CITY OF BIRMINGHAM EDUCATION DEPARTMENT

BASKERVILLE SCHOOL

DATA PROTECTION POLICY

BASKERVILLE SCHOOL - Data Protection Policy
School Address: Fellows Lane, Harborne, Birmingham, B17 9TS
Telephone: 0121 427 3191
Email: enquiries@baskerville.bham.sch.uk
Date Reviewed: August 2025
Next Review: August 2026
Approved by: Governing Body

1. EXECUTIVE SUMMARY

This policy outlines how Baskerville School processes personal data in compliance with UK data protection law, specifically the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. The UK GDPR sets out key principles, rights and obligations for processing personal data in the UK.

Key Points:

- We are committed to protecting the privacy and security of all personal data we process
- All staff must follow this policy and receive appropriate training
- We have clear procedures for handling data subject rights and data breaches
- We only collect and use personal data when necessary for our educational purposes

---

2. SCOPE AND APPLICATION

This policy applies to:

- All governors, employees, volunteers, and contractors at Baskerville School
- All personal data we collect about pupils, parents/carers, staff, and visitors
- All methods of data processing (paper-based and electronic)

---

3. VISION AND COMMITMENT

Our Vision We ensure each student can access opportunities for academic, social, emotional and physical development. We use autism-specific, empathetic approaches and create an autism-sympathetic learning environment that maximises potential and builds on strengths and interests.

Data Protection Commitment We are committed to being transparent about how we collect and use personal data, and to meeting our data protection obligations. We will protect the fundamental rights and freedoms of individuals and their right to the protection of personal data.

---

4. LEGAL FRAMEWORK

Our data protection practices are governed by:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Data (Use and Access) Act 2025 (where applicable)
- Children's Code (Age-Appropriate Design Code) - as best practice

---

5. KEY DEFINITIONS

Personal Data: Information relating to an identified or identifiable living person, including names, addresses, phone numbers, email addresses, photographs, and any other information that could identify someone.

Special Category Data: Sensitive personal data including information about health, racial or ethnic origin, political opinions, religious beliefs, trade union membership, genetics, biometrics, sex life, or sexual orientation.

Data Subject: The living individual who is the subject of the personal data.

Data Controller: Baskerville School, as the organisation that determines the purposes and means of processing personal data.

Processing: Any activity involving personal data, including collecting, storing, using, sharing, or deleting it.

---

6. DATA PROTECTION PRINCIPLES

We process all personal data in accordance with the following principles:

6.1 Lawfulness, Fairness, and Transparency

- We have a lawful basis for all data processing
- We are fair and transparent about how we use personal data
- We provide clear privacy notices explaining our data processing

6.2 Purpose Limitation

- We only collect personal data for specified, explicit, and legitimate purposes
- We do not use data for purposes incompatible with the original purpose

6.3 Data Minimisation

- We only collect personal data that is adequate, relevant, and necessary
- We regularly review what data we collect and hold

6.4 Accuracy

- We take reasonable steps to ensure personal data is accurate and up to date
- We correct or delete inaccurate data promptly

6.5 Storage Limitation

- We only keep personal data for as long as necessary
- We have clear retention schedules and secure deletion procedures

6.6 Security

- We implement appropriate technical and organisational measures to protect personal data
- We protect against unauthorised access, loss, destruction, or damage

6.7 Accountability

- We can demonstrate our compliance with data protection law
- We maintain appropriate documentation and implement data protection by design

---

7. LAWFUL BASES FOR PROCESSING

We process personal data under the following lawful bases:

For Pupils:

- **Public task:** Education is a function we perform in the public interest
- **Legal obligation:** We must process certain data to comply with legal requirements
- **Vital interests:** In emergency situations to protect health or safety
- **Consent:** For some activities like school trips or photography (where required)

For Staff:

- **Contract:** To fulfil employment obligations
- **Legal obligation:** For statutory requirements like payroll and safeguarding
- **Legitimate interests:** For references and professional development (where appropriate)

For Special Category Data:

- **Substantial public interest:** For safeguarding and educational needs
- **Explicit consent:** Where specifically required
- **Vital interests:** In medical emergencies

---

8. PRIVACY NOTICES

We provide clear privacy notices explaining how and why we process personal data. These include:

- **Pupil Privacy Notice:** For students and their parents/carers

- **Staff Privacy Notice:** For all employees and volunteers
- **Visitor Privacy Notice:** For contractors and visitors

Privacy notices are available on our website and updated regularly. They explain:

- What personal data we collect
- Why we process it
- Who we share it with
- How long we keep it
- Individual rights and how to exercise them
- How to contact us with questions

---

9. DATA SHARING

We may share personal data with:

- **Local authorities:** For statutory reporting and safeguarding
- **Government departments:** For census data and regulatory requirements
- **Other schools:** When pupils transfer or for educational activities
- **Healthcare professionals:** For medical needs and safeguarding
- **IT service providers:** Under strict contractual arrangements
- **Examination boards:** For qualifications and assessments

All data sharing is:

- Lawful and necessary for specific purposes
- Subject to appropriate safeguards and contracts
- Limited to what is required
- Documented and monitored

---

10. INTERNATIONAL TRANSFERS

We may transfer personal data outside the UK for:

- School trips abroad
- Online educational services
- IT systems hosted internationally

All international transfers comply with UK GDPR requirements and include appropriate safeguards such as:

- Adequacy decisions
- Standard contractual clauses
- Explicit consent (where appropriate)

---

11. INDIVIDUAL RIGHTS

Data subjects have the following rights:

