19 – IT ACCEPTABLE USE POLICY

Agreed Summer 2024

Signed by Chair of Trustees

MINSTER TRUST FOR EDUCATION
REVIEW DATE SUMMER 2027

Table of Contents

1. Introduction

This policy aims to:

- Set guidelines and rules on the use of IT resources for staff, pupils, parents and governors;
- Establish clear expectations for the way all members of the school community engage with each other online;
- Support the Trust's policy on data protection, online safety and safeguarding;
- Prevent disruption to the School/Trust through the misuse, or attempted misuse, of ICT systems;
- Support school's in teaching pupils safe and effective internet and ICT use.

This policy covers all users across MITRE's IT facilities, including pupils, Trustees, staff, Governors, volunteers and visitors.

Breaches of this policy may be dealt with under the Minster Trust for Education disciplinary policy (see section 4.2).

2. Relevant Legislation and Guidance

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

- Data Protection Act 2018
- The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020
- Human Rights Act 1998
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Education Act 2011
- Freedom of Information Act 2000
- The Education and Inspections Act 2006
- Keeping Children Safe in Education 2023
- Searching, screening and confiscation: advice for schools 2022
- National Cyber Security Centre (NCSC): Cyber Security for Schools
- Education and Training (Welfare of Children) Act 2021
- UK Council for Internet Safety (et al.) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Meeting digital and technology standards in schools and colleges

3. Definitions

- **"ICT facilities":** includes all facilities, systems and services including but not limited to network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service which may become available in the future which is provided as part of the ICT service.

- **"Users":** anyone authorised by the school to use the ICT facilities.
- **"Personal use":** any use or activity not directly related to the users' employment, study or purpose.
- **"Authorised personnel":** employees authorised by the school to perform systems administration and/or monitoring of the ICT facilities.
- **"Materials":** files and data created using the ICT facilities including but not limited to documents, photographs, audio, video, printed output, web pages, social networking sites, and blogs
- **"Helpdesk":** Minster Trust for Education's method to contact the IT team for raising, tracking and prioritising ICT support queries and any other ICT related queries, accessible via **https://helpdesk.mitretrust.org.uk**, **itsupport@mitretrust.org.uk** or **01636 551133**.
- **"Community":** anyone associated with the Minster Trust for Education (governors, staff, pupils, volunteers, contractors and visitors, across all member school, academies or administrative units).
- **"MITRE":** Minster Trust for Education
- **"Trust":** Minster Trust for Education

4. Unacceptable Use

The following is considered unacceptable use of the ICT facilities by any member of the MITRE community.

Unacceptable use of the ICT facilities includes:

- Using MITRE's IT facilities to breach intellectual property rights or copyright;
- Using MITRE's IT facilities to bully or harass someone else, or to promote unlawful discrimination;
- Breaching the School/Trust policies or procedures;
- Any illegal conduct, or statements which are deemed to be advocating illegal activity;
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate;
- Activity which defames or disparages the school, or risks bringing the Trust into disrepute;
- Inappropriate sharing of confidential information or data about the Trust, its pupils, or other members of the MITRE community;
- Connecting any device to the MITRE's IT network without approval from MITRE's IT team;
- Setting up any software, applications or web services on MITRE's network without approval by authorised personnel, or creating or using any program, tool or item of software designed to interfere with the functioning of the ICT facilities, accounts or data;
- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel;
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's or Trust's ICT facilities;
- Causing intentional damage or defacing (including stickers) ICT equipment and facilities;
- Removing, deleting or disposing of ICT equipment, systems, programs or information without permission by authorised personnel;
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation;
- Engaging in content or conduct that is radicalised, extremist, racist, antisemitic or discriminatory in any other way;

- Using inappropriate or offensive language;
- Promoting a private business, unless that business is directly related to the Trust operations; and you have express permission to do so.
- Using websites or mechanisms to bypass filtering or monitoring mechanisms;
- Using AI tools and generative large language models (such as GPT-3):
    - During assessments, including internal and external assessments, and coursework;
    - To write the homework or assignments, where AI-generated text or imagery is presented as their own work (unless explicitly permitted);
    - When exposing personal, sensitive or intellectual property data or information

This is not an exhaustive list. MITRE reserves the right to amend this list at any time. The CEO, COO or Head of IT will use their professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the school's or Trust's ICT facilities.

