

Acceptable Use Policy (Staff)

1 Introduction

1.1 All members of staff have a responsibility to use the devices, networks and systems supplied by the Heart of Mercia Trust and its academies in a professional, lawful, and ethical manner.

This is a Trust-wide policy and applies in all academies operated by the Heart of Mercia Multi-Academy Trust. It replaces any previous academy-level Acceptable Use Policy applying to staff, governors, volunteers, contractors or other persons within its scope.

To ensure all members of staff within the Trust are fully aware of their responsibilities, they are asked to read this Acceptable Use Policy.

1.2 Relevant Legislation

This policy takes into consideration the following legislation and guidance:

- The latest Keeping Children Safe in Education Guidance
- Counter Terrorism and Security Act (2015) and Prevent Duty guidance
- UK General Data Protection Regulation and Data Protection Act 2018
- Computer Misuse Act (1990)
- Malicious Communications Act (1998)
- Freedom of Information Act (2000) and Environmental Information Regulations (2004)
- Online Safety Act (2023)

2 Scope

2.1 This Acceptable Use Policy applies to any individual that carries out an employee-like role in all Trust. academies This includes all contracted employees and the following groups:

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

The policy governs the use of Trust-owned, leased or managed: devices, networks, systems, applications and digital services, including email, internet access, cloud-based services and learning platforms. It also applies to personally owned devices when they are used to access Trust or Academy systems, data, accounts, applications or services, or when connected to Trust-managed networks, including Wi-Fi.

Author(s)	Date Authored	Date agreed	LGBs	MAT Board	Review date
Chief Data & Technology Officer and Data Protection Officer	September 2026	October 2026	Autumn 2026	October 2026	September 2027

All staff should be aware that the Trust reserves the right to monitor, record and audit any activity conducted within or via Trust-managed devices, networks, systems and digital services for safeguarding, security, operational, legal and regulatory purposes. This includes the use of Trust data, accounts, applications, services or networks, including any connection to Trust-managed Wi-Fi, from personally owned devices.

This policy operates alongside the Trust Staff Code of Conduct and forms part of the standards of professional conduct expected of all staff and other persons within its scope. Where an incident also raises a safeguarding, data-protection, information-security or professional-conduct concern, the relevant Trust policy and procedure will apply.

3 Acceptable Use Statements

Technology, digital services and associated legislation evolve rapidly. All staff are expected to ensure that their use of the Trust's devices, networks and systems remain consistent with the Trust's values and ethos, policies and procedures, relevant national and local guidance, and all applicable legal and regulatory requirements.

By using any Trust-managed device, network, or digital system, staff acknowledge and accept the following statements:

3.1 Trust-Managed and Trust-Issued Devices

- I understand I have a duty to take reasonable care of Trust devices I use (such as those in classrooms) and/or those that have been issued to me on a 1-to-1 basis.
- I understand that any hardware and software provided by my Academy for staff use can only be used by members of staff and only for Academy or Trust use.
- To prevent unauthorised access to systems or personal data, I will not leave any device unattended without first logging out or locking my login as appropriate.
- I will take reasonable steps to protect the devices in my care from unapproved access or theft.
- I understand that I may be responsible for repair/replacement costs associated with any intentional damage to devices, or where reasonable care has not been taken to prevent the theft or accidental damage of devices. I understand that any Trust-issued device must be returned to the relevant IT team at the end of my employment/involvement with the Trust.
- If requested, I agree to promptly present any Trust-issued device to the relevant IT team for maintenance or to comply with Trust policies or fulfil legal obligations.
- I understand that to comply with Trust policies or to fulfil legal obligations any Trust-managed device may be remotely accessed, modified or disabled without notice.

3.2 Software, Cloud Platforms and AI

- I will not attempt to install any purchased or downloaded software, including browser toolbars and extensions, or hardware without agreement from the IT Manager at my Academy.

Author(s)	Date Authored	Date agreed	LGBs	MAT Board	Review date
Chief Data & Technology Officer and Data Protection Officer	September 2026	October 2026	Autumn 2026	October 2026	September 2027

- I agree to seek and obtain approval through the Trust's Technology Adoption Group (TAG) before adopting, accessing, or providing Academy or Trust data to any new software, platform, application, AI application or website, or third-party service.
- I agree not to register for or use any cloud platform, application, or online service for Academy or Trust purposes, nor upload, store, share, or process Academy or Trust data within it, unless approval has first been obtained.
- I agree that I will not register for, trial, procure, or use any cloud-based platform, application, or service for Trust business until approval has been granted.
- I will only use approved AI tools (e.g. Copilot and Topmarks). I will use them responsibly and in accordance with the Trust's AI Policy and Guidance.
- I agree to never input learner work/intellectual property, learner or staff personal data, Academy or Trust commercially sensitive data to any AI tool that hasn't been approved by the Trust.
- I agree to be open, transparent and accountable about my use of AI within my Academy or Trust role.
- I understand that I am responsible for critically reviewing and verifying appropriateness, accuracy and suitability of any content I generate with AI in my Academy or Trust role.
- I have read, understood and agree to abide by the Trust's AI Policy which covers the safe and responsible use of AI in the workplace.

