Mosaic Partnership Trust

ICT and Internet Acceptable Use Policy

(Ref 02MPTCP)

Version 1.1

Policy Approval	Policy Approved	Date of Review
Audit and Risk Committee	August 2025	August 2026

ICT and Internet Acceptable Use Policy (Ref 02MPTAUP)
History of most recent Policy changes

Version	Date	Page	Change	Origin of Change
V1.0	08/04/2024	Whole Document	Adoption by the Mosaic Partnership Trust and Implementation	New Academy Trust requirement of an ICT and Internet Acceptable Use Policy
V1.1	02/08/2025	Page 6	Reference to unacceptable use of personal data in AI	Advice through the Audit and Risk Committee
V1.1	02/08/2025	Page 7	Use of other email addresses for work purposes. 5.1.1 Use of phones and email.	Some staff requiring school email addresses.
V1.1	02/08/2025	Page 12	Policy section updated to reflect current policies.	Policy changes required reference

ICT and Internet Acceptable Use Policy (Ref 02MPTAUP)

Contents

ICT and Internet Acceptable Use Policy (Ref 02MPTAUP)

1. Introduction and aims

Information and communications technology (ICT) is an integral part of the way our Trust works, and is a critical resource for pupils, staff, trustees, members, councillors, volunteers and visitors.

However, the ICT resources and facilities our Trust uses also pose risks to data protection, online safety and safeguarding.

This policy aims to:

- Set guidelines and rules on the use of ICT resources for staff, trustees and members
- Establish clear expectations for the way everyone in the Trust community engages with each other online
- Support the Trust's policy on data protection, online safety and safeguarding
- Prevent disruption to the Trust through the misuse, or attempted misuse, of ICT systems

This policy covers all users of our Trust's ICT facilities, including:

- Teaching staff
- Non-teaching staff
- Trustees
- Members
- Centrally employed staff
- Volunteers
- Visitors

Breaches of this policy may be dealt with under the Trust disciplinary policy/staff discipline policy/staff code of conduct/etc.

2. Relevant legislation and guidance

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

Data Protection Act 2018

The General Data Protection Regulation

Computer Misuse Act 1990

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 - GOV.UK (www.gov.uk)

Searching, screening and confiscation: advice for schools

National Cyber Security Centre (NCSC)

Education and Training (Welfare of Children Act) 2021

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 Trust and their schools to use the ICT facilities, including Trustees, Members and staff, volunteers, contractors and visitors

"Personal use": any use or activity not directly related to the users' employment, study or purpose

"Authorised personnel": employees authorised by the Trust 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, photos, audio, video, printed output, web pages, social networking sites and blogs

See appendix 2 for a glossary of cyber security terminology.

4. Unacceptable use

The following is considered unacceptable use of the Trust's ICT facilities by any member of the Trust community. Any breach of this policy may result in disciplinary or behaviour proceedings (see section 4.2 below). Please note that the Trust's ICT facilities include individual school ICT facilities which may be supported by different service providers.

Unacceptable use of the Trust's ICT facilities includes:

- Using the Trust's ICT facilities to breach intellectual property rights or copyright
- Using the Trust's ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the Trust's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Online gambling, inappropriate advertising, phishing and/or financial scams
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate or harmful
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams (also known as sexting or youth-produced sexual imagery)
- Activity which defames the Trust, or risks bringing the Trust into disrepute
- Sharing confidential information about the Trust, its pupils, or other members of the Trust community
- Connecting any device to the Trust's ICT network without approval from authorised personnel
- Setting up any software, applications or web services on the Trust'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 Trust's ICT facilities

- Causing intentional damage to ICT 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
- Using inappropriate or offensive language
- Promoting a private business, unless that business is directly related to the Trust
- Using websites or mechanisms to bypass the Trust's filtering mechanisms
- Engaging in content or conduct that is radicalised, extremist, racist, anti-Semitic or discriminatory in any other way
- Placing any personal data or information into Artificial Intelligence (AI), which could include policies, newsletters etc…

This is not an exhaustive list. The Trust reserves the right to amend this list at any time. The Chief Executive Officer or any other relevant member of staff will use professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the Trust's ICT facilities.

4.1 Exceptions from unacceptable use

Where the use of Trust ICT facilities is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the Chief Executive Officers discretion but with the approval of three Trustees to ensure appropriate due diligence.

Written request should be made to the Chief Executive Officer which will be shared with the Trustees as part of the decision-making process.

4.2 Sanctions

Staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with the Trust's policies on discipline/staff discipline/staff code of conduct/etc.

