Acceptable Use of the Internet and IT Systems Policy

Policy Code:	IT1
Policy Start Date:	February 2024
Policy Review Date:	February 2025

Contents:

Statement of intent

The Trust believes that ICT plays an important part in both teaching and learning over a range of subjects, and the Trust accepts that both Trust-owned and, on occasions, personal electronic devices are widely used by members of staff. The Trust is committed to ensuring that both staff and pupils have access to the necessary facilities and support to allow them to carry out their work.

The Trust has a sensible and practical approach that acknowledges the use of devices, and this policy is intended to ensure that:

- Members of staff are responsible users and remain safe while using the Internet.
- Trust ICT systems and users are protected from accidental or deliberate misuse which could put the security of the systems and/or users at risk.
- Members of staff are protected from potential risks in their everyday use of electronic devices by security systems including anti-virus, Internet filtering, two-form authentication and other cyber security systems.

Personal use of ICT equipment and personal devices is permitted at the Trust; however, this is strictly regulated and must be done in accordance with this policy, and the Social Media Policy and Online Safety Policy.

This policy applies to all employees, volunteers, supply staff and contractors using CIT ICT facilities.

In using ICT, you will follow the Trust's ethos and consider the work and feelings of others. You must not use the system in a way that might cause annoyance or loss of service to other users.

1. Legal framework

This policy has due regard to all relevant legislation and statutory guidance including, but not limited to, the following:

- Data Protection Act 2018
- Computer Misuse Act 1990
- Communications Act 2003
- Freedom of Information Act 2000
- Human Rights Act 1998
- Voyeurism (Offences) Act 2019
- The UK General Data Protection Regulation (UK GDPR)

This policy operates in conjunction with the following Trust policies:

- Data Protection Policy
- Freedom of Information Policy
- Complaints Policy
- Disciplinary Policy
- Photography Policy
- Financial Management Policy
- Records Management Policy

2. Roles and responsibilities

The Trust Board has the responsibility for the overall implementation of this policy, ensuring it remains compliant with relevant legislation.

The Strategic Lead of Technology (Lead IT) is responsible for:

- Reviewing and amending this policy with the Central ICT Team and Data Protection Officer (DPO), taking into account new legislation, government guidance and previously reported incidents to improve procedures.
- The day-to-day implementation and management of the policy.
- The overall allocation and provision of resources.
- Handling complaints regarding this policy as outlined in the Trust's Complaints Policy.
- Informing staff that the Trust reserves the right to access personal devices for the purpose of ensuring the effectiveness of this policy.

The Central ICT team is responsible for:

- Carrying out regular checks on Internet activity of all user accounts and to report any inappropriate use to the Lead IT.
- Monitoring the computer logs on the Trust's network and to report any logged inappropriate use to the Headteacher, line manager and Lead IT.
- Remotely viewing or interacting with any of the computers on the Trust's network. This may be done randomly to implement this policy and to assist in any difficulties.
- Ensuring routine security checks are carried out on all Trust-owned and personal devices that are used for work purposes to check that appropriate security measures and software have been updated and installed.
- Ensuring that, though appropriate steps will be taken to ensure personal information is not seen during security checks, staff are made aware of the potential risks.
- Accessing files and data to solve problems for a user with their authorisation.

- Adjusting access rights and security privileges in the interest of the protection of the Trust's data, information, network and computers.
- Adjusting access rights to shared drives will only be implemented once line managers have approved access.
- Disabling user accounts of staff who do not follow this policy at the request of the Headteacher, line manager and Lead IT.
- Assisting the Headteacher or line manager in all matters requiring reconfiguration of security and access rights and in all matters relating to this policy.
- Assisting staff with authorised use of the ICT facilities and devices if required and once approved by line managers.
- Immediately reporting any breach of personal devices to the DPO and Lead IT.

The DPO will work closely with the ICT technical staff:

- Ensuring that all Trust-owned and personal electronic devices have security software installed to protect sensitive data in cases of loss or theft. For example, appropriate security on personal mobile phones for the use of two-form authentication.
- Ensuring that all Trust-owned devices are secured and encrypted in line with the Trust's Data Protection Policy.
- Ensuring that all devices connected to the Trust's network and Internet have appropriate security.
- Ensuring all staff are aware of, and comply with, the Data Protection principles outlined in the Trust's Data Protection Policy.

