



St Mary's Church of England Primary School
Established 1845

Data protection policy and privacy notice

St Marys C of E Primary



Approved by:	Maddy Spinks	Date: April 2018
Last reviewed on:	April 2018	
Next review	April 2020	

Contents

1. Aims.....	3
2. Legislation and guidance	3
3. Definitions	3
4. The data controller.....	4
5. Data protection principles	4
6. Roles and responsibilities	4
7. Privacy/fair processing notice	5
8. Subject access requests.....	6
9. Parental requests to see the educational record	6
10. Storage of records	7
11. Disposal of records	7
12. Training.....	7
13. The General Data Protection Regulation.....	7
14. Monitoring arrangements.....	7
15. Links with other policies.....	7

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 expected provisions of the [General Data Protection Regulation](#), which is new legislation due to come into force 25th May 2018.

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.

This policy also complies with our funding agreement (10th December 2012) and articles of association.

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">• Contact details• Racial or ethnic origin• Political opinions• Religious beliefs, or beliefs of a similar nature• Where a person is a member of a trade union• Physical and mental health• Sexual orientation• Whether a person has committed, or is alleged to have committed, an offence• Criminal convictions
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 Principal Mr Peter Kyles. The school secretary Mrs E Stilwell is the data processor.

The school is registered as a data controller with the Information Commissioner's Office and renews this registration annually. Number **Z2832283**.

5. Data protection principles

The Data Protection Act 1998 is based on the following data protection principles, or rules for good data handling:

- Data shall be processed fairly and lawfully
- Personal data shall be obtained only for one or more specified and lawful purposes
- Personal data shall be relevant and not excessive in relation to the purpose(s) for which it is processed
- Personal data shall be accurate and, where necessary, **kept up to date**.
- Personal data shall **not be kept for longer than is necessary** for the purpose(s) for which it is processed
- Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act 1998
- Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data, and against accidental loss or destruction of, or damage to, personal data
- Personal data shall not be transferred to a country or territory outside the European Economic Area unless the country or territory ensures an adequate level of protection for the rights and freedoms of data in relation to the processing of personal data

6. Roles and responsibilities

The governing board has overall responsibility for ensuring that the school complies with its obligations under the Data Protection Act 1998.

Day-to-day responsibilities rest with the Principal, or Mrs E Stilwell in the Principals absence. The Principal 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. Data is stored on a cloud based IMS where there is limited access and which is password protected (ScholarPack).

ScholarPack are accredited under ISO 27001. 'School data is held in secure data centres within the UK that are protected by both physical and logical security and conform to industry standard security practice. School data is mirrored in real time to a standby server by streaming replication. This data is backed up at 10am, 3pm and 3am daily. ScholarPack uses high grade encryption to protect user and student data in transit. This is used by the banking system.

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.

7. Privacy/fair processing notice

7.1 Pupils and parents

We hold personal data about pupils to support teaching and learning, to provide pastoral care and to assess how the school is performing. We may also receive data about pupils from other organisations including, but not limited to, other schools (CTF), local authorities (MASH) and the Department for Education.

This data includes, but is not restricted to:

- Contact details
- Results of internal assessment and externally set tests
- Data on pupil characteristics, such as ethnic group or special educational needs
- Safeguarding issues
- Exclusion information
- Details of any medical conditions

We will only retain the data we collect for as long as is necessary to satisfy the purpose for which it has been collected. Information will be placed on Scholar-Pack and hard copies will be destroyed.

We will not share information about pupils with anyone without consent unless the law and our policies allow us to do so. Individuals who wish to receive a copy of the information that we hold about them/their child should refer to sections 8 and 9 of this policy.

We are required, by law, to pass certain information about pupils to specified external bodies, such as our local authority, MASH (Multi Agency Safeguarding Hub) and the Department for Education, so that they are able to meet their statutory obligations.

