Data Protection and Retention Policy
November 2023

THE CONGREGATION OF ST ANDREWS FREE CHURCH

OF THE FREE CHURCH OF SCOTLAND

1 Overview

1.1 St Andrews Free Church takes the security and privacy of personal information seriously. As part of our activities we need to gather and use personal information about a variety of people including members, former members, regular attenders, employees, office-holders and generally people who are in contact with us

1.2 This policy explains the provisions that we will adhere to when any personal data belonging to or provided by data subjects, is collected, processed, stored or transferred on behalf of St Andrews Free Church.

1.3 This policy has been approved by the elders who are responsible for ensuring compliance with our legal obligations.

1.4 The elders have appointed Saleem Bhatti as the Data Protection Elder to oversee data protection in St Andrews Free Church. Any questions arising from the policy should be referred to the Data Protection Elder.

1.5 It is intended that this policy is fully compliant with the Data Protection Act 2018 and the EU General Data Protection Regulation. If any conflict arises between those laws and this policy, St Andrews Free Church intends to comply with the 2018 Act and the GDPR.

1.6 We expect everyone processing personal data on behalf of St Andrews Free Church to comply with this policy in all respects. This includes elders, staff, ministry trainees, rota organisers, and anyone responsible for any area of church life.

1.7 St Andrews Free Church has a separate Privacy Notice which outlines the way in which we use personal information provided to us. A copy can be obtained from the website.

1.8 This policy does not form part of any contract of employment or contract for services. It can be amended at any time.

1.9 Any deliberate or negligent breach of this policy by an employee of the congregation may result in disciplinary action being taken in accordance with our disciplinary procedure. It is a criminal offence to conceal or destroy personal data which is part of a subject access request and such conduct by an employee would amount to gross misconduct which could result in dismissal.

1.10 Any deliberate or negligent breach of this policy by an office-holder or volunteer of the congregation would be a material breach of trust and may result in the person being removed as an office-holder or volunteer.

2 Data Protection Principles, Definitions and Legal Bases

Data protection principles

2.1 Personal data will be processed in accordance with the 'Data Protection Principles'. It must:

- be processed fairly, lawfully and transparently;
- be collected and processed only for specified, explicit and legitimate purposes;
- be adequate, relevant and limited to what is necessary for the purposes for which it is processed;
- be accurate and kept up to date;
- not be kept for longer than is necessary for the purposes for which it is processed; and
- be processed securely.

We are accountable for these principles and must be able to demonstrate compliance.

Definition of personal data

2.2 "Personal data" means information which relates to a living person (a 'data subject') who can be identified from that data on its own, or when taken together with other information which is likely to come into the possession of the data controller.

2.3 As well as including factual information (for example a name, address or date of birth), it also includes photographs and any expression of opinion or intention about the person.

2.4 This policy applies to all personal data whether it is stored electronically, on paper or on other materials.

2.5 We use one or more of the following legal bases to process personal data

- is necessary for the purposes of the congregation's legitimate interests;
- is necessary for us to comply with a legal obligation; and
- is with the explicit consent of the person.

Definition of special categories of personal data

2.6 "Special categories of personal data" are types of personal data consisting of information revealing:

> *racial or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; genetic or biometric data; health; sex life and sexual orientation; and any criminal convictions and offences*.

2.7 A significant amount of personal data held by the congregation will be classed as special category personal data, either specifically or by implication, as it could be indicative of a person's religious beliefs.

2.8 Special category personal data is particularly sensitive information and can only be processed under strict conditions. Unauthorised disclosure of this information is likely to have a material effect on an individual's right to privacy.

2.9 We use one or more of the following legal bases to process special category personal data

- is necessary for the purposes of the congregation's legitimate interests as a not-for-profit religious body; and
- is with the explicit consent of the person.

Definition of processing

2.10 "Processing" means any operation which is performed on personal data, such as collection, recording, organisation, structuring or storage; adaption or alteration; retrieval, consultation or use; disclosure by transmission, dissemination or otherwise making available; and restriction, destruction or erasure.

Use of consent to process data

2.11 Where consent is used as the legal basis for processing, we will clearly set out what we are asking consent for, including why we are collecting the data and how we plan to use it.

2.12 Consent will be specific to each process we are requesting consent for and we will only ask for consent when the data subject has a genuine choice whether or not to provide us with their data.

2.13 Where consent is used to process personal data of children aged 13 or over, consent will be obtained from both the child and their parent or guardian.

2.14 Consent should normally be captured on a digital consent form and this should be stored securely.

2.15 In exceptional circumstances, consent may be received orally rather than in writing. In such circumstances, this fact should be recorded in writing. Any proposed use of oral consent should be discussed with the Data Protection Elder.

2.16 Consent can be withdrawn at any time and if withdrawn, the processing will stop. Data subjects will be informed of their right to withdraw consent and it will be as easy to withdraw consent as it is to give consent.

3 Data Protection in Practice

3.1 Everyone who processes data on behalf of St Andrews Free Church has responsibility for ensuring that the data they collect and store is handled appropriately, in line with this policy and our privacy notice.

Transparency

3.2 At the point of collecting personal data, we will provide the individual with information in writing on how we will use their data. The individuals will also be informed in writing that they can obtain our privacy notice from the website.

Limitation of purpose

3.3 Personal data should be used only for the specified lawful purposes for which it was obtained.

3.4 Advice must be sought from the Data Protection Elder if you are considering using personal data collected for one purpose or activity, for another church related purpose.

3.5 In particular, when processing personal data under consent, we will use the data only for the explicit purpose for which consent was given.

Data minimisation

3.6 We will only collect and use sufficient personal data that is needed for the specific purposes it is required. We will not collect more than is needed to achieve those purposes. We will not collect any personal data “just in case” we want to process it later.

Accuracy

3.7 We will take every reasonable step to ensure that the personal data held is accurate and, where appropriate, kept up to date.

Data retention

3.8 We will not keep personal data longer than is necessary for the purposes for which it was collected, except to comply with our legal and regulatory obligations.

3.9 Personal data should be held in such a way that it can be deleted when there is no longer any reason to keep it.

3.10 Personal data will be disposed of securely when it is no longer needed.

3.11 Guidelines on data retention are in section 5.

Security

3.12 We will use appropriate measures to keep personal data secure at all points of the processing. Keeping data secure includes protecting it from unauthorised or unlawful processing, or from accidental loss, destruction or damage.

3.13 We will restrict access to personal data to those who need it for their specific role at St Andrews Free Church.

3.14 Personal data should not be shared with those who are not authorised to receive it, either within the church or externally. Requests for data should be referred to the main holder of the data and not shared informally.

3.15 Hard copy personal data should be stored securely in lockable storage when not in use. Such storage should be locked with the keys removed. Care must be taken to ensure that hard copy personal data is not left where unauthorised people could see them, including in the home.

3.16 All electronic personal data relating to St Andrews Free Church ministries should be stored on St Andrews Free Church cloud servers.

3.17 Automatic logins to electronic personal data should only be used on encrypted or password protected devices to which only the authorised individual has access. This includes email accounts.

3.18 Passwords should be kept secure, should be strong, changed regularly and not written down or shared with others.

3.19 Personal data transferred by email must be encrypted or password protected. The password must be communicated separately.

Sharing of data

3.20 Personal data should never be shared out with St Andrews Free Church without explicit permission from the Data Protection Elder.

3.21 We will only share personal data with other organisations or people when we have a legal basis to do so and if we have informed the data subject about the possibility of the data being shared in our privacy notice, unless legal exemptions apply to informing data subjects about the sharing.

3.22 We will only appoint other parties to process personal data on our behalf on the basis of a written contract that will require the processor to comply with all relevant legal requirements. We will continue to monitor the data processing, and compliance with the contract, throughout the duration of the contract.

Data subject rights

3.23 We will process personal data in line with data subjects' rights, including their right to

- request access to any of their personal data held by us (known as a Subject Access Request);
- ask to have inaccurate personal data changed;
- request the erasure of their personal data, in certain circumstances; and
- withdraw consent when we are relying on consent to process their data.

3.24 Any request from an individual that relates or could relate to their data subject rights should be forwarded immediately to the Data Protection Elder.

Privacy by design

3.25 Whenever a change to a ministry, activity or system is being considered, and this may have an impact on personal data, we will consider conducting a Data Protection Impact Assessment at the start and throughout the process. This will be completed in line with the guidelines from the Information Commissioner's Office.

4 Data Breaches

4.1 A data breach occurs where there is accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

4.2 In any circumstances where a data breach appears to have occurred, this must be reported immediately to the Data Protection Elder.

4.3 Similarly, any actual or suspected breach of this data protection policy must be reported immediately to the Data Protection Elder.

4.4 The Data Protection Elder will instigate an investigation into the nature and cause of the breach and the extent of the harm to individuals that could result. This will also establish whether there is anything that can be done to recover any losses and limit the potential damage. The investigation will follow the Information Commissioner's Office (ICO) guidelines.

4.5 We will report all data breaches which are likely to result in a risk to any person's rights and freedoms. Reports will be made to the ICO within 72 hours from when someone in the church becomes aware of the breach.

4.6 In situations where a personal data breach causes a high risk to any person's rights and freedoms, we will also inform data subjects whose information is affected without undue delay.

4.7 We will keep records of personal data breaches, even if we do not report them to the ICO.

5 Data Retention Guidelines

5.1 Everyone who processes personal data for St Andrews Free Church must follow the data retention guidelines in the table below.

5.2 Exceptions to these guidelines must be agreed with the Data Protection Elder.

5.3 Advice should be sought from the Data Protection Elder if it is considered that there may be legal, regulatory or potential litigation reasons to retain the personal data beyond the retention guidelines.

5.4 Personal data may be held in lots of formats including on paper, on computers, on mobile phones, in emails, and on social media.

5.5 Disposal of hard copy personal data will be by shredding. Digitally stored personal data will be deleted so as to put beyond use. This does not include archiving.

5.6 Elders, staff, ministry associates, ministry leaders and rota organisers will be required to annually confirm that they have reviewed all the personal data they hold and have followed the data retention guidelines.

Personal data relating to	Retention guideline
Personnel management	7 years after work with church ends
Recruitment	Successful candidate: 7 years after employment ends Unsuccessful candidate: 6 months after recruitment ends, 5 years after recruitment ends for name and contact details.
Donations and gift aid	7 years after donation has been made or gift aid reclaimed
Membership or regular attendance	3 years after no longer a member / regular
General church emails	Until opt-out or 1 year post-regular attendance
Internal rota administration	Until opt-out or is no longer involved in area
Ministry administration	End of relationship or after 1 year of non-attendance
Publicity	Until opt-out or indefinite
Pastoral care	3 years after to cease to be a member
Pastoral Care	3 years post-attendance or opt-out
Safeguarding	1 year post-regular contact
Formal church records	Indefinite