Staff members are responsible for:

- Requesting permission from the Headteacher, line manager or Lead IT, subject to their approval, before using Trust-owned devices for personal reasons during school hours.
- Requesting permission to loan Trust equipment from the Lead IT.
- Requesting permission from the Headteacher or line manager, subject to their approval, before using personal devices during working hours and ensuring these devices are submitted for security checks on a regular basis.
- Reporting misuse of ICT facilities or devices by staff or pupils to the Headteacher, line manager or Lead IT.
- Reading and signing a Device User Agreement to confirm they understand their responsibilities and what is expected of them when they use Trust-owned and personal devices.

The Central ICT Team are responsible for the maintenance and day-to-day management of the equipment. The Lead IT is responsible for the device loans process.

The Lead IT is responsible for:

- Maintaining a Fixed Asset Register to record and monitor the Trust's assets.
- Ensuring value for money is secured when purchasing electronic devices.
- Monitoring purchases made under the Financial Management Policy.
- Overseeing purchase requests for electronic devices.

3. Classifications

Trust-owned and personal devices or ICT facilities include, but are not limited to, the following:

- Computers, laptops and software

- Monitors
- Keyboards
- Mouses
- Scanners
- Cameras, still and video
- Other devices including furnishings and fittings used with them
- Mail systems (internal and external)
- Internet and intranet (email, web access and video conferencing)
- Telephones (fixed and mobile)
- Tablets and other portable devices
- Computers
- Photocopying, printing and reproduction equipment
- Recording and playback equipment
- Documents and publications (any type of format)

4. Acceptable use

This policy applies to any computer or other device connected to the Trust's network and computers.

The Lead IT will monitor the use of all ICT facilities and electronic devices. Members of staff will only use Trust-owned and approved personal devices for work duties and educational purposes. The duties for which use is permitted include, but are not limited to, the following:

- Preparing work for lessons, activities, meetings, reviews, etc.
- Researching any school-related task
- Any school-encouraged tuition or educational use
- Collating or processing information for school business
- Communicating with other members of staff, such as contacting the school office for assistance.
- Other general Trust-related work.

Inappropriate use of Trust-owned and personal devices could result in a breach of the Trust's Data Protection Policy.

Inappropriate use of Trust-owned and personal devices could result in a breach of legislation, including the UK GDPR and Data Protection Act 2018.

Any member of staff found to have breached the Trust's Data Protection Policy or relevant legislation will face disciplinary action.

Staff will always be an example of good practice to pupils, serving as a positive role model in the use of ICT and related equipment.

Since ICT facilities are also used by pupils, the school will have acceptable use agreements in place for pupils – staff will ensure that pupils comply with these.

Pupils found to have been misusing the ICT facilities will be reported to the Headteacher and appropriate measures taken.

Trust-owned electronic devices will not be used to access any material which is illegal, inappropriate, or may cause harm or distress to others.

Any illegal, inappropriate or harmful activity will be immediately reported to the Headteacher and Lead IT.

Members of staff will not:

- Open email attachments from unknown sources.
- Use programmes or software that may allow them to bypass the filtering or security systems.
- Upload or download large capacity files without permission from the Central ICT Team.
- Give their home address, phone number, social networking details or email addresses to pupils or parents – contact with parents will be conducted through authorised school contact channels.
- Take their allocated classroom mobile phone out of the school premises, unless permitted by the Headteacher.

All data will be stored appropriately in accordance with the Trust's Data Protection Policy.

Members of staff will only use Trust-owned electronic devices to take pictures or videos of people who have given their consent.

Staff allocated with a Trust-owned electronic device such as a mobile phone may use it to access personal social media accounts; however, they must adhere to guidance set out within the Trust's Social Media Policy.

Personal electronic devices will not be used to communicate with pupils or parents, including via social media.

