AHMAT

ICT & Electronic Devices Policy

September
2025 - 2026

Ashley Hill Multi Academy Trust

Encourage one another and build each other up
1Thessalonians 5:11

VISION STATEMENT FOR AHMAT

Ashley Hill Multi Academy Trust is committed to securing the best outcome for every child in its schools within a learning environment characterised by a distinctive Christian ethos.

We value the uniqueness and individuality of every school in the Trust, encouraging each to develop to meet the particular needs of all its pupils and the community it serves, underpinned by a common commitment to work together, making full use of all the Trust's resources, to enhance the experience and opportunities of all.

In line with our core Christian beliefs and principles, we want each school to be an educational community where:

- all are welcome, whatever their cultural, ethnic or religious background;
- all will flourish, with a particular focus on supporting any who are disadvantaged culturally, socially, economically, physically, or in any other way;
- all will have a life-enhancing encounter with the Christian faith;
- each individual is encouraged and helped to discover and develop their God-given gifts and talents to the fullest extent;
- all will fulfil their potential in a way appropriate for their age, both academically and as well-rounded, independent, emotionally mature individuals.

Contents:

Statement of Intent

Ashley Hill Multi Academy Trust believes that ICT plays an important part in both teaching and learning over a range of subjects, and the Trust accepts that both school-owned and personal

electronic devices are widely used by members of staff. The Trust is committed to ensuring that both staff and pupils have access to the necessary facilities and support to allow them to carry out their work.

The Trust has a sensible and practical approach that acknowledges the use of devices, and this policy is intended to ensure that:

- Members of staff are responsible users and remain safe while using the internet.
- Trust ICT systems and users are protected from accidental or deliberate misuse which could put the security of the systems and/or users at risk.
- Members of staff are protected from potential risks in their everyday use of electronic devices.
- A process is in place for claiming financial payments when electronic devices are lost or damaged by members of staff.

Personal use of ICT equipment and personal devices is permitted at the school; however, this is strictly regulated and must be done in accordance with this policy, and the AHMAT Online Safety Policy.

Legal Framework

This policy has due regard to all relevant legislation and statutory guidance including, but not limited to, the following:

- Data Protection Act 2018
- Computer Misuse Act 1990
- Communications Act 2003
- Freedom of Information Act 2000
- Human Rights Act 1998
- Voyeurism (Offences) Act 2019
- The UK General Data Protection Regulation (UK GDPR)

Roles and Responsibilities

The AHMAT delegate the responsibility for ICT to their Local Governing Bodies.

Local Governing Bodies have the responsibility for the overall implementation of this policy, ensuring it remains compliant with relevant legislation.

The Head of School is responsible for:

- Reviewing and amending this policy with the Chief Executive Officer (CEO) and the Data Protection Officer (DPO), in consultation with the Trust's IT Services Provider, taking into account new legislation, government guidance, and previously reported incidents.
- The day-to-day implementation and management of this policy within the school.
- The allocation and provision of resources required to support compliance with this policy.
- Handling complaints regarding this policy as outlined in the school's Complaints Procedures Policy.
- Ensuring all staff are aware of, and comply with, the data protection principles outlined in the Trust's Data Protection Policy.

The IT Services Provider is responsible for:

- The Trust's IT Services Provider, working under the oversight of the Chief Executive Officer (CEO) and the Data Protection Officer (DPO), is responsible for:
- Monitoring Trust networks, systems, and user activity through appropriate technical tools and alerts, and reporting any concerns to the Senior Leadership Team (SLT).
- Maintaining and monitoring logs of network activity, security events, and system use, and escalating any inappropriate or suspicious activity in line with Trust policies.
- Implementing technical controls to protect Trust systems and data, including encryption, antivirus, firewalling, and secure configuration.
- Supporting staff with authorised use of ICT facilities and devices.
- Managing user accounts and access rights in line with requests authorised by the Senior Leadership Team (SLT).
- Ensuring that Trust-owned devices are secured and encrypted, and that any personal devices authorised for work purposes comply with the Bring Your Own Device (BYOD) Policy.

