Greater Manchester Academies Trust

IT Acceptable Usage Policy

Greater Manchester Academies Trust

Revision Information

This document has been approved for operation within	All Trust Establishments
Document Version	Version 1.0
Date of last review	August 2022
Date of next review	August 2024
Review Period	Annually, or where they have been material changes to the relevant courses of business
Date of Trustee Approval	August 2022
Status	Approved
Person Responsible for Policy	Head of IT
Owner	Greater Manchester Academies Trust
Signature of Approval	

With you…for you…about you…

1. Introduction

Information and communications technology (ICT) is an integral part of the way our trust works, and is a critical resource for pupils, staff (including senior leadership teams), governors, volunteers and visitors. It supports teaching and learning, pastoral and administrative functions of the trust.
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 trust ICT resources for staff, pupils, parents and governors
- Establish clear expectations for the way all members of the trust community engage 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
- Support the trust in teaching pupils safe and effective internet and ICT use

This policy covers all users of our trust's ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors.

2. 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 to use the ICT facilities, including governors, staff, pupils, 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 6 for a glossary of cyber security terminology.

3. Unacceptable use

The following is considered unacceptable use of the trust's ICT facilities by any member of the trust community.

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 or disparages 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

This is not an exhaustive list. The trust reserves the right to amend this list at any time. The Trust Leadership 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.

3.1 Exceptions from unacceptable use

Where the use of trust ICT facilities (on the trust premises and/or remotely) is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the Head of IT/Chief Operational Officer's discretion. To gain permission, the request must be in writing to itsupport@gmatrust.co.uk

4. Staff (including governors, volunteers and contractors)

4.1 Access to trust ICT facilities and materials

The trust's Head of IT manages access to the trust's ICT facilities and materials for trust 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 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 Head of IT

4.1.1 Use of phones and email

The trust provides each member of staff with an email address.

This email account should be used for work purposes only.

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 DPO, immediately and follow our data breach procedure.

Staff must not give their personal phone numbers to parents or pupils. Staff must use phones provided by the trust to conduct all work-related business.

Trust phones must not be used for personal matters.

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

4.2 Personal use

Staff are permitted to occasionally use trust ICT facilities for personal use subject to certain conditions set out below. Personal use of ICT facilities must not be overused or abused. The Head of IT/Chief Operational Officer 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
- Does not constitute 'unacceptable use'
- 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 4.5). 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 guidelines on social media (see appendix 1) and use of email (see section 4.1.1) to protect themselves online and avoid compromising their professional integrity.

4.2.1 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.
The trust has guidelines for staff on appropriate security settings for Facebook accounts (see appendix 1).

4.3 Remote access

We allow staff to access the trust's ICT facilities and materials remotely. Access is via Smoothwall VPN or RDS only.

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 and take such precautions.

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.

4.4 Trust social media accounts

The trust and all trusts within has an official social media accounts, managed the trust media team. 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.

4.5 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 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

5. 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, pupils, parents and others who use the trust's ICT facilities should use safe computing practices at all times.

5.1 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 be required to reset their password every 90 days your device will prompt you to do this

5.2 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 using the trust's network must all be configured in this way.

5.3 Data protection

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

5.4 Access to facilities and materials

All users of the trust's ICT facilities will have clearly defined access rights to trust systems, files and devices.
These access rights are managed by Head of IT.

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 Head of IT 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.

5.5 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 trust if they have been specifically authorised to do so by the 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 Head of IT.

6. Protection from cyber attacks

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

The trust will:

- Work with governors and the IT department 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:

1. Check the sender address in an email
2. Respond to a request for bank details, personal information or login details
3. 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:

1. **'Proportionate'**: the trust will verify this using a third-party audit (such as this one) cyber security essentials, to objectively test that what it has in place is up to scratch
2. **Multi-layered**: everyone will be clear on what to look out for to keep our systems safe

3. **Up-to-date:** with a system in place to monitor when the trust needs to update its software
4. **Regularly reviewed and tested**: to make sure the systems are as up to scratch and secure as they can be

- Back up critical data every night and store these backups on hard disks that are based in a different building.
- Make sure staff:

1. Dial into our network using smoothwall vpn or RDS when working from home
2. Enable multi-factor authentication where they can

- 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
- Develop, review and test an incident response plan with the IT department, for example, 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 yearly and after a significant event has occurred, using the NCSC's 'Exercise in a Box'

7. Monitoring and Review

The COO and Head of IT, monitor the implementation of this policy, including ensuring it is updated to reflect the needs and circumstances of the trust.
This policy will be reviewed every 2 years.

The governing board is responsible for approving this policy.

8. Date of Next Review

The Policy must next be reviewed and signed off by the Head of IT and COO the sooner of August 2024, or when there have been material changes to the relevant courses of business.

Appendix 1: Facebook cheat sheet for staff

Don't accept friend requests from pupils on social media

10 rules for trust staff on Facebook

1. Change your display name – use your first and middle name, use a maiden name, or put your surname backwards instead
2. Change your profile picture to something unidentifiable, or if not, ensure that the image is professional
3. Check your privacy settings regularly
4. Be careful about tagging other staff members in images or posts
5. Don't share anything publicly that you wouldn't be just as happy showing your pupils
6. Don't use social media sites during trust hours
7. Don't make comments about your job, your colleagues, our trust or your pupils online – once it's out there, it's out there
8. Don't associate yourself with the trust on your profile (e.g. by setting it as your workplace, or by 'checking in' at a trust event)
9. Don't link your work email address to your social media accounts. Anyone who has this address (or your personal email address/mobile number) is able to find you using this information
10. Consider uninstalling the Facebook app from your phone. The app recognises wifi connections and makes friend suggestions based on who else uses the same wifi connection (such as parents or pupils)

Check your privacy settings

1. Change the visibility of your posts and photos to **'Friends only'**, rather than 'Friends of friends'. Otherwise, pupils and their families may still be able to read your posts, see things you've shared and look at your pictures if they're friends with anybody on your contacts list
2. Don't forget to check your **old posts and photos** – go to bit.ly/2MdQXMN to find out how to limit the visibility of previous posts
3. The public may still be able to see posts you've **'liked'**, even if your profile settings are private, because this depends on the privacy settings of the original poster
4. **Google your name** to see what information about you is visible to the public

5. Prevent search engines from indexing your profile so that people can't **search for you by name** – go to bit.ly/2zMdVht to find out how to do this
6. Remember that **some information is always public**; your display name, profile picture, cover photo, user ID (in the URL for your profile), country, age range and gender

What to do if…

A pupil adds you on social media

1. In the first instance, ignore and delete the request. Block the pupil from viewing your profile
2. Check your privacy settings again, and consider changing your display name or profile picture
3. If the pupil asks you about the friend request in person, tell them that you're not allowed to accept friend requests from pupils and that if they persist, you'll have to notify senior leadership and/or their parents. If the pupil persists, take a screenshot of their request and any accompanying messages
4. Notify the senior leadership team or the safeguarding about what's happening

A parent adds you on social media

1. It is at your discretion whether to respond. Bear in mind that:

- Responding to one parent's friend request or message might set an unwelcome precedent for both you and other teachers at the trust
- Pupils may then have indirect access through their parent's account to anything you post, share, comment on or are tagged in

2. If you wish to decline the offer or ignore the message, consider drafting a stock response to let the parent know that you're doing so