Bowbrook School

BOWBROOK HOUSE SCHOOL

GDPR (General Data Protection Regulations) and Data Protection Policy

Approved by the Head Teacher: Sept 2026
Active from: Sept 2026
Next review date: Sept 2027

INTRODUCTION

Bowbrook House School collects, stores and processes personal data relating to staff, pupils, parents/guardians, visitors and contractors as part of its educational and administrative functions. The school is committed to protecting the rights and privacy of individuals and ensuring that all personal data is processed in accordance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA 2018), the Data (Use and Access) Act 2025 (DUAA), and other relevant legislation.

This policy applies to all personal data held by the school, whether in paper or electronic format, and covers all processing activities including obtaining, recording, storing, sharing, destroying or otherwise using personal data.

GLOSSARY OF KEY TERMS

- Personal Data: Information relating to an identifiable individual.
- Data Subject: The individual whose personal data is being processed.
- Data Controller: The individual or legal person who determines the purposes and means of the processing of personal data.
- Data Processor: A third party processing data on behalf of the Data Controller.
- DPO: Data Protection Officer responsible for overseeing compliance.

1. RESPONSIBILITY UNDER GDPR

Bowbrook House School is registered with the ICO (Information Commissioners Office) as the Data Controller (registration number Z2130722). The Senior Management Team holds overall responsibility for ensuring that the school complies with all relevant data protection obligations. Mrs Ruth Hunt is the Data Protection Officer (DPO) and will deal with requests and enquiries as required.

2. COMPLIANCE

All staff are responsible for ensuring personal data is kept secure and not disclosed to unauthorised parties. Staff must only access personal data when necessary for their role.

The school will:

- Ensure personal data is accessible only to authorised individuals
- Maintain appropriate physical and electronic security measures
- Require external partners with access to personal data to comply with this policy
- Obtain consent where required, especially for special category data
- Ensure consent is freely given, informed, and never inferred from silence
- Update this policy as legislation or best practice evolves

Breaches of this policy may result in disciplinary action.

3. DATA PROTECTION PRINCIPLES

The school adheres to all UK GDPR principles:

3.1 Lawfulness, Fairness and Transparency

Personal data will only be processed for the specific, explicit and legitimate purposes.

Lawful bases include: -

- Contract
- Legal obligation
- Vital interests
- Public task
- Legitimate interests (including DUAA recognised interests)
- Consent

Special category data will only be processed under an Article 9 condition.

Privacy Notices will inform individuals about data collection, purposes, and sharing.

Sharing Personal Data

Certain data is exempt from the provisions of the DPA 2018 and the school will share personal data where the school is legally required to do so, including for:

- the prevention or detection of crime and/or fraud
- the apprehension or prosecution of offenders
- the assessment or collection of tax owed to HMRC
- in connection with legal proceedings
- where the disclosure is required to satisfy the school's safeguarding obligations
- the school may also share personal data with emergency services and local authorities to help them respond to an emergency.

3.2 Purpose Limitation and Data Minimisation

Data will only be used for the purpose for which it was collected unless additional processing is lawful or consented to. Staff must delete or anonymise data when no longer required.

3.3 Accuracy

The school will ensure personal data is accurate and up to date. Individuals must notify the school of changes. The DPO will act on requests to correct inaccurate data.

3.4 Storage Limitation

Data will not be retained longer than necessary. Regular reviews will ensure data is securely deleted or anonymised when no longer required.

3.5 Integrity and Confidentiality (Security)

The school will protect personal data against unauthorised access, alteration, disclosure, loss or destruction.

Disposal: Paper records will be shredded or securely destroyed by approved contractors. Electronic files will be securely deleted or overwritten.

Personal Data Breaches: Breaches will be reported to the ICO within 72 hours where required. Examples include:

- Safeguarding information disclosed to unauthorised persons
- Theft of unencrypted devices
- Sending data to incorrect recipients
- Unauthorised access

3.6 Accountability

The school will:

- Inform individuals why data is collected
- Inform individuals when data is shared
- Ensure data is not retained longer than necessary
- Destroy obsolete data securely
- Maintain safeguards against loss or unauthorised disclosure
- Share data only when legally appropriate
- Train staff in data protection responsibilities

4. INDIVIDUAL RIGHTS

The UK GDPR provides the following rights:

4.1 Right to be Informed

The school provides clear Privacy Notices explaining how personal data is used.

4.2 Right of Access

Individuals may request access to their personal data. The school will respond within one month.

