Staploe Education Trust

ICT, Internet, Cyber Security and Acceptable Use policy

Version:	V4.1
Author:	ICT Systems & Strategy Manager
Approved by:	Infrastructure Committee
Date:	Summer 2023
Review date:	Summer 2024

Contents

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, the Governance Team, volunteers and visitors. It supports both teaching and learning, and the pastoral and administrative functions of the Trust.

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

This policy aims to:

- Set guidelines and rules on the use of school ICT resources for staff, pupils, parents and the Governance Team
- 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, cyber security 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 the Governance Team, staff, pupils, volunteers, contractors and visitors.

Breaches of this policy may be dealt with under our Student Behaviour policies and the Staff code of conduct.

2. Relevant legislation and guidance

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

- Data Protection Act 2018
- The UK 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 2021
- Searching, screening and confiscation: advice for schools
- National Cyber Security Centre (NCSC)
- Education and Training (Welfare of Children Act) 2021

The revised core standards for teachers (implemented September 2012), regarding expected behaviour in and outside of school, and the 7 principles of public life ('Nolan Principles'), form an integral part of this policy and apply to all school staff and Users. Users are also reminded that all School policies and contracts apply at all times, particularly in this instance Acceptable Use of ICT, Code of Conduct and Safeguarding policies.

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 to use the ICT facilities, including the Governance Team, 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 school to perform systems administration and/or monitoring of the ICT facilities

“Materials”: files, data and content 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 4 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).

Unacceptable use of the Trust’s ICT facilities includes but is not limited to:

- 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 ICT Systems & Strategy Manager 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.

4.1.1. Exceptions from unacceptable use

Where the use of the Trust's ICT facilities (on the school 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 ICT System & Strategy Manager's discretion.

Please email ICTSystemsandStrategyManager@staploeeducationtrust.org.uk with any requests.

4.1.2. Sanctions

Pupils and staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with the Trust's policies on student Behaviour and Staff code of conduct.

Sanctions will be decided by the ICT Systems & Strategy Manger in conjunction with the Headteacher and may range from removal of access to ICT services for an amount of time, to referral to the police depending on the nature of the activity.

4.1.3. Internet Access

The Trust's internet connections are secured, including the use of recognised filtering products. Users should not attempt to circumvent this protection. Users should be aware that filters aren't fool-proof and should report any unexpected filtering to the ICT Services Team. Filtering levels will be based user accounts and/or devices and will be filtered appropriately for the intended uses.

5. Staff (including the Governance team, volunteers, and contractors)

5.1.1. Access to school ICT facilities and materials

The Trust's ICT Systems & Strategy Manager 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 ICT Helpdesk.

5.1.2. 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 or protected 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 the Trust's 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 as set out in section 4.

5.1.3. Personal Use

Staff are permitted to occasionally use the Trust's 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 Systems & Strategy Manager 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;
- Constitute 'unacceptable use', as defined in section 4;
- Take place when pupils are present;
- 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 are also permitted to use their personal devices (such as mobile phones or tablets) in line with the Trust's mobile phone policy.

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 and use of email (see section 5.1.1) to protect themselves online and avoid compromising their professional integrity.

5.1.4. 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, taking into consideration all policies, advice and guidance.

5.1.5. 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, and take such precautions as the ICT Systems & Strategy Manager may require 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.

The Trust's Data Protection Policy can be found on the Trust website.

5.1.6. School social media accounts

The Trust and schools have official Social Media pages. 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 accounts must ensure they abide by these guidelines at all times.

5.1.7. Monitoring of school 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, the monitoring of:

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

Only authorised ICT Services 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 school 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

6.1.1. Access to ICT facilities

There are shared computers available to pupils, either in specific computer rooms or from mobile units such as laptop/tablet trolleys. These are available during lesson times under staff supervision or for specific activities outside of lesson times with appropriate staff permission. Pupils may have remote access to online ICT Facilities from outside of school where necessary.

6.1.2. Search and deletion

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

The Trust 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 Trust's rules.

Staff members may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse contains digital element.

6.1.3. Unacceptable use of ICT and the internet outside of school

The Trust will sanction pupils, in line with the behaviour policies, if a pupil engages in any of the following at any time (even if they are not on school premises):

- Using ICT facilities or the internet to breach intellectual property rights or copyright
- Using ICT facilities 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

Sanctions are set out in Section 4.2

7. Parents

7.1.1. Access to ICT facilities and materials

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

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

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

7.1.2. Communicating with or about the school 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 Trust through our website and social media channels.