4.1 Exceptions from unacceptable use

Where the use of IT facilities is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the CEO, COO or Head of IT's discretion.

In this event a request should be submitted to the IT Services Team (via the IT Services Helpdesk), detailing your situation and wait for further guidance.

4.2 Sanctions

Pupils and staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with the Minster Trust for Educations policies on disciplinary procedures or school behaviour.

Other sanctions include suspension of IT facilities on a temporary or permanent basis.

5. Staff (Including Trustees, Governors, Volunteers and Contractors)

5.1 Access to school ICT facilities and materials

Minster Trust for Educations IT Services Team manages access to the school's and Trust's ICT facilities and materials for staff. That includes, but is not limited to:

- Computers, tablets and other devices;
- Access permissions for certain programmes or files.

Staff will be provided with unique log-in/account information and passwords that they must use when accessing ICT facilities.

Staff who have access to files they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the MITRE's IT Services Team. A request should be raised via the helpdesk (itsupport@mitretrust.org.uk) detailing the access you currently have and the access you require.

5.1.1 Use of Phones and Email

Each member of staff will be provided with an email address.

This email account should be used for work purposes, a limited amount of personal use will be tolerated but any personal use must still adhere to this policy.

All work-related business should be conducted using the email address the school has provided.

Staff must not share their personal email addresses with parents and pupils, and must not send any work-related materials using their personal email account.

Staff must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.

Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.

Staff must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient.

To send an encrypted email within Outlook, select the *Options -> Permissions -> Encrypt-Only* within an email window. Further guidance on how to send an encrypted email can be found in the IT Helpdesk article below.

- Sending encrypted emails using Outlook : MITRE IT Services Portal (helpdesk.mitretrust.org.uk)

If staff receive an email in error, the sender should be informed and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.

If staff send an email in error which contains the personal information of another person, they must inform the assigned Data Protection Officer and Head of IT immediately and follow our data breach procedure.

Staff must not give their personal phone numbers to parents or pupils.

MITRE Issued phones must not be used for personal matters.

MITRE phone systems can record incoming and outgoing phone conversations. Automated announcements have been configured to play at the start of a telephone call which is recorded. We must make callers aware that the conversation is being recorded and why. Where call recorded is enabled, this is for the purpose of safeguarding children and staff.

Staff who are provided with mobile phones as equipment for their role must abide by the same rules for ICT acceptable use as set out in section 4.

The School/Trust have the ability to record in-coming and out-going phone conversations. A given school may record all or select calls for the purpose of aiding administrators and safeguarding.

Staff who would like to record a phone conversation should speak to the IT Services Team to ascertain whether this functionality is available and has been authorised.

All non-standard recordings of phone conversations must be pre-approved, and consent obtained from all parties involved.

5.2 Personal Use

Staff are permitted to occasionally use school ICT facilities for personal use subject to certain conditions set out below. Personal use of ICT facilities must not be overused or abused. The CEO, COO or Head of IT may withdraw permission for it at any time or restrict access at their discretion.

Personal use is permitted provided that such use:

- Does not take place during teaching hours/non-break time (for student-facing staff).
- Does not constitute 'unacceptable use', as defined in section 4
- Takes place when no pupils are present
- Does not interfere with their jobs, or prevent other staff or pupils from using the facilities for work or educational purposes

Staff may not use the school's ICT facilities to store personal non-work-related information or materials (such as music, videos, or photos).

Staff should be aware that use of ICT facilities for personal use may put personal communications within the scope of the school's ICT monitoring activities (see section 5.5).

Staff are also permitted to use their personal devices (such as mobile phones or tablets) in line with the school's mobile device policy.

Staff should be aware that personal use of ICT (even when not using school ICT facilities) can impact on their employment by, for instance putting personal details in the public domain, where pupils and parents could see them.

