Saint Jérôme
Church of England
Bilingual School

Data Protection Policy

Policy created:	December 2024
Policy reviewed and updated:	September 2026
Date of next review:	September 2027
Review cycle:	Annually. The previous review date of December 2025 was not met.
Linked policies:	Freedom of Information Policy, Online Safety Policy, Safeguarding and Child Protection Policy, all five Privacy Notices, Allergy Safety Policy (for special category health data).

Version history

Date	Version	Summary of changes
December 2024	V1	Original policy. Named Rev. D Norris as Headteacher and Ian Fernandes as Chair of the Governing Body, both now out of date. Review date of December 2025 was not met. The contents page omitted section 8 (Biometric recognition systems) despite the section existing in the body. The office email address was written throughout as 'stjeromebilingal.org', missing a letter. No explicit complaints-handling section, despite this now being a requirement under the Data (Use and Access) Act 2025. The 'Links with other policies' section retained an unremoved template instruction, '*DELETE AS APPROPRIATE*'.
September 2026	V2	Corrected named governance throughout: Kate Schutte (Headteacher), Vas Lappas and Edward Stowell (Co-Chairs of Governors). Corrected the Office Manager contact throughout, in line with the same correction made to all five Privacy Notices: Natasha McCarthy has left; the current Office Manager is Anne Quigg. Fixed the email address typo, repeated many times through the original. Added the Data (Use and Access) Act 2025 to the legislation section, including the 'reasonable and proportionate search' standard for subject access requests. Added a dedicated Complaints section, addressing a genuine gap: the Data Protection Rights section referred individuals straight to the ICO, with no internal complaints step first, which the DUAA now expects to be in place. Noted that the ICO becomes the Information Commission from 30 September 2026. Strengthened the Artificial Intelligence section to name the DfE's 'Generative artificial intelligence in education' policy paper (10 June 2025) specifically, rather than referring to AI risk only in general terms. Fixed the contents page, which omitted section 8. Removed the unaddressed '*DELETE AS APPROPRIATE*' template instruction from the Links with Other Policies section and updated it to reflect the policies now in place, including the new Allergy Safety Policy. Flagged that the 'Lead Governor for Data Protection', referenced in Monitoring Arrangements, is not a role named or established anywhere else reviewed in this project, and needs confirming.

Headteacher:

.....

(Kate Schutte)

Co-Chairs of Governors: Approved by Governors on 17th September 2026

.....

(Vas Lappas and Edward Stowell)

1. Aims

Saint Jérôme Church of England Bilingual School (the School) aims to ensure that all personal data collected, stored, processed and destroyed about any natural person, whether a member of the school workforce, pupil, parent, governor, visitor, contractor, consultant or any other individual, is handled in accordance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR).

This policy applies to all personal data processed by the school, regardless of format or filing system, and whether processing is automated or manual.

2. Legislation and Guidance

This policy meets the current requirements of UK data protection legislation. It is based on guidance published by the Information Commissioner's Office (ICO) on UK GDPR, PECR 2003 and the Data Protection Act 2018, and on guidance from the Article 29 Working Party.

It also has regard to the Data (Use and Access) Act 2025, which amended the UK GDPR and Data Protection Act 2018, including introducing a 'reasonable and proportionate search' standard for subject access requests, and restructuring the ICO into the Information Commission from 30 September 2026.

This policy also meets the requirements of the Protection of Freedoms Act 2012, the ICO's code of practice on video surveillance, and the DBS Code of Practice on handling sensitive information. It complies with the Education (Pupil Information) (England) Regulations 2005, which gives parents a right of access to their child's educational record.

