



Data Protection Policy

Approved by:	Governing Body	Date:
--------------	----------------	-------

Last reviewed on:	September 2026
-------------------	----------------

Next review due by:	September 2028
---------------------	----------------

1. Policy Statement

Berry Hill Primary School is committed to protecting the privacy and rights of pupils, staff, governors, parents, carers, volunteers, contractors and all other individuals whose personal data is processed by the school.

The school recognises its responsibilities under the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and other relevant legislation. We are committed to ensuring that personal data is handled lawfully, fairly, securely and transparently.

This policy establishes the principles and procedures that govern the collection, use, storage, sharing and disposal of personal information throughout the school.

2. Scope

This policy applies to:

- all personal data processed by the school;
- all staff, including temporary and agency staff;
- governors and committee members;
- volunteers;
- contractors and service providers acting on behalf of the school;
- any individual with access to school information systems.

The policy applies regardless of whether information is held electronically, on paper or through any other medium.

3. Roles and Responsibilities

The Governing Body

- The Governing Body is responsible for:
- ensuring the school complies with data protection legislation;
- approving and reviewing this policy;
- ensuring sufficient resources are available to meet compliance obligations;
- promoting a culture of information security.

The Headteacher

The Headteacher is responsible for:

- day-to-day implementation of this policy;
- ensuring staff understand their responsibilities;
- ensuring appropriate security measures are maintained;
- notifying the Data Protection Officer of relevant issues and incidents;
- ensuring data protection is considered in strategic and operational decisions.

Data Protection Officer (DPO)

The DPO shall:

- monitor compliance with data protection legislation;
- provide advice and guidance to the school;
- support Data Protection Impact Assessments;
- act as a point of contact for the Information Commissioner's Office (ICO);
- advise on personal data breaches;
- respond to data protection enquiries where appropriate.

DPO Contact Details: mprice@berryhill.notts.sch.uk

Staff

All staff must:

- comply with this policy;
- access personal data only where necessary for their role;
- maintain confidentiality;
- report suspected data breaches immediately;
- complete required data protection training;
- follow the school's information security procedures.

Governors, Volunteers and Contractors

Individuals working with the school must comply with this policy and any associated confidentiality requirements.

4. Definitions

Personal Data

- Any information relating to an identified or identifiable living individual.

Special Category Data

- Personal data revealing:
- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- genetic data;
- biometric data used for identification;
- health information;
- information concerning a person's sex life or sexual orientation.

Processing

- Any operation performed on personal data including collection, recording, storage, use, sharing, amendment or deletion.

5. Data Protection Principles

Berry Hill Primary School will adhere to the following principles. Personal data shall be:

- Lawful, Fair and Transparent
- Information will only be processed where there is a valid lawful basis and individuals are informed how their information is used.
- Collected for Specified Purposes
- Data will only be collected for legitimate and clearly defined purposes.
- Adequate, Relevant and Limited
- Only information necessary for the intended purpose will be collected and retained.
- Accurate and Kept Up to Date
- Reasonable steps will be taken to ensure information remains accurate and current.
- Retained Only as Long as Necessary
- Information will be retained in accordance with statutory requirements and recognised retention schedules.
- Secure
- Appropriate organisational and technical measures will be implemented to protect personal data.
- Accountable
- The school will be able to demonstrate compliance with all data protection obligations.

6. Lawful Bases for Processing

The school processes personal data under one or more lawful bases, including:

- compliance with a legal obligation;
- performance of a task carried out in the public interest;
- performance of a contract;
- protection of vital interests;
- legitimate interests where appropriate;
- consent where required.

Where consent is relied upon, individuals have the right to withdraw consent at any time.

7. Special Category Data

The school processes special category data where necessary and where an appropriate condition under data protection legislation is met.

This may include information required for:

- safeguarding;

- education provision;
- medical support;
- equality monitoring;
- employment obligations;
- statutory returns.

Appropriate safeguards will be maintained at all times.

8. Privacy Notices

The school will provide clear privacy notices explaining:

- what information is collected;
- why it is collected;
- how it is used;
- who it may be shared with;
- how long it is retained;
- the rights available to individuals.

Privacy notices will be reviewed regularly and made available via the school website and on request.

9. Individual Rights

Individuals have rights under data protection legislation, including:

- the right to be informed;
- the right of access;
- the right to rectification;
- the right to erasure in certain circumstances;
- the right to restrict processing;
- the right to data portability where applicable;
- the right to object;
- rights relating to automated decision-making and profiling.

Requests relating to these rights should be directed to the school office or the Data Protection Officer.

