Bring Your Own Device (BYOD) Policy

Agreed by Governing Body	**December 2025**

1. Purpose

This policy explains how personal devices (such as phones, tablets, and laptops) may be used to access Castell Alun High School's Wi-Fi networks and online systems.

It ensures that all users understand their responsibilities when connecting non-school equipment and helps protect the school's data, systems, and users.

2. Scope

This policy applies to:

Staff who use either school-issued devices or their own personal devices for school-related activity.

Sixth Form students, who may connect their own personal devices to the CAHS Sixth Form Wi-Fi after completing the online Computer Use Agreement (CUA).

The Sixth Form Wi-Fi is a separate network that provides supervised internet access for post-16 students. It is not content filtered; instead, students are trusted to act responsibly under the terms of the CUA.

3. Acceptable Use

All users must have agreed to and signed the relevant Staff or Student Computer Use Agreement (CUA) before connecting any device.

Sixth Form students may only access the CAHS Sixth Form Wi-Fi network.

Staff and students must use connected devices in accordance with the school's ICT Acceptable Use, Data Protection, and Safeguarding policies.

Connection to school networks is a privilege, not an entitlement, and may be removed if misused.

4. Device Ownership and Responsibilities

a. School-owned devices

Are provided, configured, and maintained by the ICT Team.

Must not be altered, reset, or used for personal or non-educational purposes.

Are protected under Flintshire County Council's security standards and remote-management controls.

Staff issued with a school device must have completed and signed the Staff Device Agreement Form before use.

The device remains the property of Castell Alun High School and may be recalled for inspection, updates, or recovery at any time.

b. Personally-owned devices

Remain the responsibility of the owner.

Must not be used to store or process sensitive or confidential school data.

Should only access data through secure, approved cloud platforms such as Hwb, Google Workspace, or Microsoft 365.

The school will not install software or enforce settings on personal devices but expects users to apply reasonable security measures such as passwords and updates.

5. Monitoring and Behaviour Expectations

The school reserves the right to audit network connections for bandwidth use, device type, and security anomalies.

The Sixth Form Wi-Fi is not content filtered; users are personally responsible for complying with the Acceptable Use Agreement and the school's behaviour expectations.

Inappropriate access (e.g. obscene, hateful, or unlawful material) or use of personal devices to bypass security systems will result in disciplinary action.

Staff and students are reminded that all school policies on safeguarding, bullying, and conduct apply equally when using personal devices on school premises.

6. Data Protection

Users must access school data only via secure, approved platforms.

Downloading, copying, or storing confidential data on a personal device is not permitted.

Users are responsible for any personal data they hold on their own devices.

Any suspected data loss or compromise must be reported immediately to the ICT Manager, School Business Manager, and Data Protection Officer.

7. Responsibilities

ICT Manager / ICT Team – manage network access and respond to technical or security incidents.

School Business Manager – ensures compliance with data protection requirements and oversees BYOD processes.

All users – maintain responsible use of devices and report any misuse, loss, or security issues immediately.

8. Agreement

Connecting a personal or school device to Castell Alun's Wi-Fi or online services indicates acceptance of this policy and confirmation that the user has already agreed to the appropriate Computer Use Agreement (CUA) or Staff Device Agreement Form.