3.3 Accounts and Passwords

- I will respect system security and will not disclose any password or security information.
- I will use a 'strong' password to access Trust or Academy systems which will, where possible:
 - Use three random words
 - Contain a digit after one of the words
 - Be at least 14 characters long overall
 - Be unique for each account
- I agree to the use of multi-factor authentication (MFA) where installed to access Academy or Trust systems securely.
- I will use my Trust or academy-issued email address to register for any online accounts relating to my role at the Trust.
- I understand that access to all accounts, including my email, will be withdrawn at the end of my employment/involvement with the Trust.

3.4 Personal Devices & BYOD

- I will wherever possible, opt to use a Trust managed device to access Academy or Trust systems and data.
- Where there is a need to use a personal device to access Academy or Trust systems, I will ensure that:
 - I personally own the device.

Author(s)	Date Authored	Date agreed	LGBs	MAT Board	Review date
Chief Data & Technology Officer and Data Protection Officer	September 2026	October 2026	Autumn 2026	October 2026	September 2027

- The device complies with all applicable requirements of the Cyber Security, as published on cyber.heartofmercia.org.uk.
- If the device is routinely shared with others, I will log out of all Trust systems after each use.
- I will not store Academy or Trust data on personal devices, including (but not limited to) mobile phones, digital cameras and home computers. The exception is data used by Trust-managed apps on personal devices that have been enrolled using the Academy Intune Company Portal e.g. Outlook and Teams. Allowed exceptions are the use of your own mobile device for multi-factor authentication and access to information/systems in emergency situations.
- If I access Academy or Trust systems on a personal device, I will ensure the device:
 - is supported and receives security updates;
 - is configured to install updates automatically where possible;
 - is protected by appropriate authentication measures (for example, a strong passphrase, PIN or biometric authentication);
 - is protected by firewall and anti-malware software;
 - is free from unauthorised, unsupported, rooted or jailbroken software; and
 - complies with all requirements set out in the Trust's Cyber Security Toolkit <https://cyber.heartofmercia.org.uk/#yourdevice>
- I agree, upon request, to provide details of any personal device I use to access Academy or Trust systems.
- I agree, upon request, to provide written confirmation that any personal device I use to access Academy or Trust systems complies with the requirements outlined above.

3.5 Conduct, Communications & Online Safety

- All communication relating to Trust/Academy matters, including all communication with learners, parents and applicants will take place via Trust approved communication channels, such as a Trust-provided email address or telephone number, and not via personal communication channels, such as personal email, social networking accounts or mobile phone calls/messages.
- I will not use personal accounts on communication platforms including social media (WhatsApp, Facebook etc.) and email for discussing Academy or Trust matters. I will instead use Trust-issued or authorised accounts setup specifically for a business purpose.
- My electronic communications with current or past learners, parents/carers and other professionals will take place within clear and explicit professional boundaries and will be transparent and open to scrutiny.
- Any pre-existing relationships or situations that may compromise this will be discussed with the Designated Safeguarding Lead and/or Principal/Head Teacher.
- I have read and understood my Academy's Online Safety (or equivalent) policy which covers the requirements for safe IT use, including using appropriate devices, safe use

Author(s)	Date Authored	Date agreed	LGBs	MAT Board	Review date
Chief Data & Technology Officer and Data Protection Officer	September 2026	October 2026	Autumn 2026	October 2026	September 2027

of social media and the supervision of learners within the classroom and other working spaces.

- I will ensure that my online reputation and use of IT and information systems are compatible with my professional role, whether using Trust or personal systems. This includes the use of email, text, social media, social networking, gaming and any other devices or websites.
- I will take appropriate steps to protect myself online as outlined in my Academy's Online Safety (or equivalent) policy and will ensure that my use of IT and the internet will not undermine my professional role, interfere with my work duties and will be in accordance with the Trust Staff Code of Conduct and the law.
- If I have any queries or questions regarding safe and professional conduct online either in my Academy or off-site, I will discuss them with my line manager, the Designated Safeguarding Lead or the Principal/Head Teacher.
- I will not create, transmit, display, publish or forward any material online that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role or the Trust into disrepute. This includes, but is not limited to, explicit and illicit material, 'fake news', hoaxes and misinformation, prejudice, violent or distressing content, promotion of self-harm, suicide and eating disorders or edited or altered pictures and videos.
- I will immediately report any illegal, inappropriate or harmful material or incidents related to learners or staff, for any Academy or the Trust, that I become aware of, to the Designated Safeguarding Lead.
- I will promote online safety and responsible use of AI with the learners in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.