3. Definitions

Data controller	The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
Data processor	A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller, following the controller's instructions.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Consent	Freely given, specific, informed and unambiguous indication of the data subject's wishes via a statement or clear affirmative action, signifying agreement to specific processing.
Personal data	Any information relating to an identified or identifiable natural person, including by reference to a name, identification number, location data, an online identifier, or one or more factors specific to their physical, physiological, genetic, mental, economic, cultural or social identity.
Special category data	More sensitive personal data needing greater protection: racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetics, biometrics used for identification, health, and sex life or sexual orientation. Although not formally listed as special category data, information about criminal offences, convictions or cautions is treated with the same extra care within this policy.
Processing	Any operation performed on personal data, such as collection, recording, organisation, storage, alteration, retrieval, use, disclosure, combination, restriction, erasure or destruction, whether automated or manual.
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

The school collects and determines the processing of personal data relating to parents/carers, pupils, the school workforce, governors/volunteers, visitors and others, and also processes data on behalf of others; it is therefore both a data controller and a data processor.

The school is registered as a data controller with the ICO and will renew this registration as legally required. The registration number is ZA192462; this remains valid and unaffected by the ICO's restructuring into the Information Commission.

5. Roles and Responsibilities

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

5.1 The Governing Board

The Governing Board has overall responsibility for ensuring the school complies with all relevant data protection obligations.

5.2 Data Protection Officer

The school has appointed Grow Education Partners Ltd, LDBS's GROW service, as its Data Protection Officer (DPO); the responsible contact is Claire Mehegan, claire.mehegan@london.anglican.org.

The DPO oversees the implementation of this policy and any related policies, and reviews the school's compliance with data protection law. On request, the DPO can provide an annual report of the school's compliance status to the Governing Board, and is a named point of contact for data subjects and the regulator. Full details of the DPO's responsibilities are set out in their Service Level Agreement.

5.3 Representative of the Data Controller

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

5.4 All Employees

Employees, regardless of role, are responsible for collecting, storing and processing personal data in accordance with this policy; informing the school of any changes to their own personal data; reporting a data breach, data rights request or Freedom of Information request; and contacting the Data Protection Lead or DPO with any questions about this policy, data protection law, or how to handle a particular situation, including before capturing consent, drafting a privacy notice, transferring data outside the UK, or engaging in a new activity that may affect individuals' privacy rights.

6. The Data Protection Principles

Data protection is based on seven principles the school must comply with. Personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary for the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure.

The Accountability principle ties these together, requiring the school to take responsibility for complying with the other six, including having appropriate measures and records in place to demonstrate compliance.

7. Processing Personal Data

7.1 Lawfulness, Fairness and Transparency

We only process personal data where we have one of six lawful bases under data protection law: the individual, or their parent/carer where appropriate, has freely given clear consent; the data needs to be processed to fulfil a contract, or the individual has asked us to take steps before entering one; the data needs to be processed to comply with a legal obligation; the data needs to be processed to protect the vital interests of the individual; the data needs to be processed so the school, as a public authority, can perform a task in the public interest or carry out its official functions; or the data needs to be processed for the legitimate interests of the school or a third party, provided the individual's rights and freedoms are not overridden.

For special category data, we also meet one of the special category conditions set out in data protection law: explicit consent; necessity for employment-related obligations and rights; necessity to protect vital interests; processing by a not-for-profit body with a religious, political, philosophical or trade union aim; data manifestly made public by the

individual; establishment, exercise or defence of a legal claim; reasons of public interest in public health; necessity for preventative or occupational medicine; or archiving purposes in the public interest.

Where we collect personal data directly from individuals, we provide the information required by law through a privacy notice. Privacy notices are available in a location relevant to each group of data subjects, on the school website or via the school office, covering pupils and parents/carers, school workforce (including trainees, contractors and consultants), governors and volunteers, job applicants, and visitors. Additional copies are available on request by contacting Anne Quigg, Office Manager via office@stjeromebilingual.org.

7.2 Limitation, Minimisation and Accuracy

We only collect personal data for specified, explicit and legitimate reasons, explained via our privacy notices. If we want to use personal data for a new reason, we will inform those concerned and seek consent where necessary. Employees only access and process personal data where necessary for their role.

