

TIBSHELF COMMUNITY SCHOOL ACCEPTABLE USE OF ICT- STUDENTS

Ratified: March 2025
(Tibshelf Policy)





Introduction and aims

Information and communications technology (ICT) is an integral part of the way our school works, and is a critical resource for pupils, staff (including the senior leadership team), governors, volunteers and visitors. It supports teaching and learning, and the pastoral and administrative functions of the school.

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

This policy aims to:

- Set guidelines and rules on the use of school ICT resources for staff, pupils, parents/carers and governors
- Establish clear expectations for the way all members of the school community engage with each other online
- Support the school's policies on data protection, online safety and safeguarding
- Prevent disruption that could occur to the school through the misuse, or attempted misuse, of ICT systems
- Support the school in teaching pupils safe and effective internet and ICT use

This policy primarily focuses on student use of ICT but does incorporate other users of our school's ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors.

Breaches of this policy may be dealt with under our Behaviour for Learning Policy

Monitoring of school network and use of ICT Facilities


The school 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
- User activity/access logs
- Any other electronic communications

Unacceptable use

The following is considered unacceptable use of the school's ICT facilities. Any breach of this policy may result in disciplinary or behaviour proceedings

Unacceptable use of the school's ICT facilities includes:

- Using the school's ICT facilities to breach intellectual property rights or copyright
 - Using the school's ICT facilities to bully or harass someone else, or to promote unlawful discrimination
 - Breaching the school'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
 - Activity which defames or disparages the school, or risks bringing the school into disrepute
 - Sharing confidential information about the school, its pupils, or other members of the school community
 - Connecting any device to the school's ICT network without approval from authorised personnel
- 

- Setting up any software, applications or web services on the school's network without approval by authorised personnel, or creating or using any programme, tool or item of software designed to interfere with the functioning of the school's 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 school's ICT facilities
- Causing intentional damage to the school's ICT facilities
- Removing, deleting or disposing of the school's ICT equipment, systems, programmes or information without permission from authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not permitted by authorised personnel to have access, or without authorisation
- Using inappropriate or offensive language
- Using websites or mechanisms to bypass the school's filtering or monitoring mechanisms
- Engaging in content or conduct that is radicalised, extremist, racist, antisemitic or discriminatory in any other way

Data security

The school is responsible for making sure it has the appropriate level of security protection and procedures in place to safeguard its systems, staff and learners. It therefore takes steps to protect the security of its computing resources, data and user accounts. The effectiveness of these procedures is reviewed periodically to keep up with evolving cyber crime technologies.

Staff, pupils, parents/carers and others who use the school's ICT facilities should use safe computing practices at all times. We aim to meet the cyber security standards recommended by the Department for Education's guidance on [digital and technology standards in schools and colleges](#), including the use of:

- Firewalls
- Security features
- User authentication and multi-factor authentication
- Anti-malware software

Software updates, firewalls and anti-virus software

All of the school's ICT devices that support software updates, security updates and anti-virus products will have these installed, and 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 school's ICT facilities.

Any personal devices using the school's network must all be configured in this way.

Protection from cyber attacks

. The school will:

- Work with governors and the IT department to make sure cyber security is given the time and resources it needs to make the school secure
- Provide annual training for staff on the basics of cyber security, including how to:
 - Check the sender address in an email
 - Respond to a request for bank details, personal information or login details
 - Verify requests for payments or changes to information
- 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 school will verify this using a third-party audit to objectively test that what it has in place is effective
- **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 school needs to update its software
- **Regularly reviewed and tested:** to make sure the systems are as effective and secure as they can be
- Back up critical data at least once a day and store these backups appropriately
- Delegate specific responsibility for maintaining the security of our management information system (MIS) to our provider
- Make sure staff:
- Dial into our network using a virtual private network (VPN) when working from home
- Enable multi-factor authentication where they can, on things like school email accounts
- Store passwords securely ideally using a password manager
- Make sure ICT staff conduct regular access reviews to make sure each user in the school has the right level of permissions and admin rights
- Have a firewall in place that is switched on
- Work with our LA to see what it can offer the school regarding cyber security, such as advice on which service providers to use or assistance with procurement

Internet and Email

Tibshelf Community School provides its students with access to ICT Systems, Services and Facilities. It is policy that all students should have access to software and hardware which enhances their learning experience and provides them with tools for working.

This system provides each student with a password-protected area in which to save their work. Students work is stored on one of our servers and backed up daily.

Members of staff are unable to find out students' passwords, although staff can change them. All students must take care to safeguard their password and not give it out to anyone else. Doing so puts them at risk, of losing their files, internet abuse or email abuse. Students must not use anyone else's Username to log on to the Network.

Passwords must be complex; this must contain at least one uppercase and lowercase letter and one number. The password must also be six characters long and not contain the users name or username; the network will enforce this automatically.

Students must only use the school network for school related work or for activities authorised by a teacher. Students must not attempt to install their own software on our network. Games and executable files are not allowed.