Staff will ensure they:

- Express neutral opinions when representing the Trust online.
- Avoid disclosing any confidential information or comments regarding the Trust, or any information that may affect its reputability.
- Have the necessary privacy settings applied to any social networking sites.

Images or videos of pupils, staff or parents will only be published online for the activities which consent has been sought.

Copyrighted material will not be downloaded or distributed.

Trust-owned devices may be taken home for work purposes where remote access to the Trust network will be given to staff using these devices at home.

Trust equipment that is used outside the premises, e.g. laptops, will be returned to the Trust when the employee leaves employment, or if requested to do so by the Headteacher or line manager.

While there is scope for staff to utilise Trust equipment for personal reasons, this will not be done during working hours unless approved by the Headteacher or line manager, or in the case of a personal emergency.

Private business will not be mixed with official duties, e.g. work email addresses will be reserved strictly for work-based contacts only.

Use of a Trust-owned phone for personal use will be permitted for necessary or emergency calls.

Personal use of Trust-owned equipment can be denied by the Headteacher, line manager or Lead IT at any time. This will typically be because of improper use or over-use of Trust facilities for personal reasons.

Where permission has been given to use the Trust equipment for personal reasons, this use will take place during the employee's own time, e.g. during lunchtime or after school/work. Where this is not possible, or in the case of an emergency, equipment can be used for personal reasons during work hours, provided that disruption to the staff member's work and the work of others is minimal.

Abuse of ICT facilities or devices could result in privileges being removed. Staff will be aware of acceptable ICT use and misuse of the facilities as defined in this policy will be reported to the Headteacher, line manager and Lead IT.

Failure to adhere to the rules described in this policy may result in disciplinary action in line with the Disciplinary Policy and procedures.

5. Emails and the Internet

The Trust email system and Internet connection are available for communication and use on matters directly concerned with Trust business.

Where possible, emails should not be used as a substitute for face-to-face communication, unless it is otherwise impossible.

Unprofessional messages will not be tolerated. All emails will be written in a professional tone and will be proofread by the staff member sending the email to ensure this prior to sending.

Abusive messages will not be tolerated – any instant of abuse may result in disciplinary action.

If any email contains confidential information, the user will ensure that the necessary steps are taken to protect confidentiality.

The Trust will be liable for any defamatory information circulated either within an academy or to external contacts.

The Trust email system and accounts will never be registered or subscribed to spam or other non-work-related updates, advertisements or other personal communications. Trust email addresses will not be shared without confirming that they will not be subjected to spam or sold on to marketing companies.

All emails being sent to external recipients will contain a signature set by the Communications Team and will not be removed.

Personal email accounts will only be accessed via Trust computers outside of work hours and only if they have built-in anti-virus protection approved by the Central ICT Team. Staff will ensure that access to personal emails never interferes with work duties.

The types of information sent through emails to a personal device will be limited to ensure the protection of personal data, e.g. pupils' details.

Contracts sent via email or the Internet are as legally binding as those sent on paper. An exchange of emails can lead to a contract being formed between the sender, or the Trust, and the recipient. Staff will never commit the Trust to any obligations by email or the Internet without ensuring that they have the authority to do so.

Purchases for Trust equipment will only be permitted to be made online with the permission of the Headteacher or line manager, and a receipt will be obtained in order to comply with monitoring and accountability. Hard copies of the purchase will be made for the purchaser. This is in addition to any purchasing arrangement followed according to the Trust's Financial Management Policy.

Any suspicious emails will be reported to the Lead IT and Central ICT Team.

6. Portable equipment

All data on Trust-owned equipment will be synchronised with the Trust server and backed up daily.

Portable Trust-owned electronic devices should be kept securely when used off site and shut down or password protected when not in use.

Portable equipment will be transported in its protective case, if supplied.

Where the Trust provides mobile technologies, such as phones, laptops for off-site visits and trips, staff will only use these devices and ensure they are locked when not in use.

Parents will be discouraged from calling the phones. In emergencies, parents will contact a school's emergency contact number, not the classroom phone. Parents will be permitted to text the number for justified reasons, such as being late to collect a child at the end of the day.

