



The Stonebridge
School

DATA PROTECTION POLICY

Date: *December 2025*

Approved by:	Full Governing Body
Last reviewed:	December 2025
Next review due by:	December 2026

Headteacher: Kate Pelazza

Data Protection Officer: Veren Vaja

Contact: admin@stonebridge.brent.sch.uk

Approved by: Governing Board

1. Aims

Our school aims to ensure that all personal data collected about staff, pupils, parents and carers, governors, visitors and other individuals is collected, stored and processed in accordance with UK data protection law.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Legislation and guidance

This policy meets the requirements of the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018).

It is based on guidance published by the Information Commissioner's Office (ICO) on the UK GDPR and guidance from the Department for Education (DfE) on generative artificial intelligence in education.

It also reflects the ICO's guidance for the use of surveillance cameras and personal information.

In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

3. Definitions

Personal data

Any information relating to an identified, or identifiable, living individual. This may include the individual's name (including initials), identification number, location data, online identifier such as a username, and factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.

Special categories of personal data

Personal data which is more sensitive and so needs more protection, including information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetics, biometrics where used for identification purposes, health, sex life or sexual orientation.

Processing

Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.

Data subject

The identified or identifiable individual whose personal data is held or processed.

Data controller

A person or organisation that determines the purposes and the means of processing personal data.

Data processor

A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.

Personal data breach

A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

4. The data controller

Our school processes personal data relating to parents and carers, pupils, staff, governors, visitors and others, and therefore is a data controller.

The school is registered with the ICO and has paid its data protection fee to the ICO, as legally required.

5. Roles and responsibilities

This policy applies to all staff employed by our school, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

5.1 Governing board

The governing board has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

5.2 Data protection officer (DPO)

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

The DPO will provide an annual report of their activities directly to the governing board and, where relevant, report to the board their advice and recommendations on school data protection issues.

The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO.

Our DPO is Veren Vaja and is contactable via admin@stonebridge.brent.sch.uk.

5.3 Headteacher

The headteacher acts as the representative of the data controller on a day-to-day basis.

5.4 All staff

Staff are responsible for collecting, storing and processing any personal data in accordance with this policy; informing the school of any changes to their personal data; and contacting the DPO with questions or concerns about data protection, lawful bases, consent, privacy notices, individual rights, international transfers, data breaches, new processing activities, contracts or data sharing.

6. Data protection principles

The UK GDPR is based on data protection principles that our school must comply with.

Personal data must be processed lawfully, fairly and transparently; collected for specified, explicit and legitimate purposes; adequate, relevant and limited to what is necessary; accurate and kept up to date where necessary; kept for no longer than necessary; and processed securely.

7. Collecting personal data

7.1 Lawfulness, fairness and transparency

We will only process personal data where we have a lawful basis under data protection law. These include contract, legal obligation, vital interests, public task or official authority, legitimate interests where applicable, and consent.

For special category and criminal offence data, we will also meet the additional conditions required by data protection law.

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

We will always consider the fairness of our data processing and will not handle personal data in ways individuals would not reasonably expect or in ways that have unjustified adverse effects.

7.2 Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons and will explain these reasons when we first collect the data.

If we want to use personal data for another purpose, we will inform the individuals concerned before doing so and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

We will keep data accurate and, where necessary, up to date. When personal data is no longer needed, it will be deleted or anonymised in accordance with the school's record retention schedule.

8. Sharing personal data

We will not normally share personal data with anyone else without consent, but there are circumstances where we may be required or permitted to do so.

Where suppliers or contractors process personal data for the school, we will only appoint organisations that provide sufficient guarantees of compliance, put appropriate contractual arrangements in place and share only the data needed to provide the service.

We will share personal data with law enforcement, government bodies, emergency services and local authorities where legally required or otherwise permitted by law.

Where we transfer personal data internationally, we will do so in accordance with UK data protection law.

9. Subject access requests and other rights of individuals

9.1 Subject access requests

Individuals have a right to make a subject access request to gain access to personal information that the school holds about them.

Subject access requests can be submitted in any form. Requests may be dealt with more quickly if they include the individual's name, correspondence address, contact details and details of the information requested.

If staff receive a subject access request, they must immediately forward it to the DPO.

