



## Data Protection Policy

### 1. Aims

Our school aims to ensure that all data collected about staff, pupils, parents and visitors is collected, stored and processed in accordance with the Data Protection Act 1998. This policy applies to all data, regardless of whether it is in paper or electronic format.

### 2. Legislation and Guidance

This policy meets the requirements of the Data Protection Act 1998, and is based on guidance published by the Information Commissioner's Office and model privacy notices published by the Department for Education. It also takes into account the provisions of the General Data Protection Regulation, which came into force in 2018, and the Freedom of Information Act 2000.

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

Term	Definition
Personal data	Data from which a person can be identified, including data that, when combined with other readily available information, leads to a person being identified
Sensitive personal data	Data such as: <ul style="list-style-type: none"><li>• Contact details</li><li>• Racial or ethnic origin</li><li>• Political opinions</li><li>• Religious beliefs, or beliefs of a similar nature</li><li>• Where a person is a member of a trade union</li><li>• Physical and mental health</li><li>• Sexual orientation</li><li>• Whether a person has committed, or is alleged to have committed, an offence</li><li>• Criminal convictions</li></ul>
Processing	Obtaining, recording or holding data
Data subject	The person whose personal data is held or processed
Data controller	A person or organisation that determines the purposes for which, and the manner in which, personal data is processed
Data processor	A person, other than an employee of the data controller, who processes the data on behalf of the data controller

#### 4. The Data Controller

Our school processes personal information relating to pupils, staff and visitors, and, therefore, is a data controller. Our school delegates the responsibility of data controller to the School Business Manager.

The school is registered as a data controller with the Information Commissioner's Office and renews this registration annually.

#### 5. Data Protection Principles

The Principles of the Data Protection Act and the General Data Protection Regulation state that personal information must be:

1. Processed lawfully, fairly and in a transparent manner in relation to individuals; the lawful basis can be:
  - Consent of a data subject
  - Processing is necessary for the performance of a contract with the data subject
  - Processing is necessary for compliance with a legal obligation (e.g. The Education Act 1996, School Standards and Framework Act 1998, Education Act 2002, Children and Families Act 2014)
  - Processing is necessary to protect the vital interests of the data subject or another person (eg life or death)
  - Processing is necessary for the performance of a task carried out in the public interest

The lawful basis for sensitive personal data (racial, political, religious, trade union, genetic, health, sex life, criminal convictions or offences) is:

- Explicit consent of the data subject
  - Processing is necessary for carrying out obligations under employment, social security or social protection law
  - Processing is necessary to protect the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent
  - Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members and provided there is no disclosure to a third party without consent
  - Processing relates to personal data manifestly made public by the data subject
  - Processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity
  - Processing is necessary for reasons of substantial public interest
  - Processing is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services
  - Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices
  - Processing is necessary for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1)
2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
4. Accurate and, where necessary, kept up to date.
5. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
6. Processed in a manner that ensures appropriate security of the personal data against unauthorised processing, accidental loss, destruction or damage, using appropriate technical or organisational measures.

## **6. Compliance with the Data Protection Principles and Data Protection Legislation**

In order to comply with these principles and meet all data protection obligations as stipulated in data protection legislation, the school will:

- Raise awareness of data protection across the school
- Offer data protection training to all employees and governors
- Review the data protection policy for the school annually
- Maintain a personal data processing audit, which lists the following:
  - Name of the personal data set
  - Purpose for processing this personal data set
  - Who the data set is shared with
  - Whether the data is transferred to another country
  - How long do the personal data set is kept for (retention)
  - The technical and organisational security measures to protect the personal data set
  - The legal basis for processing as described above (1)
  - If consent is the legal basis for processing, details of the evidence of this consent.
- Put any risks found from the personal data processing audit process into a risk register
- Ensure the school's consent forms meet the standards of GDPR.
- Register with the Information Commissioners Officer as a data controller
- Publish a privacy notice that will let individuals know who we are, why we are processing their data and if we share their data.
- Maintain a system to allow data subjects to exercise their rights:
- Ensure any business contracts with suppliers conform to data protection legislation
- Implement technical and organisational controls to keep personal data secure
- Use Privacy Impact Assessments to assess the privacy aspects of any projects or systems processing personal data
- Ensure an adequate level of protection for any personal data processed by others on behalf of the school that is transferred outside the European Economic Area
- Investigate all information security breaches, and if reportable, report to the Information Commissioners Office within 72 hours
- Undertake data quality checks to ensure personal data is accurate and up to date
- Demonstrate our compliance in an accountable manner through audits, spot checks, accreditations and performance checks
- Support the pseudonymisation and encryption of personal data.