- Reporting any breaches involving devices or systems to the Senior Leadership Team (SLT) and the Data Protection Officer (DPO) without undue delay.

Staff members are responsible for:

- Using Trust-owned devices primarily for work purposes and in line with the Acceptable Use Policy.
- Following the Bring Your Own Device (BYOD) Policy when using personal devices for Trust purposes, including ensuring that such devices are encrypted and secured in line with Trust requirements.
- Requesting authorisation, via the Head of School and Chief Executive Officer (CEO), for the loan of Trust equipment where required.
- Reporting any misuse of ICT facilities or devices, by staff or pupils, to the Head of School without delay.
- Reading and signing a Device User Agreement to confirm they understand their responsibilities when using Trust-owned and authorised personal devices.

The Trust Business Manager is responsible for:

- Maintaining a Fixed Asset Register to record and monitor the school's assets.
- Ensuring value for money is secured when purchasing electronic devices.
- Monitoring purchases made under the Academies Financial .
- Overseeing purchase requests for electronic devices.

Classifications

School-owned and personal devices or ICT facilities include, but are not limited to, the following:

- Desktop computers, laptops, tablets (e.g. iPads) and associated software
- Monitors, keyboards, mice and peripherals
- Interactive whiteboards, smartboards and classroom presentation equipment
- Digital cameras and audio-visual equipment
- Telephones (fixed, mobile and VoIP systems)
- Printers, photocopiers, scanners and reproduction equipment

- Cloud-based platforms and Software-as-a-Service (SaaS) applications (e.g. Microsoft 365, collaboration tools, learning platforms)
- Email systems (internal and external)
- Internet, intranet and video conferencing services
- Trust-managed documents, records and publications (in any format, including digital or printed)

Information Security

Ashley Hill Multi Academy Trust (AHMAT) is committed to protecting all information assets, including pupil, parent, staff and school data, as well as information shared by trusted partners. Protecting information is essential to safeguarding personal data, maintaining trust, and ensuring compliance with statutory and regulatory requirements.

- Confidential information must be protected at all times.
- It may only be accessed by those with a legitimate need and must not be disclosed to unauthorised parties.
- Confidential information includes safeguarding records, staff and pupil data, financial information, unpublished materials, intellectual property, and system credentials.

Personal data must be collected, processed, stored and shared in line with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

- Names, addresses, contact details and payment information must not be shared without a lawful basis or the consent of the individual concerned.

All Trust systems, devices and services must be secured using appropriate technical and organisational measures.

- Strong authentication, encryption and access controls must be applied.
- Software must be kept up to date at all times.
- Access to information is restricted according to job role, following the principle of least privilege.
- Privileged accounts are closely controlled and monitored.

Devices and paper records must also be safeguarded.

- Devices must be physically secured when unattended.
- Sensitive information must not be left visible or accessible to unauthorised individuals.
- Paper records containing confidential information must be stored securely.

- Confidential paper records must be disposed of using approved confidential disposal methods.

Incidents involving Trust information must be reported immediately.

- This includes the loss, theft or unauthorised disclosure of information.
- Reports must be made to the Head of School, the Chief Executive Officer (CEO), and the Data Protection Officer (DPO).
- Suspected or actual cyber incidents, including attempted unauthorised access to systems or data, must also be reported without delay.

The Trust will maintain oversight of information security by:

- Putting policies in place
- Implementing technical controls
- Providing staff training
- Conducting regular monitoring

Compliance with these requirements is mandatory for all staff, governors, contractors, supply staff and volunteers.

Acceptable Use

The Trust provides ICT systems, electronic devices, email and internet access to support professional duties and the education of pupils. These resources must always be used responsibly, securely, and primarily for school business.

- Limited personal use may be permitted with Chief Executive Officer (CEO) approval, provided it does not interfere with work duties.
- The Trust monitors the use of ICT facilities and reserves the right to access systems and devices to ensure compliance.
- Pupils are required to follow their own acceptable use provisions, and staff are expected to act as role models in their use of ICT.
- ICT systems, devices and data may only be used for legitimate school purposes, including lesson preparation, research, communication, and the processing of school business.

