# St Joseph's Catholic Primary School

# Data Protection Policy

**Approved by the Governing Body in May 2018**

**Last Reviewed: January 2023**

**Next Review: Spring 2024**

## 1. Introduction and Purpose of Policy

The purpose of this policy is to provide information about our approach to collecting and using personal data in the course of our day-to-day work as well as the rights available to those whose data we hold.

It applies to personal data we collect both as an employer and as an education provider, such as that contained within pupil and staff records as well as information we hold on parents, governors, volunteers, visitors and other individuals with whom we interact.

Details of our Data Protection Officer can be found at the end of this policy document and requests for further information or queries relating to this policy can be sent directly to her.

## 2. Legislation and Guidance

This policy meets the requirements of the GDPR and the provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR, the ICO's code of practice for Subject Access Requests and guidance material published by The Department for Education (DfE).

This policy also reflects the ICO's code of practice for the use of CCTV, 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 and regulation 5 of The Education (Information About Individual Pupils) (England) Regulations 2013

## 3. Policy Statement

The Governing Body is committed to ensuring that personal data is collected and used in a way which is transparent, clearly understood and meets minimum legal requirements and best practice guidance. The Governing Body recognises the need for individuals to feel confident that their data will be used only for the purposes that they have been made aware of, and that it is stored securely and for no longer than is necessary. As part of this commitment, we want to ensure that individuals understand the rights available to them if they want to question or raise concerns about the way their data is being processed.

The School has appointed a Data Protection Officer whose role is to monitor internal compliance, including with this policy, to inform and advise on data protection obligations and act as a contact point for individuals and the Information Commissioner's Office.

## 4. Definitions and Principles

Certain terms are referred to in this policy which are explained below:

- **Personal Data.** Any information relating to an identified, or identifiable, individual. This may include the individual's name (including initials); Identification number; Location data and online identifier such as a username. It may also include 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 (such as fingerprints,retina and iris patterns) where used for identification purposes; health – physical or mental; 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. Page 4 of 15 Term: Data controller. Definition: A person or organisation (school) that determines the purposes and the means of processing of 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.

There are certain key **data protection principles** to which the school must have regard when processing personal data.

These are that personal data shall be:

- Processed lawfully, fairly and in a transparent manner;
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- Accurate and, where necessary, kept up to date;
- Kept in a form which permits identification of individuals for no longer than is necessary for the purposes for which the personal data are processed;
- Processed in a manner that ensures appropriate security of the personal data.

## 5. Our Approach to Processing Personal Data

We use privacy notices to inform individuals whose personal data we collect about how we use their information and the legal basis on which we are processing it. If we want to process data for new reasons in the future, we will inform affected individuals first.

We process special categories of personal data and criminal offence data, for example to meet our obligations under employment law. Where we do so, this processing is underpinned by policies on the use of such data.

For some of the data we process we rely on legitimate interests as the legal basis for processing. We do not rely on this basis unless we have first concluded that the rights and freedoms of individuals do not override those interests.

Personal data we hold on individuals is held in secure paper and/or electronic files to which only authorised personnel have access. Information is held for no longer than is deemed necessary, in accordance with our data retention schedules and privacy notices.

If we are planning to process data and this processing is likely to result in a high risk to individuals' interests, we will undertake a Data Protection Impact Assessment (DPIA) to help us identify and minimise the data protection risks.

We always aim to rectify inaccurate or out-of-date information promptly when notified and encourage anyone whose data we hold to inform us when their details have changed.

We do not hold biometric data in any form. If this changes we would adhere to the DfE published guidance.

## 6. Rights of Individuals

If we process your data you have a number of rights as an individual which are summarised below.

### 6.1 Right to be informed

You have the right to be informed about the collection and use of your personal data. You must be provided with privacy information about the purposes for which we process your personal data, our retention periods for that personal data, and who it will be shared with. This privacy information must be provided to you at the time that we collect your personal data. Privacy information provided by the school can be found in our privacy notices which are available on the school website.

### 6.2 Right of access

You have the right to obtain confirmation from us that your data is being processed and to gain access to your personal data by making a subject access request. You should do this by emailing your request to sbm@stjosephs-epsom.surrey.sch.uk or by post to the school's address. We are required to verify your identity before responding which may mean we ask you to provide identification documents. Parents may request information relating to their child. This will generally require the pupil's consent if the pupil is deemed competent to exercise his/her own rights.

In most cases we will respond to you within one calendar month of receipt. Please be aware that during closure periods we are unlikely to be able to deal with your request promptly so we ask that, wherever possible, you submit requests during term time.

We do not charge a fee for providing a copy of the information except where we have assessed the request as being manifestly unfounded or excessive or where further copies of the same information are asked for.

If we refuse to respond to a request we will explain why, as well as your right to complain to the Information Commissioner's Office.

**Requests for education records:** Where a parent has requested access to their child's educational record, this will be provided at no cost within 15 school days of receipt of the written request.

