Student ICT Acceptable Use Agreement

Introduction

This document forms the basis of an 'Acceptable Use' agreement that parents, carers and students are required to sign. This ICT Acceptable Use Agreement extends to all hardware and software, both fixed and mobile, provided by the School and where specifically authorised to do so, equipment which is brought into School that is owned by students.

All students should be able to take advantage of the potential of ICT to support their learning in a responsible and safe manner. To achieve this parents, carers and students need to understand the rules and systems that are in place to protect them, ensuring that no one is subject to bullying, harassment or abuse. Parents and carers also have a responsibility to monitor their child's use of technology to support the School in promoting good online safety practice and to follow this agreement. This agreement does not provide an exhaustive list of acceptable or unacceptable ICT use and all students are reminded that ICT use should be consistent with the School ethos, other appropriate policies and the law.

In the event of noncompliance with this agreement, students may be subject to internal School disciplinary procedures and or external agency involvement. Parents and carers may also be held liable for costs incurred for repair and or replacement of equipment where damage has been caused by misuse. In circumstances where the student is permitted to bring in and use their own personal computing equipment, the School shall not be held liable for any loss or damage to the equipment whilst in, or in transit to or from, the School.

Newton Road, Lowton WA3 1DU
Telephone: 01942 767040
enquiries@lowtonhs.wigan.sch.uk
www.lowtonhs.wigan.sch.uk

1. Online Safety

1. You must never reveal personal details about yourself or other people online, such as address or telephone number.
2. Only arrange to meet new friends met on-line in public places and with an appropriate adult.
3. You must not engage in “chat” activities nor engage in newsgroups, instant messaging, blogs or forums.
4. You must immediately tell your teacher if you receive any message or access any image or text that you think is inappropriate or makes you feel uncomfortable.
5. I know that the minimum age for using social networking sites like Facebook, Instagram, Snapchat and Twitter is 13 years old.
6. When using social networking websites, I will ensure that my security settings are set to private.

2. Personal Activities

1. I will not attempt to bypass the internet filtering system.
2. You must not attempt to gain unauthorised access to the Schools computer network or attempt to exceed your authorised access.
3. You must not make deliberate attempts to disrupt the computer systems, for example unplugging any cables or attempting to change any system settings.
4. You are responsible for avoiding plagiarism and must follow all copyright guidelines. This includes the downloading of any music, video, pictures or other materials which are copyrighted.
5. You must not use the School’s computer network for any business purpose including buying or selling.
6. You must not consume food or drink whilst using a computer.
7. When using the internet to find information, to take care to check that the information is accurate, as the work of others may not be truthful and may be a deliberate attempt to mislead.
8. I will report to my teacher any computer equipment which I find to be in a damaged condition.

3. Security

1. Each student is responsible for keeping their login secure, taking all reasonable precautions to prevent others from being able to use it. You must not let any other student know your password and change it immediately if you believe anyone knows it. Passwords can be changed at the IT Support office in F block. This should not be done during class times unless instructed by your teacher.
2. Always log off or lock the computer (using Ctrl + Alt + Delete, Lock) when leaving a computer, even for short periods.
3. You should not log on as someone else, nor use a computer which has been logged on by someone else.
4. You must not connect or attempt to connect mobile equipment to the computer network for example, laptops, tablets or mobile phones etc.
5. You are not allowed to use a computer allocated to a member of staff.
6. You must not introduce a computer virus, malware, ransomware or worm into the School's computer network.
7. You must not try to download, install or run computer programs that are not accessed through the normal Start Menu structure.

4. Email & Social Media

1. All students are provided with a school email address. Electronic communications with staff and other professionals should only take place via the school email address.
2. I will only communicate with staff online via my School email address and will not add staff as friends or contacts on any social networking site.
3. You must not register for email services, updates or reminders using your School email address.
4. All electronic messages must be phrased using acceptable language and in an acceptable tone.
5. Digital images or video footage of students or staff must not be posted to any website or social media platform.
6. Never open an attachment or click on a link sent by someone you do not know or by someone you are concerned about.
7. You must not email or electronically circulate chain letters or engage in "spamming".

5. Misuse of Resources

1. You must avoid unnecessary printing. Printers must only be used for school purposes. Students are not allowed to print personal pages.
2. Downloading or playing games via the Internet is not allowed.
3. You must not misuse or neglect any equipment in such a way so that it is likely to damage any School property.
4. You must not remove any ICT equipment from its original position.

6. Network Monitoring

You should expect only limited privacy with regards to your personal files on the School's network. The School routinely monitors all files and computer activity to ensure compliance with this Acceptable Use Agreement and the School's other e-safety and data security policies. Everything you do on a computer is logged and where violations of behaviour are suspected or detected by forensic security software, screenshots or video are taken automatically pending an investigation. These logs can be used to track specific actions by students at any time.

7. Personal Responsibility

You should ensure that you do not create, transmit, display, publish or forward any material that is likely to harass, offend, inconvenience or cause anxiety to any other person or anything which could bring them, their families, or the School into disrepute.

Your actions whilst using a computer are logged in detail. This includes the computer you use, where and when you used it, any printing, websites visited, emails sent and received and other details. Please use the computer resources responsibly.