

## Data Protection Policy

<b>Date approved</b>	29 <sup>th</sup> June 2020	<b>Approved by</b>	St Ralph Sherwin Trust Board
<b>Review cycle</b>	2 years	<b>Signature</b>	
<b>Due for review by</b>		<b>Name</b>	

### Introduction

The St Ralph Sherwin Catholic Multi Academy Trust (or, 'the Trust') is committed to a policy of protecting the rights and privacy of individuals (including students, staff and others) in accordance with the Data Protection Act 2018.

The Trust gathers and processes personal information about its staff, students, and other individuals to comply with obligations as a charitable company limited by guarantee that is responsible for academies. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully.

Any breach of the Data Protection Act 2018 or this Trust Data Protection Policy is considered to be an offence, and in that event relevant disciplinary procedures will apply. The contents of this policy are applicable to employees, trustees and governors, other agencies and providers working with the Trust, and who have access to personal information.

The Trust is the Data Controller and is responsible for setting the overarching policy and standards for Data Protection. The Trust see compliance with these obligations as the best method to ensure that personal information is dealt with lawfully and securely and in accordance with the GDPR and other related legislation.

It will apply to information regardless of the way it is used, recorded and stored and whether it is held in paper files or electronically. It applies to all data held in schools as part of the multi-academy trust, though the responsibility for managing data rests with each school, and the school shall provide access to a Data Protection Policy and suitable Privacy Notices.

All academies within the Trust process personal information about staff, pupils, parents and other individuals with whom they come into contact as part of their usual day-to-day business. Schools are required by law to collect and use certain types of information to comply with statutory obligations related to employment, education and safeguarding, and this policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the General Data Protection Regulation (GDPR) and other legislation.

This policy will be updated as necessary to reflect best practice, or amendments made to data protection legislation, and shall be reviewed every two years.

Each academy within the Trust will have access to relevant policies and procedures published on their own website.

A review of the effectiveness of GDPR compliance and processes will be conducted by the Data Protection Officer every twelve months.

## Background to the Data Protection Act 2018

The Data Protection Act 2018 (DPA) brings into UK law the requirements of General Data Protection Regulations (the GDPR), which is a European Directive.

The GDPR (and hence the Data Protection Act 2018) exist to look after an individual's data. These regulations are a series of safeguards for every individual. Information concerning individuals needs to be secure and to be treated with respect. The GDPR exists to protect individual rights in an increasingly digital world.

## What is Data?

Data is any information that relates to a living person which identifies them, e.g., name, address or phone number. It also relates to details about that person, which can include personal opinions. **The individual defined by the data is called the Data Subject.**

Some data is considered to be more sensitive and therefore more important to protect. This includes information about racial or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; data concerning health or sex life and sexual orientation; genetic data; or biometric data where processed to uniquely identify a person.

The Trust often collects sensitive data for Department for Education and/or Local Authority requirements. Of course, student data may contain information about safeguarding or special education or health needs. Information about other family members may also be held.

Every academy within the Trust must publish a Data Protection Policy and suitable Privacy Notices on their website which reflects the overarching principles set out by the Trust.

## What are the Key Principles of the GDPR?

### *Lawfulness, transparency and fairness*

The Trust must have a legitimate reason to hold the data; this is explained in the Privacy Notices. Consent is often sought to use data about a student for a particular purpose; however, there are other grounds for collecting and processing data to ensure that we meet our legal obligations.

### *Collect data for a specific purpose and use it for that purpose*

Data cannot be used for a purpose for which it was not originally collected, or where notice has not been given about how data may be used after collection.

### *Limited collection*

The Trust recognises that, as an organisation, only the minimum amount of data needed for a particular task or reason should be collected.

### *Accuracy*

Data collected should be accurate, and steps should be taken to check and confirm accuracy. The frequency of the checks depends on the data being collected and processed in the academies.

The Trust recognises and supports the rights of Data Subjects to object if they feel that the information held is inaccurate, should no longer be held by the Data Controller or should not be held by the Data Controller in any event. In these cases, a dispute resolution and/or complaint process can be initiated.

### *Retention*

The Trust has a records retention schedule that sets out how long records are kept. This document is available upon request.

### *Security*

Ensuring that suitable processes and procedures are in place is a requirement for each academy and for the Trust. This includes paper files, electronic records or other information.

## Who is a 'Data Controller'?

The Trust is the Data Controller (i.e., the Board of Foundation Directors). They have ultimate responsibility for how the Trust manages data. They delegate this to Data Processors to act on their behalf.

## Who is a 'Data Processor'?

A Data Processor is any person that uses, collects, accesses or amends the data that the Data Controller has collected or has authorised to be collected. It can be a member of staff, a third-party company/service provider, a governor, a contractor or a temporary employee. It can also be another organisation such as the police or the Local Authority.

Data Controllers must make sure that Data Processors are as careful with the data as the Data Controller themselves. The GDPR places additional obligations on organisations to ensure that Data Controllers require contractual agreements to confirm that this is the case.

## Data Subjects' Rights

Individuals have a right:

- to be informed
- of access to data stored about them or their children
- to rectification if there is an error in the stored data
- to erasure if there is no longer a need for school to retain their data
- to restrict processing, i.e., to limit what is done with their data
- to object to data being shared or collected

There are other rights that relate to automated decision making and data portability which are not directly relevant to academies of Academy Trusts.

Data Subjects' rights are also subject to child protection and safeguarding concerns and for sharing information for the prevention and detection of crime. The Trust also has legal and contractual obligations to share information with organisations such as the Department for

Education, Social Care, the Local Authority and HMRC, amongst others. In some cases, these obligations override individual rights.

## Consent

The Trust will seek consent from staff, volunteers, students, parents and carers to collect and process their data. The reasons for requesting the data, as well as how the data will be used, will be made clear.