### 6.3 Other individual rights

In addition to the right of access described above, individuals have certain other rights. These are:

- **Right to rectification:** the right to have inaccurate personal data rectified, or completed if it is incomplete.
- **Right to erasure:** the right to have personal data erased (also known as the 'right to be forgotten').
- **Right to restrict processing:** the right to request the restriction or suppression of your personal data in certain circumstances.
- **Right to data portability:** the right in certain circumstances to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way.
- **Right to object:** the right to object to processing based on legitimate interests or the performance of a task in the public interest / exercise of official authority; this also covers direct marketing as well as processing for purposes of scientific or historical research and statistics.
- **Rights relating to automated decision making including profiling:** automated individual decision-making refers to making a decision solely by automated means without any human involvement; profiling refers to automated processing of personal data to evaluate certain things about an individual. We do not currently use automated decision making in any of our processing activities.

If you want to exercise any of these rights, you should do so by emailing your request to sbm@stjosephs-epsom.surrey.sch.uk or by post to the school's address.

## 7. International Data Transfers

We transfer personal data to countries outside the EEA. This data relates to transfer of children's records, where children move abroad and they are requested. We do not transfer personal data outside the EEA unless the organisation concerned has provided adequate safeguards. Further information is provided in the relevant privacy policies.

## 8. Our Approach to Data Security and Breaches

Our school is committed to ensuring that the personal data we hold and process is kept secure at all times and that data protection is considered and integrated into our processing activities. We use a variety of technical and organisational measures to protect personal data from accidental or unlawful destruction, loss, alteration, unauthorised disclosure, or unauthorised access. For example, we ensure that:

- only authorised personnel can access, alter, disclose or destroy personal data;
- authorised personnel understand the limits of their authority and to whom they should escalate any issues relating to personal data;
- we have appropriate backup systems in place so that, if personal data is accidentally lost, altered or destroyed, it can be recovered;
- access to premises or equipment given to anyone outside the schpp; (for example, for computer maintenance purposes) is strictly regulated and access to data limited;
- staff receive training on data protection principles and their responsibilities as appropriate to their role, including highlighting the possibility that they may commit a criminal and/or disciplinary offence if they deliberately try to access or disclose information without authority;
- we have proper procedures in place to identify individuals who are requesting personal data before it is given out;
- there are strict guidelines in place on the appropriate use of computers to reduce the risk of the network being compromised;
- we regularly review our physical security measures, such as ease of access to the premises through entrances and internal doors, alarm systems, lockable storage, security lighting and CCTV;
- we have a process in place for the secure disposal of paper waste;
- portable IT equipment is appropriately encrypted so that data contained on such devices is secure;
- confidential paper files are not taken off site unless appropriate security measures have been implemented first;
- third parties who process data on our behalf are compliant with data protection law;
- we have an appointed Data Protection Officer in place who monitors and reports on our accountability and governance measures;

In the event of a data breach taking place, we will report the circumstances to the Information Commissioner within 72 hours of becoming aware that it has occurred. We will also keep a register of data breaches that have occurred.

If a breach is likely to result in a high risk to the rights and freedoms of individuals, we will also inform those concerned directly and without undue delay.

## 9. Our Expectations of Staff

We expect all staff working for, or on behalf of, the school whether employees, casual workers, supply staff, volunteers or consultants, to recognise and adhere to the high standards of data protection we uphold. Everyone has a responsibility for helping to ensure that personal data, whether their own or that of third parties, is accurate, kept up to date and held securely.

Certain members of staff will collect and process data as part of their role. Without exception we expect the following rules to be adhered to:

Members of staff must:

- Only access or process personal data they are authorised to as part of their role and in accordance with the documented purposes for processing (and not for any other purpose);
- Keep personal data confidential and only disclose it to individuals who are authorised to see it (if in any doubt, consulting their line manager or the Data Protection Officer);
- Not remove personal data from its authorised location without permission and, where permission is granted, to ensure that appropriate security measures are in place whilst the data is moved or relocated;
- Not keep work-related personal data on personal devices, such as mobile phones and tablets, or on local computer hard drives or unencrypted USB sticks;

- Take responsibility for ensuring that personal passwords are strong, are changed regularly and never shared;
- Adhere to all security measures designed to keep personal data safe from accidental or unlawful destruction, loss, alteration, unauthorised disclosure, or unauthorised access;
- Participate in training or briefings and read circulated documents aimed at increasing awareness of data protection legislation and good practice;
- Be aware of data protection issues as part of their day-to-day work, particularly as part of any new projects, and report any concerns relating to personal data (including any potential data breaches) as a matter of urgency to the Data Protection Officer.

These rules are an integral part of the school's data security practices in order to comply with data protection legislation. As such, a breach of these rules is likely to be treated as a disciplinary offence and potentially gross misconduct, in accordance with the disciplinary procedure.

## 10. Status of Policy and Review

The content and operation of this policy is reviewed as and when deemed necessary by the Governing Body or the Data Protection Officer. The policy is discretionary and does not confer any contractual rights.

| **Data Protection Officer Contact Details** | |
|---|---|
| **Name** | **Andrea Cooke**<br>**School Business Manager** |
| **Email Address** | **sbm@stjosephs-epsom.surrey.sch.uk** |
| **Telephone Number** | **01372 727850** |
| **Postal Address** | **St Joseph's Catholic Primary School, West Street, Epsom, Surrey KT18 7RT** |