Communication through ICT must always be professional.

- Emails and online messages must be respectful and proof-read before sending.
- Abusive or unprofessional communication will not be tolerated.

- Email is not a substitute for face-to-face communication unless circumstances make this unavoidable.
- Email and online communication are legally binding; no contractual obligations may be made on behalf of the Trust by email or internet without authorisation.
- Confidential information may only be shared with authorised recipients and must be protected appropriately.
- The Trust's standard confidentiality notice must be included in external emails and must not be removed.
- School email addresses must not be used for personal subscriptions or marketing or shared with third parties unless assured they will not be misused.
- Phishing or suspicious emails must be reported using the "Report Phishing" button in Outlook. Staff can refer to the user guide if needed. If the button cannot be used, the email must be reported immediately to the Head of School and the IT Services Provider as a fallback.
- Spam, chain emails and junk messages must be deleted without being opened or forwarded.

Security and system integrity must not be compromised.

- Security controls, filtering systems and monitoring may not be bypassed or disabled.
- Unapproved software, applications, plug-ins or browser extensions may not be installed.
- Only Trust-approved systems and applications may be used for storing or transferring information.
- Trust data must not be copied into unapproved personal applications or cloud services.
- User accounts must remain secure. Passwords are confidential and must never be shared.
- Accounts may not be used by anyone other than the authorised individual.
- Devices must be locked when unattended.

Use of ICT devices must respect privacy and safeguarding requirements.

- Images or recordings of pupils, staff or parents may only be taken or shared on Trust devices with the necessary consent.
- Communication with pupils or parents via personal devices, personal email or social media is not permitted unless specifically approved by the Chief Executive Officer (CEO).

Use of ICT systems must always remain lawful and appropriate.

- Accessing, creating, storing or sharing material that is illegal, pornographic, discriminatory, threatening or harmful is prohibited.
- Harassment, bullying, abuse or exploitation via ICT systems is not permitted.
- Chain letters, scams, impersonation, falsifying information or forging email headers are also prohibited.
- Copyright and intellectual property rights must be respected. Copyrighted material will not be downloaded, used on the Schools/Trust website, or distributed without permission.
- Unauthorised scanning, monitoring, hacking or distribution of malware, viruses, ransomware or other malicious code is strictly prohibited.
- ICT facilities may not be used for personal commercial or financial gain.
- Accessing gambling, auctions, chat lines, or inappropriate websites is not permitted.
- Trust ICT resources must not be used for premium or international calls without authorisation.

The Trust will maintain internet filtering in line with Department for Education (DfE) requirements to protect staff and pupils from inappropriate and harmful online content. Filtering controls must not be bypassed or disabled. These measures also support the statutory obligations set out in Keeping Children Safe in Education (KCSiE), ensuring that appropriate monitoring and filtering systems are in place to safeguard pupils and staff online.

Inappropriate use of Trust-owned or personal devices may lead to breaches of the Trust's Data Protection Policy and legislation, including UK GDPR and the Data Protection Act 2018. Staff found to be in breach may face disciplinary action in line with AHMAT procedures.

Bring Your Own Device

The use of personal devices for Trust purposes is only permitted where explicit approval has been granted by the Head of School, in consultation with the Chief Executive Officer (CEO). Any personal device used for Trust business must meet security requirements before it can connect to Trust systems.

- All personal devices intended for work purposes must be declared and approved before use.
- Approved devices are subject to routine security checks to confirm that appropriate security measures and software updates are installed.
- A Device User Agreement is required, confirming acceptance of these checks and the potential risk that personal information may be visible during inspections.
- Devices cannot be used if consent to this process is refused.

Personal devices must be secured to the same standard as Trust devices.

- Devices must be protected with a strong password or biometric lock.
- Devices must be encrypted.
- Multi-factor authentication must be enabled wherever supported.
- Operating systems and applications must be kept fully up to date.
- Trust-approved security software must be installed.

