Autumn | 26-27

St Joseph's Catholic Primary School

Data Protection Policy

Date ratified by Governors:	Autumn 2026-27
Date of next review of the policy:	Autumn 2027-28
This policy is reviewed:	**1 Year**

Learn together and grow in God's love

Aspiration - Compassion - Community - Faith - Respect – Responsibility

St Joseph's Catholic Primary School
Commerell Street
East Greenwich
London SE10 9AN

Table of Contents

Section 1: Introduction 3
Section 2: Legislation and guidance 3
Section 3: Definitions 3
Section 4: The data controller 4
Section 5: Roles and responsibilities 4
Section 6: Data protection principles 4
Section 7: Lawful basis for using personal data 4
Section 8: Sharing personal data 5
Section 9: Subject access requests 5
Section 10: Other rights 6
Section 11: Parents' right to see the educational record 6
Section 12: Data protection complaints 6
Section 13: CCTV 7
Section 14: Photographs and videos 7
Section 15: Artificial intelligence 7
Section 16: Data protection by design and by default 7
Section 17: Data security 8
Section 18: Keeping and disposing of records 8
Section 19: Personal data breaches 8
Section 20: Training 8
Section 21: Monitoring and review 8
Section 22: Links with other policies 8

Section 1: Introduction

St Joseph's Catholic Primary School collects and uses personal data about pupils, parents and carers, staff, governors, volunteers, visitors, suppliers and others so that it can educate and safeguard pupils and run the school. The school is committed to handling this information lawfully, fairly, securely and only for as long as it is needed.

This policy sets out how the school meets its duties under data protection law and what is expected of everyone who handles personal data on the school's behalf. It applies to all personal data held by the school, in any format, including paper records, electronic records, emails, photographs and CCTV footage.

All staff, governors and volunteers must read and follow this policy. A deliberate or serious breach of this policy may be dealt with under the school's Staff Disciplinary Policy. This policy does not form part of any employee's contract of employment.

Section 2: Legislation and guidance

This policy is based on:

- the UK General Data Protection Regulation (UK GDPR)
- the Data Protection Act 2018 (DPA 2018)
- the Data (Use and Access) Act 2025, which amends the UK GDPR and DPA 2018, including new rules on data protection complaints and subject access requests
- the Privacy and Electronic Communications Regulations 2003 (PECR), which cover electronic marketing and website cookies
- the Education (Pupil Information) (England) Regulations 2005, which give parents the right to see their child's educational record
- Keeping Children Safe in Education 2026, which makes clear that data protection law does not prevent information being shared to keep children safe
- guidance from the Information Commissioner's Office (ICO), and the DfE's data protection guidance for schools and guidance on the use of generative artificial intelligence in education

Section 3: Definitions

Term	Definition
Personal data	Any information relating to an identified or identifiable living person, such as a name, identification number, location data, online identifier, photograph, or an opinion about them
Special category data	Personal data needing extra protection: racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data used for identification, health, and sex life or sexual orientation
Criminal offence data	Personal data about criminal allegations, offences or convictions, including information from DBS checks
Processing	Anything done with personal data, including collecting, recording, storing, using, sharing and destroying it
Data subject	The person the personal data is about
Data controller	The organisation that decides how and why personal data is used. The school is a data controller
Data processor	An organisation that processes personal data on the school's behalf, such as a software or IT supplier
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration or unauthorised disclosure of, or access to, personal data

Section 4: The data controller

The Governing Body of St Joseph's Catholic Primary School is the data controller for the personal data the school holds. The school pays the annual data protection fee to the ICO and is registered on the ICO's public register of fee payers.