3.6 Personal Use

- I understand that the Trust advises against the use of any of its devices or systems for personal activity unrelated to Trust activities.
- I understand that any personal activity conducted on Trust devices or systems will be subject to monitoring, logging and audit – including web browsing and communications.
- I will not store any personal information on the Trust devices or systems that is unrelated to Academy or Trust activities, such as personal photographs, files, emails or financial information.
- I understand that the privacy of any personal information entered or accessed on Trust devices cannot be guaranteed and may be accessible within relevant monitoring and compliance tools.
- I understand that any data stored or logged in Trust systems, may turn up in a search and be seen by staff investigating an incident and in certain circumstances may have to be released e.g. as a result of a Subject Access Request (SAR).

Author(s)	Date Authored	Date agreed	LGBs	MAT Board	Review date
Chief Data & Technology Officer and Data Protection Officer	September 2026	October 2026	Autumn 2026	October 2026	September 2027

3.7 Security, Data Protection, Monitoring & Compliance

- I understand that the Computer Misuse Act 1990 makes the following criminal offences:
 - to gain unauthorised access to computer material;
 - to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.
- I will ensure that personal data of learners, staff or parents/carers is kept in accordance with the Data Protection Act 2018 (including UK GDPR). This means that all personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online or accessed remotely.
- I will respect copyright and intellectual property rights and understand that work produced in the course of my duties remains the property of the Trust, unless otherwise agreed by the relevant Principal or Head Teacher.
- I will not attempt to bypass any filtering and/or security systems put in place by the Trust or Academy.
- I will report any suspected cyber-security incident, personal-data breach, loss or theft of a device, compromised account, suspicious message, unauthorised disclosure, inappropriate online content or other digital safeguarding concern immediately through the Trust or academy's designated reporting route. I will not delay reporting while attempting to investigate or resolve the matter myself. Where the matter concerns a learner or creates a safeguarding risk, I will also notify the Designated Safeguarding Lead without delay.
- I understand that my use of any Academy or Trust's information systems, including any trust-issued devices, internet access and email, may be monitored, filtered and recorded to ensure the safety of learners and staff and to ensure policy or legal compliance. This monitoring will be proportionate and undertaken lawfully, fairly and transparently, in accordance with applicable data-protection, privacy and human rights legislation, and all relevant Trust policies.
- I understand that the Trust may exercise its right to monitor the use of information systems and CCTV, including internet access and the interception of emails, to monitor policy compliance. Where it believes unauthorised and/or inappropriate use, or unacceptable or inappropriate behaviour may be taking place, the Trust may invoke its disciplinary procedures. If the Trust suspects criminal offences have occurred, the matter will be brought to the attention of the relevant law enforcement organisation.
- I understand I should have no expectation of total privacy when using Trust-owned or Trust-managed devices, systems, networks, applications, email services, internet access, cloud services, or other digital resources.
- The Trust reserves the right to access, monitor, record, review, analyse and retain any communications, activity, data, files, logs, searches, and messages within its devices or systems.

Author(s)	Date Authored	Date agreed	LGBs	MAT Board	Review date
Chief Data & Technology Officer and Data Protection Officer	September 2026	October 2026	Autumn 2026	October 2026	September 2027

- I am aware such information may be accessed and used for legitimate business, safeguarding, security, regulatory, legal, disciplinary, audit, data protection or operational purposes. This may include investigations into suspected breaches of Trust policies, misconduct, safeguarding concerns, security incidents, complaints, legal proceedings, Subject Access Requests (SARs), Freedom of Information requests (Fol), disclosure obligations and other statutory requirements.
- This monitoring and review extends to all forms of digital communication and interactions undertaken whilst using Trust or Academy resources, including but not limited to email, messaging services, collaboration platforms, internet activity, cloud-based services, uploaded or stored content and any use of AI.
- I understand the Trust has a duty to allow UK law enforcement agencies to access data stored and/or created on the Trust's devices, network and systems where a warrant/request is properly executed in relation to an investigation.
- I understand that I will receive compulsory annual training relating to cyber security and data protection.
- I understand that any breach or failure to adhere to the terms of this policy may be considered as a disciplinary matter dealt with under the relevant Trust disciplinary procedures.

4 Related Policies and Procedures

- Academy Online Safety Policies
- Academy Acceptable Use Policy for Learners / Guests
- Heart of Mercia Staff Anti-Bullying and Harassment Policy
- Heart of Mercia Safeguarding and Child Protection Policy
- Heart of Mercia Staff Code of Conduct
- Heart of Mercia AI Policy
- Heart of Mercia Data Protection Policy
- Heart of Mercia Data Retention Policy
- Heart of Mercia Information Security Policy

5 Equality Impact

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

Author(s)	Date Authored	Date agreed	LGBs	MAT Board	Review date
Chief Data & Technology Officer and Data Protection Officer	September 2026	October 2026	Autumn 2026	October 2026	September 2027