their organisational email address.

Management of Learner Accounts

- Learner accounts may be created in advance on enrolment, but credentials must be issued no earlier than the day of their enrolment at the relevant academy.
- Learner accounts must be deactivated after the learner has ceased studying at the relevant academy according to the following conditions:
    - Learners leaving before the end of an academic year, without pending examination or qualification results must have their accounts deactivated no later than the day after they leave.
    - Learners leaving at the end of an academic year, or with pending examination or qualification results, shall have their accounts deactivated no later than 60 days after they receive their examination results.
- Unless technically prohibitive, the management of learner accounts must be automated and based on an appropriate central data source, managed by learner-records or equivalent role.
- The process for managing all learner accounts, including additional accounts, must be clearly documented, followed, and reviewed annually.
- Actions taken outside of the documented process must only be permitted:
    - At the discretion of an appropriate senior leader
    - When a learner account is suspected to have been compromised

7.4 Multi-Factor Authentication

- Unless technically prohibitive, multi-factor authentication must be enabled, required, and technically enforced for all staff and learners accessing any Trust system.
- Exemptions may be applied if systems are being accessed from trusted devices or networks.
- The secondary authentication factor must be one or more of:
    - One-time passcodes
    - SMS messages
    - App-based notifications
    - Physical tokens

- Other secondary factors including 'memorable questions' must not be allowed or utilised.
- When procuring systems, significant weighting must be given to systems that support the technical enforcement of multi-factor authentication for all users.
- If a system does not support enforceable multi-factor authentication, the system must be captured on the Risk Register according to section 3.3 of this policy.

7.5 Access Management

- Staff and learners accounts must have a standard set of permissions issued to all accounts of each type.
- A formal process to request additional access to systems must be documented, followed, and reviewed annually.
- Access to systems must always be applied on a 'least-privilege' basis: accounts will be given the minimum access required for the associated user or system to perform their role or within the Trust.
- Any additional access should be documented and reviewed annually – any access no longer required should be revoked.
- Unless technically or practically prohibitive, access to systems should be provisioned using a 'role-based access control' approach – ensuring access is issued to roles based on functions within the Trust, and accounts linked to the appropriate roles.
- When an account is disabled, it must be removed from all roles and any other access to any system revoked.
- Where technically feasible, accounts must be monitored for suspicious activity and in response, depending on the level of suspicion, either prompt the user for additional authentication steps or block usage.
- Where technically feasible, access to systems for staff and learners must be restricted to locations within the United Kingdom. Temporary exemptions are permitted (e.g. for short-term international travel).

Administrator Accounts and Permissions

- Where staff are required to be administrators of a system, the account used to perform administrator duties should be distinct from the any account used by the individual to perform day-to-day tasks within the system. If a user only performs administrator duties within a particular system and does not access the system for day-to-day use, it may be acceptable to maintain only a single account. Exceptions may also be made within systems with limited access controls features.
- A process for requesting administrator permissions to a system must be documented, followed, and reviewed annually.
- Any administrator access granted must be captured on the Risk Register according to section 3.3 of this policy.
- An inventory of administrator accounts must be maintained and reviewed annually.
- To ensure administrator access to systems is available in an emergency, systems must be configured with at least two administrator accounts. Both these accounts could be issued to

staff users, or one account issued to a staff user and the other held as a 'break-glass' account with the credentials generated and stored according to section 12, with access restricted to limited named staff.

System and Service Accounts

- An inventory of system or service accounts, used for system-to-system interaction, must be maintained, and reviewed annually. Any unused accounts must be disabled.
- Any single service account must be utilised within as few systems as possible.
- Service accounts should never be repurposed; new service accounts must be created for new systems or significant changes in functionality or required permissions.

Temporary and Guest Accounts

- There may be a requirement for external users to access to certain systems on a temporary basis, for example:
    - Visitors accessing the network segment intended for personal devices (as in 6.2).
    - Limited scope engagements for external security assessments (as in 8.3).
    - Short-term contracts for installation or maintenance of systems.
- In these cases many of the processes outlined in this section can be relaxed assuming that:
    - Accounts are issued for an agreed time period and disabled as soon as possible.
    - Access to systems is strictly limited to what is required.
    - Accounts are not shared between users and usage can be traced to an individual.
    - Other security measures (e.g. monitoring) are the same as for staff accounts.
    - Credentials are generated and shared according to section 12.
    - When practical, usage is supervised by a member of staff.

