Acceptable Use of IT Policy

Author	**Director of IT**
Date of issue	03/12/2024
Date ratified	12/11/2025
Date for review	Autumn Term 2025

DOCUMENT CONTROL

Unless there are legislative or regulatory changes in the interim, this policy will be reviewed annually. Should no substantive changes be required at that point, the policy will move to the next review cycle.

Version	Date	Changes
1.0	06/2022	• Reviewed and updated to ensure policy reflects current IT best practice
1.1	06/2023	• Reviewed and updated to include generative AI Guidance
1.2	09/2024	• Transferred to new template
1.3	11/2024	• Updated to include Student Guidance. One AUP now covers staff, pupils, governors and trustees
1.4	11/25	• Updated references for post-centralisation

Contents

1. Introduction

1.1. IT is an integral part of the way our schools work, and is a critical resource for pupils, staff, governors, volunteers and visitors. It supports teaching and learning, pastoral and administrative functions of our trust.

1.2. However, the IT resources and facilities our schools use, also pose risks to data protection, online safety and safeguarding.

2. Purpose

2.1. The purpose of this policy is to advise all those individuals described under 'Scope' on the effective, safe, and productive use of IT systems across Mercia Learning Trust ("our trust").

2.2. The policy is designed to be a succinct as possible whilst remaining comprehensive and relevant.

2.3. Updates to this policy will be made to ensure the guidance and requirements remain up to date and are adjusted to the changing needs of our trust and the developments in technology and cyber security.

2.4. Although our trust has a duty to implement this policy and inform employees about this policy, it is the responsibility of all students, employees, volunteers, governors and other third parties to take personal responsibility by ensuring:

- 2.4.1. they read and understand the policy.
- 2.4.2. familiarise themselves with the requirements of the policy.
- 2.4.3. ensure compliance with the policy.
- 2.4.4. where they are unsure or unclear about any aspect of the policy, take appropriate steps to discuss such concerns with their headteacher.

2.5. Individuals are advised to speak to any member of our trust IT Services if they are unsure of any aspects of this policy.

2.6. The policy and statements are designed to ensure employees in our trust are aware of their professional responsibilities when using the IT systems provided. All individuals covered by this policy should always follow these guidelines.

2.7. All individuals are responsible for their own behaviour and actions when accessing the internet at work, whether on their own device or using trust equipment, and when using trust IT equipment at other locations such as home.

3. Scope

3.1. This policy applies to all pupils, employees, volunteers, casual, temporary, agency staff, contractors, governors, trustees and other third parties regarding the use of IT.

3.2. The policy covers the use of all IT systems managed or controlled by our trust, including but not limited to, Windows and macOS network devices, school MIS systems, remote access systems and communication platforms.

3.3. It is the responsibility of each employee to read and understand the requirements and expectations set out within this policy. It will not be regarded as a legitimate defence in any subsequent disciplinary investigation that individuals did not read or understand the requirements of the policy. Any breaches of this policy could result in disciplinary action being taken up to and including dismissal.

4. Legislation and Guidance

4.1. This policy refers to, and complies with, the following legislation and guidance:

- 4.1.1. Data Protection Act 2018
- 4.1.2. The General Data Protection Regulation
- 4.1.3. Computer Misuse Act 1990
- 4.1.4. Keeping children safe in education - GOV.UK (www.gov.uk)
- 4.1.5. Searching, screening and confiscation: advice for schools
- 4.1.6. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- 4.1.7. Human Rights Act 1998
- 4.1.8. Education Act 2011
- 4.1.9. Freedom of Information Act 2000
- 4.1.10. The Education and Inspections Act 2006

5. Definitions

5.1. The following terms are used throughout this policy:

MLT IT Services	The collective term for the IT support team and services offered to all our trust schools and offices
IT Systems	Any digital system owned and/or managed by IT Services on behalf of our trust and its schools. This includes hardware and software purchased by our trust and managed by IT Services
Users/User	Any individual with an account on any IT system owned and/or managed by IT Services on behalf of our trust and its schools
IT Services Portal	The online portal provided by IT Services to provide support to users of IT Systems
Bring your own device (BYOD)	The ability to connect a personal device to a school or trust owned internet connection
Remote Desktop	A remote connection to on-site IT systems often used to access onsite files and folders
MIS	The Bromcom MIS platform used across all our trust schools

6. Trust IT Services

6.1. MLT IT Services provide a centralised IT support programme across all our schools and offices in our trust.

6.2. The MLT IT Services team operate onsite IT support at all secondary schools and provide IT support visits to all primary schools and office locations.