We keep data accurate and, where necessary, up to date, rectifying or erasing inaccurate data when appropriate. When personal data is no longer required, employees must ensure it is destroyed, in line with our data retention policy, available on request from Anne Quigg, Office Manager via office@stjeromebilingual.org.

8. Biometric Recognition Systems

Where we use pupils' biometric data as part of an automated biometric recognition system, for example fingerprints used to pay for school dinners instead of cash, we comply with the Protection of Freedoms Act 2012.

Parents/carers are notified before any biometric recognition system is introduced or before their child first takes part in it, and we obtain written consent from at least one parent or carer before first processing a child's biometric data. Parents/carers and pupils have the right not to use the school's biometric systems, and we provide alternative means of accessing the relevant services. They can object or withdraw consent at any time, and any data already captured will be deleted. As required by law, if a pupil refuses to participate, we will not process their biometric data, irrespective of any parental consent given.

9. Sharing Personal Data

To function efficiently, effectively and legally as a data controller, we share information with appropriate third parties, including but not limited to: where there is an issue with a pupil or parent/carer that puts staff safety at risk; where we need to liaise with other agencies or services, seeking consent where possible; and where suppliers or contractors need data to provide services to employees and pupils. In the latter case, we only appoint suppliers who can provide sufficient guarantees of compliance and satisfactory security, establish a data sharing agreement, and share only the data necessary for the service.

We also share personal data with law enforcement and government bodies where required, including for the prevention or detection of crime or fraud, the apprehension or prosecution of offenders, tax assessment or collection, legal proceedings, safeguarding obligations, and sufficiently anonymised research and statistics. We may share personal data with emergency services and local authorities to help them respond to an emergency affecting our pupils or employees.

10. Artificial Intelligence (AI)

AI tools, including generative chatbots such as ChatGPT and Google Gemini, are now widespread and easy to access. We recognise AI has many uses to help pupils learn, but also poses risks to sensitive and personal data. This policy has regard to the DfE's policy paper 'Generative artificial intelligence (AI) in education' (10 June 2025), which recommends that personal data is not entered into generative AI tools at all, to ensure adherence to data protection law.

To keep personal and sensitive data secure, no one will enter such data into unauthorised generative AI tools or chatbots. If personal or sensitive data is entered into an unauthorised generative AI tool, the school will treat this as a data breach and follow the personal data breach procedure set out in this policy.

11. Transferring Data Internationally

We may send information to other countries where we, or a company we work with, store information on computer servers based overseas, or where we communicate with an individual while they are overseas.

We carry out due diligence on companies we share data with, noting whether they process data in the UK, the EEA (the European Union, Liechtenstein, Norway and Iceland), or outside the EEA. The UK and EEA countries adhere to

equivalent data protection standards. For organisations processing data outside the UK and EEA, we assess the circumstances, ensure there is no undue risk, and check that adequate legal provisions are in place.

12. Individuals' Data Protection Rights

12.1 Access Rights

Individuals have a right to make a 'subject access request' to gain access to personal information the school holds about them. If we hold information about you, we will give you a description of it, tell you why we are holding and processing it and how long we will keep it for, explain where we got it from if not from you, tell you who it has been or will be shared with, and let you know whether any automated decision-making is applied to it. We will not provide information where it would compromise the privacy of others, and will give you a copy in an intelligible form.

Under the Data (Use and Access) Act 2025, you are entitled to the personal data we are able to provide based on a reasonable and proportionate search; we are not required to conduct an exhaustive search of every system if doing so would be disproportionate to the request. If we need more information from you to carry out a reasonable search, the one-month response clock pauses until we receive it.

In most cases, we will respond within one month, as required under data protection legislation. We may extend this by up to two months for complex requests or exceptional circumstances. We reserve the right to verify the requester's identity by asking for photo ID; if this proves insufficient, further identification may be required.