Some Staff have full access to the students' work areas and use this access to mark the students work. Should unsuitable material be found in a student's Work Area, the account will immediately be disabled while the matter is investigated.

Students must not attempt to gain access to network system files, other students', or Staff accounts. Stealing passwords and deleting files can be viewed as a hacking attempt. Both are offences under the Misuse of Computers Act.

Students must not eat or drink near computers.

Printing Policy

All Students will have access to a printer when required; the ICT Department can monitor printouts for unacceptable materials.

Only valid schoolwork that the teacher has asked them to print should be printed.

Students must also take care not to waste resources; printing off whole internet pages is not usually appropriate. All documents printed can be identified by the user who printed them.



Printouts that contravene this policy will result in printing privileges being removed.

Internet Use Policy

Tibshelf School provides Internet access to all students via the network. This is through a 1GB/sec Broadband connection.

The Internet is a powerful learning resource which can greatly enhance the curriculum. However, it is recognised that it also contains a large amount of material which is offensive or unsuitable for students.

Students may only use the Internet when there is a teacher or supervisor in the room.

Our Internet Service Provider filters out most of the unsuitable content. In addition, we use our own filters programs as a further protection. We constantly monitor and update our filters. When accessing the Internet students must not try to download anything that is unlawful, obscene, inappropriate, or abusive.

Any student who is found to be intentionally accessing unsuitable material or downloading games will have their Internet access withdrawn. After the incident has been investigated further action may be taken.

In addition, any student who is found to be using the Internet when they should be doing other work, may also have Internet access withdrawn.

The use of file-sharing utilities can lead to the school being in breach of licence agreements or copyright laws. As this is unacceptable, such utilities are not allowed, and any student using or attempting to use them may have internet access withdrawn. No student should have any executable file in the work area; regular checks are made for these and offenders have network access temporarily withdrawn.

The school has the facility to enable Students access to their work whilst offsite. This policy applies whilst off site and students must not let unauthorised people have access to data whilst offsite.

Students must not use the Internet for buying or selling goods.

Students must not log onto chat sites or messaging programs on the Internet.

Email Policy

Tibshelf School recognises email as an excellent means of communication, which is fast, cheap and does not rely on the recipient being available to read it immediately. In the school situation it can also be used to send work between school and an internet-enabled home.


However, there are also dangers. It is not guaranteed that the email will be read by the intended recipient. It is possible, in fact easy, for a person to pose as someone else, to hide behind an internet identity. Students should not give full names, addresses or telephone numbers in emails. Emails should only be sent using the school's internal email program. Web based email is not allowed.


"Spam" is a common term for junk or bulk email. The school takes steps to filter out as much of this as possible.

Any student found using or attempting to use the school network to send spam will be dealt with severely.

The sending of abusive or defamatory emails will not be tolerated. Email access may be withdrawn in this case. Students must realise that information stored electronically could potentially be used as evidence in court.

The sending of pornographic or otherwise offensive material will not be tolerated. Email access will be withdrawn. If such material is received, students should alert staff who will investigate its source and act accordingly.





The intentional sending of viruses is an offence under the Misuse of Computers Act. Our Internet Service Provider actively filters emails for viruses, and in addition we run antivirus software which is updated daily.

Anyone who is the recipient of Spam or other unwanted/inappropriate e-mails should take appropriate action, Students will initially be taught how to deal with this.

Unwanted Electronic Mail

Unwanted E-mail can arrive from one of two sources, either internally (from an email address within the school) or externally (from an e-mail address outside the school i.e. Yahoo, Hotmail, etc.). You can deal with these in several ways:

Unwanted E-mail from outside the school

You may receive unwanted e-mail from many different sources such as commercial solicitations, worthy causes, and misdirected e-mail. You have several choices on how to respond:

Delete the message from your Inbox without replying. It is often pointless to reply to junk e-mail (spam) asking to be taken off their list. The reply-to address may be bogus, or you may provoke more email by showing that your e-mail address is a real one.

Reputable companies usually offer an e-mail address or Web site through which you can turn on or off their informational e-mail messages. When you register a product you have just purchased, for example, you may be added to their marketing e-mail list. Check the message itself for instructions on how to get off the list or go to the company's Web site.

If the e-mail is obviously a misaddressed personal message, a courteous reply would probably be appreciated.

The UK has laws relating to computer misuse, including junk e-mail. These can be found in the Data Protection Act, the Computer Misuse Act and the Freedom of Information Act

When junk e-mail is consistently coming from the same address, the address can be banned by informing the ICT Operations Manager who will investigate the problem

Unwanted E-mail from an internal source

If you receive unwanted e-mail messages from anyone at School (staff or student):

- Reply to the sender that you would prefer to not receive any further messages.
- If the messages continue, or if you feel that the message is breaching the computer guidelines, forward them to helpdesk@Tibshelf.derbyshire.sch.uk with a brief explanation.

Complaints will be investigated and persons engaging in this form of harassment will have their e-mail accounts withdrawn.