5. Staff (including Trustees, Members, volunteers, and contractors)

5.1 Access to Trust and/or school ICT network and materials

Trust level

The Trust's ICT provider manages access to the Trust's ICT network and materials for Trust central staff. That includes, but is not limited to:

- Computers, tablets, mobile phones 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 the Trust's ICT network.

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 Chief Executive Officer.

School level

The school ICT provider manages access to the school's ICT network and materials for school staff. That includes, but is not limited to:

- Computers, tablets, mobile phones 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 the school's ICT network.

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 their Executive Head/Headteacher.

5.1.1 Use of phones and email

The Trust and their schools provide each member of staff with an email address.

This email account should be used for work purposes only. Staff should enable multi-factor authentication on their email accounts. Staff should not use other email addresses for work purposes.

All work-related business should be conducted using the email address the Trust 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.

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 that contains the personal information of another person, they must inform the following personnel:

- Trust Central Team: Governance Professional and Compliance Officer and the Chief Executive Officer immediately and follow our data breach procedure.
- School level: Governance Professional and Compliance Officer and the Chief Executive Officer immediately and the Executive Headteacher/Headteacher of the school.

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

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.

5.2 Personal use

Staff are permitted to occasionally use Trust facilities for personal use subject to certain conditions set out below. Personal use of ICT facilities must not be overused or abused. The Chief Executive Officer at Trust level and the Executive Head/Headteacher at school level may withdraw permission for it at any time or restrict access at their discretion.

Personal use is permitted provided that such use:

- 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 Trust'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 the Trust's ICT facilities for personal use may put personal communications within the scope of the Trust's ICT monitoring activities (see section 5.5). Where breaches of this policy are found, disciplinary action may be taken.

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

Staff should take care to follow the Trust's protocol on email and communications (see section 5.1.1 and the Trust Email and Communication Protocol) to protect themselves online and avoid compromising their professional integrity.

5.2.1 Personal social media accounts

Members of staff should ensure their use of social media, either for work or personal purposes, is appropriate at all times.

5.3 Remote access

We allow staff to access the Trust's ICT facilities and materials remotely.

Staff accessing the Trust's 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 Trust's ICT facilities outside the Trust central office or their school and take such precautions against importing 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 Trust social media accounts

The Trust has an official X page (only), managed by Governance Professional and Compliance Officer. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access the account.

The Trust 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.

Schools are able to have their own official social media accounts for Twitter and Facebook which are managed locally, with schools required to provide details of the account, platform and administrator to the Governance Professional and Compliance Officer. Social media accounts beyond Twitter and Facebook require the approval of the Chief Executive Officer.

5.5 Monitoring of Trust network and use of ICT facilities

The Trust reserves the right to monitor the use of its ICT facilities and network. 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 ICT staff (from respective providers) may inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law.

The Trust monitors ICT use in order to:

- Obtain information related to Trust business
- Investigate compliance with Trust policies, procedures and standards
- Ensure effective Trust and 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

Laptops and equipment at school level are available to children only under the supervision of staff. Any specialist ICT equipment, such as that used for SEND, music or design and technology must only be used under the supervision of staff. Children will be provided with the appropriate log in details and information.

Unacceptable use of ICT by children. The school will sanction pupils, in line with their behaviour policy if a pupil engages in any of the following at any time:

- 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 Trust's/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 Trust, or risks bringing the Trust/school into disrepute
- Sharing confidential information about the school, other pupils, or other members of the 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 academy'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

The Trust's central ICT equipment is not available to children under any circumstances.

7. Parents and carers

7.1 Access to ICT facilities and materials

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

However, parents working for, or with, a school 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 academy's facilities at the headteacher's discretion.

8. Data security

The Trust is responsible for making sure it has the appropriate level of security protection and procedures in place. It therefore takes steps to protect the security of its computing resources, data and user accounts. However, the Trust cannot guarantee security. Staff and others who use the Trust's ICT facilities should use safe computing practices at all times.

8.1 Passwords

All users of the Trust's 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.

Members of staff who disclose account or password information may face disciplinary action.

All staff will use a password manager to help them store their passwords securely.

8.2 Software updates, firewalls and anti-virus software

All of the Trust's 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 Trust's ICT facilities.

Any personal devices including mobile phones using the Trust's network must all be configured in this way.

8.3 Data protection

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

The Trust Data Protection Policy can be found on the Mosaic Shared Admin Drive

8.4 Access to facilities and materials

Trust Level

All users of the Trust's central team ICT facilities will have clearly defined access rights to Trust systems, files and devices.

