Academy
Transformation
Trust

ICT Policy

September 2020

Published date: September 2020	**Next review deadline: September 2023**	**Non-statutory**	**Executive Lead at ATT: Ed Thomas, Director of Operations**

Links to:	
• **Esafety Policy** • **Data Protection policy** • **Disciplinary Policy** • **Staff Code of Conduct** • **Governors Code of Conduct** • **Behaviour Policy**	

Our Vision

We have one core purpose:
To have the biggest positive impact in the varied communities we serve through ensuring top drawer education for our learners. #TransformingLives

How do we ensure this across our trust?
In all we do we are:

1. Ethical to the core, ensuring that education is always front and centre
2. Futures focused system leaders – never simply followers
3. Collaborative in every endeavour
4. Resolutely learner centred.

What does this look like across our trust?
Education
We are:

1. Ruthlessly ambitious for all who learn and work with us
2. Unwaveringly inclusive – determined on eradicating barriers to educational success
3. Committed to excellent teaching
4. Determined upon academic excellence for all in our communities
5. Compassionate, ethical and caring advocates for all in our communities
6. Outwardly facing and globally conscious

Operations
We are:

1. Committed to the very best people development and empowerment
2. Determined to shout loudly and share proudly our successes
3. The best professional and technical experts (supporting education) in the sector
4. Committed to the very best understanding and management of risk

Financial
We are:

1. Providing the best possible public service for the best possible value
2. Determined to supplement our public income with shrewd income generation
3. Building financially sustainable models of educational improvement in our communities
4. Demonstrably efficient in all we do

Our values

- We will work inclusively within our communities, embracing the varied localities we serve while sharing our common vision and values.
- We will develop the very best leaders of the future, working to improve education and transform lives.
- We will adhere unwaveringly to the 'Nolan Principles' of Public Service, which is made clear in our commitment to Ethical Leadership.

Contents

Statement of Intent 4

1 Introduction and intent 4

2 Definitions 4

3 Unacceptable use 5

4 Staff 6

5 Pupils 8

6 Parents 9

7 Data and cyber security 9

8 Internet access 11

9 Social media 12

Statement of Intent

As the world becomes more digitally connected, the use of ICT is an ever-increasing part of daily life in our trust, and its power is immense. If used incorrectly, it has unintended consequences. This policy seeks to ensure all stakeholders trust-wide use ICT responsibly and with due care and attention.

1. Introduction and aims

ICT is an integral part of the way our academies work, and is a critical resource for pupils, colleagues, non-executives, volunteers and visitors. It supports teaching and learning, operations, pastoral and administrative functions across our Trust.

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

This policy aims to:

- Set guidelines and rules on the use of academy ICT resources for colleagues, pupils, parents and non-executives
- Establish clear expectations for the way all members of the academy community engage with each other
- Support the academy's policy on data protection, online safety and safeguarding
- Prevent disruption to the academy through the misuse, or attempted misuse, of ICT systems
- Support the academy in teaching pupils safe and effective internet and ICT use

This policy covers all users of our ICT facilities, including non-executives, colleagues, pupils, volunteers, contractors and visitors.

Breaches of this policy may be dealt with under our disciplinary policy/behaviour policy/code of conduct/etc.

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 academy to use the ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors
- **"Social media"** may include (but is not limited to): blogs; wikis; social networking sites; forums; bulletin boards; online gaming; apps; video/photo sharing sites; chatrooms and instant messenger
- **"Personal use":** any use or activity not directly related to the users' employment, study or purpose
- **"Authorised personnel":** employees authorised by the academy/our 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

3 Unacceptable use

The following is considered unacceptable use of the our ICT facilities by any member of the academy community. Any breach of this policy may result in disciplinary or behaviour proceedings.

Unacceptable use of the ICT facilities includes:

- Using the ICT facilities to breach intellectual property rights or copyright
- Using the ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the 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 our Trust, or risks bringing us into disrepute
- Sharing confidential information about the academy, its pupils, or other members of the academy community
- Connecting any device to the ICT network without approval from authorised personnel
- Setting up any software, applications or web services on the 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 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
- Using websites or mechanisms to bypass the academy's filtering mechanisms

This is not an exhaustive list. We reserve the right to amend this list at any time. The Principal 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 ICT facilities.

Sanctions

Pupils and staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with the academy policies on behaviour/disciplinary/code of conduct.

4 Staff (including governors, volunteers, and contractors)

Access to academy ICT facilities and materials

The academy ICT support team manages access to the ICT facilities and materials for staff. That includes, but is not limited to:

- Computers, tablets and other devices
- Access permissions for certain programs or files

Staff will be provided with unique log-in/account information and passwords that they must use when accessing the 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 ICT support team by creating a help desk ticket via the Every system.

