EHS ICT Acceptable Use Policy

Name of Policy / Procedure	**ICT Acceptable Use Policy**
Issue date	September 2022
Review date	September 2027
GB committee responsible for the policy / procedure	Curriculum
Staff member responsible for writing, reviewing and updating the policy / procedure	Headteacher
Person responsible for monitoring implementation of the policy / procedure	Headteacher
Workload impact assessment (see below)	Low

Teacher Workload Impact Assessment

High impact: *Policy implemented by teachers on a daily / weekly basis*
Medium impact: *Policy implemented by teachers on a monthly / termly basis*
Low impact: *Policy implemented by teachers on an annual basis*
n/a *Policy is not implemented by teachers.*

EHS ICT Acceptable Use Policy

Acceptable use of electronic communication relates to students and all staff. The purpose of using electronic communication is to raise educational standards, support the professional work of staff, support the professional development of staff and to enhance the school's management information and business administration systems.

Access to electronic communication systems is a necessary tool for staff and an entitlement for students who show a responsible and mature approach.

The use of a computer system without permission or for a purpose not agreed by the school may constitute a criminal offence under the Data Protection Act 2018 or Computer Misuse Act 1990. Use of electronic communications is permitted outside of working hours subject to the Flintshire's security policies for schools.

Risk Assessment, Authorisation and Security of using ICT technologies

The school allocates access to the internet on the basis of educational need. Students are required to apply for internet access individually, by signing an Electronic Communication Acceptable Use Statement, and a parent must have agreed to use of electronic communication. All internet connections are achieved via Flintshire's Wide Area Network (FlintNet) to ensure compliance with the security policy, thus every use by staff or students requires a unique identity and password.

Students are educated in taking responsibility for internet access and informed that checks can be made on files held on the system and on access to remote computers. Teachers monitor and control access and inform students that the secure retention of individual identity and password is essential. Inappropriate use by students will be investigated by the School and sanctions applied in line with the Behaviour Policy. Staff of Flintshire ICT Unit and Council Officers may also need to take appropriate action.

In common with other media, some material available via electronic communication and the internet is unsuitable for students. The school will supervise students and take all reasonable precautions to ensure that users access only appropriate material suitable to their age and maturity. Senior staff will monitor and regularly review the effectiveness of access strategies for electronic communication. If staff or older students require less restricted internet access a separate arrangement can be provided.

Teachers who access YouTube or other video streaming sites as part of everyday teaching activities are responsible for checking that the content of videos streamed or downloaded from YouTube and other video hosting sites is both educationally suitable and appropriate for students to view.

However, due to the international scale and linked nature of information available via the internet, it is not possible to guarantee that particular types of material will never appear on a screen. Neither the school nor Flintshire County Council can accept liability for the material accessed, or any consequences thereof.

Access to social networking sites is filtered and, where appropriate, blocked. Newsgroups are blocked unless a specific use is approved. Students are advised never to give out personal details of any kind which may identify them or their location, or to publish specific and detailed private thoughts. The School is aware that bullying can take place through social networking especially when a space has been setup without a password and others are invited to see the bully's comments.

The security of the whole system is regularly reviewed with regard to threats to security resulting from use of electronic communication. Virus protection is installed and updated regularly, and all files held on the school's network are regularly checked. Portable media is subject to a virus check, and unapproved system utilities and executable files will not be allowed in students' work areas.

If staff or pupils discover unsuitable sites, the URL (address) and content will be reported to the ICT Unit. The ICT Unit will immediately prevent access to any site considered unsuitable and appropriate investigation will be undertaken.

Staff are permitted to use electronic communications, including the internet, outside of working hours provided it is in a responsible and professional manner. Any complaint about staff misuse must be referred to the Headteacher.

Remote access from the ICT Unit to computers in school allows problems and performance to be investigated without the need for a visit to school. Additionally, new and updated software can be downloaded directly and quickly to computers in school. File servers in school are able to automatically log, with the ICT Unit, potential faults before they occur. This allows preventative action to be taken to ensure continuity of operation. In using remote access the School understands that the principle adopted is that the action being taken is exactly the same as would be carried out of the support was given by visiting the school. Remote access to school servers is only be available via the secure virtual private network connection managed jointly by Corporate IT and the ICT Unit. All remote access is subject to the Flintshire Commitment Statement.

E-mail

Students are granted school e-mail accounts if their course requires it. All staff are allocated a school e-mail account. External e-mail users are encouraged to send initial messages to the school e-mail address, rather than to an individual, although subsequent contact may be via an individual address. The content of electronic mail messages transmitted via FlintNet are checked via software in a process managed by the ICT Unit. However, care needs to be taken that the potential consequences of reading and sending messages, for both the student and the school, are appreciated.

