

Student ICT Acceptable Use Policy



Formby High School
'Determined to Achieve'

1. Introduction

This policy has been prepared to ensure that all students are able to use the Information and Communication Technology (ICT) facilities and services at the School in a safe and secure way. General School Rules regarding courtesy and good behaviour apply when using ICT facilities.

The Formby High School network is School property and therefore the right is reserved to take action if there is a reason to suspect improper use.

The Student Acceptable Use Policy is an extension of the School rules and any breaches will be dealt with through the usual channels and in line with the School Behaviour and Discipline Policy.

2. Purpose of the Policy

The School aims to comply at all times with the following current legislation and statutory guidance, and students are responsible for following School policy to ensure that they do not personally infringe the legislation:

- Obscene Publications Acts 1959 and 1964
- Copyright, Designs and Patents Act 1988
- Computer Misuse Act 1990
- Defamation Acts 1996 and 2013
- Protection from Harassment Act 1997
- General Data Protection Regulation and UK Data Protection Act 2018
- Human Rights Act 1998
- Protection of Children Act 1999
- Freedom of Information Act 2000
- Electronic Communications Act 2000
- Communications Act 2003
- Police and Justice Act (Computer Misuse) (2006)
- Equality Act (2010)
- Malicious Communications Act (1988)
- Regulation of Investigatory Powers Act (2000)
- Investigatory Powers Act (2016)
- Counter-Terrorism and Security Act (2015)
- Keeping Children Safe in Education Prevent Duty
- FHS Data Protection Policy
- FHS Child Protection Policy
- FHS Online Safety Policy
- FHS Internet Consent Form
- FHS Home School Agreement

This policy provides a framework for all students to ensure safe, appropriate and acceptable use of the School's ICT facilities.

3. Definitions

The ICT facilities at the School are defined as:

- Hardware owned by the School (including, but not limited to computers, laptops, mobile devices, monitors, keyboards, mice, printers, portable storage devices,

scanners, cameras, telephones (including mobile phones), fax machines, televisions, projectors, interactive white boards, DVD players).

- The School network (including software stored on the network, SIMS and remote access services).
- The School's internet facility, Wi-Fi, and all other approved services (e.g. email, storage, remote access etc.) regardless if hosted (or accessed) onsite, offsite (e.g. 'cloud') or via approved third party service providers

This definition also includes the students' personal devices that they may use for work purposes in school and / or accessing the school's ICT facilities remotely.

4. Policy Statement

The ICT facilities must only be used for authorised purposes and to carry out those activities that can reasonably be considered necessary for educational purposes.

Students will be taught about acceptable use of ICT facilities, both within school and more widely, through their Computing and RESPECT (PSHEE Personal Social Health and Economic Education) lessons. Additional important information and guidance will be shared with students during assemblies.

5. Responsibilities

All students have a responsibility to comply with this policy and failure to do so may result in disciplinary action being taken.

Any breaches or suspected breaches of the ICT Acceptable Use Policy must be reported immediately to a member of staff

Any damage to School ICT equipment must be reported immediately to a member of staff. Any student found to have caused wilful damage to School ICT equipment may be sanctioned and charged for the cost of repair or replacement.

6. Network

Students must only use their own username and password on the School network and must never disclose this information to any other person.

Students are responsible for anything that is carried out using their username. If they suspect someone else may know their password they are responsible for ensuring it is changed at once.

Students must never attempt to run or install software onto, nor remove software from the School ICT facilities.

Students must not attempt to gain administrative access to the School network or bypass safeguarding restrictions. If students discover a problem with the School network security, they must immediately report it to a member of staff and must not demonstrate the problem to other users.

A member of staff must be immediately notified of any virus or security alerts.

The use of portable USB storage (including mobile) devices are **not** permitted.

Students must not leave unattended PCs logged into the network.

7. Internet

In line with other educational establishments, Formby High School uses third party systems to block sites which are illegal or which it regards as inappropriate. Inevitably, not all unsuitable sites will be blocked. Use of the internet to access inappropriate material such as pornographic, racist, homophobic, radicalisation or other offensive material is forbidden and may be a criminal offence. If an unsuitable website is accidentally accessed, students must report the incident to a member of staff so that it can be investigated.

Students must not use the School internet for personal financial gain, gambling, political purposes or advertising. All non-educational games are forbidden at all times on the School ICT facilities.

Attempting to bypass the School internet filtering or gaining unauthorised access to any computer system for any purpose is strictly forbidden.

The School logs and monitors all network and internet access as part of routine security measures and reserves the right to access and report on this information to ensure that network and internet access is being utilised in accordance with this policy. The School also maintains the right to restrict access to the School network, internet or web sites at its discretion.

The above requirements also apply to those students who access the internet via a wireless connection using their own laptop computer, hand held device or remotely.

8. Social Media

For the purpose of this policy, social media is the term commonly used for websites which allow people to interact with each other in some way – by sharing information, opinions, knowledge and interests. Social networking websites such as Facebook are perhaps the most well-known examples of social media but the term also covers other web-based services such as blogs, video and audio podcasts, wikis, message boards, photo document and video sharing websites such as YouTube and micro-blogging services such as Twitter. This definition of social media is not an exhaustive list.

Messages must not be posted on any internet message board, other similar web-based service or any online communication service that could potentially bring Formby High School's name or reputation into disrepute or lead to a breach of confidentiality, or which might reasonably be considered to be offensive, abusive or otherwise inappropriate. This includes the uploading of photographs which might bring the School or individuals into disrepute.

Access to social networking sites (Facebook, Twitter, etc) is not permitted on the School network unless required for a compulsory element of the course that the student is undertaking and authorised by a member of staff.

If you belong to a social networking site outside of School, you must adhere to the following guidelines to protect yourself and the School:

- Students must not invite School staff to be 'friends' on social networking sites.
- Students are advised that privacy settings for such sites must be set at a high level so as to ensure personal information is not publicly available.
- Students must never reveal their own or another person's personal address, telephone number or exact location to someone they do not know.

The School will investigate any allegation of bullying that has occurred through the use of ICT facilities in accordance with the Anti-Bullying Policy, even if it occurs outside school, and offenders will be dealt with in an appropriate manner. Any student who feels they are a victim of cyberbullying must approach a member of staff and explain the situation.

Students and parents must refer to the guidance contained in Appendix One of the Anti-Bullying Policy concerning staying safe on-line.

9. Plagiarism

Students must not plagiarise the work of others, nor attempt to pass others' work off as their own. Formby High School insists that copyright legislation is respected.

10. Monitoring

It is the School's policy to constantly monitor ICT activity, including internet usage.

Students must be aware that the School has a right to access personal data on the network and it may also be necessary to access a student's personal device. If an investigation is requested by the Headteacher then this will be followed in line with the Child Protection Policy.

By logging onto the Formby High School Network students agree to abide by this Acceptable Use Policy.