ICT Acceptable Use Policy

Agreed by Governing Body	**October 2022**
Reviewed	**December 2025**

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 Flintshire's security policies for schools.

All ICT use must also comply with the UK General Data Protection Regulation (UK GDPR). The school operates under the Flintshire County Council Information Security Policy and Welsh Government PSBA standards to ensure data protection, filtering, and monitoring are compliant and effective.

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/carer must have agreed to use of electronic communication. Standard 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. The school also has a Sixth Form WiFi which is assigned by the MAC address of the student's device, students are required to sign an additional WiFi Agreement Use Statement.

Below is the wording:
I will use the internet responsibly and will not visit websites I know to be banned by the school. I am also aware that during lessons I should visit websites that are appropriate for my studies.
I am aware that some websites and social networks have age restrictions and I should respect this and not access unsuitable websites. I will not access obscene or pornographic materials.
I will not bypass the school's security software in any way.
I am responsible for the use and safety of my own personal data when using the sixth form WiFi.
I will not transmit hate mail, discriminatory remarks, profane or inappropriate language, offensive or inflammatory communication. Any messages promoting hate are not appropriate.

The Sixth Form Wi-Fi is not content-filtered. Students accessing this network are personally responsible for safe and appropriate use under the terms of their signed Sixth Form Computer Use Agreement (CUA). Breaches may result in withdrawal of access privileges or disciplinary action.

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.

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.

All ICT systems and internet activity are subject to monitoring by Flintshire ICT and school safeguarding staff to ensure network integrity and compliance with statutory guidance.

Email and Electronic Communication

All staff and students are allocated a school email account. External email users are encouraged to send initial messages to the school email 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.

Email and communication systems must be used for educational and professional purposes only. Users must not send or store personal, confidential, or inappropriate material through school systems. Flintshire's monitoring tools automatically scan for malware and prohibited content to protect users and the network.

Removable Storage and Personal Devices

Students are not permitted to connect USB drives or other removable storage devices to school computers. Staff may only use removable storage if it is encrypted and approved by the ICT Manager. All removable devices must be virus-scanned before use.

Staff and Sixth Form students using personal devices must follow the school's Bring Your Own Device (BYOD) Policy. Staff issued with a school device must have completed and signed the Staff Device Agreement Form.

Remote Access and Monitoring

Remote access to school systems is available only through secure, authorised methods provided by Flintshire ICT. Monitoring software such as Impero may be used to view or control devices for safeguarding or support purposes. Third-party suppliers may be granted limited remote access only with prior authorisation.

Sanctions

Inappropriate use of electronic communication by staff or students will be investigated and may result in sanctions in line with the Behaviour Policy or the staff disciplinary process.

Serious misuse, such as deliberate damage, data breaches, or illegal activity, may result in removal of access, disciplinary action, or referral to external authorities.

Policy Monitoring and Review

Due to the constantly changing state of technology this policy will be reviewed annually to ensure it stays relevant. Small changes may be made at any time to incorporate any new technologies or systems brought into school throughout the year.

This policy should be read alongside the following related documents:
- ***Data Protection Policy***
- ***Password & Access Control Policy***
- ***Bring Your Own Device (BYOD) Policy***
- ***AI Risk Assessment and Student AI Use Policy***
- ***Cyber Incident Response Plan***
- ***Staff and Student Computer Use Agreements (CUAs)***