7.6 Additional Considerations

- As per section 1.4 of this policy, an Acceptable Use Policy must be in place and reviewed by all users before accessing any systems. The AUP must cover the obligations of users defined throughout this policy and collated in Appendix A.3.
- Where feasible, all accounts must be monitored for recent activity:
    - any accounts that have not been used within 3 months must be investigated to ensure they are still required and disabled if not.
    - any accounts that have not been used within 6 months, must be disabled.
- All accounts must have a password that meets the requirements in section 12 of this policy.
- Any accounts that have been disabled for more than 3 months should have their passwords changed to a random string, at least 32 characters long, and the value discarded.

8 Vulnerability and Patch Management

8.1 Updates and Patching

- Where supported, automatic security updates must be enabled on all systems, ensuring security updates are applied without manual intervention.
- A staggered or delayed approach may be taken to applying security updates to ensure releases do not cause disruption to systems.
- Where a system does not or cannot support the automatic application of security updates, a process of manually applying security updates must be documented as part of sections 4.1 or 4.3.
- All security updates must be applied within 14 days of release by the vendor.

8.2 Vulnerability Scanning and Management

- The Trust shall implement the tools and processes necessary to regularly assess the security posture and vulnerability of its systems.
- The tools and processes must be documented and reviewed annually.
- Where practical, assessments must be conducted monthly.
- Where it is impractical to assess all systems, a representative sample could be scanned and remediations applied to all similar systems.
- Reports on findings should be collated centrally and reviewed in line with the assessment schedule.
- Using the Common Vulnerability Scoring System (CVSS) scores and classifications, findings should be remediated within the following timelines:
    - 10.0-7.0 - Critical / High - 14 days
    - 6.9-4.0 - Medium - 60 days
    - 3.9-0.1 - Low – 6 months
- Where a CVSS score is not available for a finding, a sensible mapping must be applied based on the tooling used.

8.3 External Security Assessment

- The Trust shall regularly engage a competent independent third-party to assess the security posture and vulnerability of its systems.
- Assessments shall be completed at least once per-academic year.
- The scope of assessments shall be variable between years, based on several factors including:
    - The relative risk of systems
    - The period since a system was last externally assessed.
    - Newly introduced or recently modified systems
- Findings from assessments must be captured in the Risk Register according to section 3.3 of this policy.

8.4 Vulnerable, Unpatched and Out of Support Systems

- Additional steps must be taken to manage the risk associated with a system when:
    - a vulnerability or assessment finding cannot be remediated.
    - a security update cannot be applied.
    - a system no longer receives security updates from the original vendor.

- When practical, the system must be decommissioned.
- If the system cannot be decommissioned then steps should be taken to isolate the system from other systems and networks, and if possible, reduce the number of users accessing the system. The choice to maintain the system must be captured on the Risk Register according to section 3.3 of this policy.

9 Log Management & Monitoring

9.1 Log Management

- All systems must log security-relevant usage and operation, and data transfers. The scope and frequency of logs must be proportional to the criticality of the system and associated risk. Relevant items include outgoing DNS queries, URL requests, command line usage, sensitive data access, network traffic flow.
- All logs must be detailed enough to track and aid in the investigation of a security incident, including covering 'the 4 Ws': who, what, where, when.
- Logs must be treated as data and protected according to section 5 of this policy.
- Wherever possible, logs must be collated centrally.
- All logs must be retained for at least 180 days.
- Timestamps within logs must be standardised to Coordinated Universal Time (UTC).
- Steps must be taken to ensure systems have adequate storage for logs, independent of a system's main storage area.

9.2 Monitoring and Alerting

- Critical and sensitive systems must be actively monitored, and appropriate security alerts configured.
- Monitoring and alerting must be centralised wherever possible.
- Where feasible, any usage or traffic deemed suspicious must be logged, blocked, and investigated. This includes traffic between network segments and application-layer traffic.

10 Awareness and Training

10.1 Staff Pre-Start Training

- All staff must complete adequate training prior to starting as required in section 7.2 of this policy. This training must include topics covering:
    - Recognising social engineering attacks
    - Authentication and passwords according to sections 7.4 and 12.
    - Data handling and data protection breaches
    - Recognising and reporting security incidents
    - Use of personal devices according to section 13.