Parents will be asked to consent to providing their phone numbers to the school, which will be kept in on the school MIS system. This will be used to identify the number, protecting against safeguarding risks as the caller can be easily identified, and to track parents who may be abusing the system.

7. Personal devices

Staff members will use personal devices in line with the Trust policies.

Members of staff will not contact pupils or parents using their personal devices.

Personal devices will only be used for off-site educational purposes when mutually agreed with the Headteacher.

Inappropriate messages will not be sent to any member of the Trust community.

Permission will be sought from the owner of a device before any image or sound recordings are made on their personal device. Consent will also be obtained from staff, pupils and other visitors if photographs or recordings are to be taken.

Members of staff bringing personal devices into school will ensure that there is not any inappropriate or illegal content on their device.

During lesson times, unless required for the teaching activity being undertaken, personal devices will be locked away.

8. Removable media

Only recommended removable media will be used including, but not limited to, the following:

- USB drives
- DVDs
- CDs

All removable media will be securely stored when not in use.

Personal and confidential information will not be stored on any removable media.

The Central ICT Team will encrypt all removable media with appropriate security measures.

Removable media will be disposed of securely by the Central ICT Team.

9. Cloud-based storage

Data held in remote and Cloud-based storage is still required to be protected in line with the UK GDPR and DPA 2018; therefore, members of staff will ensure that Cloud-based data is kept confidential and no data is copied, removed or adapted.

10. Storing messages

Emails and messages stored on Trust-owned devices will be stored digitally or in a suitable hard copy file and disposed of in line with the Records Management Policy.

Information and data on the Trust's network and computers will be kept in an organised manner and should be placed in a location of an appropriate security level.

If a member of staff is unsure about the correct message storage procedure, help will be sought from the Central ICT Team.

Employees who feel that they have cause for complaint as a result of any communications on Trust-owned devices will raise the matter initially with the Headteacher, line manager and/or Lead IT as appropriate. The complaint will then be raised through the grievance procedure in line with the Grievance Policy.

11. Unauthorised use

Staff will not be permitted, under any circumstances, to:

- Use the ICT facilities for commercial or financial gain without the explicit written authorisation from the Headteacher or line manager.
- Physically damage ICT and communication facilities or Trust-owned devices.
- Relocate, take off-site or otherwise interfere with the ICT facilities without the authorisation of the Central ICT Team, line manager or Headteacher. Certain items are asset registered. Once items are moved after authorisation, staff will be responsible for notifying the Lead IT of the new location. The exception to this point is when items are moved to the designated secure room for insurance purposes over holiday periods.

- Use or attempt to use someone else's user account. All users of the ICT facilities will be issued with a unique user account and password. The password will be changed every 60 days. User account passwords will never be disclosed to or by anyone.
- Use the ICT facilities at any time to access, download, send, receive, view or display any of the following:
    - Any material that is illegal.
    - Any message that could constitute bullying, harassment (including on the grounds of sex, race, religion/religious belief, sexual orientation or disability) or any negative comment about other persons or organisations.
    - Online gambling.
    - Remarks which may adversely affect the reputation of any organisation or person, whether or not you know them to be true or false.
    - Any sexually explicit content, or adult or chat-line phone numbers.
- Generate messages or documents that appear to originate from someone else, or otherwise impersonate someone else.
- Install hardware or software without the consent of the Central ICT Team, Lead IT, line manager or the Headteacher.
- Introduce any form of stand-alone software or removable hardware likely to cause malfunctioning of the ICT facilities or that will bypass, over-ride or overwrite the security parameters on the network or any of the Trust's computers.
- Use or attempt to use the Trust's ICT facilities to undertake any form of piracy, including the infringement of software licenses or other copyright provisions whether knowingly or not. This is illegal.
- Purchase any ICT facilities without the consent of the Central ICT Team, line manager or Headteacher. This is in addition to any purchasing arrangements followed according to the Financial Management Policy.
- Use or attempt to use the Trust's phone lines for Internet or email access unless given authorisation by the Headteacher, line manager or Lead IT. This will include using or attempting to use any other form of hardware capable of telecommunication, regardless of ownership.
- Use any chat-lines, bulletin boards or pay-to-view sites on the Internet. In addition, staff will not download or attempt to download any software of this nature.
- Use the Internet for any auctioning activity or to purchase items unless given authority to do so by the Headteacher or line manager. This is in addition to any purchasing arrangement followed according to the Financial Management Policy.
- Knowingly distribute or introduce a virus or harmful code onto the Trust's network or computers. Doing so may result in disciplinary action, including summary dismissal.
- Use the ICT facilities for personal use without the authorisation of the Headteacher or line manager. This authorisation will be requested on each occasion of personal use.
- Copy, download or distribute any material from the Internet or email that may be illegal to do so. This can include computer software, music, text and video clips. If a staff member is not clear that they have permission to do so, or if the permission cannot be obtained, they will not download the material.
- Use or attempt to use the communication facilities to call overseas without the authorisation of the Headteacher or line manager.
- Obtain and post on the Internet or send via e-mail any confidential information about other employees, the Trust, its customers or suppliers.
- Interfere with someone else's use of the ICT facilities.
- Be wasteful of ICT resources, particularly printer ink, toner and paper.
- Use the ICT facilities when it will interfere with their responsibilities to supervise pupils.
- Share any information or data pertaining to other staff or pupils at the Trust with unauthorised parties. Data will only be shared for relevant processing purposes.