Use of phones and email

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

This email account should be used for work purposes only.

Work email maybe be accessed on a personal device providing security mechanism is in place on the device (PIN number, passwords, facial recognition, fingerprint etc.)

Be extra vigilant when opening emails/clicking on links as they could be phishing emails or contact viruses.

All work-related business should be conducted using the email address the academy/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/digital communication messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 (GDPR) 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. Rather than sending attachments it is safer to store the file in a central location such as SharePoint or OneDrive and then securely share the file with the intended recipients. If this is not possible, you should consider encrypting the email and its attachments if this contains sensitive or confidential information to ensure this 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 which contains the personal information of another person, they must inform the academy Data Protection Lead immediately and follow our data breach procedure.

Staff must not give their personal phone numbers to parents or pupils. Staff should aim to use phones provided by the academy to conduct all work-related business. In exceptional circumstances, when personal phones are used, numbers should be withheld.

Academy phones must not be used for anything that contravenes this policy.

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

The academy may have the ability record in-coming and out-going phone conversations. If calls are recorded, the caller must be made aware of this and the reasons why they are being recorded.

4.1 Personal use

Staff are permitted to occasionally use academy ICT facilities for personal use subject to certain conditions set out below. Personal use of ICT facilities must not be overused or abused. The ICT support team or principal 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 contact time/teaching hours/non-break time
- Does not constitute ‘unacceptable use’, as defined in section 3
- 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 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 ICT facilities for personal use may put personal communications within the scope of the ICT monitoring activities (see section 4.3). Where breaches of this policy are found, disciplinary action may be taken.

Staff are also permitted to use their personal devices (such as mobile phones or tablets) in line with the academy’s esafety and code of conduct policy.

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

Staff should take care to follow the academy guidelines on social media and use of email/digital communication to protect themselves online and avoid compromising their professional integrity.

4.2 Remote access

We may provide remote access that allows staff to access the academy ICT facilities and materials remotely. This allows staff to login from home and access the ICT facilities such as SIMS, user area and shared areas. Remote access is managed by the ICT support team.

Staff accessing the academy 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 and ensure they have up to date anti-virus software installed on their computer and take such precautions to protect the ICT facilities from 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.

4.3 Monitoring of academy network and use of ICT facilities

The academy 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 academy monitors ICT use in order to:

- Obtain information related to academy business
- Investigate compliance with policies, procedures and standards
- Ensure the ICT facilities are operating correctly
- 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 Pupils

5.1 Access to ICT facilities

Pupils will have access to a range of ICT facilities within the academy.

- ICT facilities in the academy are available to pupils only under the supervision of staff
- Post-16 pupils can use the computers independently for educational purposes only

5.2 Search and deletion

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

The academy 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 academy rules.

5.3 Unacceptable use of ICT and the internet outside of academy

The academy 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 academy 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 academy 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 our Trust, or risks bringing the us into disrepute
- Sharing confidential information about our Trust, academy, other pupils, or other members of the academy 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 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

Pupils and staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with the academy policies on behaviour/staff discipline/staff code of conduct.

6 Parents

6.1 Access to ICT facilities and materials

Parents do not have access to the academy ICT facilities as a matter of course.

However, parents working for, or with, the academy 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 principals discretion.

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

6.2 Communicating with or about ATT/academy online

We believe it is important to model for pupils, and help them learn, how to communicate respectfully with, and about, others online.

Parents play a vital role in helping model this behaviour for their children, especially when communicating with the academy through our website and social media channels.

7 Data and cyber security

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

Our Trust Office 365 platform will have multi factor authentication enabled for accounts with access to sensitive data.

Multiple backup copies of academy data are made, including cloud backups of critical data for disaster recovery.

You will be provided with a personal account for accessing the ICT facilities, with your own username and password. This account will be tailored to the level of access you require and is for your use only.

You must not allow anyone to have access to your account under any circumstances, for any length of time, even if supervised.

The use of USB memory sticks and portable hard drives are strongly discouraged. More secure methods for transporting data are available via Office 365 (SharePoint/OneDrive) or remote access functions. USB storage devices pose unnecessary risks around data breaches, viruses and ICT security.

Do not use non ICT-authorised third party hosting services, like Dropbox, when processing data.

If you use a personal computer at home for work purposes, you must ensure that any sensitive or personal information is secured to prohibit access by any non-Trust member of staff. The computer/device must also be encrypted.

You must not use an internet/cyber café to access our Trust ICT facilities.

You must ensure that items of portable computer equipment (such as laptops, tablets, or digital cameras) are securely stored in a locked cupboard or room when left unattended. No equipment should be left unattended in a car, even if this is out of sight in the boot.