10.2 Staff Awareness

- All staff must receive an update on information security at least once per academic year.
- This update could include any new or evolving risks to the Trust or the sector, any changes or additions to relevant policies and procedures; and changes or additions end-user relevant security controls; applicable guidance; awareness resources; refresher training topics.

10.3 Student Awareness

- As part of their curriculum, academies must have a learner awareness programme in place that meets the DfE standard: Create and implement a cyber awareness plan for students and staff

11 Incident Management

11.1 Incident Reporting and Escalation

- A process for staff, learners, and the public to report possible information security incidents should be documented and reviewed annually. The process should be communicated to staff and learners annually and made readily available.
- An escalation process, that determines if and how reports are declared as major incidents, must be documented, followed and reviewed annually. This process should include who is authorised to declare a major incident.

11.2 Major Incidents & Plans

- Information security incident response plans must be in place.
- These plans must define how a major information security incident will be managed.
- All plans must include:
    - A clearly defined incident response manager role or equivalent, who will implement the plan and coordinate the response. This should be assigned to an individual, with a reserve.
    - Other clearly defined roles and associated responsibilities, with assigned individuals and reserves.
    - A clearly defined process for managing the incident.
    - Steps for conducting a post-incident review.
    - Clear plans for public, learner, and staff communications.
    - A clearly defined communication method for incident responders and details to reach all responders using this method. The method must be independent of all other systems.
    - A list of services as defined in 11.3
    - A list of organisations and individuals that must be notified of an incident, including contact details, and which responder is responsible for making the notification.

      Organisations should include:
        - National Cyber Security Centre
        - Department for Education

- JISC
- Action Fraud
- Information Commissioner's Office (when applicable)
- Local Police
- The Trusts' insurer

- Plans must be reviewed and exercised annually.
- An open and honest approach to incidents must be taken.
- Any ransom demanded must not be paid, under any circumstances.

11.3 Service List

- Any Information Security Response plans must maintain a list of the distinct information *services* utilised by the Trust or academy.
- A service may comprise of several systems and processes; the list should not detail these components instead focusing on the overall operational function provided the service.
- This list shall include the high-level services that are used as part of general operation and those that are used temporarily, for critical processes such as enrolment or exams.
- For each service, the following must be documented:
    - Is the service essential to the day-to-day operation of the Trust or relevant academy
    - The owner of the service
    - Steps required to check if the service is functioning as expected.
    - Steps to intentionally disable or 'turn off' the service.
    - Where applicable, steps required to restore the service to an acceptable state from backups
    - Where applicable, steps required to restore the service to an acceptable state without backups
    - A priority rating to determine the order services should be restored in the event of widespread disruption
- As well as being reviewed annually with the rest of the incident response plan, this list must also be amended when a new service is introduced, or an existing service is retired.

12 Passwords

12.1 Learner and Staff Accounts

- Passwords for learner and staff accounts (except administrators, see below) must meet the following requirements:
    - For staff and KS4+ learners: at least 14 characters in length
    - For KS3 learners: at least 10 characters
    - Chosen at random or generated using a reputable password generator
    - Contains 1 element of complexity - uppercase letter, digit or symbol
    - Unique for each account

- For staff and KS4+ learners: remembered or stored in a reputable password manager
- For KS3 leaners: remembered or physically printed/noted down.

- Any passcodes or PINS required for learner or staff accounts must meet the following requirements:
  - At least 6 digits in length for staff and KS4+ learners
  - Chosen at random or generated using a reputable password generator
  - Unique for each account
  - Remembered or stored in a reputable password manager.
- There must be no expectation for learners and staff to periodically change their password, passcodes or PINs.

12.2 Physical-Use Administrator Accounts

- Where copying the password from a password manager is not possible, passwords for administrator accounts must meet the following requirements:
  - At least 20 characters in length
  - Generated using the Trust-managed password manager or the Trust-managed password generator (see 12.5)
  - Contains 2 elements of complexity - uppercase letters, digits or symbols
  - Unique for each account
  - Remembered or stored in the Trust-managed password manager (see 12.5)
- Any passcodes or PINS required for the above administrator accounts must meet the following requirements:
  - At least 8 digits in length
  - Generated using the Trust-managed password manager (see 12.5)
  - Unique for each account
  - Remembered or stored in the Trust-managed password manager (see 12.5)
- Physical-use administrator passwords, passcodes and PINs must be changed every 90 days or less.
- Where technically feasible, once 90 days have elapsed, changes must not be allowed without the intervention of another administrator account.

