Great Academies
Education Trust

ICT Acceptable Use Policy

Prepared/reviewed by	IT Manager
Date	January 2024
Approved by	Audit and Risk Committee
Date	February 2024
Review date	January 2025

CONTENTS PAGE

Table of Contents

1. POLICY AIM

1.1 Information and communications technology (ICT) is an integral part of the way our trust works, and is a critical resource for pupils, employees, 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 employees, 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, employees, pupils, volunteers, contractors, and visitors.
- Breaches of this policy may be dealt with under the GAET Code of Conduct.

2. DEFINITIONS

2.1. **"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 trustees, governors, employees, 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 3 for a glossary of cyber security terminology.

3. UNACCEPTABLE USE

3.1 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

3.2 Unacceptable use of the trust’s ICT facilities includes the below list. This is not an exhaustive list. The trust reserves the right to amend this list at any time. The trust 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

- 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

- Leaving ICT equipment anywhere other than on your person, at work or at home e.g., in the car
- Using a (generic portable solid-state data storage device): data stick, pen drive, thumb drive, USB drive

3.2 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 principal/CEO discretion.

Employees will seek advice and if needed permission from the principal/CEO should technology need to be used in other circumstances e.g., on residentials and day visits.

3.3 SANCTIONS

Pupils and employees who engage in any of the unacceptable activity listed above may face disciplinary action in line with the trust's policies on behaviour and Code of Conduct.

4. EMPLOYEES (including trustees, governors, volunteers and contractors

4.1 ACCESS TO TRUST ICT FACILITIES AND MATERIALS

The trust's IT provider manages access to the trust's ICT facilities and materials for trust employees. That includes, but is not limited to:

- Computers, tablets, mobile phones, and other devices
- Access permissions for certain programmes or files

Employees will be provided with unique log-in/account information and passwords that they must use when accessing the trust's ICT facilities.

Employees 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 owner.

4.2 USE OF EMAILS

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

This email account should be used for work purposes only. Employees should enable multi-factor authentication on their email accounts.

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

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

Employees 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.

Employees 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 employees 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 employees send an email in error that contains the personal information of another person, they must inform the Data Protection Officer/Principal immediately and follow our data breach procedure.

4.3 USE OF PHONES

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

Trust phones must not be used for personal matters unless authorised by the CEO to use a personal dual SIM.

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

4.4 PERSONAL USE

Employees 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 principal/CEO 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 time
- Does not constitute 'unacceptable use'
- Takes place when no pupils are present
- Does not interfere with their jobs, or prevent other employees or pupils from using the facilities for work or educational purposes
- Employees may not use the trust's ICT facilities to store personal non-work-related information or materials (such as music, videos or photos)
- Employees 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
- Where breaches of this policy are found, disciplinary action may be taken
- Employees 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

- Employees should take care to follow the trust’s guidelines on social media (and use of email to protect themselves online and avoid compromising their professional integrity

4.5 PERSONAL SOCIAL MEDIA ACCOUNTS

Employees should follow the employees of code of conduct and ensure their use of social media, either for work or personal purposes, is appropriate at all times.

4.6 REMOTE ACCESS

We allow employees to access the trust’s resources remotely.

Employees accessing the trust’s ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on-site. Employees should note in particular this means that all monitoring in section 4.7 also applies to trust ICT facilities and materials used remotely. Employees must be particularly vigilant if they use the trust’s ICT facilities outside the trust and take such precautions as they may require from time to time against importing viruses or compromising system security.

Our ICT facilities contain information that 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.

4.7 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 employees 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
- Meet safeguarding requirements
- Prevent or detect crime
- Support and manage wellbeing of staff, students and visitors
- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation

5. PUPILS

5.1 ACCESS TO ICT FACILITIES

Laptops and tables are available to pupils to use onsite and in some cases available for home use.

Pupils will be provided with a TEAMs account linked to the trust's virtual learning environment, which they can access from any device.

5.2 UNACCEPTABLE USE OF ICT

The trust will sanction pupils, in line with the behaviour policy, if a pupil engages in any of the following at any time (even if they are not on trust 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 trust'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
- 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, other pupils, or other members of the trust 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 trust'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

6. DATA SECURITY

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

6.1 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.

Employees or pupils who disclose account or password information may face disciplinary action.

6.2 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.

6.3 DATA PROTECTION

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

6.4 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 the principal/CEO and IT support.

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 principal/CEO immediately.

Users should always close windows, 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 or when moving working location.

6.5 ENCRYPTION

The trust ensures that its devices and systems have an appropriate level of encryption. Users can only store trust related work using TEAMs, SharePoint and OneDrive. Memory sticks/external hard drives are not permitted to be used.

7. PROTECTION FROM CYBER ATTACKS

7.1 Please see appendix 6 to help you understand cyber security terminology.

The trust will:

- Work with trustees and the IT department to make sure cyber security is given the time and resources it needs to make the trust secure
- Provide annual updates for employees and timely reminders regarding password protection

- Make sure employees 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
- Ensure that there is a complete backup of systems and data, which is stored offsite and providing at least 30 days of snapshots to ensure recovery from ransomware attacks

Put controls in place that are:

Proportionate: the trust will verify this using a third-party audit set by the trust to objectively test that what it has in place is up to scratch

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

Make sure employees:

- Use TEAMs to access information offsite
- Enable multi-factor authentication where they can, on things like trust email accounts
- Store passwords securely using a password manager
- Make sure ICT employees conduct regular access reviews to make sure each user in the trust has the right level of permissions and admin rights

8. RELATED POLICIES & STRATEGIES

- Data Protection Policy
- Safeguarding Policy
- Behaviour Policy
- Staff Disciplinary Policy and other staff related policies

APPENDIX ONE: Acceptable Use Agreement for Pupils

Acceptable use of the trust's ICT facilities and internet: agreement for pupils.

Name of pupil:

When using the trust's ICT facilities and accessing the internet in trust, I will not:

- Use them for a non-educational purpose
- Use them without a teacher being present, or without a teacher's permission
- Use them to break trust 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 any semi-nude or nude images, videos or livestreams, even if I have the consent of the person or people in the photo
- Share my password with others or log in to the trust's network using someone else's details
- I understand that the trust will monitor the websites I visit and my use of the trust's ICT facilities and systems
- I will immediately let a teacher or other member of Employees know if I find any material which might upset, distress or harm me or others
- I will always use the trust's ICT systems and internet responsibly
- I understand that the trust can discipline me if I do certain unacceptable things online, even if I'm not in trust when I do them

Signed (pupil):	**Date:**

APPENDIX TWO: Acceptable Use Agreement for Employees, Governors, Volunteers and Visitors

Acceptable use of the trust's ICT facilities and the internet: agreement for employees:

Name of employee:

When using the trust's ICT facilities and accessing the internet in trust, or outside trust 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 trust's reputation Access social networking sites or chat rooms
- 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 trust's network
- Share my password with others or log in to the trust's network using someone else's details Share confidential information about the trust, its pupils or Employees, 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 trust

- I understand that the trust will monitor the websites I visit and my use of the trust's ICT facilities and systems
- I will take all reasonable steps to ensure that work devices are secure and password- protected when using them both on and outside of trust premises, and keep all data securely stored in accordance with this policy and the trust's data protection policy
- I will let the designated safeguarding lead (DSL) and ICT manager 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 trust's ICT systems and internet responsibly and ensure that pupils in my care do so too.
- I will abide by the trust Acceptable Use Policy

Signed:

Date:

APPENDIX THREE: Glossary of Cyber Security Terminology

These key terms will help you to understand the common forms of cyber-attack and the measures the trust 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.
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.