Section 5: Roles and responsibilities

Role	Responsibilities
Governing Body	Has overall responsibility for making sure the school complies with data protection law; approves this policy; receives the DPO's annual report
Headteacher (Suzanne Long)	Acts for the data controller day to day; makes sure this policy is followed; is the first point of contact for data breaches (see the Data Breach Policy)
Data Protection Officer: Judicium Consulting Limited (lead contact Craig Stilwell)	Advises the school on data protection law; monitors compliance; advises on DPIAs, subject access requests, complaints and breaches; is the point of contact for the ICO and for anyone with questions about their data; reports to the Governing Body each year
Records Lead (Amanda Weston)	Manages the school's records and retention schedule, in line with the Records Management Policy
All staff, governors and volunteers	Handle personal data in line with this policy; keep it secure; tell the school when their own details change; report any data breach straight away; pass on any request from someone about their data to the school office without delay

Contacting the DPO: Judicium Consulting Limited, 5th Floor, 98 Theobalds Road, London WC1X 8WB. Email dataservices@judicium.com, telephone 0345 548 7000 (option 1). Lead contact: Craig Stilwell.

Staff should contact the DPO, through the Headteacher, if they:

- have questions about this policy or about using, keeping or sharing personal data
- are unsure whether there is a lawful basis for using personal data in a particular way
- need to rely on consent, write a privacy notice, or transfer personal data outside the UK
- are planning a new activity or system that may affect people's privacy, such as a new app
- need help with a contract or data sharing arrangement

Section 6: Data protection principles

The school makes sure that personal data is:

- processed lawfully, fairly and in a transparent way
- collected for specified, explicit and legitimate purposes
- adequate, relevant and limited to what is necessary
- accurate and, where necessary, kept up to date
- kept for no longer than necessary
- kept secure

The school is also responsible for being able to show that it complies with these principles (accountability).

Section 7: Lawful basis for using personal data

The school only uses personal data where it has a lawful basis under UK GDPR. The bases the school mainly relies on are:

- **public task:** to carry out its functions as a school, such as educating and safeguarding pupils

- **legal obligation:** to comply with the law, such as the school census, attendance registers and safeguarding duties
- **vital interests:** to protect someone's life, such as sharing medical information in an emergency
- **contract:** for example, staff employment contracts and lettings agreements
- **consent:** where there is a genuine choice, such as using pupils' photographs on the school website or social media

As a public authority, the school does not rely on legitimate interests for anything it does as part of its public tasks.

Special category data and criminal offence data. When the school uses special category data, such as health or SEND information, or criminal offence data, such as DBS check information, it also meets a condition under Article 9 or 10 of the UK GDPR and Schedule 1 of the DPA 2018. The main conditions are employment and social security law, substantial public interest (including safeguarding children and statutory purposes), vital interests, health and social care, and explicit consent. The school's Appropriate Policy Document explains how it uses this information safely.

Transparency. The school tells people how it uses their personal data through privacy notices for pupils and parents, staff, governors and volunteers, job applicants and visitors. These are on the school website.

Using data for a new purpose. If the school wants to use personal data for a reason other than the one it was collected for, it will tell the people concerned first, and ask for consent where needed.

Section 8: Sharing personal data

The school shares personal data only where it is lawful and necessary, for example with the DfE, the Royal Borough of Greenwich, other schools, health services and children's social care.

- **Safeguarding.** Data protection law does not prevent the school from sharing information to keep a child safe. Staff must never let fears about data protection stop them sharing safeguarding concerns with the DSL. The school follows Keeping Children Safe in Education 2026, and the duty in the Children's Wellbeing and Schools Act 2026 to share information that is relevant to safeguarding or promoting the welfare of a child.
- **Suppliers.** Where a supplier processes personal data for the school, such as SIMS, CPOMS, the text messaging service or the CCTV maintenance company, the school makes sure there is a written contract that meets UK GDPR Article 28, and that the supplier keeps the data secure.
- **Police and other authorities.** Requests from the police and other authorities are referred to the Headteacher and considered on a case-by-case basis, with advice from the DPO where needed.
- **Transfers outside the UK.** The school only transfers personal data outside the UK where the law allows it and appropriate safeguards are in place. Staff must check with the DPO before using any service that stores school data outside the UK.