Trust data must only ever be stored or transferred through approved systems.

- Only Trust-approved applications and services may be used for storing, processing or communicating Trust data.
- Personal applications or unapproved cloud services must not be used.
- Sensitive or confidential data must not be stored on personal devices unless encrypted and specifically authorised.

The use of personal devices in relation to staff, pupils and parents is tightly controlled.

- Personal devices must not be used to contact pupils or parents, including via messaging, personal email or social media, unless Chief Executive Officer (CEO) approval has been given.
- Personal devices may not be used during lesson times unless directly required for teaching purposes.
- Devices used within the school network must not contain inappropriate or illegal content.

Lost or stolen devices used for Trust purposes must be reported immediately.

- The Trust reserves the right to remotely wipe Trust data from lost or stolen personal devices to protect confidentiality.

Images and recordings must never be taken or stored on personal devices.

- All images or recordings for Trust purposes must only be captured, stored and shared using Trust-owned devices in accordance with Trust policies.
- Inappropriate messages or communications through personal devices are strictly prohibited.

Password Policy

Passwords provide essential protection for Trust systems, data and devices. Strong, unique passwords are required for all accounts to reduce the risk of unauthorised access.

- Each Trust account must have its own unique password, and passwords may not be reused across personal and professional accounts.
- Passwords must be created using either the three random words approach (e.g. green-bottle-road) or secure passphrases.
- Passwords must meet system requirements, including at least eight characters and at least three of the four character types: uppercase, lowercase, numbers and symbols.
- Where possible, passphrases of 14 characters or more should be used to provide stronger protection.

Passwords must never be predictable or easy to guess.

- They must not include personal information such as names, birthdays, addresses or hobbies.
- Common or predictable sequences such as 12345, qwerty, or password1 must not be used.
- Obvious substitutions such as P@ssw0rd are not acceptable.

Passwords must always remain confidential.

- They must never be shared with anyone else.
- They must not be written down in insecure locations or included in emails, messages or documents.
- A Trust-approved password manager may be used where necessary to store passwords securely.
- Devices must be locked when unattended, and accounts must be logged out after use.
- Use of another person's account is not permitted under any circumstances.
- Accounts and login credentials must never be shared, and authentication or security controls must not be bypassed.

Multi-Factor Authentication (MFA) is required for all accounts wherever supported.

- MFA is mandatory for all users and must be applied unless there is a genuine technical limitation, in which case the IT Services Provider will put in place additional security measures.

Passwords must be changed immediately if compromise is suspected or on instruction from the IT Services Provider.

- Routine periodic password changes are not required unless a security risk has been identified.

- Any suspicion of compromised passwords must be reported immediately to the Head of School and IT Services Provider.

Password Construction Guidelines

Strong passwords are essential to the security of Trust systems and data. They must be easy to remember but difficult for others to guess.

- The recommended approach is to use the three random words method, for example green-bottle-road.
- Passwords must contain at least eight characters and include a mix of uppercase, lowercase, numbers and symbols.
- Where possible, passphrases of 14 characters or more should be used for stronger protection.

Passwords must never be weak or predictable.

- They must not include personal details such as names, birthdays, addresses or hobbies.
- Common or predictable sequences such as 12345, qwerty, or password1 must not be used.
- Obvious substitutions such as P@ssw0rd are not acceptable.

Each account must always have its own unique password.

- Reuse of the same password across multiple accounts is not permitted.

Passwords must always remain secure.

- They must not be written down in insecure places.
- They must not be shared by email, messaging or documents.
- Where needed, a Trust-approved password manager may be used to store passwords securely.

Access Control

Access to Trust systems, applications and data is carefully managed to ensure that only authorised individuals can use them, in line with the principles of least privilege, role-based access and need-to-know.

- User accounts are created only with approval from the Head of School, Chief Executive Officer (CEO) and the IT Services Provider.

- Access rights are based on job role and responsibilities, and privileges are restricted to the minimum level necessary to carry out duties.
- Critical tasks require multiple levels of approval.