12.3 Other Passwords

- Passwords required for any other purposes including system or service accounts, system root accounts, and other administrator accounts must meet the following requirements:
  - Generated using the Trust-managed password manager (see 12.5)
  - Be the maximum length allowed by password generator tool or, where shorter, the maximum length allowed for the relevant system
  - Composed of entirely random characters, unless limited by the relevant system.
  - Unique for each account
  - Stored in the Trust-managed password manger (see 12.5).
- Any passcodes or PINS required for any other purpose must meet the following requirements:
  - Generated using the Trust-managed password manager (see 12.5)

    - Be the maximum length allowed by the password generator tool or, where shorter, the maximum length allowed for the relevant system.
    - Unique for each account
    - Stored in the Trust-managed password manager
- Where practically and technically feasible, applicable passwords, passcodes and PINs must be periodically changed every 90 days or less.
- Where technically feasible, once 90 days have elapsed, changes must not be allowed without the intervention of another administrator account.

12.4 Password Compromise

- Learners and staff must change their password immediately if they suspect their account or the password may have been compromised.
- In the event it is suspected a password has been compromised the password should be immediately changed and the individual contacted to perform a reset.

12.5 Additional Considerations

- Unless technically prohibitive, systems must check new passwords against lists of common or previously compromised passwords.
- Wherever possible, password requirements must be technically enforced.
- Unless technically prohibitive, systems must allow staff and learners to reset their password using secure methods to verify their identity. This excludes methods such as security questions.
- Where systems can prevent the reuse of previous passwords for a given account, this feature must be enabled and set to the maximum value supported.
- The Trust shall maintain a centrally managed password management tool to support staff who require multiple administrator accounts across different systems and, when necessary, to store shared credentials within teams. Use of another password management tool to store administrator or shared credentials is prohibited. As of June 2025, the centrally managed password management tool is 1Password, available at: https://heart-of-mercia.1password.eu
- The Trust shall maintain a publicly accessible password generator to support learners and staff in generating passwords compliant with this policy. As of June 2025, this is available at: https://cyber.heartofmercia.org.uk
- Except for temporary use, 'break-glass' use, or unless otherwise stated, passwords must be remembered or stored in a reputable password manager.

13 Personal Devices

13.1

- Any laptop, smartphone, tablet, desktop, or other device used to access Trust systems, that is not issued or fully controlled by the Trust must be considered a 'personal device.'
- Access to Trust systems from personal devices shall be limited to:

- Systems accessible from the public internet
- Adequately isolated networks that provide access only to the public internet

13.2 Staff Personal Devices

- Staff must, wherever possible, opt to use a Trust managed device to access Trust systems.
- If staff choose to use a personal device to access applicable Trust systems, the device must meet the following requirements:
  - They must personally own the device.
  - The device must comply with all applicable requirements of *Cyber Essentials*.
  - If the device is routinely shared with others, they must log out of all Trust systems after use.
- Staff must not save or store Trust data on any personal device, except where this storage is fully contained within an approved application (e.g. Microsoft Outlook on a smartphone).
- Staff must, upon request, provide details of any personal device they use to access Trust systems. Details may include:
  - Device manufacturer
  - Device model number
  - Installed operating system, including precise version numbers
  - Installed web browser, including precise version numbers
  - Installed anti-malware software, including precise version numbers
- Staff must, upon request, provide written confirmation that any personal device they use to access Trust systems meets the requirements outlined.
- The Trust must maintain a list of all mobile and desktop devices owned by staff, that are used to access any Trust systems or data.
- For each device the following must be recorded:
  - The person who owns the device
  - The device manufacturer, model, operating system, and operating system version
- This list must be reviewed and updated annually.

13.3 Learner Personal Devices

- Learners can access applicable Trust systems using any device available to them, where they can reasonably trust that the device has not been compromised and would not represent a credible risk or threat to the relevant system.
- Learners must not be routinely blocked from using a device to access Trust systems, except where there is sufficient evidence that the device has been compromised or would represent a credible risk or threat to the relevant system.