4.2.1 Subject Access Requests (SARs)

Subject Access Requests may be made verbally or in writing to the Data Protection Officer. The school will record verbal requests appropriately and respond within the statutory timescale.

Certain data is exempt, including:

- Information identifying other individuals
- Information likely to cause harm
- Legally privileged information
- Examination scripts

The school may seek clarification of broad requests. Where permitted by law, the response period may be paused while clarification is obtained

4.2.2 Children and SARs

A child may exercise their own information rights where the school considers them mature enough to understand the nature of the request and its consequences. The school will assess requests on a case-by-case basis, taking account of the child's age, maturity and understanding.

4.3 Right to Rectification

The school will correct inaccurate data within one month (or two months if complex).

4.4 Right to Erasure

The school will delete personal data where no lawful basis for retention exists, unless retention is required by law or safeguarding obligations.

4.5 Right to Restrict Processing

Processing may be restricted where:

- Accuracy is contested
- Processing is unlawful
- Data is needed for legal claims
- An objection is pending

International transfers will not occur without explicit consent unless lawful safeguards exist.

4.6 Right to Data Portability

Applies only where:

- Processing is based on consent or contract
- Data is provided directly by the individual
- Processing is automated

4.7 Right to Object

Individuals may object to processing. The school will stop processing unless compelling legitimate grounds exist.

4.8 Rights Related to Automated Decision Making and Profiling

Any significant automated decisions affecting individuals would be subject to lawful safeguards, transparency, and human review.

5. CCTV

The school operates CCTV in accordance with UK GDPR, the Data Protection Act 2018, current ICO guidance and relevant surveillance camera legislation and guidance.

5.1 Security Measures

- Footage encrypted and password-protected
- Access logged and restricted
- Retention period: **30 days** unless required for investigations
- Equipment securely maintained
- Cybersecurity controls in place

5.2 Data Protection and Access

- Cameras positioned to avoid private areas
- Clear signage displayed
- No audio recording
- No monitoring of private spaces

5.3 CCTV System Purposes

- Safeguarding
- Disciplinary investigations
- Accident/incident investigation
- Crime prevention
- Protection of property

5.4 CCTV System Restrictions

CCTV is **not** used for:

- Audio recording
- Commercial purposes
- Tracking individuals without lawful basis
- Monitoring private areas

6. PHOTOGRAPHS & VIDEOS

The school will identify an appropriate lawful basis before using photographs or videos. Where consent is the lawful basis, written consent will be obtained and may be withdrawn. Images will not be accompanied by identifying personal information.

The school obtains written parental consent for photographs and videos used for:

- School publications
- External agencies
- Website and social media

7. INCIDENT RESPONSE

The school will report qualifying breaches to the ICO within 72 hours and notify affected individuals where high risk exists.

8. COOKIES AND TRACKING TECHNOLOGIES

- **Essential cookies** do not require consent
- The school will provide clear cookie information and opt-out options
- The school will comply with PECR and any applicable exemptions introduced under the Data (Use and Access) Act 2025 when using analytics or statistical cookies.

9. RECOGNISED LEGITIMATE INTERESTS

Where applicable, the school may rely on the recognised legitimate interests, lawful basis introduced by the Data (Use and Access) Act 2025.

Although a balancing test is not required for recognised legitimate interests, the school must still demonstrate that processing is necessary and comply with all other UK GDPR requirements.

10. COMPLAINTS

Parents, pupils, staff or other who believe their personal data has been mishandled must make a complaint to the School in the first instance and **not** directly to the ICO. All complaints will be acknowledged within 30 days of receipt and the School will take appropriate steps to investigate complaints without undue delay, and will communicate the outcome promptly.

Concerns should be directed to:

Mrs Ruth Hunt, DPO Email: ruth.hunt@bowbrookhouseschool.co.uk Telephone: 01905 841 242 Address: Bowbrook House School, Peopleton, Pershore, WR10 2EE

10.1 Internal Complaints Procedure

The school will investigate data protection complaints promptly and transparently. If unresolved, individuals may escalate to the ICO.

11. DATA SHARING & INFORMATION SHARING AGREEMENTS (ISA)

Bowbrook House School is committed to ensuring that any sharing of personal data is lawful, proportionate, transparent, and compliant with the UK GDPR, the Data Protection Act 2018, and the Data (Use and Access) Act 2025. The school follows the ICO's *Information Sharing Code of Practice (2023)* and will maintain formal Information Sharing Agreements (ISAs) with relevant partners as necessary.

