Data Protection Policy

Agreed by Governing Body	**May 2023**
Renewed	**December 2025**

1. Introduction

Castell Alun High School collects and uses personal information about staff, students, parents, governors, and others to perform its functions as a school. This includes data needed to support learning, recruitment, safeguarding, health and safety, and compliance with statutory obligations. The school is committed to ensuring that all personal data is handled responsibly, in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

---

2. Purpose

The purpose of this policy is to outline how Castell Alun High School ensures that personal data is processed fairly, lawfully, and transparently, protecting the privacy and rights of individuals while maintaining compliance with data protection law.

---

3. Status of this Policy

Compliance with this policy is a condition of employment for all staff. Any breach of this policy may be treated as a disciplinary matter and, in serious cases, may also constitute a criminal offence under the Data Protection Act 2018.

---

4. Scope

This policy applies to all personal data held by the school in any format (digital, paper, photographic, or recorded) relating to staff, students, parents, governors, or third parties.

---

5. Data Protection Principles

The school adheres to the following principles as set out in Article 5 of the UK GDPR:

1. **Lawfulness, fairness, and transparency**
2. **Purpose limitation**
3. **Data minimisation**
4. **Accuracy**
5. **Storage limitation**
6. **Integrity and confidentiality**
7. **Accountability**

---

6. Roles and Responsibilities

- **The Data Controller is Castell Alun High School.**
- **The Headteacher has overall responsibility for data protection compliance.**
- **The Data Protection Officer (DPO) oversees compliance and advises on data protection matters.**
- **The School Business Manager acts as the Designated Data Controller for operational data management.**
- **The ICT Manager ensures systems security, access control, and incident reporting.**
- **All staff are responsible for maintaining confidentiality, accuracy, and security of personal data.**

---

7. Lawful Basis for Processing

The school processes data under one or more lawful bases as defined in Article 6 of the UK GDPR: legal obligation, public task, contract, vital interests, consent, or legitimate interest.
Special category data is processed under Article 9 when necessary for safeguarding, employment, or medical purposes.

---

8. Consent and Special Category Data

Where consent is required for processing, it must be freely given, specific, informed, and unambiguous.
Parental or student consent will be obtained where appropriate (e.g. use of photographs, biometric data).
Sensitive personal data such as health, ethnicity, or religion is handled with particular care and stored securely with restricted access.

---

9. Data Security and Storage

All personal data is stored securely within Flintshire County Council's managed network or approved cloud services (Hwb, Google Workspace, or Microsoft 365).
Data is encrypted both in transit and at rest wherever possible.
Staff must follow the Password & Access Control Policy, BYOD Policy, and Backup & Continuity Procedure.

Paper records are kept in locked cabinets accessible only to authorised staff. Portable devices must be encrypted and not used to store personal data unless authorised by the ICT Manager.

---

10. Data Sharing and Publication

The school only shares data where legally required or necessary for educational, safeguarding, or administrative purposes.
All third-party processors must have written Data Processing Agreements confirming compliance with the UK GDPR.

The school may publish limited staff information (e.g. names, roles) on its website and newsletters, in line with transparency principles. No personal or sensitive data will be published without consent.

---

11. Rights of Individuals

All data subjects have the following rights under data protection law:

- **The right to access personal data (Subject Access Request)**
- **The right to rectification or erasure**
- **The right to restrict or object to processing**
- **The right to data portability (where applicable)**

Requests should be made in writing to the Data Protection Officer (DPO), who will respond within statutory timeframes.

---

12. Data Breaches

All suspected or actual data breaches must be reported immediately to the ICT Manager and DPO.
The school will follow its Cyber Incident Response Plan to contain, assess, and mitigate any incident.
Where personal data is at risk, the DPO will notify the Information Commissioner's Office (ICO) within 72 hours and inform affected individuals as appropriate.

---

13. Retention and Disposal

Personal data is retained only as long as necessary, following the Information and Records Management Society (IRMS) retention schedule.
Data will be securely deleted or destroyed once it is no longer required.

---

14. AI and Emerging Technologies

The school recognises that Artificial Intelligence (AI) and new technologies can support teaching and management but also pose privacy risks.
Any use of AI must comply with the AI Risk Assessment, AI Use Policy (Students), and undergo a Data

Protection Impact Assessment (DPIA).
Staff must not input personal or identifiable data into public AI systems.

15. Training and Awareness

All staff receive annual training on data protection and cybersecurity.
Students are taught about privacy and responsible data use through ICT and PSHE lessons.

---

16. Related Documents

- **ICT Acceptable Use Policy**
- **Bring Your Own Device (BYOD) Policy**
- **Password & Access Control Policy**
- **Cyber Incident Response Plan**
- **AI Risk Assessment**
- **Data Breach Impact Assessment**

---

17. Conclusion

Compliance with this policy is the responsibility of every member of the school community.
Failure to comply may result in disciplinary action and, in serious cases, may constitute a criminal offence.
All staff are expected to handle data lawfully, fairly, and securely to protect the privacy of students, parents, and colleagues.