- Operate equipment to record an image beneath a person's clothing with the intention of observing or enabling another person to observe.

Any unauthorised use of email or the Internet will likely result in disciplinary action, including summary dismissal, in line with the Disciplinary Policy and procedure.

If a member of staff is subjected to, or knows about harassment, upskirting or bullying that has occurred via staff email or through the use of Trust-owned devices, they will report this immediately to the Headteacher, line manager and Lead IT.

12. Purchasing

Funding for electronic devices, predetermined by the Executive Leadership Team (ELT), will be available each year, based on need and refresh requirements.

Requests for equipment or electronic devices will be made in writing to the Finance staff using the Purchase Request Form.

Requests will be submitted in sufficient detail for an informed decision to be made.

Requests will be responded to within three working days. If sufficient detail is not provided or other conditions specified by the Finance staff are not met, the request will not be processed.

Requests made for equipment or electronic devices that exceed the predetermined amount allocated will require discussion and authorisation by the ELT.

Individual staff members will not be permitted to purchase equipment or devices, or process payments for such goods, on the Trust's behalf unless permission has been sought from the Lead IT.

The cost of any equipment or devices personally purchased by staff members will not be reimbursed by the Trust, unless otherwise specified by the Lead IT.

In relation to devices for a specific project, project budget holders will provide evidence and a written statement requesting the necessary funds for the equipment required.

The Lead IT will seek three written quotes for all IT equipment or, where applicable, use an official purchasing framework.

All equipment and electronic devices will be sourced from a reputable supplier.

The Lead IT will maintain a Fixed Asset Register which will be used to record and monitor the Trust's assets. All equipment and electronic devices purchased using Trust funds will be added to this register.

When devices are not fit for purpose, or are at least four years old, staff members may request new equipment. If their request is granted, the old equipment or electronic device will be returned to the IT staff, including any accessories which were originally included with the device. Any old devices will then be disposed of or wiped clear by the Central ICT Team and recycled by an official registered IT recycling company.

13. Safety and security

The Trust's network will be secured using firewalls in line with new DfE guidance, National Cyber Security Centre and other reputable IT security company guidelines.

Filtering of websites using the current filtering software, Securly, will ensure that access to websites with known malware are blocked immediately and reported to the Central ICT Team.

Approved anti-virus software and malware protection will be used on all approved devices and will be updated on a regular basis.

The Trust will use mail security technology to detect and block any malware transmitted via email – this will be reviewed on a regular basis.

Members of staff will ensure that all Trust-owned electronic devices are made available for anti-virus updates, malware protection updates and software installations, patches or upgrades, on a regular basis. All updates can be installed remotely and automatically.

Approved personal devices, for example mobile phones, will be checked when required by the Central ICT Team so that appropriate security and software updates can be installed to prevent any loss of data. Consent for such access will be obtained before the approval of a device – if consent if refused, the Trust reserves the right to decline a request to use a personal device.

