



DATA PROTECTION POLICY

JUNE 2022

1. Data Protection Policy Statement

During the course of our activities, Sion Catholic Community for Evangelism (Sion Community) will collect, store, use and otherwise process Personal Data (which may also include Sensitive Personal Data) about the people with whom it interacts.

This may include information about members of the public and the community, volunteers, clergy, employees, contractors, suppliers and other third parties. This data is gathered in order to enable Sion Community to comply with its statutory obligations and to achieve its charitable objects of advancing and maintaining the Roman Catholic religion through proclamation of the Good News of Jesus Christ and to equip others for this task of evangelisation.

Everyone has rights with regard to how their Personal Data is handled by organisations. Sion Community is committed to ensuring that Personal Data is properly and securely managed in accordance with the Data Protection Act 1998 ("DPA") and believes this is an important part of achieving trust and confidence between Sion Community and those with whom it interacts. Sion Community will make every effort to achieve best practice in relation to data protection and will regularly review its procedures to ensure they are adequate and up to date.

Any breach of this, any other Sion Community data protection policy or data protection legislation will be taken seriously and may result in legal action being taken against Sion Community or the individual responsible for the breach.

2. Introduction

The Sion Community Leadership Team have overall responsibility for compliance with data protection legislation, and the Data Protection Officer, Gareth Leyshon, is responsible for ensuring day to day compliance with this policy and the relevant legislation. The Data Protection Officer will undergo training at least once every 12 months.

Sion Community will comply as a Data Processor with the eight data protection principles, which provide that Personal Data must be:

1. Processed fairly and lawfully
 2. Obtained for specified and lawful purpose(s)
 3. Adequate, relevant and not excessive for the purpose(s)
 4. Accurate and kept up to date
 5. Not kept longer than necessary for the specified purpose(s)
 6. Processed in accordance with Data Subjects' rights
 7. Secure
 8. Not transferred outside of the UK without adequate data protection
- Data Protection policy for Sion Community Catholic Community for Evangelism

Updated: 6th June 2022

Review due by: 6th June 2023

This policy applies to all Personal Data created, stored or otherwise processed by Sion Community in whatever format (e.g. paper, electronic, film) and however it is stored (e.g. electronically or in filing cabinets). It also includes information that is in paper form but which is intended to be put onto a computer.

All clergy, staff, volunteers and members of Sion Community who are involved in the Processing (which includes collecting, accessing, using and/or disclosing) of Personal Data held by Sion Community have a duty to protect the data they process by complying with this policy as they are part of Sion Community.

3. General Statement

This policy is intended to ensure that Personal Data is dealt with in accordance with the data protection principles and with data protection legislation generally. Sion Community will therefore:

- Ensure that, when personal information is collected, the Data Subject is informed what data is being collected and for what legitimate purpose(s).
- Be transparent and fair in processing Personal Data.
- Take steps to ensure the accuracy of data at the point of collection and at regular intervals thereafter, including advising Data Subjects of their right to ask for rectification of Personal Data held about them.
- Securely dispose of inaccurate or out-of-date data, or data which is no longer required for the purpose(s) for which it was collected.
- Share information with others only when it is lawful to do so and inform individuals with whom their data may be and/or has been shared and for what purpose(s).
- Ensure that data is processed in line with Data Subjects' rights, which include the right to:
 - Request access to any Personal Data held about them by Sion Community;
 - Prevent the processing of their data for direct-marketing purposes;
 - Ask to have inaccurate data amended;
 - Ask Sion Community to prevent Processing of their Personal Data which is likely to cause unwarranted or substantial damage or distress to themselves or anyone else.
 - Ensure that all clergy, volunteers, employees and members are aware of and understand Sion Community's data protection policies and procedures.

