

# TIBSHELF COMMUNITY SCHOOL ACCEPTABLE USE OF ICT- STUDENTS

Ratified: February 2024  
(Tibsshelf Policy)





## **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, the school also has guidelines that are displayed in the ICT Suites.


## **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 Network 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](mailto: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.