11.1 Right of Access (Subject Access Request)

- We respond to subject access requests within one month
- Parents can request their child's educational records (separate right with 15 school day response time)
- We provide information free of charge unless requests are excessive

11.2 Right to Rectification

- We correct inaccurate personal data promptly
- We notify relevant third parties of corrections where appropriate

11.3 Right to Erasure

- We delete personal data when no longer needed
- We consider requests for deletion carefully, balancing individual rights with our legal obligations

11.4 Right to Restrict Processing

- We can limit how we use personal data in certain circumstances
- We maintain secure records of restricted data

11.5 Right to Data Portability

- We provide data in a structured, machine-readable format where applicable
- This mainly applies to data processed automatically with consent or contract

11.6 Right to Object

- Individuals can object to processing based on legitimate interests
- We stop processing unless we have compelling legitimate grounds

11.7 Rights Related to Automated Decision-Making

- We do not use purely automated decision-making for significant decisions
- We explain any automated processing and provide human review opportunities

---

12. CONSENT

When we rely on consent, it must be explicit and freely given. We ensure:

- Consent requests are clear and separate from other terms
- We explain what we're asking consent for
- We make it easy to withdraw consent
- We regularly review and refresh consent
- For children, we consider their age and understanding

Note: For most school activities, we don't rely on consent as we have other lawful bases like public task.

---

13. DATA SECURITY

We protect personal data through:

13.1 Technical Measures

- Secure IT systems with appropriate access controls
- Regular software updates and security patches
- Encryption for sensitive data and portable devices
- Secure backup systems
- Anti-virus and firewall protection

13.2 Organisational Measures

- Clear desk and clear screen policies
- Locked storage for paper records
- Staff training on data protection
- Regular security reviews and risk assessments
- Incident response procedures

13.3 Access Controls

- Role-based access to personal data
- Regular review of user permissions
- Secure password policies
- Two-factor authentication where available

---

14. DATA RETENTION

We keep personal data only as long as necessary. Our retention periods are based on:

- Legal requirements
- Information and Records Management Society (IRMS) guidance for schools
- Business needs
- Individual circumstances

Key Retention Periods:

- **Pupil records:** Until age 25 (or 7 years after leaving if longer)
- **Staff records:** 6 years after employment ends
- **Safeguarding records:** Until age 35 (or 10 years after concern if longer)
- **Accident records:** Until age 21 (or 3 years after if longer)

We securely dispose of data that is no longer needed.

---

15. DATA BREACHES

A personal data breach is any incident that compromises the security, confidentiality, integrity, or availability of personal data.

15.1 Breach Response Process

1. **Immediate action:** Contain the breach and assess the risk
2. **Investigation:** Determine the cause, scope, and impact
3. **Notification:** Report to the ICO within 72 hours if high risk
4. **Communication:** Inform affected individuals if high risk to their rights
5. **Review:** Learn from the incident and improve our procedures

15.2 Staff Responsibilities

All staff must:

- Report suspected breaches immediately to the Data Protection Officer
- Not attempt to investigate or resolve breaches themselves
- Preserve evidence and take immediate steps to minimise harm

---

16. ROLES AND RESPONSIBILITIES

16.1 Governing Body

- Ensures the school complies with data protection law
- Approves this policy and monitors its implementation
- Ensures adequate resources for data protection compliance

16.2 Headteacher

- Overall responsibility for data protection in the school
- Ensures staff understand and follow this policy
- Reports data protection issues to governors

16.3 Data Protection Officer (DPO)

Contact: [DPO Name and Contact Details]

The DPO:

- Monitors compliance with data protection law
- Provides advice and guidance to staff
- Acts as contact point for the ICO
- Conducts privacy impact assessments
- Handles data subject requests
- Maintains data protection records

16.4 All Staff

All staff must:

- Follow this policy and associated procedures
- Complete data protection training
- Report data protection concerns promptly
- Only access personal data needed for their role
- Keep personal data secure and confidential

---

17. TRAINING AND AWARENESS

We ensure all staff understand their data protection responsibilities through:

- Induction training for new staff
- Regular refresher training
- Updates on changes to law or procedures
- Specific training for those with particular responsibilities
- Clear guidance documents and procedures

---

18. MONITORING AND REVIEW

We monitor compliance through:

- Regular audits of data processing activities
- Review of privacy notices and procedures
- Analysis of data subject requests and complaints
- Staff feedback and training needs assessment
- Incident reporting and analysis

This policy is reviewed annually or when:

- There are changes to data protection law
- We identify new risks or processing activities
- Following significant incidents
- As part of our continuous improvement process

---

19. PRIVACY IMPACT ASSESSMENTS

We conduct Privacy Impact Assessments (PIAs) for new processing activities that pose high privacy risks, including:

- New IT systems processing personal data
- Sharing data with new third parties
- New surveillance systems (CCTV)
- Significant changes to existing processing

PIAs help us identify and mitigate privacy risks before they occur.

---

20. COMPLAINTS AND CONCERNS

If you have concerns about how we handle personal data:

1. **Contact us first:** Speak to our Data Protection Officer
2. **Formal complaint:** Follow our school complaints procedure
3. **External complaint:** Contact the Information Commissioner's Office (ICO)
    - Website: ico.org.uk
    - Phone: 0303 123 1113

We take all data protection concerns seriously and will investigate promptly.

This policy complies with current UK data protection legislation including the UK GDPR, Data Protection Act 2018, and relevant updates from the Data (Use and Access) Act 2025.