Data Protection policy for Sion Community Catholic Community for Evangelism

Updated: 6th June 2022

Review due by: 6th June 2023

4. Data Security

Sion Community shall ensure that appropriate security measures are taken to prevent unauthorised or unlawful Processing, damage to or loss (accidental or otherwise), theft, or unauthorised disclosure of Personal Data. In particular, all clergy, employees, volunteers and members shall take the following steps to secure personal information:

- Only those who are authorised will be able to access Personal Data and process it.
- Personal Data will only be stored on the central computer system and not on individual PCs, portable electronic devices or removable storage media unless those devices have been encrypted.
- Passwords will be kept confidential and will be changed regularly.
- PCs will be locked or logged off and paper documents will be securely locked away when individuals are away from their desks.
- Offices, desks and filing cabinets/cupboards will be kept locked if they hold Personal Data of any kind, whether on computer or on paper.
- When destroying Personal Data, paper documents will be securely shredded and electronic data will be securely deleted.
- Personal Data removed from an office will be subject to appropriate security measures, including keeping paper files away from public visibility, the use of passwords/passcodes and encryption of portable electronic devices. All such data must be stored securely (for example, not left in the boot of a car).

When receiving telephone or email enquiries, employees, volunteers and members will be required to exercise caution before disclosing any Personal Data and will:

- Not give out Personal Data over the telephone unless in very limited circumstances where they know or can verify the caller's identity and their entitlement to receive the information requested;
- Require callers to put their requests in writing so their identity and entitlement to receive the information may be verified;
- Ensure Personal Data is securely packaged and consider the most appropriate means by which the data should be sent (such as special delivery, courier or hand delivery);
- Refer to the Data Protection Officer for assistance in difficult situations and in all cases involving Sensitive Personal Data.

Personal Data will only be transferred to a third-party acting as a Data Processor (such as a contractor or supplier) if the Data Protection Officer is satisfied that the third party has in place adequate policies and procedures to ensure compliance with data protection legislation. Data sharing agreements will be used where appropriate.

Data Protection policy for Sion Community Catholic Community for Evangelism

Updated: 6th June 2022

Review due by: 6th June 2023

5. Subject Access Requests

Any individual has a right of access to the Personal Data which Sion Community holds about them. To be valid, a Subject Access Request from a Data Subject for the information Sion Community holds about them must be made in writing and provide enough information that is reasonably required to enable a search for the requested information to be undertaken. This includes requests made via email or on social media.

All Subject Access Requests will be dealt with by the Data Protection Officer.

Clergy, employees, volunteers or members who receive a Subject Access Request must forward it to the Data Protection Officer immediately in order that such requests can be replied to 'promptly' and in any event no later than 40 calendar days from receipt of the request (or receipt of the fee).

A fee of up to £10 may be charged for dealing with Subject Access Requests.

Sion Community cannot limit the number of Subject Access Requests made by a Data Subject but, where there has not been a reasonable interval between two requests from the same Data Subject, or where identical requests have been received, Sion Community may lawfully refuse to respond and, if so, the Data Protection Officer will inform the Data Subject of this in writing within the 40 day period.

6. Monitoring and Review

This policy will be reviewed every 12 months and may be subject to change.

7. Contacts

Any queries regarding this policy should be addressed to the Data Protection Officer. Complaints relating to data protection should in the first instance be addressed to Gareth Leyshon: frgareth@sioncommunity.org.uk

Further advice and information can be obtained from the Information Commissioner's Office at www.ico.org.uk

Glossary

Data Processor means any person who or organisation which processes personal data on behalf and on the instruction of Sion Community. Data processors have a duty to protect the information they process for and on behalf of Sion Community by following this and other Sion Community data protection policies at all times.

Data Subjects include all living individuals about whom Sion Community processes personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal data and the information that Sion Community holds about them.

Personal Data means data relating to a living individual who can be identified from that data, or from that data *and* other information which is in, or is likely to come into, Sion Community's possession. Personal data can be factual (such as a name, address or date of birth) or it can be an opinion (e.g. a performance appraisal). It can even include a simple email address. Mere mention of someone's name in a document does not necessarily constitute personal data, but personal details such as someone's contact details or salary (if it enabled an individual to be identified) would fall within the definition. Processing is any activity that involves use of personal data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring or disclosing personal data to third parties.

Sensitive Personal Data means information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, the commission or alleged commission of any offence or any criminal proceedings or sentencing involving that person. Sensitive personal data can only be processed under strict conditions and such processing will usually, although not always, require the explicit consent of the data subject.