



**ST GILBERT OF SEMPRINGHAM  
CATHOLIC ACADEMY TRUST**

**DATA PROTECTION POLICY**

**Approved October 2017**

**Review October 2019**

*'I have come that they may have life and have it to the full'*  
John 10:10

## **Contents**

Contents .....	2
Introduction.....	3
Status of this Policy .....	3
The Data Controller and the Designated Data Controllers.....	3
Responsibilities of Staff .....	3
Data Security .....	4
Rights to Access Information.....	4
Subject Consent .....	5
Processing Sensitive Information .....	5
Publication of Trust Information.....	5
Retention of Data .....	5
Conclusion.....	5

This document is a statement of the aims and principles of the Trust, for ensuring the confidentiality of sensitive information relating to staff, pupils, parents and governors.

## **Introduction**

St Gilbert of Sempringham Catholic Academy Trust needs to keep certain information about its employees, students and other users to allow it to monitor performance, achievements, and health and safety, for example. It is also necessary to process information so that staff can be recruited and paid, courses organised and legal obligations to funding bodies and government complied with.

To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To do this, the Trust must comply with the Data Protection Principles which are set out in the Data Protection Act 1998. In summary these state that personal data shall:

- Be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met.
- Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose.
- Be adequate, relevant and not excessive for that purpose.
- Be accurate and kept up to date.
- Not be kept for longer than is necessary for that purpose.
- Be processed in accordance with the data subject's rights.
- Be kept safe from unauthorised access, accidental loss or destruction.

St Gilbert of Sempringham Catholic Academy Trust and all staff or others who process or use personal information must ensure that they follow these principles at all times. In order to ensure that this happens, the Trust has developed this Data Protection Policy.

## **Status of this Policy**

This policy does not form part of the contract of employment for staff, but it is a condition of employment that employees will abide by the rules and policies made by the Trust from time to time. Any failures to follow the policy can therefore result in disciplinary proceedings.

## **The Data Controller and the Designated Data Controllers**

The Trust as a body incorporate the Data Controller under the 1998 Act, and the Trust Board are therefore ultimately responsible for implementation. However, the Designated Data Controllers will deal with day to day matters.

The Trust has Designated Data Controllers: They are the Headteacher and the School Business Manager.

Any member of staff, parent or other individual who considers that the Policy has not been followed in respect of personal data about himself or herself or their child should raise the matter with the appropriate Designated Data Controller.

## **Responsibilities of Staff**

All staff are responsible for:

Checking that any information that they provide to the Trust in connection with their employment is accurate and up to date. Informing the Trust of any changes to information that they have provided, e.g. change of address, either at the time of appointment or subsequently. The Trust cannot be held responsible for any errors unless the staff member has informed the Trust of such changes.

If and when, as part of their responsibilities, staff collect information about other people (e.g. about a student's course work, opinions about ability, references to other academic institutions, or details of personal circumstances), they must comply with the guidelines for staff set out in the Trust's Data Protection Code of Practice.

## **Data Security**

All staff are responsible for ensuring that:

- Any personal data that they hold is kept securely.
- Personal information is not disclosed either orally or in writing or via Web pages or by any other means, accidentally or otherwise, to any unauthorised third party.
- Staff should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases.

Personal information should:

- Be kept in a locked filing cabinet, drawer, or safe; or if it is computerised, be coded, encrypted or password protected both on a local hard drive and on a network drive that is regularly backed up
- If a copy is kept on a diskette or other removable storage media, that media must itself be kept in a locked filing cabinet, drawer, or safe.

## **Rights to Access Information**

All staff, parents and other users are entitled to:

- Know what information the Trust holds and processes about them or their child and why.
- Know how to gain access to it.
- Know how to keep it up to date.
- Know what the Trust is doing to comply with its obligations under the 1998 Act.

This Policy document and the Trust's Data Protection Code of Practice address in particular the last three points above. To address the first point, the Trust will, upon request, provide all staff and parents and other relevant users with a statement regarding the personal data held about them. This will state all the types of data the Trust holds and processes about them and the reasons for which they are processed.

All staff, parents and other users have a right under the 1998 Act to access certain personal data being kept about them or their child either on computer or in certain files. Any person who wishes to exercise this right should complete the *Subject Access Request Form* and submit it to the Designated Data Controller.

The Trust will make a charge of £10 on each occasion that access is requested, although the Trust does have discretion to waive this.

The Trust aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 40 days, as required by the 1998 Act.

## **Subject Consent**

In many cases, the Trust can only process personal data with the consent of the individual.

In some cases, if the data is sensitive, as defined in the 1998 Act, express consent must be obtained. Agreement to the Trust processing some specified classes of personal data is a condition of acceptance of employment for staff. This included information about previous criminal convictions.

Jobs will bring the applicants into contact with children. The Trust has a duty under the Children Act 1989 and other enactments to ensure that staff are suitable for the job. The Trust has a duty of care to all staff and students and must therefore make sure that employees and those who use Trust facilities do not pose a threat or danger to other users.

The Trust may also ask for information about particular health needs, such as allergies to particular forms of medication, or any medical condition such as asthma or diabetes. The Trust will only use this information in the protection of the health and safety of the Individual, but will need consent to process this data in the event of a medical emergency, for example.

## **Processing Sensitive Information**

Sometimes it is necessary to process information about a person's health, criminal convictions, or race. This may be to ensure that the Trust is a safe place for everyone, or to operate other Trust policies, such as the Sickness Absence Policy or the Equal Opportunities Policy. Because this information is considered sensitive under the 1998 Act, staff (and students where appropriate) will be asked to give their express consent for the Trust to process this data. An offer of employment may be withdrawn if an individual refuses to consent to this without good reason.

## **Publication of Trust Information**

Certain items of information relating to Trust staff will be made available via searchable directories on the public Web site, in order to meet the legitimate needs of researchers, visitors and enquirers seeking to make contact with the Trust.

## **Retention of Data**

The Trust has a duty to retain some staff and student personal data for a period of time following their departure from the Trust, mainly for legal reasons, but also for other purposes such as being able to provide references or academic transcripts. Different categories of data will be retained for different periods of time.

## **Conclusion**

Compliance with the 1998 Act is the responsibility of all members of the Trust. Any deliberate breach of the Data Protection Policy may lead to disciplinary action being taken, or even to a criminal prosecution.