Password and Access Control Policy

Agreed By Governing Body	**December 2025**

1. Purpose

The purpose of this policy is to ensure that all staff, students, and authorised users of Castell Alun High School's ICT systems follow secure password and access control practices to protect the school's data and systems from unauthorised access or compromise.

2. Scope

This policy applies to all members of staff, students, contractors, and third parties who have authorised access to the school's ICT systems, networks, or data.

3. Storage & Encryption

• Staff are responsible for creating their own passwords. Passwords must be at least eight (8) characters long and reasonably complex, avoiding obvious words or personal information such as names or dates.

• Students are issued randomised passwords by the ICT Department. These passwords cannot be changed without notifying ICT Support, who will assist with any approved password changes.

• Passwords must remain confidential and never be shared with others.

• Users must change their password immediately if they suspect it has been compromised.

4. Multi-Factor Authentication (MFA)

MFA is mandatory for all staff accounts that access school systems, including email, cloud platforms, and administrative systems.

MFA is provided via Microsoft Authenticator or another school-approved app.

5. Account Management

• Accounts must be created, modified, and deleted only by authorised ICT staff.
• Temporary accounts (e.g. supply staff or contractors) must have defined expiry dates.
• Leavers' accounts are disabled within 24 hours of their end of contract date.

• All user accounts are linked to a unique school identity and must not be shared, even temporarily.

6. Password Storage and Protection

All systems storing passwords must use industry-standard encryption or hashing protocols to protect credentials. Passwords must never be written down or stored in plain text.

Passwords for shared administrative accounts (where unavoidable) must be stored securely in an encrypted password manager accessible only to authorised ICT staff.

7. Breach and Reporting

Suspected account compromises, lost devices, or unauthorised access must be reported immediately to the ICT Manager and the Data Protection Officer (DPO).

All incidents will be logged in the Cyber Incident Register and linked to the school's Cyber Response Plan.