Birchwood High School

your dreams, your future, our challenge

Data Protection Policy 2026

Committee	Audit
SLT Link	Mr C Gilbank
Approval Date	March 2026
Scheduled Review Date	March 2027

Birchwood High School

your dreams, your future, our challenge

Contents

1. Purpose, legislation and guidance 4
2. Scope 4
3. Definitions 4
4. Data Protection Principles 5
5. Lawful Basis for Processing 5
6. Roles and Responsibilities 6
   Governing Body 6
   Headteacher 6
   Staff 7
7. Data Security 7
8. Data Sharing 7
9. Data Subject Rights 8
10. CCTV, photographs and videos 8
11. Artificial Intelligence (AI) 8
12. Data Protection by design and default 9
13. Data Breaches 9
14. Data Retention and Disposal of Records 9
15. Training and Awareness 10
16. Monitoring and Review 10

Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

This policy applies to all personal data processed by the school.

It is based on guidance published by the Information Commissioner's Office (ICO) on the UK GDPR and guidance from the Department for Education (DfE) on generative artificial intelligence in education.

It meets the requirements of the Protection of Freedoms Act 2012 where relevant.

It also reflects the ICO's guidance on the use of surveillance cameras and personal information.

In addition, this policy complies with the funding agreement and articles of association.

The policy should be read alongside Birchwood's privacy notices, Data Breach policy and FOI policy.

2. Scope

This policy applies to:

- All staff, governors, volunteers, contractors, and temporary staff
- All personal data relating to pupils, parents/carers, staff, governors, volunteers, and other individuals
- All forms of data, including paper records, electronic records, emails, images, and audio recording

Birchwood does not use any form of biometric data

3. Definitions

- Personal Data: Any information relating to an identified or identifiable living individual.
- Special Category Data: Personal data revealing racial or ethnic origin, health, biometric data, religious or philosophical beliefs, or other sensitive information.
- Processing: Any operation performed on personal data, including collection, storage, use, disclosure, or deletion.
- Data Subject: The individual to whom the personal data relates.
- Data Controller: The organisation that determines the purposes and means of processing personal data. Birchwood High School is the data controller for

personal data relating to pupils, parents / carers, staff, governors, visitors and others.

- Data Processor: A person or other body, other than the data controller, who processes personal data on the behalf of the data controller.
- Personal Data Breach: A breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure, or access to, personal data.

4. Data Protection Principles

The school will comply with the data protection principles, ensuring that personal data is:

1. Processed lawfully, fairly, and transparently
2. Collected for specified, explicit, and legitimate purposes
3. Adequate, relevant, and limited to what is necessary
4. Accurate and kept up to date
5. Kept for no longer than necessary
6. Processed securely and protected against unauthorised access or loss

5. Lawful Basis for Processing

The school processes personal data under one or more of the following lawful bases:

- To fulfil a contract with the individual or the individual has asked the school to take specific steps before entering a contract
- To comply with a legal obligation
- To ensure the vital interests of an individual (example: to protect life)
- To perform a task carried out in the public interest or in the exercise official authority
- Where processing is necessary for the legitimate interests of the school or a third party, provided the individual's rights and freedoms are not overridden
- The individual has given clear consent

Special category data is processed under additional lawful conditions, including substantial public interest and safeguarding of children:

- The individual has given explicit consent
- Processing is necessary to perform obligations or exercise rights in relation to employment, social security or social protection law

- Processing is necessary to ensure the vital interests of an individual who is physically or legally incapable of giving consent
- The data has been made manifestly public by the individual
- Processing is necessary for the establishment, exercise or defence of legal claims
- Processing is necessary for reasons of substantial public interest, as defined in legislation
- Processing is necessary for health or social care purposes and is carried out by a professional subject to a duty of confidentiality
- Processing is necessary for public health reasons
- Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes

Criminal offence data will only be processed where both a lawful basis and a specific condition under data protection law apply. Conditions include:

- The individual (or parent/carer in the case of a pupil) has given consent
- Processing is necessary to protect vital interests where consent cannot be given
- The data has been manifestly made public by the individual
- Processing is necessary in connection with legal proceedings
- Processing is necessary for reasons of substantial public interest

6. Roles and Responsibilities

Governing Body

The Governing Body has overall responsibility for ensuring compliance with data protection legislation.

Headteacher

The Headteacher acts as the representative of the data controller on a day-to-day basis.

