Southside Christian Fellowship

Data Protection Policy

Table of Contents

1. Introduction

Southside Christian Fellowship (SCF) must comply with the European Union General Data Protection Regulation (GDPR), UK Data Protection Act, 2018 (DPA) and other relevant legislation protecting privacy rights. This policy, applies to all processing of personal data by and for SCF, regardless of where the processing takes place.

SCF must also comply with relevant legislation in other jurisdictions where it operates.

These data protection laws require SCF to protect personal information and control how it is used in accordance with the legal rights of the data subjects - the individuals whose personal data is held.

2. **Purpose and Aims**

2.1 This policy supports SCF compliance with its obligations as a Data Controller and , where applicable, a Data Processor under data protection law.

2.2 SCF is responsible for, and must be able to demonstrate, compliance with the following Data Protection Principles (2accountability").

2.3 In summary, these state that personal data shall be:

- Processed lawfully, fairly and in a way that is transparent to the data subject ("lawfulness, fairness and transparency");
- Collected or created for specified, explicit and lawful purposes and not be further processed in a manner that is incompatible with those purposes. ("data limitation");
- Adequate, relevant and limited to what is necessary for those purposes ("data minimization");
- Accurate and kept up to date ("accuracy");
- Retained in a form that can identify individuals for no longer than is necessary for that purpose ("storage limitation"); and
- Kept safe from unauthorized access, processing, accidental or deliberate loss or destruction ("integrity and confidentiality").

2.4 Under data protection law SCF must also:

- Proactively inform data subjects about its data processing activities and their rights under the law;
- Meet its legal obligations as a data controller or processor, including: ensuring that data protection is 'designed in' to its processes by default; that we carry out data protection impact assessment; that we maintain records of processing activities; that we take measures to ensure the security of processing and the proper handling of data breaches and; that we have identified an appropriate Data Protection Officer.

3. Scope

This policy sets out a framework of governance and accountability for data protection compliance writing.

3.1 What information is included in the policy

This policy applies to all personal data created or received in the course of operating SCF. Personal data may be held or transmitted in paper, physical and electronic formats or communicated verbally in conservation or over the telephone.

3.2 Who is affected by this policy

3.2.1 Data subjects

These include, but are not confined to: volunteers, ministry leads, employees, leaders and the congregation.

3.2.2 Users of personal data

The policy applies to anyone who obtains records, can access, store or use personal data at SCF. Users of personal data include employees and ministry leads.

3.3 Where the policy applies

This policy applies to all locations from which SCF personal data is accessed.

As the SCF operates internationally, through arrangements with partners in other jurisdictions the policy applies to international activities.

4. Policy Statement

SCF will apply the Data Protection Principles and the other requirements of data protection law to the management of all personal data.

4.1 We will process personal data fairly and lawfully

This means that we will:

- Only collect and use personal data in accordance with the lawful principles set down under the GDPR;
- Treat people fairly by using their personal data for purposes and in a way that they would reasonably expect;
- Ensure that if we collect someone's personal data for one purpose we will not reuse their data for a different purpose that the individual did not agree to or expect.
- Rely on consent as a condition for processing personal data only where:
    - We first obtain the data subject's specific, informed and freely given consent
    - The data subject gives consent, by a statement or a clear affirmative action that we document and
    - The data subject can withdraw their consent at any time without detriment to their interests.

4.2 We will inform Data Subjects what we are doing with their personal data

This means at the point that we collect their personal data, we will explain to Dtata Subjects in a clear, concise and accessible way:

- What personal data we collect;
- For what purposes we collect and use their data;

- What lawful conditions we rely on to process data for each purpose and how this affects their rights;
- Whether we intend to process the data for other purposes and their rights to object;
- The sources from which we obtain their data. Where we have received the data from third parties;
- Whether they need to provide data to meet a statutory or contractual requirement;
- Our obligations to protect their personal data;
- To whom we may disclose their data and why;
- Where relevant, what personal data we publish and why;
- How data subjects can update the personal data that we hold;
- How long we intend to retain their data;
- How to exercise their rights under data protection law;
- The identity and contact details of the Data Protection Officer; and
- We will publish this information on our website and where appropriate in printed formats. We will review the content of these Privacy Notices regularly and inform our data subjects of any significant changes that may affect them.

Where we process personal data to keep people informed about SCF activities and events we will provide in each communication a simple way of opting out of further marketing communications.

