Pencaitland Parish Church
Data Protection Policy

CONTENTS

1. **Overview**

2. **Data Protection Principles**

3. **Personal Data**

4. **Special Category Data**

5. **Processing**

6. **How personal data should be processed**

7. **Privacy Notice**

8. **Consent**

9. **Security**

10. **Sharing personal data**

11. **Data security breaches**

12. **Subject access requests**

13. **Data subject rights**

14. **Contracts**

15. **Review**

Data Protection Policy

1 Overview

1.1 The congregation 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, adherents, employees, office-holders and generally people who are in contact with us. The Data Protection Act 2018 (the "2018 Act") and the EU General Data Protection Regulation ("GDPR") regulate the way in which personal information about living individuals is collected, processed, stored or transferred.

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 the congregation. We expect everyone processing personal data on behalf of the congregation (see paragraph 5 for a definition of "processing") to comply with this policy in all respects.

1.3 The congregation has a separate Privacy Notice which outlines the way in which we use personal information provided to us. A copy can be obtained from Eileen Henderson, Data Protection Officer for PPC.

1.4 All personal data must be held in accordance with the congregation's Data Retention Policy, which must be read alongside this policy. A copy of the Data Retention Policy can be obtained from Eileen Henderson. Data should only be held for as long as necessary for the purposes for which it is collected.

1.5 This policy does not form part of any contract of employment (or contract for services if relevant) and can be amended by the congregation at any time. It is intended that this policy is fully compliant with the 2018 Act and the GDPR. If any conflict arises between those laws and this policy, the congregation intends to comply with the 2018 Act and the GDPR.

1.6 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 (see Paragraph 12 below) and such conduct by an employee would amount to gross misconduct which could result in dismissal.

2 Data Protection Principles

2.1 Personal data will be processed in accordance with the six '**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. Any inaccurate data must be deleted or rectified without delay;
- 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.

3 Definition of personal data

3.1 **"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. It includes any expression of opinion about the person and an indication of the intentions of the data controller or others, in respect of that person. It does not include anonymised data.

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

4 Definition of special category personal data

4.1 '**Special category personal data**' is personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership; genetic or biometric data; data concerning health; or data concerning a person's sex life and sexual orientation.

4.2 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.

5 Definition of processing

5.1 **'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.

6 How personal data should be processed

6.1 Everyone who processes data on behalf of the congregation has responsibility for ensuring that the data they collect and store is handled appropriately, in line with this policy, our Data Retention policy and our Privacy Notice.

6.2 Personal data should only be accessed by those who need it for the work they do for or on behalf of the congregation. Data should be used only for the specified lawful purpose for which it was obtained.

6.3 The legal bases for processing personal data (other than special category data, which is referred to in Paragraph 8 below) are that the processing is necessary for the purposes of the congregation's legitimate interests; or that (so far as relating to any staff whom we employ) it is necessary to exercise the rights and obligations of the congregation under employment law; or that (in relation to the processing of personal data relating to criminal convictions and offences or related security measures in a safeguarding context) the processing meets a condition in Part 1, 2 or 3 of Schedule 1 of the Data Protection Act 2018.

6.4 Personal data held in all ordered manual files and databases should be kept up to date. It should be shredded or disposed of securely when it is no longer needed. Unnecessary copies of personal data should not be made.

7. Privacy Notice

7.1 If someone would not reasonably expect the way in which we use their personal data, we will issue information about this using a Privacy Notice which will be given to them at the point when the data is provided.

7.2 If our use of personal data is what someone would reasonably expect, we will provide information about this using a Privacy Notice which is available on the

congregation's website and can be found on the noticeboard in the Winton Aisle of the Church.

8. When is consent needed for the processing of personal data?

8.1 A significant amount of personal data held by the congregation will be classed as special category personal data, as it could be indicative of someone's religious beliefs.

8.2 Processing of such special category data is prohibited under the GDPR unless one of the listed exemptions applies. Three of these exemptions are especially relevant (although others may also apply):

- the individual has given **explicit consent** to the processing of the personal data for one or more specified purposes; OR

- processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data is not disclosed outside that body without the consent of the data subjects; OR

- processing is necessary for reasons of substantial public interest, and in particular for the purpose of (a) protecting an individual from neglect or physical, mental or emotional harm; or (b) protecting the physical, mental or emotional well-being of an individual, where that individual is either aged under 18 or is aged 18 or over and is "at risk" (has needs for care and support, experiencing or at risk of neglect or any type of harm, and unable to protect themselves).