7.2 Staff

We process data relating to those we employ to work at, or otherwise engage to work at, our school. The purpose of processing this data is to assist in the running of the school, including to:

- Enable individuals to be paid (Hoople Payrole)
- Facilitate safe recruitment
- Support the effective performance management of staff
- Improve the management of workforce data across the sector
- Inform our recruitment and retention policies
- Allow better financial modelling and planning
- Enable ethnicity and disability monitoring
- Support the work of the School Teachers' Review Body

Staff personal data includes, but is not limited to, information such as:

- Contact details
- National Insurance numbers
- Salary information
- Qualifications
- Absence data
- Personal characteristics, including ethnic groups
- Medical information
- Outcomes of any disciplinary procedures

We will only retain the data we collect for as long as is necessary to satisfy the purpose for which it has been collected.

We will not share information about staff with third parties without consent unless the law allows us to.

We are required, by law, to pass certain information about staff to specified external bodies, such as our local authority (restricted as we are a FREE school) and the Department for Education, so that they are able to meet their statutory obligations.

Any staff member wishing to see a copy of information about them that the school holds should contact the Principal.

8. Subject access requests

Under the Data Protection Act 1998, 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 or email. All requests should be signed

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
- Information in the case of parental separation about the other parent
- 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.

If a subject access request does not relate to the educational record, we will respond within 40 calendar days. The maximum charge that will apply is £10.00.

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 (ICO), 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 may be required to pay the cost of making the copies.

Parents of pupils at this school do not have an automatic right to access their child's educational record. The school will decide on a case-by-case basis whether to grant such requests, and we will bear in mind guidance issued from time to time from the Information Commissioner's Office (the organisation that upholds information rights).

10. Storage of records

- Paper-based records (reduced to a minimum) and portable electronic devices, such as laptops and hard drives, that contain personal information are kept under lock and key when not in use is placed in a locked cabinet.
- 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
- Where personal information needs to be taken off site (in paper or electronic form), staff must sign it in and out from the school office. This will include pupil contact details and medical details on trips and sporting activities.
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices with access to data. Staff and pupils are reminded to change their passwords at regular intervals.
- Encryption software is not used to protect portable devices as sensitive data is not transported on hardware such as laptops and USB devices. Information that is sent to the local authority is via ANYCOMS. Information populating Scholar-Pack is also encrypted as it enters the cloud. To the DFE data is also encrypted.
- Staff, or governors who store personal information on their personal devices are expected to follow the same security procedures for school-owned equipment. The Chair of Governors has access to ScholarPack.

11. Disposal of records

Personal information that is no longer needed, or has become inaccurate or out of date, is disposed of securely. If data needs to be removed from ScholarPack deletion requirements are adhered to by the MIS system.

For example, we will shred or incinerate paper-based records, and override and delete electronic files.

12. Training

Our staff and governors are provided with data protection training as part of their induction process and forms part of our annual INSET programme.

Data protection will also form part of continuing professional development, where changes to legislation or the school's processes make it necessary.

13. The General Data Protection Regulation

We acknowledge that the law is changing on the rights of data subjects and that the General Data Protection Regulation is due to come into force in May 2018.

We will review working practices when this new legislation takes effect and provide training to members of staff and governors where appropriate.

14. Monitoring arrangements

Maddy Spinks (Chair of Governors) is currently responsible for monitoring/auditing and reviewing this policy.

The Principal checks that the school complies with this policy by, among other things, reviewing school records. This will be reviewed at least annually.

This document will be reviewed when the General Data Protection Regulation comes into force (May 2018), and then **every 2 years**.

At every review, the policy will be shared with the governing body and scrutinised.

15. Links with other policies

This data protection policy and privacy notice is linked to the freedom of information publication scheme.

ScholarPack's data retention policy

Currently all student and staff data will remain on the system unless deleted by St Mary's or the school moves to a different MIS supplier. All backups are held by ScholarPack for six months. ScholarPack will work with our school to implement a data retention policy. This data is not shared with other organisations.