

ICT Acceptable Use (Students)

Ellesmere Port Catholic High School



| | |
|---------------------|---|
| Approved by: | Mrs C Vile, Headteacher |
| Lead of Review: | Mr M Hughes, Assistant Headteacher and ECC Member |
| Last reviewed on: | July 2023 |
| Next review due by: | July 2024 |

All users of the school computer network are expected to adhere to the Acceptable Use Policy when using the school's computer systems.

Accessing the network

Every user of the network has a unique username and password which are used to connect to the network. Users should only logon using their own username and a password that should be kept private and not made known to anyone else. When finished, or when leaving their computer unattended, users should log off properly to protect their work and allow someone else to use the computer.

All passwords need to meet the following requirements:

- Contain 8 or more characters.
- Contain a mix of upper- and lower-case characters, numbers and symbols.

Using another user's logon details to access the computers will result in being banned from the computers and a report being sent to the Pastoral Leader.

Email

All students are provided with an email account. This can be accessed in school by accessing office 365. There is also a link on the VLE and the school website. At home, this can be accessed from www.outlook.com/edu. Although mobile phones and tablets are not allowed in school, you can link your school email account to your home devices, and we encourage you to use this at home to collaborate and keep on top of work.

Please note IT Services do monitor the email system, and any inappropriate use (for example, sending offensive emails) will be reported to the Pastoral Leader and disciplinary action will be taken.

Saving / Printing your work

Students have been allocated space on OneDrive to store their work. We recommend you use clear file names and that you make use of folders (for example give each subject a folder). These folders are backed up regularly, if you lose a file see IT Services as soon as possible and they will show you how to recover it. The most effective way to ensure you do not lose work is to save regularly.

There are many times you will need to print your work, but you should take care that you do not waste paper or print work that is not necessary. A student's code will be used to access printers. Make sure your name and form are on each piece of work you print.

Sixth Form Digital Devices

With written permission from the Head of Sixth Form, we can join a sixth former's personal laptop to our internet connection. To get this set up, please bring the letter, your laptop and its power supply to IT Services.

Due to the way they access the internet, we cannot currently join iPads or other tablets to our internet connection.

Acceptable use of the network

Whether the computers are being used during lessons or outside of lessons, they should only be used for appropriate purposes. The following uses are not allowed at any time:

- Streaming/downloading Music or Video files (except Royalty free music for ICT lessons)
- Playing/downloading games
- Bypassing internet filtering (e.g. using proxy websites)
- Attempts to bypass network security
- Accessing a VPN

We ask students to avoid using the computers for these reasons to ensure that the internet can be a stable usable resource for the whole school. As with your home internet, streaming or downloading media/games slows down internet access for anyone wishing to use it for their work. Using the network in an unacceptable way will result in a disciplinary action. The filtering and monitoring is in place to help protect everybody, and to ensure that all students and staff can only get safe, relevant results to their searches.

Damage to the equipment

Equipment should be treated with care and any damage reported to a teacher or a member of IT Services immediately. When students have finished using their computer, they should leave the workspace tidy and the computer ready for the next user. Parents will always be informed if a student damages ICT equipment and they will be expected to meet the cost of repair.

Online Safety

Online Safety awareness will be delivered on a regular basis through assemblies, Personal Development and curriculum subjects using ICT facilities. If a student is having difficulties at any point with an online safety issue, they should report it to a responsible adult who will pass this information on to the school's online safety coordinator and the student's Pastoral Leader so the issue can be resolved quickly.

Cyberbullying or the passing on of inappropriate images will be referred to our Safeguarding lead in the first instance who will then make the decision for referral to CEOP or Cheshire Police.

Reporting incidents or concerns

If you would like to report incident or concerns or ask any questions regarding the computer systems and Online safety, please phone the school and ask to speak to Mr M Hughes, Assistant Headteacher for Personal Development.

Disciplinary action

The typical action taken for the breach of this policy is an internet ban of up to a month. For repeat or severe offences, this can then result in a ban of up to 6 months. Serious incidents such as cyber bullying, sending of inappropriate images, will be reviewed by members of the Ethos, Culture and Character Team and Mrs C Vile who will decide on the appropriate action to be taken, but will often include Cheshire Police.

Acceptable Use document for parental signature

Acceptable Use Policy

The school assumes that parents will ensure that their son/daughter read this policy before coming to school, or before working from home.

The use of Ellesmere Port Catholic High School ICT resources and services is a facility granted, at the school's discretion, to students. This AUP is essential for managing and sustaining the integrity and legality of the Ellesmere Port Catholic High School network and computing resources.

Remote Learning and using Microsoft Teams

- Students are unable/may not attempt to call, chat or set up private groups between each other on Microsoft Teams (this feature has been disabled).
- Students are unable/may not attempt to start or record a meeting/lesson (this feature has been disabled).
- Students are not permitted to share recorded videos/lessons made by teachers within or outside of the EPCHS Teams Account.
- Students should switch off their camera or blur their background if in a conference meeting which involves a camera (if this facility is available to them).
- Students should think carefully about what is acceptable language with regards to what they type and post.
- Students must hang up at the end of the lesson once instructed to do so. The teacher must be the last person in the meeting to hang up.

General

- Use of the EPCHS school network constitutes agreement to comply with this policy.
- These rules apply to the use of any of the school computers, wherever they may be. They also apply whenever a user is logged on to the EPCHS School network.
- Students are given a user account to enable them to use the facilities on the school network, use of this account is monitored – it is neither private nor privileged.
- Students are given an e-mail account to use, the account is monitored and filtered, the user is responsible for the content on their account and is permitted to follow the generally accepted rule of network etiquette. These include but are not limited to: a. Users are not allowed to reveal their date of birth, personal address or contact number, nor the date of birth, personal address or contact number of other users. b. Users are not allowed to distribute images of themselves or others c. Users should be polite and use appropriate language. Do not swear or use vulgarities. Do not harass or bully.

- Students use of computers in school will be monitored by Senso classroom monitoring software.
- You must not use someone else's username to gain access to the school network.
- You must not write down your password, nor share your password with another.
- You may not attempt to circumvent security of any host, network or account, or penetrate security measures (“hacking”) on or accessed through the EPCHS School network.
- You must not probe, scan or test the vulnerability of the network or other networks.
- You must not use the network or your own property to access or process pornographic material, inappropriate text files, games or files dangerous to the integrity of the network.
- You must not transmit, re-transmit, publish or store material on or through the EPCHS School network which; is bullying, threatening, abusive, hateful, indecent, or defamatory.
- You must report any unpleasant material or message sent to you. This report would help protect other students and you.
- Students are not permitted to have personal computers at the school unless they have properly documented educational needs or permission from a member of the senior leadership team. Where a computer may be used to access Special Education Needs “SEN” services. A separate SEN AUP will need to be signed.
- If a student or user account breaches the above rules, their account may be inspected and their access stopped. They may also render themselves liable to sanction from the Headteacher up to and including suspension and exclusion.
- Any property owned by students, such as mobile phones and iPods may not be used to watch any moving images whatsoever and must be switched off and in bag if brought into school.
- You may not access the internet except through the school network.
- Above all, you should be KIND ONLINE