

# STC Sheffield

## Data Protection Policy

*taking into account the General Data Protection Regulation (GDPR) 2018*

### Introduction

STC Sheffield holds and processes personal data about living individuals for the purpose of general church administration and communication, and to run St Thomas Crookes Nursery.

As a church we are committed to complying with data protection law and the rights of individuals under it, as well as to the principles set out below. We recognise that this relates to all personal data, whether it is held on paper, on computer or other media.

All church staff, volunteers or members who obtain, handle, process or store personal data for STC Sheffield must adhere to these principles.

STC Sheffield is registered with the Data Protection Commissioner, Registration No ZA176029. A copy of this registration is included below.

The **Data Controller** of STC Sheffield is defined as St Thomas Crookes, meaning that the Council of Trustees is the responsible body.

The **Data Protection Officer** for STC Sheffield is Ruth Aidley. She is responsible for advising on legal obligations, monitoring compliance, and dealing with any breaches. Any questions on this subject should be directed to Ruth in person, by telephone to 0114 2671090 or extension 101 or by email to [ruth.aidley@stcsheffield.org](mailto:ruth.aidley@stcsheffield.org).

Policy version no. 001

Approved: June 2018

## Contents

1. Data Processing .....	2
a. Personal data.....	2
b. How we legally use personal data .....	2
c. Special categories of data .....	3
d. Children's personal data.....	3
2. Working with Data Subjects - Individuals' Rights .....	3
3. Sharing and Disclosing Data .....	4
4. Retention Schedules.....	4
5. Destroying Data.....	4
6. Data Security .....	5
7. Data Protection Breaches .....	5
8. ICO (Information Commissioner's Office) Registration .....	6

# 1. Data Processing

An Information Audit has identified the classes of data we process and the classes of individual to whom this data relates. For each class of data it also identifies the basis and purpose for such processing, who has access to it, and the data retention schedule. The Audit is appended to this policy and will be updated approximately once every two years.

STC Sheffield processes data for the following purposes:

- To maintain our lists of church members, attenders and supporters
- To provide pastoral support for members
- To provide services to the community and church members, such as Toddler groups, Natter, Food Bank, STC College, etc.
- To safeguard children, young people and vulnerable adults
- To recruit, support and manage staff and volunteers
- To maintain our accounts and records
- To promote our events, courses, Sunday gatherings etc.
- To respond effectively to enquiries, complaints etc.
- For crime prevention (CCTV)

We will make sure that all personal data is:

- Processed lawfully, fairly and in a transparent manner
- Processed for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary
- Accurate and up to date
- Not kept longer than necessary
- Processed securely
- Processed in keeping with the rights of data subjects

## a. Personal data

Personal data is any data which can identify a living individual (“data subject”). This includes:

- Contact details
- Family details
- Lifestyle and social circumstances
- Membership details
- Goods & services (e.g. signups to courses, weekends away etc)
- Financial details
- Education & employment details
- Photos/videos/CCTV

## b. How we legally use personal data

Processing is only lawful if at least one of these conditions in Article 6 of the GDPR is met:

- The processing is necessary for a **contract** with the data subject
- The processing is necessary for us to comply with a **legal obligation**
- The processing is necessary to protect someone’s life (**‘vital interests’**)
- The processing is necessary for us to perform a task in the **public interest** which has a clear basis in law
- The processing is necessary for **legitimate interests** of the data subject or of STC Sheffield or another organisation **UNLESS** these are overridden by the interests, rights and freedoms of the data subject.
- If the data subject has given their clear **consent**.

c. **Special categories of data**

Special categories of data include information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trades union membership, health, genetic or biometric data, sexual life and orientation. Processing of this data is only lawful if **in addition to** one of the categories above, one of the following conditions in Article 9 of the GDPR is met:

- **Consent** of the data subject
- It is necessary for carrying out **obligations under employment, social security or social protection law**
- It is necessary to protect someone's **vital interests** and the individual is incapable of giving consent
- Processing relating only to **members and former members** and provided there is no disclosure to a third party without consent
- Processing relating to personal data manifestly **made public by the data subject**
- Processing necessary for **pursuing legal claims**
- Processing necessary for **substantial public interest** (proportional to the aim pursued and with appropriate safeguards)
- Processing necessary for **medical assessment** (such as assessing the working capacity of an employee)
- Processing necessary for **public health**
- Processing necessary for **archiving purposes** in the public interest or scientific, historical or statistical research purposes

d. **Children's personal data**

Consent cannot be given by children under 16; consent of a parent or guardian is needed in this case. Data processing not relying on consent is not affected.

## 2. **Working with Data Subjects - Individuals' Rights**

All requests from data subjects relating to their data protection rights should be forwarded to the Data Protection Officer immediately, before any action is taken. Note that data protection rights do not outweigh other legal requirements, in particular safeguarding.

Data subjects' rights must be made explicitly clear to them at the point of first communication and in privacy notices.

### **The right to be informed**

- Data privacy notices will be published wherever data is collected, particularly on website forms, email circulars and paper forms.

### **The right of access**

- An individual is entitled to obtain confirmation that their data is being processed, access to that personal data, and other supplementary information.
- Information will be provided without delay, and at the latest within one month of request.
- No fees will be charged unless requests are manifestly unfounded, excessive or repetitive. However there are statutory charges for some services such as searches in marriage registers.

### **The right of rectification**

- An individual is entitled to have personal data rectified if it is inaccurate or incomplete.
- Data will be rectified as soon as possible and at the latest within one month.
- If incorrect data has been passed on to third parties, they will be informed of the rectification where possible.