Accounts are regularly reviewed to make sure access remains appropriate.

- Changes in role or responsibilities require a reassessment of access rights.
- Accounts that remain inactive for extended periods will be disabled.
- Access is removed immediately when a user leaves the Trust.

All system access must be unique and secure.

- Unique user IDs are required for all system access.
- Shared accounts are not permitted.
- Administrative or privileged accounts are strictly limited and closely monitored.

Multi-Factor Authentication (MFA) is required for all Trust accounts and systems wherever it is supported.

Personal devices may only be used to access Trust systems in line with the Bring Your Own Device (BYOD) Policy.

Access for external vendors or third parties is tightly controlled.

- Vendor or third-party access to Trust systems is only granted where necessary.
- Such access must be time-limited and is subject to monitoring.

Access logs are kept for audit purposes and are subject to regular review.

Anti-Malware

The Trust is committed to protecting its systems and data from malware, including viruses, ransomware, spyware, trojans and other malicious code. Malware infections can cause disruption, data breaches, financial loss and reputational harm, so strict precautions must be followed.

- All Trust-owned devices, and any approved personal devices, must run Trust-approved anti-malware and antivirus software.
- This software must remain active and always updated.
- Operating system and application updates must be installed promptly when released.

Files, applications and software must only come from safe sources.

- Downloads are permitted only from approved and trusted sources.

- Downloads from unknown or suspicious websites are prohibited.
- Mobile applications may only be installed from official app stores.

Suspicious messages must be handled with care.

- Spam, junk mail and chain emails must be deleted without being opened or forwarded.
- Attachments or links in emails from unknown or suspicious sources must never be opened.
- Phishing or suspicious emails must be reported using the “Report Phishing” button in Outlook. Staff can refer to the user guide if needed. If the button cannot be used, the email must be reported immediately to the Head of School and the IT Services Provider as a fallback.
- Malware protection measures must never be tampered with.
- Malware protection systems must not be bypassed, disabled or overridden.
- Any suspected infection, unusual device behaviour or potential compromise must be reported immediately to the Head of School and the IT Services Provider.

The Trust will maintain technical measures to keep systems safe.

- Email filtering and mail security technology will be used to detect and block malware, phishing attempts and spam.
- Anti-virus and malware protection software will be deployed and updated regularly across all approved devices.
- Routine checks will be carried out by the IT Services Provider to confirm compliance.

Remote Working

Remote working is permitted where required, but it must never expose Trust systems, devices or data to unauthorised access or compromise.

- Trust devices are the default for remote working.
- Personal devices may only be used where explicit approval has been granted in line with the Bring Your Own Device (BYOD) Policy.
- Approval from the Head of School, in consultation with the Chief Executive Officer (CEO), is required before Trust devices are taken home for work purposes or for use on school trips or visits.

Portable devices must always be kept secure.

- Devices must not be left unattended in public places.

- Devices must be locked away when not in use.
- Where protective cases are provided, these must be used.
- Devices must not be used by non-Trust staff, family members or pupils.

All mobile devices used for Trust work must be protected.

- Devices must be encrypted.
- Devices must be secured with strong passwords or biometric access controls.
- Devices must auto-lock after no more than five minutes of inactivity.
- Trust data stored locally must be removed after ten working days if it is no longer required.

Sensitive data must only be stored or accessed through approved systems.

- Trust databases or sensitive data may not be downloaded or stored locally unless written approval has been granted.
- All work must be saved to approved Trust systems such as Microsoft 365.
- Local copies must be removed once synchronised.

Safe practices must be followed when working off-site.

- Public Wi-Fi should be avoided wherever possible.
- Where public Wi-Fi must be used, a connection through the Trust VPN is required.
- Work must be conducted in environments where screens cannot be overlooked.
- Privacy filters should be used if necessary.

Any incident affecting remote working security must be reported immediately.

- Lost or stolen devices, unauthorised access, or suspected compromise must be reported at once to the Head of School, Chief Executive Officer (CEO), and the IT Services Provider.