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

8.1.1. Passwords

All users of the Trust's ICT facilities should set strong passwords for their accounts and keep these passwords secure. Guidance on the effective use of strong passwords can be obtained from the ICT Services Team.

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.

Guidance on the effective use of strong usernames and passwords can be obtained from the ICT Services Team.

8.1.2. 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 meet these minimum requirements.

8.1.3. Data Protection

All personal data must be processed and stored in line with data protection regulations. The Trust's data protection policy which can be found on the Trust website.

8.1.4. 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 ICT Systems & Strategy Manager.

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 ICT Systems & Strategy Manager 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.

8.1.5. 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 school if they have been specifically authorised to do so by the ICT Systems & Strategy Manager.

Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption, as defined by the ICT Systems & Strategy Manager.

9. Protection from cyber attacks

Please see the glossary (Appendix 4) to help you understand cyber security terminology.

The Trust will:

- Work with the Governance team and the ICT Services 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) on the basics of cyber security.
- 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, 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 date and secure as they can be
- Back up critical data and store these backups on devices/systems that aren't connected to the Trust's network and which can be stored off the school premises as required.

- Delegate specific responsibility for maintaining the security of our management information system (MIS) to Cambridgeshire County Council's ICT Service
- Make sure ICT Services 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 either the Cyber Essentials or ISO 27001 certification.
- Review and test the cyber response plan with ICT Services, for example, including how the Trust will communicate with everyone if communications go down, who will be contacted when, and who will notify the relevant agencies and authorities. This will be reviewed and tested regularly and after a significant event has occurred, using the NCSC's 'Exercise in a Box'

10. Policy Monitoring and review

The ICT Systems & Strategy Manager 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 year.

11. Related Policies

This policy should be read alongside the Trust/School policies on:

- Safeguarding and Child Protection
- Behaviour
- Code of Conduct for All Adults
- Data Protection
- Mobile Phones

Appendix 1: Acceptable use agreement for staff, governors, volunteers and visitors

Acceptable use of the Trust's ICT facilities and the internet: agreement for staff, governors, volunteers and visitors	
Name:	
When using the Trust's ICT facilities and accessing the internet in school, or outside of the schools, 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 • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software on, 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 staff, or other members of the community • Access, modify or share data I'm not authorised to access, modify or share • Promote private businesses, unless that business is directly related to the 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 outside of the Trust, 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 Systems & Strategy Manager know if anyone 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.	
Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 2: Acceptable use agreement for older pupils

Acceptable use of the school's ICT facilities and internet: agreement for pupils	
Name:	
When using the school's ICT facilities and accessing the internet in school, I will not: • Use them for a non-educational purpose • Use them without a teacher being present, or without a teacher's permission • Use them to break school rules • Access any inappropriate websites • Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity) • Open any attachments in emails, or follow any links in emails, if they are from anyone I don't recognise without first checking with a teacher • Use any inappropriate language • 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 school's network using someone else's details • Bully other people I understand that the Trust will monitor the websites I visit and my use of the Trust's ICT facilities and systems, including printing, email and online meeting spaces. I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others. I will always use the Trust's ICT systems and internet responsibly. I understand that the school can discipline me if I do certain unacceptable things online, even if I'm not in school when I do them.	
Signed (pupil):	**Date:**

Appendix 3: Acceptable use agreement for younger pupils

Acceptable use of the school's ICT facilities and internet: agreement for pupils and parents/carers	
Name of pupil:	
When I use the school's ICT facilities (like computers and equipment) and get on the internet in school, I will not: • Use them without asking a teacher first, or without a teacher in the room with me • Use them to break school rules • Go on any inappropriate websites • Go on Facebook, Instagram, Twitter, TikTok or other social networking sites • Open any attachments in emails, or follow any links in emails, if they are from anyone I don't know without first checking with a teacher • Use mean or rude language when talking to other people • Send any photos, videos or livestreams of people (including me) who aren't wearing all of their clothes • Share my password with others or log in using someone else's name or password • Bully other people I understand that the school will check the websites I visit and how I use the school's computers and equipment. This is so that they can help keep me safe and make sure I'm following the rules. I will tell a teacher or a member of staff I know immediately if I find anything on a school computer or online that upsets me, or that I know is mean or wrong. I will always be responsible when I use the school's ICT systems and internet. I understand that there may be consequences if I do certain unacceptable things online, even if I'm not in school when I do them.	
Signed (pupil):	**Date:**
Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 4: 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.

TERM	DEFINITION
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.