8.3 Most of the processing carried out by the congregation will fall within the latter two exemptions and will be carried out by the congregation with appropriate safeguards to keep information safe and secure. This information will not be disclosed outside the Church without consent. Such processing will not require the explicit consent of the data subject.

8.4 Where personal data is to be shared with a third party, the congregation will only do so with the explicit consent of the data subject. For example, personal data will only be included in a directory for circulation or included on a website where consent has been obtained.

8.5 If consent is required to process the information this should be recorded using the style consent form. If consent is given orally rather than in writing, this fact should be recorded in writing.

9. Keeping personal data secure

9.1 Personal data should not be shared with those who are not authorised to receive it. Care should be taken when dealing with any request for personal information over the telephone or otherwise. Identity checks should be carried out if giving out information to ensure that the person requesting the information is either the individual concerned or someone properly authorised to act on their behalf.

9.2 Hard copy personal information should be stored securely (in lockable storage, where appropriate) and not visible when not in use. Filing cabinets and drawers and/or office doors should be locked when not in use. Keys should not be left in the lock of the filing cabinets/lockable storage.

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

9.4 Emails containing personal information should not be sent to or received at a work email address (other than an @churchofscotland.org address) as this might be accessed by third parties.

9.5 The 'bcc' rather than the 'cc' or 'to' fields should be used when emailing a large number of people, unless everyone has agreed for their details to be shared amongst the group.

9.6 If personal devices have an @churchofscotland.org account linked to them these should not be accessed on a shared device for which someone else has the pin code.

9.7 Personal data should be encrypted or password-protected before being transferred electronically.

9.8 Personal data should never be transferred outside the European Economic Area except in compliance with the law.

10. Sharing personal data

10.1 We will only share someone's personal data where we have a legal basis to do so, including for our legitimate interests within the Church of Scotland (either within the Presbytery or to enable central databases held within the Church Office at 121 George Street, Edinburgh to be maintained and kept up to date). This may require information relating to criminal proceedings or offences or allegations of offences to be processed for the protection of children or adults who may be at risk and to be shared with the Church's Safeguarding Service or with statutory agencies.

10.2 We will not send any personal data outside the European Economic Area. If this changes all individuals affected will be notified and the protections put in place to secure your personal data, in line with the requirements of the GDPR, will be explained.

11. How to deal with data security breaches

11.1 Should a data security breach occur, the congregation will notify the Presbytery Clerk **immediately.** If the breach is likely to result in a risk to the rights and freedoms of individuals then the Information Commissioner's Office must be notified within 72 hours.

9.2 Breaches will be handled by the Presbytery Clerk in accordance with the Presbytery's data security breach management procedure.

12. Subject access requests

12.1 Data subjects can make a subject access request to find out what information is held about them. This request must be made in writing. Any such request received by the congregation should be forwarded immediately to the Presbytery Clerk who will coordinate a response within the necessary time limit (30 days).

12.2 It is a criminal offence to conceal or destroy personal data which is part of a subject access request.

13. Data subject rights

13.1 Data subjects have certain other rights under the GDPR. This includes the right to know what personal data the congregation processes, how it does so and what is the legal basis for doing so.

13.2 Data subjects also have the right to request that the congregation corrects any inaccuracies in their personal data, and erase their personal data where we are not entitled by law to process it or it is no longer necessary to process it for the purpose for which it was collected. Data should be erased when an individual revokes their consent (and consent is the basis for processing); when the purpose for which the data was collected is complete; or when compelled by law.

13.3 All requests to have personal data corrected or erased should be passed to Eileen Henderson who will be responsible for responding to them in liaison with the Presbytery Clerk.

14. Contracts

14.1 If any processing of personal data is to be outsourced from the congregation, we will ensure that the mandatory processing provisions imposed by the GDPR will be included in the agreement or contract.

15. Policy review

The Kirk Session will be responsible for reviewing this policy from time to time and updating the congregation in relation to its data protection responsibilities and any risks in relation to the processing of data.

* * *