14 Equality Impact

The Trust's responsibilities towards promoting equality, diversity and inclusion have been considered when drafting this policy.

Policy document

Date of review	Date agreed	LGBs	MAT Board	Review date	Comments
June 2025	November 2025	Spring 2026	December 2025	June 2026	

Information Security Policy - Appendix

A.1 Framework Adoption

A.1.1 CIS - Critical Security Controls

Where possible, this policy aligns with the safeguards within the *Centre for Internet Security's (CIS) Critical Security Controls – Version 8*.

The table below lists these safeguards, grouped within their CIS Control. A Yes/No column has been included indicating whether this policy addresses that safeguard.

Note that safeguards within CIS Control 15 'Service Provider Management' and CIS Control 16 'Application Software Security' have been omitted entirely due those areas being outside the scope of this policy.

Where individual safeguards have not been adopted, justification is provided in the second table.

Code	Title	IG1	IG2	IG3	Y/N
1	**Inventory and Control of Enterprise Assets**				
1.1	Establish and Maintain Detailed Enterprise Asset Inventory	O	O	O	Y
1.2	Address Unauthorized Assets	O	O	O	Y
1.3	Utilize an Active Discovery Tool		O	O	Y
1.4	Use Dynamic Host Configuration Protocol (DHCP) Logging to Update Enterprise Asset Inventory		O	O	Y
1.5	Use a Passive Asset Discovery Tool			O	Y
2	**Inventory and Control of Software Assets**				
2.1	Establish and Maintain a Software Inventory	O	O	O	Y
2.2	Ensure Authorized Software is Currently Supported	O	O	O	Y
2.3	Address Unauthorized Software	O	O	O	Y
2.4	Utilize Automated Software Inventory Tools		O	O	Y
2.5	Allowlist Authorized Software		O	O	Y
2.6	Allowlist Authorized Libraries		O	O	Y
2.7	Allowlist Authorized Scripts			O	Y
3	**Data Protection**				
3.1	Establish and Maintain a Data Management Process	O	O	O	N
3.2	Establish and Maintain a Data Inventory	O	O	O	N
3.3	Configure Data Access Control Lists	O	O	O	Y
3.4	Enforce Data Retention	O	O	O	N
3.5	Securely Dispose of Data	O	O	O	Y
3.6	Encrypt Data on End-User Devices	O	O	O	Y
3.7	Establish and Maintain a Data Classification Scheme		O	O	N

3.8	Document Data Flows		O	O	N
3.9	Encrypt Data on Removable Media		O	O	Y
3.10	Encrypt Sensitive Data in Transit		O	O	Y
3.11	Encrypt Sensitive Data at Rest		O	O	Y
3.12	Segment Data Processing and Storage Based on Sensitivity		O	O	N
3.13	Deploy a Data Loss Prevention Solution			O	Y
3.14	Log Sensitive Data Access			O	Y
4	**Secure Configuration of Enterprise Assets and Software**				
4.1	Establish and Maintain a Secure Configuration Process	O	O	O	Y
4.2	Establish and Maintain a Secure Configuration Process for Network Infrastructure	O	O	O	Y
4.3	Configure Automatic Session Locking on Enterprise Assets	O	O	O	Y
4.4	Implement and Manage a Firewall on Servers	O	O	O	Y
4.5	Implement and Manage a Firewall on End-User Devices	O	O	O	Y
4.6	Securely Manage Enterprise Assets and Software	O	O	O	Y
4.7	Manage Default Accounts on Enterprise Assets and Software	O	O	O	Y
4.8	Uninstall or Disable Unnecessary Services on Enterprise Assets and Software		O	O	Y
4.9	Configure Trusted DNS Servers on Enterprise Assets		O	O	N
4.10	Enforce Automatic Device Lockout on Portable End-User Devices		O	O	Y
4.11	Enforce Remote Wipe Capability on Portable End-User Devices		O	O	Y
4.12	Separate Enterprise Workspaces on Mobile End-User Devices			O	N
5	**Account Management**				
5.1	Establish and Maintain an Inventory of Accounts	O	O	O	N
5.2	Use Unique Passwords	O	O	O	Y
5.3	Disable Dormant Accounts	O	O	O	Y
5.4	Restrict Administrator Privileges to Dedicated Administrator Accounts	O	O	O	Y
5.5	Establish and Maintain an Inventory of Service Accounts		O	O	Y
5.6	Centralize Account Management		O	O	Y
6	**Access Control Management**				
6.1	Establish an Access Granting Process	O	O	O	Y
6.2	Establish an Access Revoking Process	O	O	O	Y
6.3	Require MFA for Externally Exposed Applications	O	O	O	Y
6.4	Require MFA for Remote Network Access	O	O	O	Y
6.5	Require MFA for Administrative Access	O	O	O	Y
6.6	Establish and Maintain an Inventory of Authentication and Authorization Systems		O	O	N
6.7	Centralize Access Control		O	O	N
6.8	Define and Maintain Role-Based Access Control			O	Y
7	**Continuous Vulnerability Management**				
7.1	Establish and Maintain a Vulnerability Management Process	O	O	O	Y