Removable Media

The use of removable media presents a significant security risk, including the potential spread of malware and the loss of confidential information.

- Removable media such as USB drives, external hard drives, CDs, DVDs and SD cards are not permitted for use with Trust-owned devices.
- Technical controls are in place to block the use of removable media, and any attempt to bypass or override these restrictions is prohibited.

- Approved Trust systems, including secure cloud storage and collaboration platforms, must be used for all data transfer and storage needs.

Physical Security

The physical protection of ICT assets and confidential information is essential to maintaining security and safeguarding Trust data.

- Trust devices must not be left unattended in public places.
- Laptops, tablets and phones must be locked away when not in use and secured overnight in appropriate storage.
- Devices must not be left in vehicles.
- Screens must be locked when unattended, even for short periods.

Confidential paper records must always be kept secure.

- Records must be stored in locked cabinets.
- Work areas must be kept clear of sensitive information when unattended.
- Confidential waste must be disposed of using shredding or approved confidential disposal methods.

Only authorised people may access Trust ICT systems and information.

- Unauthorised persons, including visitors, pupils, family members or contractors, must not be allowed to use or access Trust devices, systems or confidential information.

Secure areas must remain protected.

- Access to areas such as server rooms or network cupboards is restricted to authorised staff only.
- Doors to these areas must remain locked when not in use.

Any loss or theft must be reported immediately.

- Devices, ID cards, access passes or keys that are lost or stolen must be reported without delay to the Head of School, Chief Executive Officer (CEO) and the IT Services Provider.

The Trust will provide appropriate secure storage for devices and paper records and will maintain access control measures to protect ICT assets.

Message and Records Retention

Emails and digital communications must be managed responsibly. Messages stored on Trust devices or systems will be retained for no longer than twelve months unless they are required for ongoing business or safeguarding purposes.

Where there is uncertainty about the correct procedure for storing or disposing of messages, guidance must be sought from the Head of School or Chief Executive Officer (CEO).

Complaints relating to inappropriate communications will be addressed in line with the Trust's Complaints and Grievance procedures.

Device Loaning

Trust equipment, including laptops, tablets and other electronic devices, will only be issued where necessary for the performance of duties. Devices will not normally be loaned for personal or non-essential purposes.

All Trust equipment and accessories must be returned when requested or when employment ends.

ICT Procurement and Asset Management

ICT equipment and infrastructure will be procured and managed under the oversight of the Chief Executive Officer (CEO) and the Board of Trustees. Only the Chief Executive Officer (CEO) and Board of Trustees are authorised to approve ICT purchasing decisions.

The Trust Business Manager will maintain a Fixed Asset Register to record all ICT assets purchased with Trust funds. Equipment will be sourced from reputable suppliers, considering value for money, security and safeguarding requirements.

Devices that are no longer fit for purpose, or have reached end of life, will be securely wiped or disposed of in line with the Trust's IT Asset Disposal Policy.

Loss, Theft and Damage

For the purpose of this policy, **"damage"** is defined as any fault in a Trust-owned electronic device caused by the following:

- Connections with other devices, e.g. connecting to printers which are not approved by the IT Services Provider
- Unreasonable use of force
- Abuse
- Neglect
- Alterations

- Improper installation

The Trust's insurance will cover part of the cost of Trust-owned electronic devices that are damaged or lost during school hours if they are being used on the school premises.

- Staff must use Trust-owned electronic devices within the parameters of the Trust's insurance cover.
- If a Trust-owned device is damaged or lost outside of school hours and/or off-site, the member of staff at fault may be responsible for paying damages.
- Any incident that leads to a Trust-owned device being lost will be treated in the same way as damage.

The Chief Executive Officer (CEO) will decide whether a device has been damaged due to the actions described above.

- The IT Services Provider will be contacted if a Trust-owned device has a technical fault.
- If it is decided that a member of staff is liable for the damage, they will be required to pay 20 percent of the total repair or replacement cost.
- A written request for payment will be submitted to the member of staff who is liable to pay for damages.

