COWLEY
SIXTH FORM COLLEGE

ACCEPTABLE USE POLICY including BRING YOUR OWN DEVICE

Introduction

Information and Communication Technology (ICT) is an essential tool to support teaching and learning, as well as playing an important role in the everyday lives of children, young people and adults. All schools and students in St Helens have access to ICT facilities to provide our students with the skills they will need for life-long learning and employment.

ICT is a fast moving environment and covers a wide range of tools and resources including mobile learning and web-based learning. Some of the technologies available to students include:

- Mobile / Smartphone's features include; video, pictures, texts and web access
- Blogs & Wikis
- Online Forums, Chat Rooms and Social Networking,
- Laptops & Desktop PCs
- Websites
- Podcasting
- Email
- Virtual Learning Platforms

This Acceptable Use Policy covers both fixed and mobile technologies within the school.

All students must follow the conditions described in this policy when using school equipment and any networked resources, both in and outside of school. This apply equally to a student's own device used within school or accessing a school's resources.

Breaking these conditions may lead to:

- withdrawal of the student's access;
- close monitoring of the student's network activity;
- investigation of the student's past network activity;
- contacting parents and carers;
- informing our Safer Schools Police Officer and in some cases, criminal prosecution.

Students will be provided with guidance by staff in the use of the resources available through the schools network. School staff will regularly monitor the network to make sure that it is being used responsibly.

The school will not be responsible for any loss of data as a result of the system or student mistakes in using the system. Use of any information obtained via the network is at the student's own risk.

Conditions of Use

Student access to the ICT equipment and the networked resources is a privilege, not a right. Students will be expected to use the resources for the educational purposes for which they are provided.

It is the personal responsibility of every student to take all reasonable steps to make sure that they follow the conditions set out in this Policy. Students must also accept personal responsibility for reporting any misuse of the network to their teacher or House Manager.

Acceptable Use

Students are expected to use the ICT resources and network systems in a responsible manner. It is not possible to set a complete set of rules about what is, and what is not, acceptable.

All use however should be consistent with the school's ethos and code of conduct. The following list provides some examples that must be followed:

1.	I will not create, send or post any material that is likely to cause offence or needless anxiety to other people or bring the school into disrepute.
2.	I will use appropriate language – I will remember that I am a representative of the school on a global public system. Illegal activities of any kind are strictly forbidden.
3.	I will not use language that could stir up hatred against any ethnic, religious or other minority group.
4.	I realise that files held on the school network will be regularly checked by members of staff using Securus software.
5.	I will not reveal any personal information (e.g. home address, telephone number) about myself or other users over the network.
6.	I will not trespass into other users' files or folders.
7.	I will not share my login details (including passwords) with anyone else. Likewise, I will never use other people's username and password.
8.	I will ensure that if I think someone has learned my password then I will change it immediately and/or contact a member of staff.
9.	I will ensure that I log off after my network session has finished.
10.	If I find an unattended machine logged on under other users username I will **not** continuing using the machine – I will log it off immediately.
11.	I understand that I am will not be allowed access to unsupervised and/or unauthorised social media sites and should not attempt to gain access to them.
12.	I am aware that e-mail is not guaranteed to be private. Messages supporting of illegal activities will be reported to the authorities. Anonymous/unnamed messages are not permitted.
13.	I will not use the network in any way that would disrupt use of the network by others.
14.	I will report any accidental access to other people's information, unsuitable websites or being sent inappropriate materials that make me feel uncomfortable to a member of staff.
15.	I will not introduce USB drives or other portable devices into the network without having permission from Agilisys staff and then checked for viruses.
16.	I will not attempt to visit websites that might be considered inappropriate or illegal. I am aware that downloading some material is illegal and the police or other authorities may be called to investigate such use.
17.	I will not download and/or install any unapproved software, system utilities or resources from the internet.
18.	I realise that students under reasonable suspicion of misuse in terms of time, activity or content may have their usage closely monitored or have their past use investigated.
19.	I will not receive, send or publish material that violates copyright law. This includes materials sent/ received using Video Conferencing or Web Broadcasting.

20.	I will not attempt to harm or destroy any equipment, work of another user on the school network, or even another website or network connected to the school system.
21.	I understand that unapproved system utilities and executable files are not allowed in my work areas or attached to e-mails.
22.	I agree to comply with the acceptable use policy of any other networks that I access.

Unacceptable & Prohibited Use

Examples of unacceptable use include, but are not limited to:

- Logging in with another person's user ID and password, or using a machine left unattended, but logged in by another user.
- Creating, transmitting, displaying or publishing any material (text, images or sounds) that is likely to harass, cause offence, inconvenience or needless anxiety to any other person.
- Unauthorised access to data and resources on the school network system that belong to other "users".
- User action that would cause:
    - corruption or destruction of other users' data;
    - violate the privacy or dignity of other users;
    - intentionally waste time or resources on the school network or elsewhere.
- Illegal activities
- Violation of copyright or software licenses
- Plagiarism

Network Security

If you discover a security problem, for example being able to access other user's data, you must inform a member of staff immediately and not show it to other users. Students identified as a security risk will be denied access to the network.

Use of Own Device (BYOD)

The schools "Bring Your Own Device" ("BYOD") scheme will enable students to bring their own device to school for use in the school.

The BYOD scheme will run on the existing school network of which the students will be required to register their device. The network will only provide access to the schools filtered Internet, and usage will be subject to the schools acceptable use policy.

The BYOD scheme is entirely optional and students can choose whether to participate or not.

If a student wishes to participate in the BYOD scheme, the ACCEPTABLE USE POLICY must be adhered to. Any breach of this policy will be taken seriously and may result in all student devices' being deregistered.

Subject to registration to the network all students will be eligible to subscribe to the BYOD scheme. If a student wishes to subscribe to the BYOD scheme, they will need to register their devices with the managed service representative, who will provide the necessary access information, which will be unique to the student allowing them to connect up 3 devices.

The school Service Desk will not provide support related to device hardware or related to software installed on the device with the exception of access to the network.

On leaving the school, students will be required to delete any information relating to the School's network stored on the portable device and, on request, provide a signed statement that you have complied fully with your obligations under this clause.

The school reserves the right in its sole discretion to withdraw and/or terminate the BYOD scheme and/or to vary any aspect of it, at any time.

Students Responsibility for BYOD

- Maintain your device in good working order;
- Arrange appropriate hardware and software support contracts as necessary for your device
- Ensure that the device is fully charged before taken into school, as charging devices will not be permitted in school.
- Ensure your device is properly insured. This is the responsibility of the student or guardian. The school will not be responsible for loss or damages.
- Adhere to the Fair Use Policy. Internet access on a student owned device will be provided to aid student's studies as such bandwidth usage should reflect this. Typically students should be accessing less than 5GB per month of data via the internet unless a special arrangement has been made.