7.2	Establish and Maintain a Remediation Process	O	O	O	Y
7.3	Perform Automated Operating System Patch Management	O	O	O	Y
7.4	Perform Automated Application Patch Management	O	O	O	Y
7.5	Perform Automated Vulnerability Scans of Internal Enterprise Assets		O	O	Y
7.6	Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets		O	O	Y
7.7	Remediate Detected Vulnerabilities		O	O	Y
8	**Audit Log Management**				
8.1	Establish and Maintain an Audit Log Management Process	O	O	O	Y
8.2	Collect Audit Logs	O	O	O	Y
8.3	Ensure Adequate Audit Log Storage	O	O	O	Y
8.4	Standardize Time Synchronization		O	O	Y
8.5	Collect Detailed Audit Logs		O	O	Y
8.6	Collect DNS Query Audit Logs		O	O	Y
8.7	Collect URL Request Audit Logs		O	O	Y
8.8	Collect Command-Line Audit Logs		O	O	Y
8.9	Centralize Audit Logs		O	O	Y
8.10	Retain Audit Logs		O	O	Y
8.11	Conduct Audit Log Reviews		O	O	N
8.12	Collect Service Provider Logs			O	Y
9	**Email and Web Browser Protections**				
9.1	Ensure Use of Only Fully Supported Browsers and Email Clients	O	O	O	Y
9.2	Use DNS Filtering Services	O	O	O	Y
9.3	Maintain and Enforce Network-Based URL Filters		O	O	Y
9.4	Restrict Unnecessary or Unauthorized Browser and Email Client Extensions		O	O	Y
9.5	Implement DMARC		O	O	Y
9.6	Block Unnecessary File Types		O	O	Y
9.7	Deploy and Maintain Email Server Anti-Malware Protections			O	Y
10	**Malware Defences**				
10.1	Deploy and Maintain Anti-Malware Software	O	O	O	Y
10.2	Configure Automatic Anti-Malware Signature Updates	O	O	O	Y
10.3	Disable Autorun and Autoplay for Removable Media	O	O	O	Y
10.4	Configure Automatic Anti-Malware Scanning of Removable Media		O	O	Y
10.5	Enable Anti-Exploitation Features		O	O	Y
10.6	Centrally Manage Anti-Malware Software		O	O	Y
10.7	Use Behaviour-Based Anti-Malware Software		O	O	Y
11	**Data Recovery**				
11.1	Establish and Maintain a Data Recovery Process	O	O	O	Y
11.2	Perform Automated Backups	O	O	O	Y
11.3	Protect Recovery Data	O	O	O	Y