11.1 Principles for Data Sharing

The school will only share personal data when:

- There is a **clear and lawful basis** for sharing (legal obligation, vital interests, public task, consent, or recognised legitimate interests under DUAA 2025).
- Sharing is **necessary**, **proportionate**, and **minimises risk**.
- The individual has been informed through the school's Privacy Notice unless an exemption applies.
- The receiving organisation agrees to maintain **equivalent or stronger security standards**.

11.2 Categories of External Partners

The school may share personal data with the following categories of authorised partners:

- **Local Authorities** (education, safeguarding, attendance, SEND services)
- **Law Enforcement Agencies** (crime prevention, investigations)
- **Health & Social Care Providers** (NHS, CAMHS, social services)
- **Emergency Services** (police, fire, ambulance)
- **Regulatory Bodies** (ICO, Ofsted, HMRC)
- **Professional or Educational Bodies** (exam boards, awarding organisations)

- **Contracted Service Providers** (IT support, school photographers, safeguarding platforms)
- **Other Schools or Educational Institutions** (transfers, safeguarding continuity)

Each partner must have a valid reason for receiving the data and must comply with the terms of the relevant ISA.

11.3 Lawful Bases for Sharing

Data may be shared under the following lawful bases:

- **Legal obligation** – e.g., safeguarding, attendance returns, statutory reporting
- **Vital interests** – preventing harm or protecting life
- **Public task** – delivering education and safeguarding functions
- **Recognised legitimate interests (DUAA 2025)** – safeguarding, crime prevention, public safety
- **Consent** – where no other lawful basis applies and consent is freely given

Special category data will only be shared where an additional condition under UK GDPR Article 9 is met.

11.4 Decision-Making Process for Sharing

Before sharing any personal data, staff must follow the ISA decision framework:

1. **Purpose Test** – Why is the data needed? Is sharing necessary?
2. **Lawful Basis Test** – Which lawful basis applies?
3. **Proportionality Test** – Is the minimum amount of data being shared?
4. **Risk Assessment** – Are there risks to the individual? Can they be mitigated?
5. **Security Check** – Is the recipient able to protect the data appropriately?
6. **Record Keeping** – The decision and justification must be logged.
7. **Transparency** – Inform the individual unless an exemption applies (e.g., safeguarding concerns).

11.5 Information Sharing Agreements (ISAs)

Where regular or ongoing data sharing occurs, the school will establish and maintain Information Sharing Agreements where appropriate.

Where information is relevant to safeguarding and promoting the welfare of a child, the school will comply with the statutory information sharing duty under Section 16LA of the Children Act 2004. Staff should presume that relevant information ought to be shared unless there is a lawful reason not to do so and should refer to the school's Safeguarding policy for full guidance.

11.6 Emergency or Safeguarding Situations

In urgent circumstances, data may be shared **without consent** where:

- A child or individual is at risk of significant harm
- There is a threat to life
- Law enforcement requires information for crime prevention or investigation

The school will always document the decision and rationale.

11.7 International Transfers

Personal data will not be transferred outside the **United Kingdom** unless:

- The destination country has an **adequacy decision**, or
- Appropriate safeguards (e.g., IDTA, SCCs) are in place, and
- where lawful transfer mechanisms and safeguards are in place
- A transfer risk assessment will be completed where required

The school will not publish personal data online (including photographs) without explicit consent where it may be accessed internationally.

11.8 Retention and Disposal of Shared Data

Data shared with external partners will be retained only for the period necessary to fulfil the purpose of sharing. Partners must:

- Follow the school's retention schedule
- Dispose of data securely
- Confirm destruction upon request where appropriate

11.9 Pupil Medication and Health Information

Bowbrook House School recognises that information relating to a pupil's medication, medical conditions, treatment plans, allergies, healthcare needs and the administration of medicines constitutes **special category personal data** and requires enhanced protection. The school will process such information in accordance with UK GDPR, the Data Protection Act 2018, safeguarding obligations and statutory guidance relating to supporting pupils with medical conditions.

The school may collect, hold and process medication information for the purposes of:

- Safeguarding and promoting pupil welfare
- Supporting pupils with medical conditions
- Ensuring medicines are administered safely and appropriately
- Responding to medical emergencies
- Meeting legal and regulatory obligations
- Facilitating educational access and participation

Access to medication records will be restricted to authorised staff who require the information to fulfil their duties, including the School Nurse, designated first aiders, relevant teaching staff, pastoral staff, school leaders and healthcare professionals where appropriate.