5.2.1 Personal Social Media Accounts

Members of staff should ensure that their use of social media, either for work or personal purposes, is appropriate at all times and aligns with the guidenance under Minster Trust for Education's policy "POLICY 9 – EMPLOYEE CODE OF CONDUCT".

5.3 Remote Access

We allow staff to remotely access selected IT systems and resources. Should you require remote access to an IT system or resource, please contact the MITRE IT Services team via the Helpdesk who will be able to assist you with detailing which services are available remotely and how to gain access.

Staff accessing ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on-site. Staff must be particularly vigilant if they use the ICT facilities outside the school/trust and take such precautions to protect the IT systems from viruses or compromising system security.

Our ICT facilities contain information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with our data protection policy.

5.4 School Social Media Accounts

Social media accounts representing the School/Trust must approved by their senior management team prior to creation. Staff members who have not been authorised to manage, or post to the account, must not access, or attempt to access the account.

Minster Trust for Education has guidelines for what can and cannot be posted on its social media accounts. Those who are authorised to manage the account must ensure they abide by these guidelines at all times.

The IT Services Team must be provided access to said social media accounts for the purpose of removing content and manging permissions as directed by the senior management team.

5.5 Monitoring of ICT Infrastructure

Minster Trust for Education reserves the right to monitor the use of its ICT facilities and networks. This includes, but is not limited to, monitoring of:

- Internet sites visited
- Bandwidth usage
- Email accounts
- Telephone calls
- User activity/access logs
- Any other electronic communications

Only authorised IT Services Team members may access, monitor, intercept, record and disclose the above, to the extent permitted by law as directed by the Head of IT. Only authorised staff may view data obtained by the IT Services Team members, under direction of the Trust's senior management team

MITRE monitors ICT use in order to:

- Obtain information related to school and Trust business
- Investigate compliance with policies, procedures and standards
- Ensure effective ICT operation
- Conduct training or quality control exercises
- Prevent or detect crime
- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation

6. Pupils

6.1 Access to ICT facilities

Students will be provided with unique log-in/account information and passwords that they must use when accessing ICT facilities.

- Computers and IT equipment in the school's ICT suite/laptop trolley are available to pupils only under the supervision of staff
- Specialist ICT equipment, such as that used for music, or design and technology, must only be used under the supervision of staff
- Sixth-form pupils can use the computers independently, for educational purposes only

6.2 Search and deletion

Under the Education Act 2011, and in line with the Department for Education's guidance on searching, screening and confiscation, the school has the right to search pupils' phones, computers or other devices for pornographic images or any other data or items banned under Trust/school rules or legislation.

The Trust/school can, and will, delete files and data found on searched devices if we believe the data or file has been, or could be, used to disrupt teaching or break the school's rules.

6.3 Unacceptable use of ICT and the Internet Outside of School

The school will sanction pupils, in line with the school's behaviour policy and/or section 4.2, if a pupil engages in any of the following **at any time** (even if they are not on school premises):

- Using ICT or the internet to breach intellectual property rights or copyright;
- Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination;
- Breaching the school's policies or procedures;
- Any illegal conduct, or statements which are deemed to be advocating illegal activity;
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate;

- Activity which defames or disparages the school/Trust, or risks bringing the school/Trust into disrepute;
- Sharing confidential information about the school, other pupils, or other members of the school community;
- Gaining or attempting to gain access to restricted areas of the network, or to any password protected information, without approval from authorised personnel;
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities;
- Causing intentional damage to ICT facilities or materials;
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation;
- Using inappropriate or offensive language.

7. Parents

7.1 Access to ICT facilities and materials

Parents do not have access to the school's/Trust's ICT facilities as a matter of course.

However, parents working for, or with, the school/Trust in an official capacity (for instance, as a volunteer or as a member of the PTA) may be granted an appropriate level of access, or be permitted to use the ICT facilities at the CEO, COO or Head of IT's discretion.

Where parents are granted access in this way, they must abide by this policy as it applies to staff.

8. Data Security

The Trust takes steps to protect the security of its computing resources, data and user accounts. However, the Trust cannot guarantee security. Staff, pupils, parents and others who use the ICT facilities should use safe computing practices at all times.