11.4	Establish and Maintain an Isolated Instance of Recovery Data	O	O	O	Y
11.5	Test Data Recovery		O	O	Y
12	**Network Infrastructure Management**				
12.1	Ensure Network Infrastructure is Up to Date	O	O	O	Y
12.2	Establish and Maintain a Secure Network Architecture		O	O	Y
12.3	Securely Manage Network Infrastructure		O	O	Y
12.4	Establish and Maintain Architecture Diagram(s)		O	O	Y
12.5	Centralize Network Authentication, Authorization, and Auditing (AAA)		O	O	N
12.6	Use of Secure Network Management and Communication Protocols		O	O	Y
12.7	Ensure Remote Devices Utilize a VPN and are Connecting to an Enterprise's AAA Infrastructure		O	O	N
12.8	Establish and Maintain Dedicated Computing Resources for All Administrative Work			O	N
13	**Network Monitoring and Defence**				
13.1	Centralize Security Event Alerting		O	O	Y
13.2	Deploy a Host-Based Intrusion Detection Solution		O	O	N
13.3	Deploy a Network Intrusion Detection Solution		O	O	N
13.4	Perform Traffic Filtering Between Network Segments		O	O	Y
13.5	Manage Access Control for Remote Assets		O	O	N
13.6	Collect Network Traffic Flow Logs		O	O	Y
13.7	Deploy a Host-Based Intrusion Prevention Solution			O	N
13.8	Deploy a Network Intrusion Prevention Solution			O	N
13.9	Deploy Port-Level Access Control			O	N
13.10	Perform Application Layer Filtering			O	Y
13.11	Tune Security Event Alerting Thresholds			O	N
14	**Security Awareness and Skills Training**				
14.1	Establish and Maintain a Security Awareness Program	O	O	O	Y
14.2	Train Workforce Members to Recognize Social Engineering Attacks	O	O	O	Y
14.3	Train Workforce Members on Authentication Best Practices	O	O	O	Y
14.4	Train Workforce on Data Handling Best Practices	O	O	O	Y
14.5	Train Workforce Members on Causes of Unintentional Data Exposure	O	O	O	Y
14.6	Train Workforce Members on Recognizing and Reporting Security Incidents	O	O	O	Y
14.7	Train Workforce on How to Identify and Report if Their Enterprise Assets are Missing Security Updates	O	O	O	N
14.8	Train Workforce on the Dangers of Connecting to and Transmitting Enterprise Data Over Insecure Networks	O	O	O	N
14.9	Conduct Role-Specific Security Awareness and Skills Training		O	O	N
17	**Incident Response Management**				
17.1	Designate Personnel to Manage Incident Handling	O	O	O	Y

17.2	Establish and Maintain Contact Information for Reporting Security Incidents	O	O	O	Y
17.3	Establish and Maintain an Enterprise Process for Reporting Incidents	O	O	O	Y
17.4	Establish and Maintain an Incident Response Process		O	O	Y
17.5	Assign Key Roles and Responsibilities		O	O	Y
17.6	Define Mechanisms for Communicating During Incident Response		O	O	Y
17.7	Conduct Routine Incident Response Exercises		O	O	Y
17.8	Conduct Post-Incident Reviews		O	O	Y
17.9	Establish and Maintain Security Incident Thresholds			O	Y
18	**Penetration Testing**				
18.1	Establish and Maintain a Penetration Testing Program		O	O	Y
18.2	Perform Periodic External Penetration Tests		O	O	Y
18.3	Remediate Penetration Test Findings		O	O	Y
18.4	Validate Security Measures			O	Y
18.5	Perform Periodic Internal Penetration Tests			O	Y

Notes on Non-Adoption

Code	Title	Justification
3.1	Establish and Maintain a Data Management Process	This safeguard is outside the remit of this policy. Please see to Data Protection and Data Retention policies.
3.2	Establish and Maintain a Data Inventory	This safeguard is outside the remit of this policy. Please see to Data Protection and Data Retention policies.
3.4	Enforce Data Retention	This safeguard is outside the remit of this policy. Please see to Data Protection and Data Retention policies.
3.7	Establish and Maintain a Data Classification Scheme	This safeguard is outside the remit of this policy. Please see to Data Protection and Data Retention policies.
3.8	Document Data Flows	This safeguard is outside the remit of this policy. Please see to Data Protection and Data Retention policies.
3.12	Segment Data Processing and Storage Based on Sensitivity	Not practical or necessary to implement in the Trust context. Systems must uniformly meet the requirements of this policy as nearly all systems will process sensitive learner data.
4.12	Separate Enterprise Workspaces on Mobile End-User Devices	Unnecessary requirement for Trust managed devices and risks relating to personal devices are addressed in section 13 of this policy.
5.1	Establish and Maintain an Inventory of Accounts	This is impractical to generate for all Trust services, though requirements of section 7.1 of this policy recommends a single directory of accounts which would support this safeguard.
6.6	Establish and Maintain an Inventory of Authentication and Authorization Systems	Unnecessary burden and the Trust does not utilise enough authentication systems to warrant this safeguard. Section 7.1 of this policy recommends a single directory of