9.2 Children and subject access requests

Personal data about a child belongs to that child, not to their parents or carers. Whether a parent or carer may exercise a child's rights on their behalf depends on the child's ability to understand their rights and the implications of the request. This will be considered on a case-by-case basis.

9.3 Responding to subject access requests

We will respond to subject access requests without undue delay and within the timescales required by data protection law. Information will normally be provided free of charge, subject to the circumstances in which the law permits a reasonable fee or refusal.

Where a request is refused, we will explain why and inform the individual of their right to complain to the ICO or seek to enforce their rights through the courts.

9.4 Other data protection rights of the individual

Individuals may also have rights to withdraw consent, request rectification, erasure or restriction, object to certain processing, challenge certain automated decisions, be notified of a breach in certain circumstances, complain to the ICO, and request data portability where applicable.

Requests to exercise these rights should be directed to the DPO via admin@stonebridge.brent.sch.uk.

10. Parental requests to see the educational record

Parents, or those with parental responsibility, have a legal right to access their child's educational record in accordance with the Education (Pupil Information) (England) Regulations 2005.

The school will respond within the statutory timescale and may charge a fee for a copy where permitted.

12. CCTV

We use CCTV in various locations around the school site to help keep the site safe and secure. We will follow the ICO's guidance for CCTV and comply with data protection principles.

We make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to the school via admin@stonebridge.brent.sch.uk.

13. Photographs and videos

As part of our school activities, we may take photographs and record images of individuals within our school.

We will obtain consent where required for photographs and videos used for communication, marketing and promotional materials and will explain how they will be used.

Consent can be refused or withdrawn at any time. Where consent is the lawful basis and is withdrawn, we will stop the relevant use in accordance with data protection law.

14. Artificial intelligence (AI)

Artificial intelligence tools are increasingly widespread. The Stonebridge School recognises that AI has educational uses but can also pose risks to personal and sensitive data.

Personal or sensitive data must not be entered into unauthorised generative AI tools or chatbots. Where this occurs, the school will treat it as a potential data breach and follow the personal data breach procedure in appendix 1.

15. Data protection by design and default

We will integrate data protection into our processing activities by appointing and supporting a DPO, processing only data necessary for each purpose, completing data protection impact assessments where required, integrating data protection into policies and privacy notices, training staff, reviewing and auditing our arrangements, applying safeguards to international transfers and maintaining records of processing activities.

16. Data security and storage of records

We will protect personal data against unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

Appropriate organisational and technical measures will be used to protect paper and electronic records. Staff must follow the school's security, online safety and acceptable-use requirements.

Where personal data is shared with a third party, the school will carry out appropriate due diligence and take reasonable steps to ensure it is stored securely and adequately protected.

17. Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely where it cannot or does not need to be rectified or updated.

Where a third party disposes of records on the school's behalf, the school will require sufficient guarantees that the provider complies with data protection law.

18. Personal data breaches

The school will take reasonable steps to prevent personal data breaches.

In the event of a suspected breach, we will follow the procedure in appendix 1. Where required, the school will report a breach to the ICO within 72 hours of becoming aware of it.

19. Training

All staff and governors are provided with data protection training as part of their induction process.

Data protection will also form part of continuing professional development where changes to legislation, guidance or school processes make this necessary.

20. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed annually and approved by the full governing board.

21. Links with other policies

This data protection policy is linked to our Freedom of Information Publication Scheme, privacy notices, staff code of conduct and relevant online safety and acceptable-use policies.

Appendix 1: Personal data breach procedure

On finding or causing a breach or potential breach, the staff member, governor or data processor must immediately notify the DPO via admin@stonebridge.brent.sch.uk.

The DPO will investigate and determine whether a breach has occurred. Staff and governors will co-operate with the investigation.

If a breach has occurred or is likely to have occurred, the DPO will alert the headteacher and chair of governors and will take reasonable steps to contain and minimise its impact.

The DPO will assess the potential consequences, determine whether the ICO and affected individuals must be notified, and document the decision.

Where the ICO must be notified, the DPO will do so within 72 hours of the school becoming aware of the breach, providing the information required by law as soon as it is available.

Where the school is required to communicate with affected individuals, the DPO will provide clear information about the breach, likely consequences and measures taken or proposed.

The DPO will document each breach, irrespective of whether it is reported to the ICO, including the facts, effects and remedial action taken.

The DPO and headteacher will review breaches and identify any action needed to reduce the risk of recurrence.