If a request is manifestly unfounded or excessive, for example if it is repetitive or asks for further copies of the same information, we may refuse to act on it or charge a reasonable fee covering only administrative costs. Where we refuse a request, we will explain why and tell the individual they have the right to complain, as set out in section 13.

Requests should preferably be submitted in writing, and should include the individual's name, correspondence address, contact number and email address, and details of the request. Requests can be made to Anne Quigg, Office Manager via office@stjeromebilingual.org or 020 3019 6363, Saint Jérôme Church of England Bilingual School, 120–138 Station Road, Harrow, Middlesex HA1 2DJ. If any employee receives a request, they must immediately forward it to Anne Quigg, Office Manager.

When responding to requests, we will not disclose information that might cause serious harm to the physical or mental health of the pupil or another individual, would reveal that a child is at risk of abuse where disclosure would not be in their best interests, is contained in adoption or parental order records, or is given to a court in proceedings concerning the child.

12.2 Other Rights Regarding Your Data

You may also: withdraw consent to processing at any time, where the school relies on consent; ask us to rectify, erase or restrict processing of your personal data, or object to it in certain circumstances; prevent the use of your personal data for direct marketing; challenge processing justified on the basis of public interest, official authority or legitimate interests; request a copy of agreements transferring your data outside the UK; object to decisions based solely on automated decision-making or profiling; request a cease to processing likely to cause damage or distress; be notified of a data breach in certain circumstances; submit a complaint, as set out in section 13; and ask for your data to be transferred to a third party in a structured, machine-readable format, in certain circumstances.

12.3 Children and Data Rights/Requests

An individual's data belongs to them; a child's data therefore belongs to the child, not their parents or carers. Children below the age of 12 are generally not regarded as mature enough to understand their rights and the implications of a data request, so for children under 12, most requests from parents or carers may be granted without the pupil's express permission. This is not a fixed rule; a pupil's ability to understand their rights is judged case by case. Where a child is judged old and mature enough to exercise their rights and a request is made on their behalf, we require their consent before acting on it.

13. Complaints

We take any complaints about our collection and use of personal information very seriously. If you think our collection or use of personal information is unfair, misleading or inappropriate, or you have any other concern, please raise this with us in the first instance, by contacting Anne Quigg, Office Manager or our Data Protection Officer, Claire Mehegan.

Alternatively, if you remain dissatisfied, you can refer a complaint to the regulator, currently known as the Information Commissioner's Office (ICO), becoming the Information Commission from 30 September 2026. Its powers, staff and existing functions transfer across unchanged; only its name and governance structure change.

- Report a concern online at ico.org.uk/concerns
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.

14. Parental Requests to See the Educational Record

Academies are not required to provide educational records if a parent requests one, since the Education (Student Information) Regulations 2005, which places this obligation on maintained schools, does not apply to academies. An academy may choose to comply, but parents no longer have a legal right to this information; please refer instead to the subject access request provisions above. The Independent School Standards Regulations, which apply to academies through their funding agreement, are met if the Academy Trust ensures an annual written report of each registered pupil's progress and attainment in the main subject areas is sent to their parents.

15. Closed-Circuit Television (CCTV)

We use CCTV in various locations around the school site for the detection and prevention of crime; footage may be used for other reasons set out more fully in our CCTV Policy. We adhere to the ICO's code of practice on video surveillance and provide staff training in its use.

We do not need individuals' permission to use CCTV, but make clear where recording takes place, with visible cameras and prominent signage, and provide directions on how to find further information where this is not clear. The full CCTV Policy can be obtained from the school office; enquiries about the CCTV system should be directed to Anne Quigg, Office Manager via office@stjeromebilingual.org.

16. Photographs and Videos

We may take photographs and record images of individuals as part of school activities, including for use within school on noticeboards and in newsletters and prospectuses; outside school by external agencies such as the school photographer or local press; and online on our website or social media.