Through these actions we demonstrate both accountability for our use of personal data that we manage people's data in accordance with their rights and expectations.

4.3 We will uphold individual's rights as data subjects

This means that we will uphold their rights to:

- Obtain a copy of the information comprising their personal data, free of charge within one month of their request;
- Have inaccurate personal data rectified and incomplete personal data completed;
- Have their personal data erased when it is no longer needed, if the data has been unlawfully processed or if the data subject withdraws their consent, unless there is an overriding legal or public interest in continuing to process the data;
- Object to and prevent further processing of their data for the legitimate interests or public interest unless SCF can demonstrate compelling lawful grounds for continuing;
- Prevent processing of their data for direct marketing;
- Object to decisions that affect them being taken solely by automated means (if applicable); and
- Claim compensation for damages caused by breach of data protection law.

4.4 We will apply data protection principles to all our personal data processing

This means that we will:

- Use proportionate privacy and information risk assessment, and where appropriate data protection impact assessment, to identify and mitigate privacy risks at each stage of every project or initiative involving processing personal data and in managing upgrades or enhancements to systems and processes used to process personal data;
- Adapt data minimization: we will collect, disclose and retain the minimum personal data for the minimum time necessary for the purpose; and

- Anonymise personal data wherever necessary and appropriate, e.g. when using it for statistical purposes, so that individuals can no longer be identified.

4.5 We will protect personal data

This means that we will use appropriate measures to:

- Control access to personal data so that employees, office bearers and ministry leads can only see such personal data as is necessary for them to fulfil their duties;
- Require all SCF staff and employees to complete basic data protection training
- Set and monitor compliance with security standards for the management of personal data.
- Reduce risks of disclosure by pseudonymising personal data where possible;
- Maintain data sharing agreements with partners and other external bodies.
- Where transferring personal data to another country put in place personal agreements.
- Ensure that all those associated with SCF are aware of how data protection law applies to their use of personal data and how they can take appropriate steps to protect their own personal data and respect the privacy of others;
- Manage all subject access and third party requests for personal information about data subjects in accordance with our procedures for responding to requests for personal data; and
- Make appropriate and timely arrangements to ensure the confidential destruction of personal data.

4.6 We will retain personal data only as long as required

This means that we will:

- Apply SCF's records retention schedules to keep records and information containing personal data only as long as required for the purposes for which they were collected;
- Apply exemptions to public rights of access to information as appropriate in accordance with the data subject's rights to privacy;
- Redact personal data, e.g. by pseudonymisation; and
- Withhold access when it is necessary to do so.

4.7 We will manage any breaches of data security promptly and appropriately

This means that we will take all necessary steps to reduce the impact of incidents involving personal data by following the data breach procedures.

Where a data breach is likely to result in a risk to the rights and freedoms of data subjects, the Data Protection Officer will liaise with the Information Commissioner's Office and report the breach, in line with regulatory requirements, within 72 hours of discovery. The Data Protection Officer will also recommend, where necessary, actions to inform data subjects and reduce risks to their privacy arising from the breach.

5. Definitions

Data Protection Officer: the member of staff/leadership with oversight of organisational and technical measures and controls to comply with the Data Protection Act.

Personal Data: data which relates to a living person who can be identified from the data and other information that the Data Controller holds or is likely to receive.

Subject Access Request: A formal written request for a copy of one's own personal data.

Data Subject: the living individual whose personal data we hold.

Data Controller: any person who determines the purposes for which ant the manner in which any personal data is to be processed. For the purposes of this policy SCF is the data controller.

Data Processor: in relation to personal data, means any person (other than an employee) of the data controller who processes data on behalf of the data controller.

6. Responsibilities

6.1 All uses of SCF information are responsible for:

- Completing relevant training and awareness activities provided by the SCF to support compliance with the Data Protection Policy and relevant procedures;
- Taking all necessary steps to ensure that no breaches of information security result from their actions;
- Reporting all suspected information security breaches or incidents promptly to SCF's Secretary so that appropriate action can be taken to minimize harm; and
- Informing SCF of any changes to the information that they have providedto SCF in connection with their employment, for instance, changes of address or bank details.

6.2 The Data Protection Officer is responsible for:

- Providing a point of contact for data subjects with regard to all issues related to their rights under data protection law;
- Investigating personal data breaches, recommending actions to reduce their impact and likelihood of recurrence;
- Acting as the contact point for and cooperating with the Information Commissioner's Office on issues relating to processing;