Section 9: Subject access requests

Everyone has the right to ask whether the school holds personal data about them and, if so, to receive a copy along with information about how it is used. This is called a subject access request.

Making a request. A request can be made in any form, including verbally, to any member of staff. It does not need to mention data protection law. Staff must pass any request to the school office straight away, as the time limit starts when any member of staff receives it. Requests are easier to deal with if they are in writing and include the person's name, contact details and the information they want.

Children and subject access requests. Personal data about a child belongs to that child, not to their parents or carers. A parent or carer can make a request on behalf of their child where the child is not mature enough to understand their rights, or where the child has given their consent. Children of primary school age are generally not regarded as mature enough, so most requests from parents of St Joseph's pupils can be granted without the pupil's express permission. Each case is still judged individually.

Responding to requests. The school will:

- check the identity of the person making the request, and that a parent or carer is entitled to act for a child
- ask the person to clarify their request if it is unclear
- carry out a reasonable and proportionate search for the information requested
- respond without undue delay and within one calendar month
- tell the person within one month if it needs to extend the time limit by up to two further months because the request is complex or there are several requests, and explain why
- provide the information free of charge

The time limit does not start until the school has the information it needs to confirm the requester's identity, and pauses while the school waits for any clarification it has asked for.

Information that may be withheld. The school may withhold some information, for example where releasing it:

- might cause serious harm to the physical or mental health of the pupil or another person
- would reveal that a child is at risk of abuse, where disclosure would not be in the child's best interests
- would reveal another person's personal data, where it cannot be removed and it would be unreasonable to release it without their consent
- is covered by another exemption, such as legal professional privilege, confidential references, or information about crime prevention

Unfounded or excessive requests. If a request is manifestly unfounded or excessive, for example because it repeats an earlier request, the school may refuse it or charge a reasonable fee. The school will explain its reasons.

If the school refuses all or part of a request, it will explain why and tell the person about their right to complain to the school (Section 12), to the ICO, or to apply to the courts.

Section 10: Other rights

In certain circumstances, people also have the right to:

- withdraw consent at any time, where the school relies on consent
- ask the school to correct inaccurate personal data
- ask the school to delete personal data, or to restrict how it is used
- object to the school using their personal data for its public tasks
- object to direct marketing
- not be subject to decisions made solely by automated means that have a significant effect on them, and to challenge such decisions
- receive their personal data in a structured, machine-readable format (data portability)
- be told about a personal data breach that is likely to put them at high risk
- complain to the school and to the ICO

Requests should be made to the school office or the DPO. Staff must pass any such request to the school office straight away.

Section 11: Parents' right to see the educational record

Parents and carers with parental responsibility have a legal right to see their child's educational record, free of charge, within 15 school days of a written request. If they ask for a copy, the school may charge a fee that covers no more than the cost of supplying it. This right applies until the pupil is 18. Access may be refused if it could cause serious harm to the pupil or another person.

Section 12: Data protection complaints

Anyone can complain to the school if they are unhappy with how the school has handled their personal data.

1. Complaints can be made using the data protection complaint form on the school website, by email to support@stjosephs.greenwich.sch.uk, by letter, or in person at the school office. The school will help anyone who needs support to make a complaint.
2. The school will acknowledge the complaint within 30 days of receiving it.
3. The school will look into the complaint without undue delay, with advice from the DPO, and tell the complainant the outcome.

If the complainant is not satisfied, they can complain to the ICO at ico.org.uk or on 0303 123 1113.

Section 13: CCTV

The school uses five external CCTV cameras for safety and security, in line with ICO guidance. Signs show where cameras are in use. Full details are in the CCTV Policy.

Section 14: Photographs and videos

The school takes photographs and videos of pupils as part of school life.