We obtain consent from the responsible individual before using pupil images, clearly explaining how the photograph or video will be collected and used. Consent can be refused or withdrawn at any time; if withdrawn, we delete the image and do not distribute it further. Consent can be withdrawn by writing to the school office or emailing office@stjeromebilingual.org. We do not accompany images used in this way with other personal information about the child, to ensure they cannot be identified. See our Child Protection and Safeguarding Policy for further information.

17. Data Protection by Design and Default

We put measures in place to show that data protection is integrated into our data collection and processing activities, including: appointing a suitably qualified DPO with the resources to fulfil their duties; only processing personal data necessary for each specific purpose; completing data protection impact assessments where processing presents a high risk or involves new technology, with advice from the DPO; integrating data protection into internal documents, including this policy and our privacy notices; periodic audits to monitor and review our privacy measures; and maintaining records of our processing activities, including the name and contact details of our DPO, and an internal record of the data we hold, how and why we use it, who we share it with, and how long we keep it.

18. Data Security and Storage of Records

We protect personal data from unauthorised or unlawful access, alteration, processing or disclosure, and from accidental or unlawful loss, destruction or damage. Our measures include: keeping paper-based records and portable electronic devices under lock and key when not in use, under a clear desk policy; not leaving confidential personal data on display when not in use, unless there is a compelling lawful basis, such as displaying allergy information in the medical room; using passwords of at least eight characters, changed at regular intervals; encrypting laptops, tablets and USB devices where saving to the hard drive is enabled; expecting the same security standards for personal devices as for school-owned equipment, as set out in our Online Safety Policy and ICT policies; and carrying out due diligence when sharing data with third parties, to ensure it is stored securely.

19. Disposal of Records

Personal data no longer needed is disposed of securely; data that has become inaccurate or out of date is rectified, updated, or disposed of if no longer useful. We shred paper-based records and overwrite or delete electronic files, or use a third party who can provide sufficient guarantees of compliance and a certificate of destruction. Disposals under the Data Retention Schedule are recorded in our record of destruction log.

20. Personal Data Breaches

The school makes all reasonable endeavours to prevent personal data breaches. Potential or confirmed breaches should be reported to Anne Quigg, Office Manager via office@stjeromebilingual.org or 020 3019 6363, where they are assigned a unique reference number and recorded in the school's data breach log. Incidents are then investigated, their potential impact assessed, and appropriate remedial action taken, with the DPO consulted as required. Where appropriate, we report the breach to the regulator and affected data subjects within 72 hours.

The full procedure is set out in the School Breach Management Policy, available via the school office. Examples of a data protection breach include, but are not limited to: personal data left unattended in a meeting room, staffroom or PPA room; information about a pupil or family sent to the wrong member of staff or parent; a non-anonymised dataset published on the school website showing exam results of pupils eligible for pupil premium; safeguarding information made available to an unauthorised person; and the theft of a school laptop containing unencrypted personal data about pupils.

21. Training

All employees and governors receive data protection training as part of induction, with periodic refreshers in line with ICO best practice or in response to changes in legislation, guidance or the school's processes. Records of attendance are kept, to ensure all data handlers receive appropriate training.

22. Monitoring Arrangements

The DPO is responsible for monitoring and reviewing this policy as part of their general compliance work. They work with the school's Office Manager and the Lead Governor for Data Protection to ensure this policy remains current and appropriate.

This policy is reviewed annually, with changes recommended when appropriate. Governors are asked to sign off the policy review and any necessary changes.

23. Links with Other Policies

This Data Protection Policy is linked to our:

- Freedom of Information Policy
- Online Safety Policy
- ICT User Agreements and Email Use Policy
- Data Retention Schedule
- Breach Management Policy
- Disaster Recovery / Business Continuity Planning and Risk Register
- Child Protection and Safeguarding Policy
- CCTV Policy
- Allergy Safety Policy, for the handling of special category health data
- All five Privacy Notices: Pupils, Parents and Carers; School Workforce; Job Applicants; Governors and Volunteers; and Visitors.