8.1 Passwords

All users of the ICT facilities should set strong passwords for their accounts and keep these passwords secure.

Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control.

You must not share your IT credentials. Members of staff or pupils who disclose account or password information may face disciplinary action. Parents or volunteers who disclose account or password information may have their access rights revoked.

When selecting a password, we request the following are taken into considering:

- Don't use a password that is the same or similar to one you use on any other websites;
- Don't use a single word, for example, ***password***, or a commonly-used phrase;
- Make passwords hard to guess, even by those who know a lot about you, such as the names and birthdays of your friends and family, your favourite bands, and phrases you like to use.

8.2 Multifactor Authenticaiton (MFA)

Members of MITRE will be asked to setup multi-factor authentication as a requirement to authenticate with Trust IT systems. Information given to MITRE for MFA purposes will be stored securely. Not having a valid MFA methan setup on your account will result in being unable to access systems outside of MITRE premises.

8.3 Software Updates, Firewalls, and Anti-Virus Software

All of the ICT devices that support software updates, security updates, and anti-virus products will be configured to perform such updates regularly or automatically.

Users must not circumvent or make any attempt to circumvent the administrative, physical and technical safeguards we implement and maintain to protect personal data and the ICT facilities.

Any personal devices using MITRE's network must all be configured in this way.

8.4 Data Protection

All personal data must be processed and stored in line with data protection regulations and the Trust's data protection policy.

MITRE's data protection policy can be found on our website under Key Documents.

8.5 Access to Facilities and Materials

All users of the IT facilities will have clearly defined access rights to school systems, files and devices.

These access rights are managed by MITRE's IT Services Team.

Users should not access, or attempt to access, systems, files or devices to which they have not been granted access. If access is provided in error, or if something a user should not have access to is shared with them, they should alert the IT Services Team via the Helpdesk immediately.

Users should always log out of systems and lock their equipment when they are not in use to avoid any unauthorised access. Equipment and systems should always be logged out of and closed down completely at the end of each working day.

8.6 Encryption

The School/Trust ensures that its devices and systems have an appropriate level of encryption.

The use of removable storage is not permitted unless specifically authorised by the IT Services Team.

Staff may only use personal devices (including computers and USB drives) to access school data, work remotely, or take personal data (such as pupil information) out of school if they have been specifically authorised to do so by the CEO, COO or Head of IT.

Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption, as defined by the IT Services Team.

9. Internet Access

MITRE wireless internet connections are secured. Various wireless networks existing across the MITRE each with a specific purpose. MITRE owned devices will be configured to automatically connect to the correct Wi-Fi Network. The IT Services Team will be able to provide further guidance on which wireless networks to use and for which purpose for any other devices.

In the event that an inappropriate website or service is accessible on a Wi-Fi network, please report this immediately to the IT Services Team via the Helpdesk.

9.1 Pupils

Dependent on the location, a Wi-Fi network may be available for use by pupils if permitted by the Head Teacher. Any Wi-Fi services for pupils is to aid learning and is not for recreational use.

Pupil Wi-Fi/Internet usage is subject to filtering and monitoring as detailed in this policy and in E-safety/Online Safety policies.

9.2 Parents and Visitors

Parents and visitors are not permitted to use the Wi-Fi unless:

- A dedicated guest Wi-Fi exists at the required location AND,
- Parents are working with the school in an official capacity (e.g. as a volunteer or as a member of the PTA)
- Visitors need to access the school's Wi-Fi in order to fulfil the purpose of their visit.

A request should be made to the IT Services Team to validate these criteria and provide a unique authorisation code for Wi-Fi access. This request should be made in advance to the IT Services Team via the Helpdesk (itsupport@mitretrust.org.uk).

Staff must not give the Wi-Fi password to anyone who is not authorised to have it.

10. Monitoring and review

The CEO, COO and Head of IT monitor the implementation of this policy, including ensuring that it is updated to reflect the needs and circumstances of the Trust.