10. Subject Access Requests

Individuals are entitled to request access to personal information held about them.

Requests should:

- be made in writing where possible;
- provide sufficient information to identify the applicant;
- provide evidence of identity where required.

The school will respond without undue delay and normally within one calendar month of receiving a valid request. The timescale may be extended where permitted by legislation. Information may be withheld where an exemption applies.

11. Data Sharing and Disclosure

The school may share information with:

- local authorities;
- the Department for Education;
- examination and assessment organisations;
- health professionals;
- safeguarding partners;
- education support providers;
- law enforcement agencies;
- courts and regulators.

Information will only be shared where there is a lawful basis to do so.

The school will take reasonable steps to ensure data shared with third parties remains secure.

12. International Transfers

The school will not transfer personal data outside the United Kingdom unless:

- an adequacy regulation applies; or
- suitable safeguards are in place; or
- another lawful exemption is available.

Any such transfer will be subject to appropriate risk assessment.

13. Records Management and Retention

The school will maintain records in accordance with legal and operational requirements.

Information will be retained only for as long as necessary and then securely destroyed.

Retention periods will be determined using:

- statutory requirements;
- regulatory guidance;
- recognised sector retention schedules;
- operational necessity.

Paper records will be shredded or confidentially disposed of.

Electronic records will be securely deleted.

14. Information Security

The school will implement appropriate measures to protect personal information against unauthorised access, disclosure, loss, destruction or misuse.

Security measures may include:

- secure passwords;
- multi-factor authentication where appropriate;
- encryption;
- access controls;
- user permissions;
- secure networks;
- anti-malware protection;
- secure backups;
- physical security measures.

Staff must:

- lock devices when unattended;
- keep passwords confidential;
- use approved systems and software;
- report cyber security concerns immediately;
- take reasonable precautions when handling confidential information.

15. Artificial Intelligence and Emerging Technologies

The school recognises the increasing use of artificial intelligence and other emerging technologies.

Where AI-enabled systems are used, the school will ensure that:

- data protection obligations are met;
- risks are assessed appropriately;
- personal data is processed securely;
- transparency is maintained;
- appropriate human oversight is applied.

Staff must not enter personal, confidential or safeguarding information into publicly available AI systems unless expressly authorised by the school.

All AI-related processing involving personal data will be subject to suitable governance and oversight arrangements.

16. Automated Decision Making

Berry Hill Primary School does not routinely make decisions based solely on automated processing that produce legal or similarly significant effects for individuals.

Should this change, appropriate safeguards and rights will be implemented in accordance with data protection legislation.

17. Data Protection Impact Assessments

The school will undertake a Data Protection Impact Assessment (DPIA) when processing is likely to result in a high risk to individuals.

A DPIA may be required for:

- new information systems;
- cloud-based solutions;
- CCTV expansion;
- biometric technologies;
- large-scale data processing;
- AI-enabled services;
- significant changes to existing systems.

The DPO will be consulted where appropriate.

18. Personal Data Breaches

A personal data breach includes any accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

All actual or suspected breaches must be reported immediately to the Headteacher.

The school will:

- investigate incidents promptly;
- maintain a breach register;
- take corrective action where necessary;
- assess risks to affected individuals;
- notify the ICO where legally required;
- inform affected individuals where required.

Lessons learned following any breach will be recorded and used to strengthen procedures.

19. Operational Communications Systems

School communication systems, including radios, telephones, messaging services and emergency communication devices, must be used appropriately and securely.

Users must:

- avoid sharing confidential information unnecessarily;
- follow relevant school procedures;
- report any loss or misuse immediately.

20. Training and Awareness

All staff will receive appropriate data protection training.

This will include:

- induction training;
- regular refresher training;
- updates on legislative developments;
- role-specific guidance where required.

Training records will be maintained.

21. Monitoring and Review

The school will monitor compliance with this policy through:

- policy reviews;
- audits;
- incident monitoring;
- staff training records;
- advice from the DPO.

This policy will be reviewed every two years or sooner if legislative, organisational or operational changes require amendment.

22. Complaints

Individuals who are dissatisfied with how the school has handled their personal data should first raise concerns with the school.

Complaints may also be directed to the Data Protection Officer.

Individuals have the right to lodge a complaint with the Information Commissioner's Office.

Related Policies

This policy should be read alongside:

- Safeguarding and Child Protection Policy;
- Artificial Intelligence Policy
- Online Safety Policy;
- Staff Code of Conduct;
- Acceptable Use Agreements;
- Freedom of Information Publication Scheme.