Programmes and software will not be installed on Trust-owned electronic devices without permission from the Central ICT Team and Lead IT.

Staff will not be permitted to remove any software from a Trust-owned electronic device without permission from the Central ICT Team and Lead IT.

Members of staff who install or remove software from a Trust-owned electronic device without seeking authorisation from the Central ICT Team may be subject to disciplinary measures.

All staff account logins will be secured by a password and two-form authentication enabled. However, two-form authentication is only enabled when devices are used off site.

Passwords will be kept confidential and must not be shared with pupils, unauthorised members of staff or third parties.

Devices will be configured so that they are automatically locked after being left idle for a set time. In addition, all laptops will be locked when the screen is closed.

All devices must be encrypted using a method approved by the Lead IT.

13. Loss, theft and damage

For the purpose of this policy, "damage" is defined as any fault in a Trust-owned electronic device caused by the following:

- Connections with other devices, e.g. connecting to printers which are not approved by the Central ICT Team
- Unreasonable use of force
- Abuse
- Neglect
- Alterations
- Improper installation

The Trust insurance will cover Trust-owned electronic devices that are damaged or lost during working hours if they are being used on Trust premises.

Staff members will use Trust-owned electronic devices within the parameters of the Trust's insurance cover.

Any incident that leads to a Trust-owned electronic device being lost will be treated in the same way as damage.

The Lead IT will decide whether a device has been damaged due to the actions described above.

The Central ICT Team will be contacted if a Trust-owned electronic device has a technical fault.

In cases where a member of staff repeatedly damages Trust-owned electronic devices, the Lead IT may decide to permanently exclude the member of staff from accessing devices.

If a Trust-owned device is lost or stolen, or is suspected of having been lost or stolen, the Lead IT and DPO will be informed as soon as possible to ensure the appropriate steps are taken to delete data from the device that relates to the Trust, its staff and its pupils, and that the loss is reported to the relevant agencies.

The Trust will not be responsible for the loss, damage or theft of any personal device, including phones, cameras, tablets, removable media, etc.

14. Implementation

Staff will report any breach of this policy to the Lead IT.

Regular monitoring and recording of email messages will be carried out on a random basis.

Hard copies of email messages can be used as evidence in disciplinary proceedings.

Use of the telephone system will be logged.

Use of the Trust Internet connection will be recorded and monitored.

The Lead IT will conduct random checks of Trust-based equipment.

The Central ICT Team will check computer logs on the Trust network on a regular basis.

Unsuccessful and successful log-ons will be logged on every computer connected to the Trust's network.

Unsuccessful and successful software installations, security changes and items sent to the printer will also be logged.

The Central ICT Team may remotely view or interact with any of the computers on the Trust's network. This may be used randomly to implement this policy and to assist in any difficulties.

The Trust's network has anti-virus software installed with a centralised administration package; any virus found will be logged to this software package.

The Trust's database systems are computerised. Unless given permission by the Headteacher or line manager, members of staff will not access the system. Failure to adhere to this requirement may result in disciplinary action.

All users of the database system will be issued with a unique individual password, which will be changed on a regular basis. Staff will not, under any circumstances, disclose this password to any other person.

Attempting to access the database using another employee's user account and/or password without prior authorisation will likely result in disciplinary action, including summary dismissal.

User accounts will be accessible by the Headteacher, line manager, Central ICT Team and Lead IT.

Users will ensure that critical information is not stored solely within the Trust's computer system. Hard copies will be kept or stored separately on the system. If necessary, documents will be password protected.

Users will be required to familiarise themselves with the requirements of the UK GDPR and Data Protection Act 2018, and to ensure that they operate in accordance with the requirements of the regulations and the Data Protection Policy.

Any breach of the rules in this policy may result in disciplinary action, which may lead to dismissal.

A misuse or breach of this policy could also result in criminal or civil actions being brought against the persons involved or the Trust.

15. Monitoring and review

This policy will be reviewed annually by the Lead IT.

Any changes or amendments to this policy will be communicated to all staff members by the Lead IT.