Student ICT Policy

UPDATED: 08/11/2017

Guide Updated By: S.Stevens (ICT Network Manager)

St John Fisher Catholic High School

Tel – 01942 510715

Website – www.sjfhs.co.uk

Introduction

As you will be aware the use of ICT and the Internet are an important part of learning and teaching at St John Fisher Catholic High School.

To access the school network each student has a unique username and password. It is important the student password is kept secure at all times. I would ask that students learn their password and that they do not write it on books, homework diaries or keep their password on them in person.

For a student to have continued access to the computer systems it is important that they have read and fully understood the terms and conditions of use. I have enclosed our Student ICT Policy for you to read through.

The school places a great deal of importance in teaching our students about all areas of internet and mobile device safety. All students receive the CEOP ‘Think you know’ programme and the school has CEOP trained staff who advise on child protection issues when necessary. For more information on internet safety please check out the “Think you know” website at http://www.thinkyouknow.co.uk/

Before logging on to any computer or laptop around the school, students will be asked to accept the Student ICT Policy in a digital format, if they do not accept the policy they will be denied access to our computer systems.

All students have filtered and content controlled access to the internet on our computer systems if you would like you child not to have access to the internet once logged in to our systems this can be arranged.

Kind regards

Mrs A.Rigby

Headteacher

Student ICT Policy

The school is offering an increasing number of opportunities for students to benefit from the use of computers and the Internet as part of their studies. With these opportunities, however, comes the possibility of students misusing the network or the Internet and thereby causing serious harm to themselves, to other students or to the network. In order to limit possible misuse of the ICT facilities students should accept and follow this policy.

User Accounts & Passwords

As security is essential, each student will be assigned a user account and password by the school. Each student must then change their password on their first login and this must remain confidential. Students will be forced to change their password every 45 days. Parents should impress upon their child the importance of not divulging it to anyone.

In order to protect the confidentiality of the passwords:

- students should memorise their password i.e. it should NOT be kept in their homework diary, on a slip of paper, on their mobile phone etc.
- try not to use your name or a plain word as a password, instead mix it up with alphanumeric characters.
- students must either lock their computer or log off when they have finished or walk away from their computer.

Record Keeping

Students should be aware that logs of their computer activity are recorded every time they log on to the network including when they log onto our system from home. This includes a list of all websites accessed, files opened, printed documents, any software they open, and any downloads they acquire from the internet or other locations. The school will also keep a log of times and dates they have logged on to computers around the school and time and dates they log into our system from home.

Proper Use

The school uses a technological protection measure that blocks or filters some internet sites that are not in accordance with this policy. School computers must only be used for educational purposes. Students' folders on the network should therefore only contain material relating to their studies and may be inspected without the students' permission at any time. Students must only use their own account, use of another students account may result in disciplinary action, if another student has left their computer unlocked and is not present you agree to either lock their computer or log them off.

Websites

Students must not include any text or images referring to any St John Fisher Catholic High School student, member of staff or member of the Board of Governors in a website or a file saved on the network without the prior permission of that person.

Email

The general email principles are as follows:

- school accounts are to be used for mainly educational purposes and only limited personal use;
- the school may directly access a student's email account in the pursuit of an appropriately authorised legal or disciplinary investigation;
- use of email may be subject to monitoring for security and / or network management reasons;
- users may be subject to limitations in their use of it.

It is unacceptable to:

- send or receive any material that is obscene or defamatory or which is intended to annoy, harass or intimidate another person;
- upload, download or otherwise transmit commercial software or any copyrighted materials;
- waste time on non-school related business.

Students should:

- keep emails brief and use meaningful subject lines;
- re-read messages before sending to check for clarity and to make sure that they contain nothing which will embarrass the school or make it liable;
- understand how to use - and don't mismanage - CC and BCC: only CC in people that really need to receive the email;
- use file compression techniques for large documents or send them using an alternative method;
- never reply to spam;
- avoid using email for sensitive or emotional messages, or offensive content;
- be careful when replying to emails previously sent to a group;
- ensure your computer is locked or logged out when you leave your desk, otherwise I is possible that a malicious user could send messages in your name.

The school accepts that the use of email is an extremely valuable educational resource and learning tool. However misuse of such a facility can have a detrimental effect on other users and potentially the school's reputation. As a result:

- the school maintains the right to access user email accounts in the pursuit of an appropriately authorised investigation;
- the specific content of any transactions will automatically be checked by a filtering application and on detection of inappropriate content and SLT will be informed, who will take the necessary action.

Disciplinary Action

In keeping with the School's Behaviour For Learning Policy, action will be taken in the event of a student failing to abide by the conditions included in this Acceptable Use Policy.

- General misuse of the internet during class such as visiting a site not appropriate to the work set, logging on as another user or playing games etc. will lead to an appropriate sanction set by the class teacher.
- Repeated general misuse (such as downloading or playing games) or a more serious internet offence such as visiting an inappropriate site (non-adult material), will result in the removal of internet access for an appropriate period of time. In cases were a student's internet log shows consistent misuse a longer ban or more serious sanction may be given.
- In the case of more serious websites (such as those featuring vulgar or adult material or websites used to circumvent the school filtering system), an exclusion may be given.

- The school will take a particularly serious view of any cases in which threatening or derogatory material about other students, teachers or members of the school community is published on a website or where a student has accessed unacceptable material of a very serious nature. A fixed term exclusion may be given and the school may be obliged to report the matter further.

Parents will be informed of all misuse as appropriate.