Students should be made aware of the appropriate actions to take if they receive unwanted interactions by email. Bullying, abuse or harassment by e-mail will be dealt

with in the school's anti-bullying policy and students should be advised to guard against giving out personal information at all times.

E-mail accounts that are available to staff in school and at home come with an on-line storage facility which allows access to documents and other files from a range of internet capable devices. It should be noted that these types of mail systems aren't backed up, so important files or mail should be copied to another secure location. Staff should ensure that no sensitive materials or files should be hosted on the cloud without due thought to protecting that data. Personal information should be anonymised wherever possible and documents deleted when no longer required.

Learning Environments and Awareness Raising

Students are taught what internet use is acceptable and what is not and given clear objectives for internet use. Staff will guide students in on-line activities that will support the learning outcomes planned for the students' age and maturity. Students are educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.

Students are taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy. They are made aware that the writer of an electronic mail message or the author of a web page may not be the person claimed or the intended recipient. They are also taught to expect a wider range of content, both in level and in audience, than is found in the school library or on television, and are encouraged to tell a teacher immediately if they encounter any material that makes them feel uncomfortable.

The School has a website and a Virtual Learning Environment (VLE) to inform and inspire students to publish work to a high standard for a very wide range of audiences. These are available from within and beyond school and, as they can be accessed by anyone on the internet, the security of staff and students will be maintained. No students or staff will be named on the website unless permission had been granted, and pictures will be reduced in quality and size to prevent misuse.

Rules for responsible use of the internet and school network are displayed near computer systems. All staff are provided with the Electronic Communication Acceptable Use Policy and its importance explained. Parents' attention is drawn to the policy in the school prospectus. Responsible use of electronic communication, covering both school and home use, will be included in the induction programme for all students when they join the school.

Internet use in students' homes is rapidly increasing and the school is sensitive to internet-related issues experienced by students out of school, e.g. social networking sites, and offers appropriate advice (see the ICT e-Safety policy). Parents are routinely updated regarding the school's use of electronic communications and a careful balance will be

maintained between keeping parents informed and raising issues of concern.

Critical E-Safety incidents

A critical e-safety incident is when unlawful or suspected unlawful material is found on any computer or digital device where criminal or inappropriate activity has or is taking place, or where an e-crime has been or is being committed. In such cases, the power lead should be taken out (not a normal shutdown) or the battery removed (laptop). Do not show (suspected) unlawful material to anyone else or undertake any further investigation; report to the Headteacher or child protection officer immediately.

Notes should be made that help in any subsequent local or police investigations. Flintshire County Council takes all incidents of criminal activity very seriously and has worked with the North Wales Police Hi Tech Crime Unit to produce guidance on how to deal with critical e-safety incidents. Appropriate action will be taken by Flintshire County Council and there may be occasions when the police must be contacted.

Guidance for Staff on the use of the Internet

Personal use of the Internet is permitted outside working hours but must be in a responsible and professional manner. Use of internet access facilities that contravenes any other school policies and procedures is prohibited.

• Flintshire Internet facilities may not be used to download images or videos unless there is an express business related use for the material. Sexually explicit material may not be intentionally displayed, archived, stored, distributed, edited or recorded using any Flintshire IT equipment.
• Flintshire Internet facilities may not be used to download entertainment software or games or to play games against opponents over the Internet.
• Use of any Flintshire resources for illegal activity is grounds for immediate dismissal.
• No employee may use Flintshire IT facilities to knowingly download or distribute pirated software or data.
• No employee may use Flintshire Internet facilities to deliberately propagate any virus, worm, trojan horse, or trap-door program code. No employee may use Flintshire's Internet facilities, including a web site or virtual learning environment, to disable or overload any computer system or network, or to circumvent any system intended to protect the privacy or security of another user. It is not permitted to disable, defeat or circumvent any Flintshire IT security facility.
• Employees must not release confidential or sensitive information via a newsgroup or chat line, whether or not the release is inadvertent.
• Employees must ensure that the use of Artificial Intelligence (AI) tools is ethical, accurate, and appropriate, avoiding misuse, bias, or the disclosure of personal or confidential information

EHS ICT Acceptable Use Policy

I confirm that I have read and understand the contents of the Policy set out under the above title.

I agree to adhere to its terms, to include giving consent to the monitoring of my Internet and email usage by Flintshire County Council.

Name: .....

Signed: .....

Position: .....

Dated: .....

Please return to the Headteacher.