6.3. MLT IT Services provide a centralised helpdesk to allow individuals to get help with IT related issues. Individuals requesting support can log a request by logging in to the IT Services portal or by emailing ithelpdesk@merciatrust.co.uk.

6.4. Individuals are encouraged to log tickets via email or the IT Services portal rather than in person or via phone.

6.5. MLT IT Services staff may at times be required to access and view data on MLT owned devices, servers and services. This policy grants permission for MLT IT Services employees to access data on any MLT owned and supported device or system for the purpose of use support and troubleshooting.

6.6. MLT IT Services employees should not and must not access data of another user without a business need.

7. Use of IT Systems

7.1. Individuals must only use IT Systems for professional purposes.

7.2. IT systems and services provided by MLT IT Services are designed to support the requirements of our trust and the individual schools within it.

7.3. Employees should not breach any other laws or ethical standards for example never use IT systems/equipment in a false or misleading way, such as claiming to be someone other than yourself or by making misleading statements.

7.4. Users must not search for, download, upload or forward any content that is illegal, or that could be considered offensive by another user. If you accidentally encounter such material, you should report it to MLT IT Services immediately.

7.5. IT systems may be restricted and locked down to prevent damage, cyber-attack or misuse.

7.6. Changes to IT systems will be communicated by IT Services in advance wherever possible. It may sometimes be necessary to make swift changes in response to an incident or outage. In these circumstances, IT Services will endeavour to communicate to users as soon as possible.

7.7. Individuals must not install or reconfigure IT systems without consultation with a Trust Network Manager, IT Service Delivery and Infrastructure Manager or our Director of IT.

7.8. Individuals must ensure that no offensive or inappropriate personal data is stored or accessed on any IT system in scope of this policy.

7.9. User access details are only provided to individuals on the day they start employment or study within our trust.

7.10. Users are prompted to change their login details on first login. Users must ensure they choose a safe and secure password and keep this password safe. Users are advised to use multiple words and include numbers and special characters where possible.

7.11. Users are not permitted to share their login details with anyone else. This includes any other employee of our trust past or present.

7.12. If a user suspects another individual has access to their account, they must report it immediately to IT Services via the IT Services portal.

7.13. Users are permitted to change their own password when logged into a Windows device. Users can do this by pressing Ctrl + Alt + Del and choosing 'change password'.

7.14. Any activity on IT systems owned and operated by our trust may be monitored for appropriate use. This includes but is not limited to activity on Windows and macOS desktops and laptops, mobile devices and personal devices connected to school 'bring your own device' WiFi networks.

7.15. Internet activity on personally owned devices connected to school WiFi is monitored and logged. Users should be aware of any open internet browsing tabs, apps or social media accounts before connecting to school WiFi networks.

7.16. Automated security reports are used to report safeguarding information to school safeguarding leads.

7.17. Any online activity should not harass, harm, offend or insult other users.

7.18. Users must not search for, download, upload or forward any content that is illegal, or that could be considered offensive by another user. If you accidentally encounter such material, you should follow your school's procedure and report this immediately.

8. Generative AI Guidance

8.1. Generative AI (GenAI) is a type of artificial intelligence (AI) that creates new content, such as text, images, videos, music and software code, based on large amounts of generic training data.

8.2. At Mercia Learning Trust, we support the use of AI to reduce workload, support inclusive practice and enhance teaching and learning. However, there are some expectations we expect all users to follow:

8.2.1. AI-generated content can be wrong. Everyone should check all output from AI tools very carefully and never assume it is correct. Individuals are always responsible for making sure any work submitted is accurate and appropriate. It is important not to assume that AI output will necessarily be comparable with a human-designed resource that has been developed in the context of our curriculum.

8.2.2. Whatever tools or resources are used in the production of administrative plans, policies or documents, the quality and content of the final document remains the professional responsibility of the person who produces it and our trust.

8.2.3. AI can be used to trick or offend people. Never use AI to create harmful content and never use AI to pretend to be other people or organisations. Report any worries you have about harmful or inappropriate creations in the same way that you would report anything upsetting online.

8.2.4. AI can reinforce unfair and harmful biases. Be critical of what AI produces – especially for sensitive or cultural topics – and make sure you cross-reference your research and evidence with other reliable sources.

8.2.5. AI tools can store personal information. Do not share any personal information with any AI tool. This includes personal details about yourself or anyone else. Personal information includes your name, age, address, contact details, school name and photos. If you are unsure, do not submit it.