The school may share medication or healthcare information with:

- Parents and those with parental responsibility
- NHS professionals and other healthcare providers
- Local authority services
- Emergency services
- Other educational settings where a pupil transfers, when lawful and necessary

Where medication information is shared, the school will ensure that only the minimum necessary information is disclosed and that appropriate security and confidentiality measures are maintained.

Individual Healthcare Plans (IHPs), medication consent forms, records of medicine administration and related healthcare documentation will be stored securely, either electronically or in paper form, with access restricted to authorised personnel. These records will be retained in accordance with the school's retention schedule and safeguarding requirements.

In emergency situations, relevant medical information may be shared without consent where necessary to protect the vital interests of the pupil or another individual. Such disclosures will be documented and reviewed appropriately.

12. Data Protection Impact Assessments (DPIAs)

A school should conduct a DPIA when introducing:

- new CCTV systems
- safeguarding software
- biometric systems
- AI tools
- monitoring technologies
- large-scale processing of special category data

13. Linked policies

- Complaints
- Online Safety
- Cybersecurity
- IT Acceptable Use
- Safeguarding

Appendix: Data Retention Schedule

This schedule sets out how long Bowbrook House School retains personal data before secure deletion or anonymisation. Retention periods are based on statutory requirements, safeguarding duties, educational regulations, and ICO guidance.

1. Pupil Records

Category	Retention Period	Notes
Pupil Admission Records	6 years after pupil leaves	Required for legal claims & DfE audits
Pupil Educational Record	Until pupil reaches age 25	Includes academic, pastoral, attendance
Safeguarding / Child Protection Files	Until pupil is 35	Statutory requirement (KCSIE + ICO)
Attendance Registers	3 years	Education (Pupil Registration) Regulations
Behaviour & Exclusion Records	6 years after pupil leaves	For legal defence
Accident/Incident Reports	3 years (pupils) / 6 years (staff)	RIDDOR requirements
Photographs & Videos	Until consent withdrawn or 2 years after use	Deleted immediately upon withdrawal
CCTV Footage	30 days unless required for investigation	Surveillance Camera Code of Practice

2. Staff Records

Category	Retention Period	Notes
Personnel Files	6 years after employment ends	Standard HR retention
Payroll & Salary Records	6 years	HMRC requirement
DBS Certificates	Not retained	Only outcome recorded
Training Records	6 years	Includes safeguarding training
Sickness & Absence Records	6 years	HR & legal defence
Disciplinary Records	6 years	Unless safeguarding-related
Recruitment Records	1 year for unsuccessful candidates	ICO guidance

3. Parent / Guardian Records

Category	Retention Period
Contact Information	Until pupil leaves + 1 year
Financial Records / Fee Payments	6 years (HMRC)
Complaints	6 years

4. School Administration Records

Category	Retention Period
School Census Data	6 years
Health & Safety Records	6 years
Risk Assessments	3–6 years depending on type
Visitor Logs	2 years
Contractor Records	6 years

5. Financial & Legal Records

Category	Retention Period
Invoices, Receipts, Accounts	6 years (Companies Act)
Tax Records	6 years
Insurance Claims	6 years
Contracts	6 years after expiry

6. IT & Digital Records

Category	Retention Period
Email Accounts	Subject to legal hold, ongoing investigations, SARs, complaints, or safeguarding requirements.
Network Logs	12 months
Device Usage Logs	12 months
Website Cookies	Session or up to 12 months
Learning Platform Data	Until pupil leaves + 1 year

7. Special Category Data

Category	Retention Period
SEN / EHCP Records	Until pupil is 30
Medication Administration Records (MARs)	Date of entry + 3 years
Individual Healthcare Plans (IHPs)	Until pupil leaves + 6 years
Medication Consent Forms	Until superseded or pupil leaves + 6 years
Records relating to serious medical incidents	In line with accident/incident and safeguarding requirements
Safeguarding Records	In accordance with current safeguarding guidance and risk assessment, normally until at least age 35, with longer retention where records concern serious safeguarding or abuse matters

8. Data Shared Under ISA Agreements

Category	Retention Period
Local Authority Shared Data	As per ISA terms (typically 6 years)
Police Shared Data	As required for investigations
NHS / Social Care Shared Data	As per statutory safeguarding requirements

9. Secure Destruction Methods

- Paper → cross-cut shredding or certified disposal
- Digital → secure deletion, overwriting, cryptographic erasure
- Backups → deleted on rotation schedule
- Third parties → must provide destruction certificates

10. Review Cycle

Retention periods are reviewed:

- Every **two years**, or
- Immediately following legislative changes (UK GDPR, DPA 2018, DUAA 2025, KCSIE updates)