In the event of theft, loss or damage you must contact ICT support team immediately.

Training and systems are put in place to minimise the risk of cyber security risks, phishing or other email scams.

Passwords

All users of our Trust ICT facilities should set strong passwords for their accounts and keep these passwords secure. Apart from early years and key stage 1, will have passwords set.

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

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.

Software updates, firewalls, and anti-virus software

All of our Trust ICT devices that support software updates, security updates, anti-virus and monitoring 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 the network must all be configured in this way.

Data protection

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

Access to ICT facilities and materials

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

These access rights are managed by the ICT support 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 ICT support team 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.

Encryption

Our 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 data, work remotely, or take personal data (such as pupil information) off-site if they have been specifically authorised to do so by the senior leadership team.

Use of such personal devices will only be authorised if the devices have appropriate levels of anti-virus software, security and encryption, as defined by the ICT support team.

8 Internet access

Our Trust has wifi/wireless networks that will provide access to the internet, these are secured and have the appropriate level of filtering. The academy may have separate wifi/wireless networks such as ATT WIFI, Domain (academy devices connected to the network), BYOD (bring your own device) and Guest network. Details about the networks available and how to access is available from the ICT support team.

8.1 Pupils

Pupils will only be able to use the wifi/wireless network that have already been setup for the domain devices (academy devices connected to the network) unless a BYOD network is available.

8.2 Parents and visitors

Parents and visitors to the academy will not be permitted to use the wifi/wireless unless specific authorisation is granted by the principal, ICT support team, or there is a Guest network available.

Authorisation will only be granted if:

- Parents are working with the academy in an official capacity (e.g. as a volunteer or as a member of the PTA)
- Visitors need to access the academy's wifi to fulfil the purpose of their visit (for instance, to access materials stored on personal devices as part of a presentation or lesson plan)

Staff must not give the wifi password to anyone who is not authorised to have it. Doing so could result in disciplinary action.

9 Social media

Social media sites have become important learning, communication and marketing tools as they allow users (individual, academy or Trust) to interact and raise their profile with a wide cross section of other users. Social networking is defined as sharing your interests and thoughts in an online forum with like-minded individuals. Social media is the means by which this is completed.

Our Trust and academies have an official social media page(s). Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access the account.

Social media should never be used in a way that breaches any Trust policy.

There are 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.

Social media principles

9.1 Staff members must be conscious at all times of the need to keep your personal and professional lives separate. You should not put yourself in a position where there is a conflict between your work for the academy and your personal interests.

9.2 Staff members must not engage in activities involving social media which might bring our Trust into disrepute.

9.3 Staff members must not represent your personal views as those of our Trust, on any social medium. If you express any idea or opinion, then you should add the disclaimer such as 'these are my own personal views and not those of the academy'.

9.4 Staff members must not discuss personal information about pupils, our Trust staff and other professionals you interact with as part of your job on social media. You must not divulge any information that is confidential about our Trust or partner organisation.

9.5 Staff members must not use social media and the internet in any way to attack, insult, abuse or defame pupils, their family members, colleagues, other professionals, other organisations, or our Trust.

9.6 The ATT logo, academy logo or intellectual property may not be used in connection with any blogging or social networking activity without permission from the Principal/Trust.

9.7 No post should cause others embarrassment or harm.

Personal use of Social Media

9.8 Staff members must not knowingly have contact through personal social media with any pupil, across our Trust, unless the pupils are family members.

9.9 Employees should ensure that they adopt suitably high security settings on any personal profiles they may have.

9.10 Employees must exercise caution in their use of all social media or any other web based presence that they may have, including written content, videos or photographs, and views expressed either directly or by liking, sharing certain pages or posts established by others. This may also include the use of dating websites where employees could encounter pupils either with their own profile or acting covertly.

9.11 Staff members must not have any contact with pupils' family members through personal social media if that contact is likely to constitute a conflict of interest or call into question their objectivity.

9.12 If staff members wish to communicate with pupils through social media sites or to enable pupils to keep in touch with one another, they can only do so with the approval of our Trust (where applicable) and through official sites created.

9.13 Staff members must not allow anyone they can identify as a pupil to follow them or accept friend requests. If any such requests from pupils who are not family members, are received they must discuss this with our Trust or academy Designated Safeguarding Lead. They can be directed to follow our corporate social media accounts.

9.14 On leaving our Trust, staff members must not contact Trust pupils by means of personal social media sites. Similarly, staff members must not contact children and young people from their former academy by means of personal social media sites.

9.15 Photographs, videos or any other types of digital images depicting pupils wearing uniforms or clothing with academy logos or images identifying academy premises must not be published on staff members' personal web space or personal social media sites.