8.2.6. Different AI tools have different age limits. Check the limits carefully before signing up and using them, pupils must have permission from a trusted adult before using any new AI tool.

8.2.7. Sometimes, using AI can be a form of cheating, this is especially relevant for pupils. AI could be a tool to help pupils create work, but it should never be the only tool. Pupils must always be ready to explain which AI tool/s they used, and what prompt/s. A staff member should direct when and how pupils can use AI for school work.

8.2.8. Staff should support pupils to use AI appropriately. AI tools and their proper use should be taught, including communicating the advantages and inherent risks.

8.2.9. Using AI too much can lead to a loss of learning opportunities. Everyone should make sure they are thinking for themselves and not just letting AI tools do the work.

9. Data Protection and Intellectual Property

9.1. Users must not transfer any school data (including but not limited to pupil and employee data) to any personal device for any reason.

9.2. No personal data should be entered into any generative AI tools.

9.3. Every user has access to a secure, personal OneDrive store as well as a range of shared drives, shared OneDrive folders or Microsoft Teams sites specific to their job role.

9.4. Users have access to 1TB of cloud storage through Microsoft OneDrive.

9.5. Users should respect intellectual property and ownership of online resources you use in your professional context and acknowledge such sources if used.

9.6. Our trust holds the rights to data produced by users using our trust IT systems during their employment.

9.7. Our trust is under no obligation to provide users with copies of data stored by the user on any IT system should they no longer be employed by our trust.

9.8. Secure backups are taken each day with weekly, off-site backups taken each week.

9.9. Users are encouraged to use Microsoft OneDrive accounts provided by our trust for storing and sharing files.

9.10. The use of removable USB storage devices is prohibited across all trust owned devices.

9.11. For the purposes of removing data from devices such as cameras and audio recorders, a whitelist of USB devices that are read only is in place. The read only whitelist will be removed during the Christmas and Summer break. Devices needing access will be re-added after each of these school holidays.

9.12. For the purposes of exam coursework, USB devices in read-write mode are allowed on devices not connected to the school network. For devices connected to the school network, only IT Teams are permitted to transfer data to a removable device.

9.13. Removable USB storage devices in read-write mode are removed from the whitelist after 7 days unless specific permission is granted.

9.14. Only trust supplied USB devices are permitted for the purposes outlined above.

9.15. Users are not permitted to use personal cloud accounts for storing data or emails. Including but not limited to personal Microsoft or Google accounts.

9.16. Any still or video images of pupils or employees should be for professional purposes only. They should be taken on school equipment and stored and used onsite. Such images should not be taken offsite without permission and valid reason.

10. IT Security and Safeguarding

10.1. MLT IT Services implements a wide range of IT security systems. Users must adhere to all IT security practices and complete any IT security training as and when required.

10.2. All remote access to trust systems is secured with two factor authentication systems. These systems require an app installed on a smartphone. Users wishing to use IT systems remotely must install and configure the required apps. Support and guidance on this process is available from IT Services.

10.3. Certain software applications may not be installed on IT systems if there is a concern that they do not comply with cyber security requirements.

10.4. Software installations requested by users will undergo a series of checks by IT Services to ensure the software meets security, reliability and licence requirements.

10.5. Emails are the number one security risk. Users must be confident that an email is genuine before opening any attachment. Users are encouraged to speak to IT Services if they are unsure about an email.

10.6. Users must report any suspicious account activity to IT Services as soon as possible.

10.7. IT Services may reset a user account password without warning if they suspect the account has been compromised or is not secure.

10.8. Digital safeguarding is covered in the trust Safeguarding policy.

11. Remote Working/Working from Home

11.1. Users working from home must ensure their workspace is secure. Monitors and data should not be visible through windows.

11.2. If personal devices are used to access trust IT resources, users must ensure that up to date security and antivirus is installed and correctly configured.

11.3. Any smart speaker devices in the same room as the user should have their microphones muted if the user is planning to take video or voice calls.

12. Breaches of Policy

12.1. By agreeing to this policy, employees understand that files, communications and internet activity may be monitored and checked at any time to protect their own and others' safety. Action may be taken if deemed necessary to safeguard the individual or others.

12.2. Disciplinary action may be taken against employees if they:

12.2.1. do not follow all statements in this policy.

12.2.2. commit a criminal offence.

12.2.3. do something that may bring our trust into disrepute, whether within working hours or outside of them.

12.3. Disciplinary action includes the possibility of being dismissed with or without notice.

13. Declaration

13.1. By submitting an acceptance response to the online form associated with this policy employees accept that they have read and understood the policy.