



THE BISHOPSWOOD SCHOOLS FEDERATION

DATA PROTECTION POLICY

Bishopswood Schools Federation collects and uses personal information (referred to in the UK General Data Protection Regulation (UK GDPR) as personal data) about staff, pupils, parents and other individuals who come into contact with the school. This information is gathered in order to enable the provision of education and other associated functions. In addition, the school may be required by law to collect, use and share certain information.

The school is the Data Controller, of the personal data that it collects and receives for these purposes. Data Controllers have a General Duty of accountability for personal data.

The school has a Data Protection Officer, who may be contacted at 0118 981 2836 (infants), 0118 981 2738 (juniors)

The school issues Privacy Notices (also known as a Fair Processing Notices) to all pupils/parents and staff. These summarise the personal information held about pupils and staff, the purpose for which it is held and who it may be shared with. It also provides information about an individual's rights in respect of their personal data.

Purpose

This policy sets out how the school complies with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and the Data (Use and Access) Act 2025 (DUAA). This policy reflects recent legal updates to UK data protection law, including new rights for individuals and additional organisational responsibilities coming into force between 2025–2026.

This policy applies to all personal information however it is collected, used, recorded and stored by the school and whether it is held on paper or electronically.

What is Personal Information/ data?

Personal information or data means any information relating to an identified or identifiable individual. An identifiable individual is one who can be identified, directly or indirectly by reference to details such as a name, an identification number, location data, an online identifier or by their physical, physiological, genetic, mental, economic, cultural or social identity. Personal data includes (but is not limited to) an individual's, name, address, date of birth, photograph, bank details and other information that identifies them.

Data Protection Principles

The UK GDPR establishes six principles as well as a number of additional duties that must be complied with at all times:

1. **Lawfulness, fairness and transparency.** Personal data shall be processed lawfully, fairly and in a transparent manner. In order for personal data to be processed lawfully, it

must be processed on the basis of one of the legal grounds set out in the UK GDPR. These include (amongst other relevant conditions) where processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority exercised by the school. Where the special categories of personal data are processed, this shall include (amongst other relevant conditions) where processing is necessary for reasons of substantial public interest. When processing personal data and special category data in the course of school business, the school will ensure that these requirements are met where relevant.

2. **Purpose limitation.** Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (subject to exceptions for specific archiving purposes). The school will only process personal data for specific purposes and will notify those purposes to the data subject when it first collects the personal data or as soon as possible thereafter.
3. **Data minimisation.** Personal data shall be adequate, relevant and limited to what is necessary to the purposes for which they are processed and not excessive. Personal data which is not necessary for the purpose for which it is obtained will not be collected.
4. **Accuracy.** Personal data shall be accurate and where necessary, kept up to date; Personal data should be reviewed and updated as necessary and should not be retained unless it is reasonable to assume that it is accurate. Individuals should notify the school of any changes in circumstances to enable records to be updated accordingly. The school will be responsible for ensuring that updating or records takes place where appropriate.
5. **Storage limitation.** Personal data shall be kept in a form that permits the identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. The school will not keep personal data for longer than is necessary for the purpose or purposes for which they were collected and will take reasonable steps to destroy or erase from its systems all data which is no longer required.
6. **Integrity and confidentiality.** Personal data shall be processed in a manner that ensures appropriate security of the personal data and which includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Duties

Personal data shall not be transferred to a country or territory outside the UK and the European Union (EU)/European Economic Area (EEA), unless that country or territory ensures an adequate level of data protection.

The school recognises that **children's data requires enhanced protection** and will apply stricter scrutiny when processing such data, especially when using digital platforms or third-party services. The school will ensure that all data sharing arrangements and relationships with third parties are regularly reviewed to maintain compliance with data protection requirements. This includes reviewing third-party processors, existing data sharing agreements, and the safeguards in place for any international transfers of personal data. These reviews are conducted in line with updated Information Commissioner's Office (ICO) guidance and reflect the need to meet evolving legal and regulatory expectations.

Commitment

The school is committed to maintaining the principles and duties in the UK GDPR at all times. Therefore the school will:

- Inform individuals of the identity and contact details of the data controller.
- Inform individuals of the contact details of the Data Protection Officer
- Inform individuals of the purposes that personal information is being collected and the basis for this.

- Inform individuals when their information is shared, and why and with whom unless the UK GDPR provides a reason not to do this.
- If the school plans to transfer personal data outside the UK and the EU/EEA the school will inform individuals and provide them with details of where they can obtain details of the safeguards for that information.
- Inform individuals of their data subject rights.
- Inform individuals that the individual may withdraw consent (where relevant) and that if consent is withdrawn that the school will cease processing their data although that will not affect the legality of data processed up until that point.
- Provide details of the length of time an individual's data will be kept
- Should the school decide to use an individual's personal data for a different reason to that for which it was originally collected the school shall inform the individual and where necessary seek consent.
- Check the accuracy of the information it holds and review it at regular intervals.
- Ensure that only authorised personnel have access to the personal information whatever medium (paper or electronic) it is stored in.
- Ensure that clear and robust safeguards are in place to ensure personal information is kept securely and to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded.
- Ensure that personal information is not retained longer than it is needed.
- Ensure that when information is destroyed that it is done so appropriately and securely.
- Share personal information with others only when it is legally appropriate to do so.
- Comply with the duty to respond to requests for access to personal information (known as Subject Access Requests) [see section below]
- Ensure that personal information is not transferred outside the UK and the EU/EEA without the appropriate safeguards.
- Ensure that all staff and governors are aware of and understand these policies and procedures.

Subject Access Requests (SARs)

When responding to Subject Access Requests, the school will carry out reasonable and proportionate searches for personal data, in line with updated legal requirements and guidance. This means the school will take practical and appropriate steps to locate personal data without undertaking excessive or unnecessary searches, while still ensuring that individuals' rights of access are respected.

Retention and Disposal of Personal Data

The school will dispose of personal data in a way which protects the rights and privacy of data subjects (e.g. shredding, disposal as confidential waste, secure electronic deletion) as appropriate. The school maintains a Retention Schedule that is specific and relevant to the specific types of information retained. The schedule outlines the appropriate periods for retention in each case.

Complaints

The school has a formal Data Protection Complaints Procedure in line with new statutory requirements released in June 2026. This procedure provides multiple accessible channels for individuals to raise concerns, including by email, telephone, or in writing, and is supported by clear guidance within the school's privacy notice. All complaints are formally logged and tracked, receipt acknowledged within 30 days and responded to without undue delay. Where appropriate, matters will be escalated to the Data Protection Officer (DPO). Individuals are also informed of their right to escalate concerns to the Information Commissioner's Office (ICO) if they are not satisfied with the school's response.

The Use of Artificial Intelligence (AI)

Where the school uses automated systems, including software or AI tools, that may have a significant effect on individuals, it ensures that appropriate safeguards are in place. These include providing transparency about how decisions are made, offering the opportunity for human review, and allowing individuals to challenge decisions. The school may also rely on the expanded lawful bases for automated decision-making introduced under the Data (Use and Access) Act 2025, where this is permitted and appropriate safeguards are maintained.

Review

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 2 years. The policy review will be undertaken by the Data Protection Officer, Executive Head teacher, or nominated representative.

Contacts

If you have any enquires in relation to this policy, please contact Mr Glen Golding (Executive Headteacher) who will also act as the contact point for any queries.

Policy Reviewed – June 2026

Next Review – June 2028