

Avon House School

Data Protection Policy



**CELEBRATING & SUPPORTING
EVERY CHILD**

To be reviewed: Summer 2026

Review date:	Summer 2025	August 2024	August 2022	August 2021	August 2020
Reviewed by:	ZM	ZM	NB	NB	NB

Data Protection Policy

1. Introduction

Avon House Preparatory School ("the School") is committed to protecting personal data and handling it responsibly.

This policy outlines how the School collects, processes, stores, shares, and protects personal information, in compliance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and guidance from the Information Commissioner's Office (ICO).

This policy applies to all stakeholders, including pupils, parents, staff, governors, visitors, and contractors.

2. Responsibilities

All members of the School community have a responsibility to handle personal data in accordance with this policy.

The School is the data controller for the purposes of the UK GDPR.

The Data Protection Officer (DPO) is responsible for overseeing the School's compliance with data protection law.

The DPO is the Bursar and can be contacted via bursar@ahsprep.co.uk

Senior leaders are responsible for ensuring departmental compliance, and all staff must undertake regular data protection training.

3. Data Protection Principles

We process personal data in accordance with the following principles:

1. **Lawfulness, fairness and transparency:** Data is processed lawfully, fairly and in a transparent manner.
2. **Purpose limitation:** Data is collected for specified, explicit and legitimate purposes.
3. **Data minimisation:** Data is adequate, relevant and limited to what is necessary.
4. **Accuracy:** Data is accurate and kept up to date.
5. **Storage limitation:** Data is kept in a form which permits identification of individuals for no longer than is necessary.
6. **Integrity and confidentiality:** Data is processed securely to ensure appropriate protection.
7. **Accountability** — with documented evidence of compliance

4. Lawful Basis for Processing Personal Data

We process personal data under one or more of the following lawful bases:

Consent

- Contract
- Legal obligation
- Vital interests
- Public task
- Legitimate interests

We document the lawful basis for each processing activity in our Data Asset Register and review it regularly.

5. Collecting Personal Data

We collect personal data directly from individuals or from third parties (e.g., local authorities, previous schools, health professionals). This may include:

- Name, address, date of birth
- Contact details
- Academic records
- Health and medical information
- Attendance and behavioural records
- CCTV footage
- Safeguarding information
- Special educational needs and disabilities (SEND) data
- Biometric data (if used, with consent)

6. Use of Personal Data

We use personal data for purposes such as:

- Providing education and pastoral care
- Administering admissions and enrolment
- Managing safeguarding and health & safety
- Communicating with parents and carers
- Meeting legal and regulatory obligations
- Monitoring ICT and device use in accordance with Acceptable Use policies
- Managing trips, clubs and extracurricular activities
- Managing school finances, including fee billing and bursary processing

7. Sharing Personal Data

We share data where necessary with:

- Other schools or educational institutions
- Local authorities and regulatory bodies
- The Department for Education (DfE)
- School service providers (e.g., IT, catering, transport)
- Health and social care professionals

- External exam boards
- Law enforcement agencies or legal representatives, when required
- Our insurance and professional advisers
- We have data sharing or data processing agreements in place where appropriate, and review these regularly.

8. Security and Storage of Personal Data

We take appropriate technical and organisational measures to protect personal data from loss, misuse, unauthorised access or disclosure. Access to data is restricted to authorised personnel.

Personal data is stored securely, whether electronically or in physical files, and is retained in accordance with the School's Data Retention Schedule and relevant legal timeframes.

Once data is no longer needed, it is securely deleted, anonymised, or archived in line with legal requirements and IRMS guidance.

Security measures include encryption, access controls, regular backups, antivirus protection, and physical safeguards.

9. International Data Transfers

Where personal data is transferred outside the UK, we ensure adequate safeguards are in place in accordance with UK GDPR requirements. This may include reliance on adequacy regulations, standard contractual clauses or other approved mechanisms.

We follow the most recent guidance from the ICO regarding international data transfers, including Transfer Risk Assessments where required.

10. CCTV

The School uses CCTV for safety, security and monitoring purposes. We do not require consent to use CCTV as it is processed under our legitimate interests to ensure the safety and security of pupils, staff and visitors. CCTV footage may be disclosed in line with our Data Protection and Safeguarding policies.

Signage is in place to inform individuals of CCTV use, and retention periods are defined in our CCTV policy.

CCTV is not used in private areas such as toilets or changing rooms.

11. Subject Access Requests

Individuals have the right to request access to their personal data. Requests should be made in writing to the Head Teacher and include:

- Name and contact details
- Relationship to the School (e.g., pupil, parent, staff member)
- Details of the information requested
- We may request proof of identity to verify the requester's identity.
- We aim to respond within one calendar month of receiving a valid request.
Extensions may apply in complex cases.

The School may require proof of identity before disclosing personal data to ensure requests are legitimate and to protect the rights of individuals. We will respond within one month of receiving a valid request.

12. Other Individual Rights

Under data protection law, individuals also have the following rights:

- To request correction of inaccurate data
- To request erasure of personal data ("right to be forgotten") in certain circumstances
- To restrict processing
- To object to processing where applicable
- To data portability (in certain limited circumstances)
- To withdraw consent at any time (where consent is the legal basis)
- To object to automated decision-making and profiling (if applicable)
- Some rights may be limited by legal or safeguarding obligations.

13. Data Breaches

We have procedures in place to deal with suspected data breaches. If a breach occurs, we will:

- Assess the risk to individuals
- Notify the ICO within 72 hours if required
- Inform affected individuals where necessary
- Maintain a record of all breaches, even if not reportable
- Review our processes to reduce recurrence

14. Training and Awareness

Staff receive regular training on data protection.

Training is provided at induction and updated annually.

Staff also receive reminders and updates during the year.

Pupils and parents are given appropriate data protection guidance through notices and school communications.



15. Complaints and Concerns

If you have any concerns about the way your personal data is being used, please contact the DPO. If you are not satisfied with the School's response, you have the right to lodge a complaint with the Information Commissioner's Office at www.ico.org.uk. We take concerns seriously and aim to respond promptly and transparently.

16. Review and Monitoring

This policy will be reviewed annually and updated as required to reflect changes in legislation, guidance or practice.

We may also review the policy earlier in response to changes in legislation, ICO guidance, or data incidents.

Policy Owner: Bursar / Data Protection Officer