BRIGANTIA
LEARNING TRUST
Creating Excellence Together, through a culture of care

ICT AND INTERNET ACCEPTABLE USE POLICY

June 2024

Document Control

Title:	ICT and Internet Acceptable Use Policy
Policy Lead:	COO
Category:	IT
Date Approved:	10/07/2024
Approved by:	Trustees
Review Date:	01/07/2025
Review Period:	Annually
Status:	Non-Statutory
Website:	Yes/No
Annual Agreement:	Yes/No

Review

Date:	Version:	Author:	Revisions:
20/02/2023	1	SM	
01/06/2024	2	AK	Updated 5.2 to include 'Code of Conduct'
			Removed Section 5.3 – Remote Access - and added Section 8 - Remote Systems

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 (including senior leadership teams), Trustees, volunteers, and visitors. It supports teaching and learning, pastoral, and administrative functions of the Trust.

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

This policy aims to:

- Set guidelines and rules on the use of Trust ICT resources for staff, pupils, parents and Trustees
- 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 Trustees, staff, pupils, volunteers, contractors, and visitors.

Breaches of this policy may be dealt with under our disciplinary policy/behaviour policy/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 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 2022

Searching, screening and confiscation: advice for Trust's

National Cyber Security Centre (NCSC)

Education and Training (Welfare of Children Act) 2021

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 Trustees, staff, pupils, volunteers, contractors and visitors.

"Personal use": any use or activity not directly related to the users' employment, study or purpose.

"Authorised personnel": employees authorised by the Trust to perform systems administration and/or monitoring of the ICT facilities.

"Materials": files and data created using the ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites and blogs.

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. Unacceptable use of the Trust's ICT facilities includes:

- Using the Trust's ICT facilities to breach intellectual property rights or copyright
- Using the Trust's ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the Trust's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Online gambling, inappropriate advertising, phishing and/or financial scams
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate or harmful
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams (also known as sexting or youth-produced sexual imagery)
- Activity which defames or disparages the Trust, or risks bringing the Trust into disrepute
- Sharing confidential information about the Trust, its pupils, or other members of the Trust community
- Connecting any device to the Trust's ICT network without approval from authorised personnel
- Setting up any software, applications or web services on the Trust's network without approval by authorised personnel, or creating or using any program, tool or item of software designed to interfere with the functioning of the ICT facilities, accounts or data
- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging or enabling others to gain (or attempt to gain) unauthorised access to the Trust's ICT facilities
- Causing intentional damage to ICT facilities
- Removing, deleting or disposing of ICT equipment, systems, programs or information without permission by authorised personnel

- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
- Using inappropriate or offensive language
- Promoting a private business, unless that business is directly related to the Trust
- Using websites or mechanisms to bypass the Trust's filtering mechanisms such as proxy servers and VPN's
- Engaging in content or conduct that is radicalised, extremist, racist, anti-Semitic or discriminatory in any other way

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

Pupils and staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with the Trust's behaviour policy and staff code of conduct.

5. Staff (including Trustees, volunteers, and contractors)

5.1 Access to Trust ICT facilities and materials

The Trust's Technical Team manages access to the Trust's ICT facilities and materials for Trust staff. That includes, but is not limited to:

- Computers, tablets, mobile phones, smart watches, 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 their line manager

5.1.1 Use of phones, communication software and email

The Trust provides each member of staff with an email address, this 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.

Electronic 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 and avoid wherever possible sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient.

If staff receive an email in error, the sender should be informed, and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.

If staff send an email in error, that contains the personal/confidential information , they must inform their line manager and the trust Senior Compliance and Operations Officer immediately. All breaches however small must be reported.

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.

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

5.2 Personal use

Staff are permitted to occasionally use Trust ICT facilities for personal use subject to certain conditions set out below. Personal use of ICT facilities must not be overused or abused. The Trust 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 4
- Takes place when no pupils are present
- Does not interfere with their jobs, or prevent other staff or pupils from using the facilities for work or educational purposes

Staff may not use the Trust's network 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) providing they do not contravene section 4.

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

5.2.1 Personal social media accounts

Members of staff should ensure their use of social media, either for work or personal purposes, is appropriate at all times and complies with the social media policy.

6. Pupils

6.1 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 pornographic images or any other 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 an online element.

6.2 Unacceptable use of ICT and the internet outside of Trust

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

7. Parents

7.1 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 headteacher's discretion.

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

7.2 Communicating with or about the Trust 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.

We ask parents to sign the agreement in appendix 2.

8. Remote Systems

The Trust allow users to access the Trust's ICT facilities and materials remotely via various cloud-based systems.

Users accessing the Trust's ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on-site.

Any member of staff using remote access must do so responsibly, safely, and legally, and take all reasonable steps to ensure that the information on screen cannot be seen by anyone else, including family members.

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.

9. 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.

9.1 Passwords

All users of the Trust's ICT facilities should set strong passwords for their accounts and keep these passwords secure.

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

Members of staff 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.

The Trust will generate passwords for pupils using a password manager/generator and keep these in a secure location in case pupils lose or forget their passwords.

Staff must use MFA when directed

9.2 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.

9.3 Data protection

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

9.4 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 Trust

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 teacher or line 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.

9.5 Encryption

The Trust ensures that its devices and systems have an appropriate level of encryption.

Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption, as defined by the Trust.

10. Monitoring of Trust network and use of ICT facilities

The Trust reserves the right to monitor the use of its ICT facilities and network. This includes, but is not limited to, monitoring of:

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

Only authorised ICT staff may inspect, monitor, intercept, assess, record, and disclose the above, to the extent permitted by law.

The Trust monitors ICT use in order to:

- Obtain information related to Trust business
- Investigate compliance with Trust policies, procedures and standards
- Ensure effective Trust and ICT operation
- Conduct training or quality control exercises
- Prevent or detect crime
- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation

11. Monitoring and review

The Trust will 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 annually.

The Trustees is responsible for approving this policy.

12. Related policies

This policy should be read alongside the Trust's policies on:

- Safeguarding
- Network Security
- Acceptable Use Agreement
- Online Safety
- Code of Conduct