#### **The right to erasure**

- An individual has 'the right to be forgotten' where there is no compelling reason for the continued processing of their data.
- A request for erasure will be considered as soon as possible and the reasons for erasure or continued processing will be investigated.
- If appropriate, erasure will happen as soon as possible.

#### **The right to restrict processing**

- An individual can block or suppress processing of personal data under circumstances. In this case all processing must cease until the grounds for restriction are investigated.

#### **The right to data portability**

- Any data provided to an individual must be in an easily accessible format.

#### **The right to object**

- An individual can object to their data being used for 'legitimate interests', tasks in the public interest, direct marketing, and for scientific/historical research and statistics.
- If an objection is lodged, all processing must cease until the grounds for objection are investigated. There are no grounds to refuse an objection to direct marketing.

### **3. Sharing and Disclosing Data**

The Information Audit identifies which data is shared with third parties.

- BirchenallHowden Ltd provides IT support to STC Sheffield and our contract with them includes specifics on data protection.
- Third party computer applications where data is held 'in the cloud', e.g. Microsoft, Google, Mailchimp, etc - data protection is included in their general terms and conditions. The cloud servers used by these companies must be within the EU.
- Government and other statutory agencies, e.g. HMRC, General Register Office, Sheffield City Council etc. The transfer of data to these bodies is regulated by legislation.
- Other companies/organisations - see Information Audit for details.

### **4. Retention Schedules**

Specific details of data retention are held in the Information Audit.

- Membership data is kept until not current. Historical membership data is kept indefinitely for archival purposes.
- Financial data is kept for at least 7 years.
- Employment data is kept for at least 10 years.
- Educational data is kept for up to 21 years, or up to 100 years if it relates to a vulnerable child.
- Data relating to safeguarding is kept indefinitely.
- Certain records such as marriage registers are kept in perpetuity or until deposited with Sheffield City Archives.
- CCTV footage is deleted after 1 week unless it is needed by the police.

### **5. Destroying Data**

- Paper records are shredded; computer records will be deleted.
- Computer hardware that has held personal data will be professionally wiped before being recycled.
- Members of staff who leave the employment of STC must delete all personal data processed as part of their employment which has been held on personal devices.

## **6. Data Security**

- Electronic data is held on password-protected computer systems.
- Data kept on paper is held in locked filing cabinets and/or locked offices.
- Access to financial data is restricted to members of the church Finance Team.
- Access to employment data is restricted to the Personnel Team.
- Access to educational data is restricted to the Nursery team.
- Access to pastoral data is restricted to the Pastoral Team, Clergy, and Church Leader of the individual concerned.

## **7. Data Protection Breaches**

- Any breach or suspected breach should be reported immediately to the Data Protection Officer.
- Records of breaches will be kept.
- Any breach which may result in a risk to any person will be reported to the ICO within 72 hours.
- Any breach which may result in a high risk to any person will be reported to the data subject(s) affected without delay.

## 8. ICO (Information Commissioner's Office) Registration

Registration Number: ZA176029

Date Registered: 31 March 2016 Registration Expires: 30 March 2018

Data Controller: St Thomas Crookes

Address: St. Thomas Church, Nairn Street, Sheffield, S10 1UL

Other Names: STC Sheffield

---

*This register entry describes, in very general terms, the personal data being processed by:  
St Thomas Crookes*

### Nature of work - Charity (Local)

#### Description of processing

The following is a broad description of the way this organisation/data controller processes personal information. To understand how your own personal information is processed you may need to refer to any personal communications you have received, check any privacy notices the organisation has provided or contact the organisation to ask about your personal circumstances.

#### Reasons/purposes for processing information

We process personal information to enable us to provide a voluntary service for the benefit of the public in a particular geographical area as specified in our constitution; administer membership records; to fundraise and promote the interests of the charity; manage our employees and volunteers; maintain our own accounts and records.

#### Type/classes of information processed

We process information relevant to the above reasons/purposes. This may include:

- personal details
- family detail
- lifestyle and social circumstances
- membership details
- goods and services
- financial details
- education and employment details

We also process sensitive classes of information that may include:

- physical or mental health details
- racial or ethnic origin
- religious or other beliefs of a similar nature

#### Who the information is processed about

We process personal information about:

- members
- staff, volunteers
- trustees
- children in our care

- complainants, supporters
- enquirers
- advisers and representatives of other organisations

### **Who the information may be shared with**

We sometimes need to share the personal information we process with the individual themselves and also with other organisations. Where this is necessary we are required to comply with all aspects of the Data Protection Act (DPA). What follows is a description of the types of organisations we may need to share some of the personal information we process with for one or more reasons.

Where necessary or required we share information with:

- members
- family, associates or representatives of the person whose personal data we are processing
- employees
- current, past and prospective employers
- healthcare, social and welfare organisations
- educators and examining bodies
- financial organisations
- employment and recruitment agencies
- survey or research organisations
- business associates and professional advisers
- providers of goods and services
- local and central government
- other voluntary and charitable organisations

### **CCTV for Crime Prevention**

CCTV is used for maintaining the security of property and premises and for preventing and investigating crime, it may also be used to monitor staff when carrying out work duties. For these reasons the information processed may include visual images, personal appearance and behaviours. This information may be about staff, customers and clients, offenders and suspected offenders, members of the public and those inside, entering or in the immediate vicinity of the area under surveillance. Where necessary or required this information is shared with the data subjects themselves, employees and agents, services providers, police forces, security organisations and persons making an enquiry.

### **Transferring information overseas**

We do not transfer data outside the European Economic Area (EEA).