

DATA PROTECTION POLICY

Brockmoor Primary School • Brierley Hill Primary School

POLICY OWNER	Senior Leadership Team
APPROVED BY	Governing Body
APPROVAL DATE	September 2026
REVIEW DATE	September 2027 or earlier if guidance changes
REVIEW CYCLE	Annual

Aspiration and opportunity for every child

1. Purpose

Black Country Federation (BCF), comprising Brockmoor Primary School and Brierley Hill Primary School, is committed to handling personal information lawfully, fairly, transparently and securely. This policy sets out the framework used across both schools to comply with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and other applicable data protection legislation.

2. Scope and accountability

This policy applies to governors, employees, agency staff, volunteers, contractors and others who process personal data on behalf of either school. Each school is responsible for the personal data it controls. The Governing Body has overall accountability for ensuring appropriate governance, resources and oversight.

The Senior Leadership Team is the document owner. Operational responsibilities may be delegated, but accountability for lawful processing remains with the relevant school and Governing Body.

3. Data Protection Officer

BCF's designated Data Protection Officer service is:

YourIG Data Protection Officer Service, Dudley MBC, The Council House, Dudley, West Midlands, DY1 1HF. Email: YourIGDPOService@dudley.gov.uk. Telephone: 01384 815607.

The DPO acts independently and advises the Governing Body and school leaders, monitors compliance, supports data protection impact assessments, provides advice on breaches and acts as a contact point for data subjects and the ICO.

4. Data protection principles

Personal data will be:

- processed lawfully, fairly and transparently
- collected for specified, explicit and legitimate purposes
- adequate, relevant and limited to what is necessary
- accurate and, where necessary, kept up to date
- kept for no longer than necessary
- processed securely, using appropriate technical and organisational measures
- managed in a way that allows the school to demonstrate compliance

5. Lawful processing

Before personal data is processed, the school will identify and record an appropriate lawful basis under Article 6 UK GDPR. Where special category data is processed, an appropriate Article 9 condition will also be identified. Criminal offence data will only be processed where there is a lawful basis and an appropriate condition or statutory authority.

Consent will only be relied upon where it is genuinely optional, specific, informed and capable of being withdrawn. The school will not use consent where another lawful basis is more appropriate.

6. Children's personal data

Children merit specific protection. Information provided to pupils will be concise, transparent and written in language appropriate to their age and understanding. Decisions about sharing children's information will place safeguarding, legal duties and the child's rights at the centre.

7. Transparency and privacy notices

BCF will make relevant privacy notices freely available. Notices will explain what information is collected, why it is used, the lawful basis, who it may be shared with, how long it is retained, individual rights and how to raise a concern. Privacy notices will be reviewed at least annually and whenever there is a significant change in processing.

8. Data minimisation, accuracy and retention

Staff must only collect and access information necessary for their role. Reasonable steps will be taken to keep information accurate. Records will be retained in accordance with the school's retention schedule, legal requirements and recognised records-management guidance, then securely deleted, destroyed or transferred as appropriate.

9. Information security

BCF will use proportionate technical and organisational measures to protect personal data from accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access. Measures include access controls, secure authentication, appropriate device and network security, secure disposal, staff training, supplier assurance and incident management.

10. Data sharing and processors

Personal data may be shared where there is a lawful basis, including with Dudley MBC, the Department for Education, other schools, health and social care services, safeguarding partners, professional advisers, regulators and contracted service providers. Information will not be shared simply because it has been requested. Staff must consider necessity, proportionality, lawful basis, security and any relevant safeguarding duties.

Where a supplier processes personal data on the school's behalf, appropriate due diligence, contractual data protection clauses and security assurances will be in place. New or materially changed systems must be considered through the school's data protection and procurement processes.

11. Data Protection Impact Assessments

A Data Protection Impact Assessment (DPIA) will be considered before processing that is likely to result in a high risk to individuals, and for significant new uses of technology or personal data. The DPO will be consulted where appropriate.

12. Photographs, video, CCTV, filtering and monitoring, and AI

Where the schools use photographs, video, CCTV, safeguarding filtering or monitoring systems, or artificial intelligence tools, leaders will ensure that the processing has a defined purpose and lawful basis, is proportionate, secure and transparent, and is subject to appropriate risk assessment. Personal data must not be entered into unapproved AI or online services.

13. Individual rights

Depending on the circumstances, individuals may have rights of access, rectification, erasure, restriction, objection, data portability and rights relating to automated decision-making. Requests must be passed promptly to the school office/DPO and handled within the statutory timescales. A pupil's right to their own information is distinct from a parent's right of access to an educational record.

14. Personal data breaches

Any actual or suspected loss, unauthorised disclosure, misdirection, cyber incident or inappropriate access involving personal data must be reported immediately through the school's incident process. The school will contain and assess the incident, consult the DPO and, where required, notify the ICO and affected individuals within the applicable statutory timescales.

15. Freedom of Information and records management

Data protection law does not prevent lawful transparency. Requests under the Freedom of Information Act 2000, Environmental Information Regulations 2004 and subject access provisions will be handled under the relevant procedures. Personal data will be protected where an exemption or other legal restriction applies.

16. Training and compliance

All staff who handle personal data will receive appropriate data protection and information-security training. Leaders will reinforce expectations through induction, updates, audits and incident learning. Failure to follow this policy may be addressed through the school's disciplinary or contractual procedures.

17. Concerns and complaints

Questions or concerns should normally be raised with the school in the first instance and may also be raised with the DPO. Individuals also have the right to complain to the ICO.

[ICO - Make a complaint](#)