11. Related policies

This policy should be read alongside the Trust's policies on:

- Staying safe online
- Safeguarding and child protection
- Behaviour
- Code of Conduct
- Data protection

Appendix 1: Acceptable use agreement for Senior & Sixth Form pupils

<table>
<tr><th colspan="2">Acceptable use of the school's ICT facilities and internet: agreement for Students and parents/carers</th></tr>
<tr><td colspan="2">Name of Student:</td></tr>
<tr><td colspan="2">When using the school's ICT facilities and accessing the internet in school, I will not:
Use them for a non-educational purpose
Use them to break school rules
Access any inappropriate websites
Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity)
Use chat rooms
Open any attachments in emails, or follow any links in emails, without first checking with a teacher
Use any inappropriate language when communicating online, including in emails
Share my password with others or log in to the school's network using someone else's details
Bully other people
Circumvent security or filtering mechanisms in place on the IT Infrastructure.
I understand that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.
I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others.
I will always use the school's ICT systems and internet responsibly.
I understand that the school can discipline me if I do certain unacceptable things online, even if I'm not in school when I do them.</td></tr>
<tr><td>Signed (pupil):</td><td>Date:</td></tr>
<tr><td colspan="2">Parent/carer agreement: I agree that my child can use the school/academy ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the ICT systems and internet, and for using personal electronic devices on site, and will make sure my child understands these.</td></tr>
<tr><td>Signed (parent/carer):</td><td>Date:</td></tr>
</table>

Appendix 2: Acceptable use agreement for Infant & Junior pupils

<table>
<tr><th colspan="2">Acceptable use of the school's ICT facilities and internet: agreement for pupils and parents/carers</th></tr>
<tr><td colspan="2">Name of pupil:</td></tr>
<tr><td colspan="2">When I use the school's ICT facilities (like computers and equipment) and get on the internet in school, I will not:
Use them without asking a teacher first, or without a teacher in the room with me
Use them to break school rules
Go on any inappropriate websites
Go on Facebook or other social networking sites (unless my teacher said I could as part of a lesson)
Use chat rooms
Open any attachments in emails, or click any links in emails, without checking with a teacher first
Use mean or rude language when talking to other people online or in emails
Share my password with others or log in using someone else's name or password
Bully other people
Using AI tools and generative large language models (such as GPT-3):
During assessments, including internal and external assessments, and coursework;
To write the homework or assignments, where AI-generated text or imagery is presented as their own work (unless explicitly permitted);
When exposing personal, sensitive or intellectual property data or information.
I understand that the school/academy will check the websites I visit and how I use the school's computers and equipment. This is so that they can help keep me safe and make sure I'm following the rules.
I will tell a teacher or a member of staff I know immediately if I find anything on a school computer or online that upsets me, or that I know is mean or wrong.
I will always be responsible when I use the school's ICT systems and internet.
I understand that the school can discipline me if I do certain unacceptable things online, even if I'm not in school when I do them.</td></tr>
<tr><td>Signed (pupil):</td><td>Date:</td></tr>
<tr><td colspan="2">Parent/carer agreement: I agree that my child can use the school/academy ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the ICT systems and internet, and for using personal electronic devices on site, and will make sure my child understands these.</td></tr>
<tr><td>Signed (parent/carer):</td><td>Date:</td></tr>
</table>

Appendix 3: Acceptable use agreement for staff, governors, volunteers and visitors

Acceptable use of the school's ICT facilities and the internet: agreement for staff, governors, volunteers and visitors	
Name of staff member/governor/volunteer/visitor:	
When using the School/Trust's ICT facilities and accessing the internet in school, or outside school on a work device, I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) • Use them in any way which could harm the school or Trust's reputation • Access social networking sites or chat rooms for personal use during working hours • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software, or connect unauthorised hardware or devices to the school's network • Share my password with others or log in to the school's/Trust's network using someone else's details • Share confidential information about the school/Trust, its pupils or staff, or other members of the community • Access, modify or share data I'm not authorised to access, modify or share • Promote private businesses, unless that business is directly related to the school/Trust • Circumvent security or filtering mechanisms in place on the IT Infrastructure.	
I understand that the Trust will monitor the websites I visit and my use of the ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and MITRE's data protection policy. I will let the designated safeguarding lead (DSL) and IT Services Team know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the ICT systems and internet responsibly, and ensure that pupils in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	Date: