

Struthers

MEMORIAL CHURCH

DATA PROTECTION POLICY

Last review date: February 2026

Next review date: February 2029

Version Control

| Date | Version | Name | Description |
|------------|---------|-----------|-----------------|
| 10.02.2026 | 1.00 | Mark Kirk | Initial Version |

Contents

| | |
|---|-----------|
| 1. Introduction | 3 |
| 2. Purpose | 3 |
| 3. Scope | 3 |
| 4. Data We Collect | 3 |
| 5. Data Protection Principles | 4 |
| 6. Legal Basis for Processing | 4 |
| 7. Data Storage and Security | 4 |
| 8. Data Sharing | 5 |
| 9. Photography, Livestreaming and Social Media | 5 |
| 10. Children’s Data | 6 |
| 11. Data Retention | 6 |
| 12. Data Subject Rights | 6 |
| 13. Data Breaches | 6 |
| 14. Responsibility and Review | 7 |
| 15. Contact and SAR | 7 |
| 16. Consent and International Data Transfers | 7 |
| 17. Roles and Responsibilities | 8 |
| 18. ROPA and Audit | 9 |
| Appendix 1 - Data Retention Schedule – Struthers Memorial Church | 10 |
| Appendix 2 — Roles and Responsibilities | 11 |
| Appendix 3 - Data Breach Identification and Response | 12 |

1. Introduction

Struthers Memorial Church (“the Church”) is committed to protecting the personal data of its members, attendees, staff, volunteers, and all those who engage with its ministries. As a Scottish charity and a company limited by guarantee, we process personal data in accordance with the UK General Data Protection Regulations (UK GDPR), the Data Protection Act 2018, and related legislation.

The Data Controller is the Board of Directors of the Church. The Church has a Data Protection Lead who receives training on data protection matters at least every three years to ensure knowledge and skills remain up to date.

Our full Privacy Notice, which outlines how we collect, use, and protect personal data, is available on the Church branch websites. We recommend all individuals review it to understand their rights and our responsibilities under data protection law.

All staff and volunteers are expected to be familiar with the content of this policy and follow the principles it sets out.

2. Purpose

This policy outlines how we collect, use, store, and protect personal data, and sets out the responsibilities of the Church, its staff, volunteers, and data processors.

3. Scope

This policy applies to:

- All personal data processed by the Church.
- All branches of Struthers Memorial Church.
- All staff, volunteers, and role holders who process personal data on behalf of the Church.

4. Data We Collect

We collect and process personal data for the following purposes:

- Membership and Congregational Communication: name, address, phone number, and email address.

- Gift Aid and Financial Records: names, bank account data (sort code and account number) and taxpayer status for those who give to the Church and consent to Gift Aid.
- Children's ministry and certain other dedicated events: names, age, contact information, dietary requirements and/or medical details (e.g. allergies or medical conditions).
- Volunteers: contact information and other data necessary for support and safeguarding.
- Employees: contact details, payroll and financial data, health related data, employee records, equality and diversity information.

5. Data Protection Principles

We adhere to the following principles under Article 5(1) of UK GDPR:

1. Lawfulness, Fairness, and Transparency
2. Purpose Limitation
3. Data Minimisation
4. Accuracy
5. Storage Limitation
6. Integrity and Confidentiality
7. Accountability

6. Legal Basis for Processing

We process personal data under the following legal bases:

- Legitimate interests: for activities such as member communication, safeguarding, church administration and employment.
- Legal obligation: to comply with charity and tax law
- Consent: where individuals have given clear consent.

Consent is obtained explicitly via written or electronic forms for specific purposes, including some communications, some event participation, and processing of children's data.

Individuals can withdraw their consent at any time by contacting the Data Protection Lead at data.protection@struthers-church.org.

7. Data Storage and Security

We store personal data securely using:

- Google Drive, with access limited to those who require it for their role. Access permissions are reviewed regularly.
- Data Developments software for processing Gift Aid and financial data. A Data Protection Impact Assessment (DPIA) has been completed for this system.
- Physical copies of data (e.g. forms collected at events) - As an organisation, we are committed to moving towards a predominantly paperless approach, particularly in the collection and handling of personal data. Where paper copies of data collection are necessary, the personal data must be uploaded to the appropriate digital system as soon as possible, and the physical copies should be destroyed immediately after uploading.

8. Data Sharing

We do not share personal data with third parties except where:

- Required by law; or
- We have a processor agreement in place (e.g., with Data Developments); or
- There is a legitimate interest that justifies the sharing.

While we do not currently have formal written agreements in place with third-party processors, we aim to work only with organisations that uphold high standards of data protection and security.

The Church conducts Data Protection Impact Assessments (DPIAs) for all new or significantly changed processing activities that are likely to result in a high risk to individuals' rights and freedoms.

9. Photography, Livestreaming and Social Media

The Church may livestream or record certain services and events for broadcast on public platforms such as Instagram or other social media accounts. These accounts are public-facing and recordings are generally retained online for up to 12 months.

Livestreams are primarily focused on those leading the service or event. However, on occasion, other individuals may appear in the background and be identifiable.

Where practicable, notices will be displayed at services or events to inform attendees if livestreaming or recording is taking place. Where the event involves children or vulnerable adults, additional care will be taken to avoid their inclusion in any livestream or published media without appropriate consent from a parent or guardian.

Individuals who have concerns about appearing in livestreams or recordings should speak to the branch minister/event organiser or the local Data Protection Champion so that reasonable steps can be taken to accommodate their preferences (e.g., seating arrangements).

All livestream recordings and related media will be managed in accordance with this policy and the Church's retention schedule.

10. Children's Data

We collect personal data about children only with the consent of a parent or legal guardian. This data is used strictly for the purpose of participation in church-related events and safeguarding. Special category data, such as medical information, is handled with enhanced protection.

For safeguarding purposes, we process children's personal data under the lawful basis of legitimate activities of a not-for-profit body (UK GDPR Article 9(2)(d)) and in compliance with our legal obligations, ensuring this data is handled with the highest level of care and protection.

11. Data Retention

We retain personal data only as long as necessary for the purpose for which it was collected and to meet legal or regulatory requirements. We have a data retention schedule to facilitate this. This schedule is reviewed periodically to ensure ongoing compliance with legal and operational requirements. See Appendix 1.

12. Data Subject Rights

Individuals have the following rights:

- Access their data.
- Correct inaccurate or incomplete data.
- Request deletion of their data.
- Object to processing.

- Withdraw consent at any time (where processing is based on consent).
- Lodge a complaint with the Information Commissioner's Office (ICO).

13. Data Breaches

All staff, volunteers, and representatives must remain vigilant in protecting personal data. In the event of a data breach or a suspected breach, it must be reported immediately to the Church's Data Protection Lead.

A data breach refers to any incident where personal data is lost, stolen, accessed without authorisation, disclosed, altered, or destroyed in error or unlawfully. This includes both digital and paper-based records.

Upon notification, the Data Protection Lead will assess the severity and potential impact of the breach. Where the breach is likely to result in a risk to individuals' rights and freedoms, it will be reported to the Information Commissioner's Office (ICO) within 72 hours, in line with UK GDPR requirements.

All incidents will be logged, regardless of severity, and reviewed to identify any necessary improvements in data handling processes.

For detailed procedures, including how to recognise, report, and respond to a breach, refer to Appendix 3: Data Breach Reporting Procedure.

14. Responsibility and Review

The Board of Directors, alongside local church leaders, are responsible for ensuring compliance with this policy. This policy will be reviewed at reasonable intervals, if significant changes to data protection law occur, to ensure it remains current and effective.

Policy Awareness

All individuals taking on roles within the church, whether paid or voluntary, should be made aware of relevant policies and procedures, including those relating to data protection. Where appropriate, individuals will be asked to acknowledge their understanding of these policies as part of their role.

15. Contact and SAR

Requests for access to personal data (Subject Access Requests) are handled by the Data Protection Lead and responded to within one month of receipt, in accordance with the UK GDPR. A log of all SARs is maintained.

To make a SAR, or for any questions or concerns regarding this policy or how your data is handled, an email should be sent to the Church's Data Protection Lead. Please email: data.protection@struthers-church.org

16. International Data Transfers

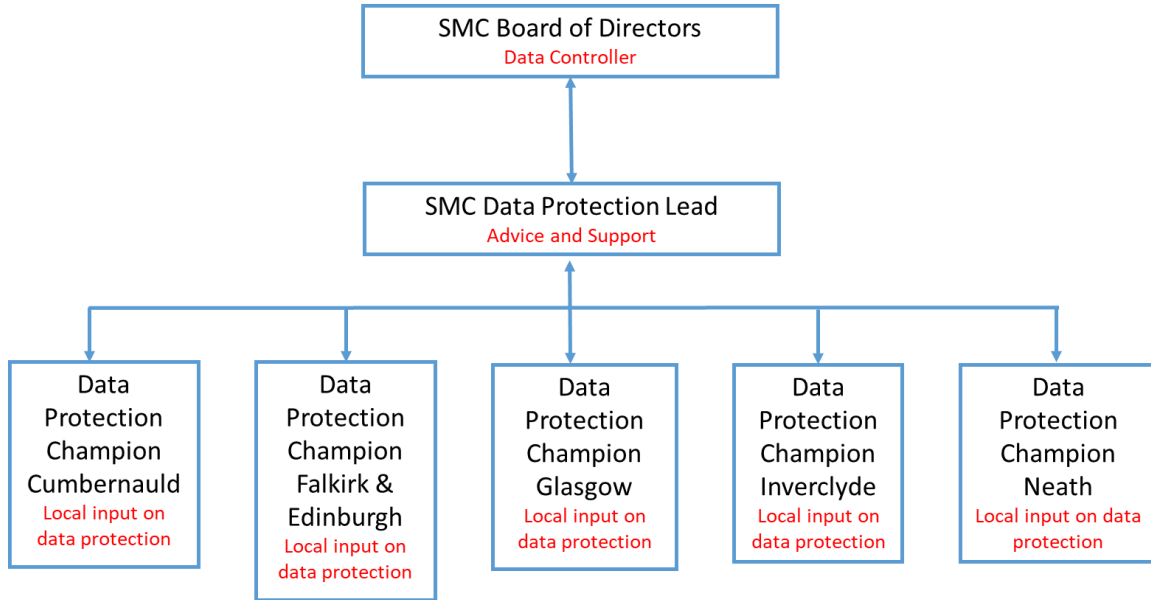
Some of the Church's data is stored using Google Drive, which may involve transfers of personal data outside the UK. We rely on safeguards such as Standard Contractual Clauses approved by the UK Information Commissioner's Office (ICO) to ensure adequate protection for any such transfers. Google has entered into the UK Addendum to the EU Standard Contractual Clauses and participates in the EU-US Data Privacy Framework, providing additional safeguards for any data stored in or transferred to the United States.

17. Roles and Responsibilities

In each branch church, a named Data Protection Champion is appointed to provide local input on data protection matters. These individuals serve as a first point of contact within their respective branches, supporting the implementation of this policy and offering guidance to staff and volunteers on data protection practices.

The Data Protection Champions liaise regularly with the Church's Data Protection Lead to ensure consistent compliance across all locations.

The Data Protection Lead provides advice and support to both the Data Protection Champions and the Board of Directors who hold ultimate responsibility for data protection across the organisation. See schematic below along with Appendix 2 which details roles and responsibilities of each role:



18. ROPA and Audit

The Data Protection Lead may carry out periodic reviews of data protection practices, with input from local Data Protection Champions, to support good practice, monitor compliance and identify areas for improvement.

The Church maintains a Record of Processing Activities (ROPA) documenting all categories of personal data processed, the purposes, legal bases, data sharing, and retention periods. This record is reviewed annually by the Data Protection Lead and Data Protection Champions.

Appendix 1 - Data Retention Schedule – Struthers Memorial Church

This retention schedule outlines how long various types of personal data are kept by Struthers Memorial Church, in line with UK GDPR and safeguarding best practices.

| Data Type | Retention Period | Notes for Volunteers |
|---|----------------------------------|---|
| Event Registration Forms (incl. children’s medical info) | 1 year after event | |
| Member Contact Records | While attendee + 3 years | |
| Gift Aid & Financial Records | 6 years after financial year end | HMRC requirement |
| Volunteer & Staff Records | While in role + 3 years | |
| Complaints | 6 years after resolution | |
| Safeguarding Concerns/Investigations | 75 years | |
| Safeguarding Policy/General Advice | 3 years | This is in relation to policy situations/advice not particular to a specific case. |
| Livestream recordings and social media posts | 12 months | Stored on public church social media accounts. Focus is on service leaders. Avoid filming children/vulnerable adults without consent. |

Appendix 2 — Roles and Responsibilities

Board of Directors (Data Controller)

- Hold ultimate responsibility for compliance with data protection law.
- Approve and oversee the Church's Data Protection Policy.
- Ensure adequate resources are in place for data protection compliance.
- Review and act on reports from the Data Protection Lead.

Data Protection Lead

- Act as the Church-wide point of contact for all data protection matters.
- Provide advice and support to the Board, Data Protection Champions, and volunteers.
- Maintain and update the Record of Processing Activities (ROPA).
- Oversee staff and volunteer data protection policy awareness.
- Investigate, assess, and report data breaches in line with UK GDPR requirements.
- Review and update policies and procedures as indicated in conjunction with the Policies and Procedures Subcommittee.
- Act as point of contact to the Information Commissioner's Office (ICO).
- Attend Data Protection Training at least 3 yearly to ensure knowledge and skills up to date.

Data Protection Champions (in each branch)

- Serve as the first point of contact for local staff and volunteers with data protection queries.
- Support local implementation of the Data Protection Policy.
- Liaise regularly with the Data Protection Lead to ensure consistent compliance.
- Promote good data protection practice in local activities (e.g., handling of registers, event forms).
- Report any suspected data breaches or safeguarding-linked data issues immediately to the Data Protection Lead.

Appendix 3 - Data Breach Identification and Response

What Constitutes a Data Breach

A personal data breach is any security incident that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data. This includes, but is not limited to:

Examples of Data Breaches:

- Lost or stolen devices containing personal data (laptops, USB drives, paper files)
- Email errors such as sending personal information to wrong recipients or using 'CC' instead of 'BCC' for group emails
- Unauthorised access to church systems, Google Drive folders, or filing cabinets
- Hacking or cyber attacks on church systems or email accounts
- Physical security failures such as leaving filing cabinets unlocked or documents unsecured
- System failures that result in data corruption or loss
- Disposal errors such as throwing away personal data without proper destruction
- Accidental publication of personal information on websites, social media, or newsletters

Not Every Incident is Reportable

Minor incidents with minimal risk may not require ICO notification, but all breaches must be:

- Reported to the Data Protection Lead immediately
- Documented and assessed for risk
- Acted upon to contain the breach and prevent recurrence

Immediate Response Steps

All staff and volunteers must:

1. Stop the breach if still occurring (e.g., recall an email, secure an unlocked filing cabinet)

2. Report immediately to the Data Protection Lead at data.protection@struthers-church.org
3. Do not attempt to "fix" the problem without guidance
4. Preserve evidence - don't delete anything or change system settings

Risk Assessment Criteria

The Data Protection Lead will assess each breach based on:

- Number of people affected
- Type of data involved (basic contact details vs. sensitive information like medical data)
- Likelihood of harm to affected individuals
- Potential consequences (identity theft, discrimination, financial loss, etc.)

ICO Notification Requirements

Breaches must be reported to the ICO within 72 hours if they are likely to result in a risk to individuals' rights and freedoms. High-risk breaches must also be communicated to affected individuals without undue delay.

Documentation and Learning

All breaches, regardless of severity, will be:

- Logged in the Church's breach register
- Investigated to determine root cause
- Used to improve our data protection practices and prevent future incidents
- Reviewed as part of our annual policy assessment