- Photographs used within school for teaching, learning and displays are part of the school's public task.
- The school asks parents and carers for written consent before using photographs or videos of their child in publications, on the school website, on social media, or by external organisations such as newspapers. The consent form explains each use clearly.
- Consent can be withdrawn at any time. The school will then stop using the image and, where possible, remove it.
- Photographs used publicly are not accompanied by a pupil's full name or other information that would identify them.
- Photographs and videos taken by parents at school events for their own family use are not covered by data protection law. The school asks parents not to share images that include other children on social media.
- Staff must not take or store photographs of pupils on personal devices.

Section 15: Artificial intelligence

The school recognises that generative AI tools, such as ChatGPT, Microsoft Copilot and Google Gemini, can support teaching and administration, but also create risks for personal data.

- Staff may only use AI tools that the school has approved for school work.
- Staff must not enter personal data, including pupils' names, safeguarding information, SEND information or staff details, into any AI tool that the school has not approved for that purpose.
- Any new AI tool that will process personal data must have a DPIA before it is used.
- Entering personal data into an unapproved AI tool is treated as a data breach and must be reported in line with the Data Breach Policy.

Full details are in the school's AI Policy. The school follows the DfE's guidance on generative AI in education and the expectations in Keeping Children Safe in Education 2026.

Section 16: Data protection by design and by default

The school builds data protection into everything it does by:

- appointing a suitably qualified DPO and giving them the resources they need
- only collecting and using the personal data it needs for each purpose

- completing a Data Protection Impact Assessment (DPIA) before starting any processing that is likely to be high risk, such as introducing new technology, with advice from the DPO
- keeping a Record of Processing Activities, showing what personal data the school holds, why, who it is shared with, how long it is kept and how it is kept secure
- training staff and governors, and keeping a record of the training
- carrying out regular checks and audits to make sure the school is complying

Section 17: Data security

The school protects personal data against unauthorised access, loss, damage and misuse. In particular:

- paper records and portable devices containing personal data are locked away when not in use, and confidential papers are not left on desks or in shared areas
- personal data is only taken off site when necessary, with the Headteacher's agreement, and is signed out from the school office
- school systems are protected by strong passwords of at least 12 characters, and multi-factor authentication is used where available
- laptops and removable media containing personal data are encrypted
- staff use only school email accounts and school systems for school business, and never forward school data to personal email accounts
- personal data sent outside the school is sent securely, for example by encrypted email
- staff, governors and volunteers who access school data on their own devices must follow the same security rules as for school equipment, as set out in the school's Online Safety and Acceptable Use Policy
- staff are alert to phishing emails and report suspicious messages to the school's IT support provider, ATS

Section 18: Keeping and disposing of records

Personal data is kept only for as long as necessary, in line with the retention schedule in the Records Management Policy. When it is no longer needed, it is disposed of securely: paper records are shredded on site, and electronic records are permanently deleted.

Section 19: Personal data breaches

The school takes all reasonable steps to prevent personal data breaches. If a breach happens, or is suspected, staff must report it to the Headteacher straight away and follow the Data Breach Policy.

Where a breach is likely to put people's rights and freedoms at risk, the school will report it to the ICO without undue delay and, where possible, within 72 hours of becoming aware of it. Where a breach is likely to put people at high risk, the school will also tell those affected.

Section 20: Training

All staff and governors receive data protection training as part of their induction, and refresher training every year. Further training is given when the law, guidance or the school's systems change.

Section 21: Monitoring and review

The DPO monitors this policy and the school's compliance with it. The policy is reviewed every year by the Headteacher, with advice from the DPO, and approved by the Governing Body.

Section 22: Links with other policies

This policy links to the school's:

- Data Breach Policy
- Privacy notices
- Records Management Policy
- Freedom of Information Policy and Publication Scheme
- CCTV Policy
- Child Protection and Safeguarding Policy
- Online Safety and Acceptable Use Policy
- Appropriate Policy Document
- AI Policy
- Cyber Security Policy
- Mobile Phone and Smart Device Policy
- Staff Code of Conduct and Staff Disciplinary Policy