		accounts which addresses the risks relating to this safeguard.
6.7	Centralize Access Control	Impractical requirement for Trust resources, provisioning permissions in systems based on Active Directory roles is not widely supported.
8.11	Conduct Audit Log Reviews	Unnecessarily burdensome on the Trust to audit all logs for all systems.
12.5	Centralize Network Authentication, Authorization, and Auditing (AAA)	Unnecessarily burdensome and some elements of this safeguard are covered in section 9 of this policy.
12.7	Ensure Remote Devices Utilize a VPN and are Connecting to an Enterprise's AAA Infrastructure	Not relevant to the context of the Trust. All services should be authenticating sufficiently to not warrant VPN usage except in high-risk systems.
12.8	Establish and Maintain Dedicated Computing Resources for All Administrative Work	Unnecessarily burdensome with current resources. May be impractical in some Trust settings.
13.2	Deploy a Host-Based Intrusion Detection Solution	Safeguard is too specific and any advanced tooling will be considered on a cost-benefit basis.
13.3	Deploy a Network Intrusion Detection Solution	Safeguard is too specific and any advanced tooling will be considered on a cost-benefit basis.
13.5	Manage Access Control for Remote Assets	Implicit in the requirements of section 7.4.
13.7	Deploy a Host-Based Intrusion Prevention Solution	Safeguard is too specific and any advanced tooling will be considered on a cost-benefit basis.
13.8	Deploy a Network Intrusion Prevention Solution	Safeguard is too specific and any advanced tooling will be considered on a cost-benefit basis.
13.9	Deploy Port-Level Access Control	Implicit in the requirements of section 6 and 7.4.
13.11	Tune Security Event Alerting Thresholds	Unnecessarily burdensome with current resources.
14.7	Train Workforce on How to Identify and Report if Their Enterprise Assets are Missing Security Updates	Not appropriate for the context of the Trust. Technical measures covered by sections 4.4. and 8.1 of this policy address the risks relating to this safeguard.
14.8	Train Workforce on the Dangers of Connecting to and Transmitting Enterprise Data Over Insecure Networks	Not appropriate for the context of the Trust.
14.9	Conduct Role-Specific Security Awareness and Skills Training	Unnecessarily burdensome with current resources.

A.2 Documentation Requirements

A.2.1 Inventories, Lists and Registers

Item	Policy Section	Review Cadence
Devices	4.1	Annually
Software	4.3	Annually
Cloud Platforms	4.5	Annually
Administrator Accounts	7.5	Annually
Additional Access Permissions	7.5	Annually
Service Accounts	7.5	Annually
Services (as part of Incident Response Plan)	11.3	Annually
Staff Personal Devices	13.2	Annually

A.2.2 Processes

Item	Policy Section	Review Cadence
New Software Requests	4.4	Annually
Backups and Restoration	5.2	Annually
Hardware Firewall Password Changes	6.3	Annually
Learner Account Management	7.3	Annually
Staff Account Management	7.2	Annually
Administrator Access Requests	7.5	Annually
Additional Access Requests	7.5	Annually
Vulnerability Scanning	8.2	Annually
Incident Reporting	11.1	Annually
Incident Escalation	11.1	Annually
Incident Response Plans	11.2	Annually

A.2.3 Documentation

Item	Policy Section	Review Cadence
Acceptable Use Policy	1.4/7.6	Annually
Network Architecture Patterns	6.2	Annually
Network Diagrams	6.2	Annually
Other Architecture Documentation	6.2	Annually
Device Configuration Patterns	6.4	Annually

A.2.4 Operational Information Security Risks

Item	Policy Section
Hardware Firewall External Configuration	6.3
Inbound Firewall Rules	6.3 and 6.4

Outbound Firewall Rules	6.3 and 6.4
Systems without enforceable MFA	7.4
Administrator Access	7.5
Findings from External Security Assessments	8.3
Vulnerable, Unpatched and Out of Support Systems	8.4

A.3 Staff and Learner Obligations

Item	Policy Section
Staff Pre-Start Training	7.2 and 10.1
Staff and Learner Password Choices	12.1
Staff Personal Devices	13.1 and 13.2
Learner Personal Devices	13.1 and 13.3