## **7. Rights of the Individual**

The list of rights that a data subject (person who the data is about) can exercise was widened by Section 2 of the General Data Protection Regulation:

- The right to be informed; via privacy notices

- The right of access; via subject access requests (SARS), the timescale for response is one calendar month. SARS must be free of charge, charges can only be made for further copies or where requests for information are unfounded or excessive
- The right of rectification; inaccurate or incomplete data must be rectified within one month
- The right to erasure; individuals have a right to have their personal data erased and to prevent processing unless we have a legal obligation to do so
- The right to restrict processing; individuals have the right to suppress processing. We can retain just enough information about the individual to ensure that the restriction is respected in future
- The right to data portability; we need to provide individuals with their personal data in a structured, commonly used, machine readable form when asked
- The right to object; individuals can object to their personal data being used for profiling, direct marketing or research purposes
- Rights in relation to automated decision making and profiling; GDPR provides safeguards for individuals against the risk that a potentially damaging decision is taken without human intervention.

The school will ensure that these rights will be exercised.

## **8. Roles and Responsibilities**

The Governing Board has overall responsibility for ensuring that the school complies with its obligations under the Data Protection Act 1998 and General Data Protection Regulation 2018.

Day-to-day responsibilities rest with the Headteacher, or the Deputy Headteacher in the Headteacher's absence. The Headteacher will ensure that all staff are aware of their data protection obligations, and oversee any queries related to the storing or processing of personal data.

Staff are responsible for ensuring that they collect and store any personal data in accordance with this policy. Staff must also inform the school of any changes to their personal data, such as a change of address.

## **9. Privacy/Fair Processing Notice**

### **9.1 Pupils and parents**

Arrangements are set out in a separate document – St Joseph's RC Primary School Privacy Notice for Pupils (how we use pupil information). This document is available on our website or on request from the School Office.

### **9.2 Staff**

Arrangements are set out in a separate document – St Joseph's RC Primary School Privacy Notice for Staff. This document is available on request from the School Office.

## **10. Subject Access Requests**

Under the Data Protection Act 1998 and General Data Protection Regulation 2018, pupils have a right to request access to information the school holds about them. This is known as a subject access request.

Subject access requests must be submitted in writing, either by letter, email or fax. Requests should include:

- The pupil's name
- A correspondence address
- A contact number and email address
- Details about the information requested

The school will not reveal the following information in response to subject access requests:

- Information that might cause serious harm to the physical or mental health of the pupil or another individual
- Information that would reveal that the child is at risk of abuse, where disclosure of that information would not be in the child's best interests
- Information contained in adoption and parental order records
- Certain information given to a court in proceedings concerning the child

Subject access requests for all or part of the pupil's educational record will be provided within 15 school days. There will be no charge for this service.

If a subject access request does not relate to the educational record, we will respond within one calendar month. There will be no charge for this.

## **9. Parental Requests to See the Educational Record**

Parents have the right of access to their child's educational record, free of charge, within 15 school days of a request.

Personal data about a child belongs to that child, and not the child's parents. This is the case even where a child is too young to understand the implications of subject access rights. For a parent to make a subject access request, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent. The Information Commissioner's Office, the organisation that upholds information rights, generally regards children aged 12 and above as mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents of pupils at our school may be granted without the express permission of the pupil.

If parents ask for copies of information, they will be required to pay the cost of making the copies.

## **10. Storage of Records**

- Paper-based records and portable electronic devices, such as laptops and hard drives, that contain personal information are kept under lock and key when not in use
- Papers containing confidential personal information should not be left on office and classroom desks, on staffroom tables or pinned to noticeboards where there is general access
- Passwords are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures for school-owned equipment

## **11. Disposal of Records**

Personal information that is no longer needed, or has become inaccurate or out of date, is disposed of securely. The timescale for disposal is that set out in the Retention Guidelines in the Information and Records Management Society Schools Toolkit.

We may use external specialist companies to safely dispose of paper based data and electronic files and equipment.

## **12. CCTV**

A separate, but linked, policy is in place regarding the use of CCTV.

## **12. Training**

Our 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 or the school's processes make it necessary.

## **13. Monitoring Arrangements**

The Headteacher is responsible for monitoring and reviewing this policy.

The School Business Manager checks that the school complies with this policy by, among other things, reviewing school records annually.

This document will be reviewed annually. At every review, the policy will be shared with the Governing Board.

September 2025