These access rights are managed by the Chief Executive Officer, Chief Finance Officer, Governance Professional and Compliance Officer and Trust ICT Provider.

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 Chief Executive Officer and Governance Professional and Compliance Officer 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.

School level

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

These access rights are managed by the Executive Headteacher/Headteacher or a delegated member of staff (delegated by the Headteacher)

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 Headteacher 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.

8.5 Encryption

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

Trust staff may only use personal devices (including computers and USB drives) to access Trust data, work remotely, or take personal data (such as pupil information) out of the Trust if they have been specifically authorised to do so by the Chief Executive Officer.

Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption, as defined by the ICT service provider.

9. Protection from cyber attacks

Please see the glossary (appendix 6) to help you understand cyber security terminology.

The Trust and their schools will:

- Work with Trustees and the IT providers to make sure cyber security is given the time and resources it needs to make the Trust secure
- Provide annual training for staff (and include this training in any induction for new starters, if they join outside of the Trust's annual training window) on the basics of cyber security, including how to:
  - Check the sender address in an email
  - Respond to a request for bank details, personal information or login details
  - Verify requests for payments or changes to information
- Make sure staff are aware of its procedures for reporting and responding to cyber security incidents
- Investigate whether our IT software needs updating or replacing to be more secure
- Not engage in ransom requests from ransomware attacks, as this would not guarantee recovery of data

Put controls in place that are:

- **'Proportionate'**: the Trust will verify this using a third-party audit (https://360safe.org.uk/) annually, to objectively test that what it has in place is robust
- **Multi-layered**: everyone will be clear on what to look out for to keep our systems safe
- **Up-to-date:** with a system in place to monitor when the Trust needs to update its software
- **Regularly reviewed and tested**: to make sure the systems are as up to scratch and secure as they can be

- Back up critical data automatically daily and store these are backed up and stored by the Trusts' ICT providers
- Delegate specific responsibility for maintaining the security of our management information system (MIS) to our ICT providers

Make sure staff:

- Access the network using a virtual private network (VPN) when working from home

- Enable multi-factor authentication where they can, on things like Trust email accounts
- Store passwords securely using a password manager

- Make sure ICT staff conduct regular access reviews to make sure each user in the Trust has the right level of permissions and admin rights
- Have a firewall in place that is switched on
- Check that its supply chain is secure, for example by asking suppliers about how secure their business practices are and seeing if they have the Cyber Essentials certification
- Develop, review and test an incident response plan including how the Trust will communicate with everyone if communications go down, who will be contacted when, and who will notify Action Fraud of the incident. This will be reviewed and tested annually and after a significant event has occurred, using the NCSC's 'Exercise in a Box'
- Work with our IT providers to see what they can offer the Trust regarding cyber security, such as advice on which service providers to use or assistance with procurement

10. Internet access

The Trust wireless internet connection is secured. Filtering systems are in place

11. Monitoring and review

The Governance Professional and Compliance Officer will monitor the implementation of this policy, including ensuring it is updated to reflect the needs and circumstances of the Trust at Trust level, whilst Executive Heads/Headteachers will monitor the implementation of this policy, including ensuring it is updated to reflect the needs and circumstances of the school at school level.

The Trust Chief Executive Officer will secure any feedback on the policy and whether changes are required at school level through the monthly Heads meetings.

This policy will be reviewed annually in the first instance until a single ICT provider is in place across the Trust.

The Audit and Risk Committee is responsible for approving this policy.

12. Related policies

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

- Online safety
- Safeguarding and child protection
- Behaviour
- Professional Conduct and Expectations
- Data Protection

Appendix A1 – Acceptable Use Form (Device Loan Agreement)

Device loan agreement for staff

1. This agreement is between:

1) The Mosaic Partnership Trust ("the Trust")

2) **XXXXXX** ("the employee" and "I")

And governs the use and care of devices assigned to individual staff members. This agreement covers the period from the date the device is issued through to the return date of the device to the Trust.

All issued equipment shall remain the sole property of the Trust and is governed by the Trust's policies including the ICT and Internet Acceptable Use Policy.

1. The Trust is lending the employee a Laptop or Macbook ("the equipment") for the purpose of their role within the Trust and for Trust business only.

2. This agreement sets the conditions for the employee taking the equipment home.

I confirm that I have read the terms and conditions set out in the agreement and my signature at the end of this agreement confirms that I have read and agree to these terms.