There are contractual, statutory and regulatory occasions when consent is not required.

Consent is defined by the GDPR as “any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her”.

Privacy Notices explain how data is collected and used.

Obtaining clear consent and ensuring that the consent remains in place is important for the Trust.

### For Students and Parents/Carers

On joining an academy within the Trust, you will be asked to complete a form giving next-of-kin and emergency contact details, as well as other essential information. You will also be asked to give consent for the use of that information for other Trust purposes, as set out on the data collection/consent form.

The contact and consent form will be reviewed on an annual basis. It is important to inform the academy/the Trust if there are changes to your details or to your decision about consent.

### Pupil Consent Procedure

Where processing relates to a child under 13 years of age, the Trust will obtain the consent from a person who has parental responsibility for the child.

Pupils may be asked to give consent or to be consulted about how their data is obtained, shared and used in certain situations.

### Withdrawal of consent

Consent can be withdrawn, subject to contractual, statutory or regulatory constraints. Where more than one person has the ability to provide or withdraw consent, the school will consider each situation on its merits and within the principles of GDPR, as well as child welfare, protection and safeguarding principles.

## Processing Data

The Trust must have a reason to process the data about an individual. Privacy notices set out how we use data. The GDPR has six conditions for lawful processing and any time we process data relating to an individual it must fall within at least one of those conditions.

The legal basis and authority for collecting and processing data in school are:

- **consent** obtained from the data subject or their parent
- performance of a **contract** where the data subject is a party
- compliance with a **legal obligation**
- to protect the **vital interests** of the data subject or other associated person
- to carry out the processing that is in the **public interest and/or official authority**
- it is necessary for the **legitimate interests of the data controller or third party**

In addition, any special categories of personal data are processed on the grounds of:

- explicit consent from the data subject or from a parent/carer about their child
- a necessity to comply with employment rights or obligations
- protection of the vital interests of the data subject or associated person
- a necessity to comply with the legitimate activities of the school
- existing personal data that has been made public by the data subject and is no longer confidential
- bringing or defending legal claims
- safeguarding
- national laws in terms of processing genetic, biometric or health data

## Data Sharing

Data sharing is only carried out within the limits set by the GDPR. Guidance from the Department for Education, health, the police, local authorities and other specialist organisations may be used to determine whether data is shared.

The basis for sharing or not sharing data is recorded on a case-by-case basis.

## Retention

Each academy within the Trust has a retention policy; some information is governed by statutory and regulatory requirements, while others are determined by local practice and practicality.

## Subject Access Requests

By way of a Subject Access Request (SAR), individuals can request copies of information held about them or a student for whom they have parental responsibility. This process is set out separately and any requests should be made directly to the relevant academy.

Information requested must be provided within a month, but this can be extended if, for example, the academy was closed for holidays. The maximum extension permitted is two months.

Information provided by a third party is not usually released without their consent.

Information will be supplied in an electronic form.

## Breaches and Non-Compliance

If there is a non-compliance with this policy or the processes it sets out, or if there is a breach as described within the GDPR and Data protection Act 2018, the Trust will be notified as soon as the breach is discovered.

There is a separate procedure to follow in the event of a data breach, including taking immediate action to remedy the situation as quickly as possible. Each academy will have a breach management action plan.

Protecting data and maintaining data subjects' rights is the purpose of this policy and its associated procedures.

## The Freedom of Information Act

This Act gives a general right of access to all types of 'recorded' information held by the Trust. All requests for information must be made in writing to us. We will accept these in the following forms:

- Letter  
St Ralph Sherwin Multi Academy Trust  
St Katherine's House 3rd Floor  
St Mary's Wharf  
Mansfield Road  
Derby  
DE1 3TQ  
FAO: Freedom of Information Officer
- Email  
mail@srsrsmat.co.uk

The following information must be included:

- The requestor's full name
- An address for correspondence (this can be a postal or email address)
- A **clear description of the information required**

We will respond to requests for information within 20 school days. If further clarification is required, our staff will write to the requestor and the request will be temporarily placed on hold until sufficient information is available to begin processing the request.

We will not charge those making a Freedom of Information request. In some circumstances, we may be allowed to charge an appropriate fee for complying with some requests for information.

## CCTV Policy

CCTV may be used in various locations around our school sites to ensure safety. Schools using CCTV will adhere to the ICO's Code of Practice for the use of CCTV and will have a CCTV policy available on their website. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use. Any enquiries about the CCTV system should be directed to individual academies.

## Data Protection Officer

The Trust have a Data Protection Officer (DPO) whose role it is to:

- inform and advise the controller or the processor and the employees who carry out processing of their obligations under the GDPR
- monitor compliance with the GDPR and DPA
- provide advice where requested about the data protection impact assessment and monitor its performance
- be the point of contact for Data Subjects if there are concerns about data protection
- cooperate with the supervisory authority and manage the breach procedure
- advise about training and CPD for the GDPR

The DPO of the St Ralph Sherwin Multi Academy Trust is John Walker, who can be contacted at [john@jawalker.co.uk](mailto:john@jawalker.co.uk), or via post at PO Box 10778, Leicester.

## Complaints and the Information Commissioner Office (ICO)

Each Academy has a Complaints Policy which deals with complaints about Data Protection issues.

There is a right to complain if you feel that data has been shared without consent or lawful authority. There is also a right to complain if you have requested that data be erased, rectified or not processed and that request has not been dealt with adequately.

In the UK, it is the ICO who has responsibility for safeguarding and enforcing the DPA obligations.

Email: [casework@ico.org.uk](mailto:casework@ico.org.uk)

Helpline: 0303 123 1113

web: [www.ico.org.uk](http://www.ico.org.uk)