Staff have the right to appeal decisions.

- If a member of staff believes the request is unfair, they may appeal to the Chief Executive Officer (CEO).
- The Chief Executive Officer (CEO) will make a final decision within two weeks.

Where the Chief Executive Officer (CEO) decides it is fair to seek payment:

- The member of staff will be required to make the payment within six weeks of receiving the request.
- Payments will be made to the Trust Business Manager (TBM) via the Trust office, and a receipt will be given.
- The Trust will accept payments by credit or debit card, cheque or cash.
- A record of the payment will be stored in the Trust office for future reference.
- The Chief Executive Officer (CEO) may allow payments to be made in instalments.

If the payment is not made within six weeks:

- The fee will increase by five percent and continue to increase for a maximum of six months.
- At that point, formal disciplinary procedures will begin.

- The member of staff will not be permitted to access school-owned devices until the payment has been made.

In cases of repeated damage:

- The Chief Executive Officer (CEO) may decide to permanently exclude the member of staff from accessing Trust-owned devices.

If a Trust-owned device is lost or stolen, or suspected to have been lost or stolen:

- The Data Protection Officer (DPO), IT Services Provider and Chief Executive Officer (CEO) must be informed as soon as possible.
- Steps will be taken to delete data from the device relating to the school, staff and pupils.
- The loss will be reported to the relevant agencies.

The Trust will not be responsible for the loss, damage or theft of any personal device, including phones, cameras, tablets, removable media or similar items.

Implementation

Any breach of this policy must be reported immediately to the Head of School, Chief Executive Officer (CEO) and Data Protection Officer (DPO).

- Email, internet and telephone use are subject to monitoring.
- Records may be retained for compliance or disciplinary purposes.
- Internet activity is logged, and suspicious or inappropriate use may lead to further investigation.

The Trust monitors ICT usage through a range of measures.

- Asset checks, system logging and remote administration are used to ensure compliance.
- The Trust Business Manager (TBM) will conduct random checks of asset-registered and security-marked items.
- Access to Trust systems is logged for audit and security purposes.
- Key events such as installations or configuration changes may also be recorded.
- The IT Services Provider, under the oversight of the Chief Executive Officer (CEO), may remotely view or interact with Trust devices for security, monitoring and support.

The Trust maintains centrally managed protection and controls.

- Centrally managed malware protection is in place across the network and devices, with detections logged and investigated.

- Access to Trust databases and systems is restricted to authorised users.
- All users are issued with a unique account and secure password, in line with the Trust's Password Policy.
- Use of another person's account or credentials is prohibited and may result in disciplinary action.
- User accounts are administered by the IT Services Provider under the oversight of the Chief Executive Officer (CEO) and Senior Leadership Team (SLT).
- Accounts may only be accessed or managed by authorised administrators for security, monitoring and support purposes.

All critical data must be stored securely.

- Data must be stored within the Trust's approved cloud repositories, such as OneDrive and SharePoint.
- These systems are protected through a secure cloud-to-cloud backup service to ensure availability and recoverability.
- Storing critical information solely on local devices or outside of approved systems is not permitted.

Users are required to familiarise themselves with relevant legislation.

- This includes the UK GDPR and the Data Protection Act 2018.
- Staff must ensure that they operate in accordance with these regulations and the Trust's Data Protection Policy.

Any breach of this policy may result in disciplinary action.

- This may include dismissal in serious cases.
- Misuse may also result in civil or criminal action against the individuals involved or the Trust.

Monitoring and Review

This policy will be reviewed annually by the Chief Executive Officer (CEO), Head of Schools and Data Protection Officer (DPO), in consultation with the IT Services Provider.

Any changes or amendments to this policy will be communicated to all staff members by the Trust Business Manager.

AHMAT ICT & Electronic Devices Policy	
First Edition:	1st September 2025

Version:	1
Updated on:	N/A
Updated by:	Isabel Cooke, CEO
Next Review:	September 2026
Review September 2026	