2. Damage/loss

By signing this agreement, I agree to take full responsibility for the equipment issued to me and I have read this agreement and understand the conditions of the agreement.

I understand that I am responsible for the equipment at all times whether on the Trust's central site, at a Trust school, at home or in another location.

I am responsible for the Portable Device whilst in my possession and will not lend the portable device to anyone including family members and friends.

If the equipment is damaged, lost or stolen, I will immediately inform the Chair of Trustees (in the context of the CEO or Director of Education), the CEO in the context of all centrally managed staff and the Headteacher in the context of an individual school.

I acknowledge that I am responsible for full replacement costs. If this Portable Device is lost or stolen, I will immediately notify IT Services, and if stolen provide a copy of the Police report or incident report.

I agree to keep the equipment in good condition and to return it to the Trust on demand from the Trust in the same condition.

I will not leave the equipment unsupervised in unsecured areas including vehicles. If travelling, I will keep the device with me at all times.

3. Unacceptable use

I am aware that the Trust monitors my activity on the equipment.

I will not carry out any activity that constitutes 'unacceptable use'.

This includes, but is not limited to:

- Accessing, creating, storing or linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- Sharing confidential information about the school, its pupils, or other members of the Trust community
- Setting up any software, applications or web services on this device without approval by the IT provider, or creating or using any programme, tool or item of software designed to interfere with the functioning of the ICT facilities, accounts or data
- Carrying out any activity which defames or disparages the Trust, or risks bringing the Trust into disrepute
- Using inappropriate or offensive language

I accept that if I engage in any activity that constitutes 'unacceptable use, I may face disciplinary action in line with the Trust's policies on staff discipline/staff code of conduct/etc.

4. Personal use

I will not use this devise for any personal use and will not loan the equipment to any other person.

5. Data protection

I agree to take the following measures to keep the data on the device protected.

- Keep the equipment password-protected - strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Make sure the equipment locks if left inactive for a period of time
- Do not share the equipment among family or friends
- Update antivirus and anti-spyware software as required
- Install the latest updates to operating systems, as prompted

6. Return date

I will return the device in its original condition to the Trust Office within 14 days of being requested to do so.

I will return the equipment to the Trust upon resignation, dismissal or if I leave the employment of the Trust for any other reason.

7. Consent

By signing this form, I confirm that I have read and agree to the rules and conditions above.

Full Name	XXXXX
Role	XXXXX
Signature (Including Electronic Signature)	XXXXXXX
Date of signature	XXXXX

Appendix A2 – Cyber Security Glossary

These key terms will help you to understand the common forms of cyber attack and the measures the school will put in place. They're from the National Cyber Security Centre (NCSC) glossary.

TERM	DEFINITION
Antivirus	Software designed to detect, stop and remove malicious software and viruses.
Cloud	Where you can store and access your resources (including data and software) via the internet, instead of locally on physical devices.
Cyber attack	An attempt to access, damage or disrupt your computer systems, networks or devices maliciously.
Cyber incident	Where the security of your system or service has been breached.
Cyber security	The protection of your devices, services and networks (and the information they contain) from theft or damage.
Download attack	Where malicious software or a virus is downloaded unintentionally onto a device without the user's knowledge or consent.
Firewall	Hardware or software that uses a defined rule set to constrain network traffic – this is to prevent unauthorised access to or from a network.
Hacker	Someone with some computer skills who uses them to break into computers, systems and networks.
Malware	Malicious software. This includes viruses, trojans or any code or content that can adversely impact individuals or organisations.
Patching	Updating firmware or software to improve security and/or enhance functionality.
Pentest	Short for penetration test. This is an authorised test of a computer network or system to look for security weaknesses.

TERM	DEFINITION
Phishing	Untargeted, mass emails sent to many people asking for sensitive information (like bank details) or encouraging them to visit a fake website.
Ransomware	Malicious software that stops you from using your data or systems until you make a payment.
Social engineering	Manipulating people into giving information or carrying out specific actions that an attacker can use.
Spear-phishing	A more targeted form of phishing where an email is designed to look like it's from a person the recipient knows and/or trusts.
Trojan	A type of malware/virus designed to look like legitimate software that can be used to hack a victim's computer.
Two-factor/multi-factor authentication	Using 2 or more different components to verify a user's identity.
Virus	Programs designed to self-replicate and infect legitimate software programs or systems.
Virtual Private Network (VPN)	An encrypted network which allows remote users to connect securely.
Whaling	Highly targeted phishing attacks (where emails are made to look legitimate) aimed at senior executives.