Data Protection Officer (DPO)

The DPO is responsible for overseeing the implementation of this policy and will:

- Advise on data protection obligations
- Monitor compliance
- Act as a contact point with the Information Commissioner's Office (ICO)

The DPO is Charles Gilbank and is contactable via dpo@birchwoodhigh.org.uk.

Staff

All staff must:

- Follow this policy and related procedures
- Complete data protection training
- Contact the DPO if they:
- Have questions about data protection
- Are unsure of the lawful basis for processing personal data
- Suspect or become aware of a data breach
- Are planning a new activity that may affect individual's privacy rights
- Require advice on contracts or data sharing with third parties
- Inform the school of any changes in their personal data

7. Data Security

The school will implement appropriate technical and organisational measures to protect personal data, including:

- Secure password protection and access controls
- Encryption where appropriate
- Secure storage of paper records
- Regular and secure data backups

8. Data Sharing

Personal data will only be shared where necessary, lawful, and secure. Data sharing agreements will be in place with external organisations where required.

The school will not normally share personal data without consent. However, there are some circumstances where sharing may be necessary, including but not limited to:

- Concerns relating to a pupil or parent/carer that puts safety of staff or others at risk
- Liaison with external agencies, where consent will be sought as necessary
- Where suppliers or contractor require data to provide services to staff and pupils.

Where third-party suppliers or contractors process personal data on behalf of the school, they will be required to provide sufficient guarantees that they comply with UK data protection law.

The school may also share personal data with law enforcement, government bodies, emergency services and local authorities where there is a legal obligation or an urgent need to protect individuals.

9. Data Subject Rights

Individuals have the right to:

- Access their personal data
- Rectify inaccurate or incomplete data
- Erase personal data (where applicable)
- Restrict or object to processing
- Data portability (where applicable)

Requests will be responded to within one month.

Children aged twelve and above are generally regarded to be mature enough to understand their data protection rights. A pupil's ability to exercise their rights will always be judged on a case-by-case basis.

To request personal data or make a Freedom of Information request, please complete the Data Request Form.

Further information is available in the school's Privacy Notices.

10. CCTV, photographs and videos

The school uses CCTV around the site to ensure it remains safe. The school follows the ICO guidance on the use of CCTV and complies with data protection principles.

For photographs and videos, the school will obtain consent from parents / carers or pupils aged over eighteen for photographs and videos to be taken of pupils for communication, marketing, or promotional purposes. Consent can be withdrawn at any time.

Videos or photographs taken by parents / carers at school events are for their own personal use and not covered by data protection legislation. The school requests that these videos and photographs are not shared publicly on social media for safeguarding reasons.

11. Artificial Intelligence (AI)

Birchwood recognises the risks to personal and sensitive data with AI tools. Nobody has permission to enter such data into unauthorised generative AI tools or chatbots. If this occurs, it will be treated as a data breach.

12. Data Protection by design and default

The school integrates data protection into all data processing activities by:

- Appointing a suitably qualified Data Protection Officer
- Only processing personal data necessary for each specific purpose
- Completing Data Protection Impact Assessments where processing is likely to present a substantial risk to rights and freedoms
- Integrating data protection into internal policies and procedures
- Regularly training members of staff on data protection law and policies
- Regularly conducting reviews and audits to test compliance
- Applying appropriate safeguards when transferring personal data outside of the UK
- Maintaining records of data processing activities

13. Data Breaches

All data breaches or suspected breaches must be reported immediately to the DPO. DPO@birchwoodhigh.org.uk, or itsupport@birchwoodhigh.org.uk, or by filling in Data Breach Form

The school will investigate and, where required, report breaches to the ICO within 72 hours.

14. Data Retention and Disposal of Records

Personal data will be retained in line with the school's Data Retention Schedule and securely disposed of when no longer required.

- Paper based records and portable devices are kept locked away when not in use
- Confidential papers must not be left visible
- Staff are reminded to use unique, strong passwords
- Encryption software is used to protect all personal devices and removable media

Staff, pupils or governors who store information on personal devices are expected to follow the same security procedures as for school-owned equipment (please refer to the Acceptable Use Agreement)

Personal data that is no longer needed, inaccurate or out of date will be disposed of securely.

15. Training and Awareness

All staff receive regular data protection training and guidance. Data protection forms part of the continuing professional development programme.

16. Monitoring and Review

This policy will be reviewed annually or sooner if there are changes in legislation or school practice.