WEST MORAY CHURCH OF SCOTLAND SC000711

Data Protection Policy

CONTENTS

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 "DPA 2018") and the UK General Data Protection Regulation ("GDPR") and associated data protection laws regulate the way in which organisations can process, collect, store, access and transfer personal information about living identifiable individuals.

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 Section 5 for a definition of "processing") to comply with this policy in all respects.

1.3 The congregation has separate Privacy Notice(s) which outlines the way in which we use personal information provided to us. A copy can be obtained from the Session Clerk.

1.4 All personal data must be held in accordance with the Records Retention & Disposal Schedules, which must be read alongside this policy. A copy of the Records Retention & Disposal Schedules can be obtained from the Session Clerk. 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 data protection legislation. If any conflict arises between those laws and this policy, the congregation intends to comply with the UK data protection legislation and this policy will be revised accordingly.

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

1.7 The congregation's employees have access to and must adhere to this policy and all other operational procedures and guidance which give them appropriate direction on the application of data protection legislation.

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 in a transparent manner;
- be collected and processed only for specified, explicit and legitimate purposes – 'Purpose Limitation'
- be adequate, relevant and limited to what is necessary for the purposes for which it is processed – 'Data Minimisation'
- be accurate and kept up to date. Any inaccurate data must be deleted or rectified without delay – 'Accuracy'
- not be kept for longer than is necessary for the purposes for which it is processed – 'Storage Limitation' and
- be processed securely – 'Integrity and Confidentiality'

There is an overarching principle – 'Accountability'. This means we are accountable for complying with the data protection laws and we must be able to evidence that compliance for the data protection regulator, the UK Information Commissioner's Office ("the ICO"), who has considerable powers including power to impose very large fines.

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 a combination of other information has the potential to identify an individual. It includes any expression of opinion about the person; an indication of the intentions of the Controller or others, in respect of that person and Pseudonymised personal data. It does not include anonymised data which is not regulated by the UK GDPR or the DPA 2018, provided the anonymisation has not been done in a reversible way.

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 or 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.

4.3 Some personal data is more sensitive and is afforded more protection. It's important to note though that this data is not special category personal data, but it is required to be handled in the same way that special category is.

'Criminal offence data'

The UK GDPR gives extra protection to personal data relating to criminal convictions and offences or related security measures. This covers information about offenders or suspected offenders in the context of criminal activity, allegations, investigations, and proceedings. It includes not just data which is obviously about a specific criminal conviction or trial, but also any other personal data relating to criminal convictions and offences. For example, it can also cover suspicion or allegations of criminal activity.

Vulnerable groups, e.g. children's personal data

The congregation must protect the interests of vulnerable groups, such as children or individuals with learning difficulties. Children need particular protection when their personal data is collected or processed because they may be less aware of the risks involved. In the UK children aged 13 or over are able to provide their own consent, so for children under this age, where processing of their data is based on consent (and not on some other lawful basis, as set out in this policy), it will be necessary to obtain this from whoever holds parental responsibility for the child.

5 Definition of processing

5.1 **'Processing'** means any operation which is performed on personal data, including collecting, recording, accessing, organising, structuring, storing; adaption or alteration; retrieval, consultation or use; disclosure by transmission, dissemination or otherwise making available; transferring, restriction, destruction or erasure. This list gives examples of what 'processing' is. It's important to note that even if data is held and no

other operation is being carried out, this constitutes 'processing' and therefore data protection laws apply.

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 Records Retention & Disposal Schedules and our Privacy Notice(s).

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. Data should only be held for as long as necessary for the purposes for which it is collected. It is therefore important that the retention and disposal schedules are followed and data is disposed of securely when it is no longer required.

6.3 The legal bases for processing personal data (other than special category data, which is referred to in Section 8 below) are that the processing is necessary for the purposes of the congregation's legitimate interests; that the data subject has given consent; 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 is necessary for the performance of a contract; that processing is necessary for legal obligations, that processing is necessary for the vital interests of the data subject; 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 accurate and kept up to date. It should be shredded or disposed of securely when it is no longer needed. Unnecessary copies of personal data must not be made.

7. Privacy Notice

7.1 The individuals from whom we collect personal data should be provided with a privacy notice prior to the point of data collection. This meets one of the data subject rights – the right to be informed - and it is important that privacy notice(s) are in place prior to the collection of data.

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. The privacy notices also include details on individual rights. Keeping the first

data protection principle in mind ('Fairness, Lawfulness and Transparency') publishing the privacy notice enables individuals to view them at any time.

8. Processing Special Category 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 UK data protection law unless one of the lawful bases applies in UK GDPR and the DPA 2018 Act. Four of these lawful bases are especially relevant (although others may also apply, if unsure seek advice from the Law Department/DPO):

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

- processing is necessary for the purposes of carrying out the obligations and exercising specific rights in the field of employment and social security and social protection law in so far as it is authorised by domestic law or a collective agreement pursuant to domestic law providing for appropriate safeguards for the fundamental rights and the interests of the data subject; and/OR

- Processing is necessary for the establishment, exercise or defence of legal claims; and/OR

- Processing is necessary for archiving purposes in the public interest; and/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; and/OR

- processing is necessary for reasons of substantial public interest to protect the vital interests of the data subject, 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 lawful bases, 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. Therefore, such processing will not require the explicit consent of the data subject, unless disclosure of the data outside the congregation is planned.

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 or unless there is a lawful basis for doing so. For example, personal data will only be included in a directory for circulation or included on a website where consent of the data subject 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 and include the date the consent expires.

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 such as addresses over the telephone or otherwise. Identity checks must 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. If it is not clear, do not disclose the information and seek advice from the Law Department/ DPO.

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. The following list will assist in ensuring your password(s) are strong and secure:

- It should be at least eight characters long
- Does not contain your user name or real name
- Does not contain a complete word
- Is significantly different from previous passwords

- Contains a combination of uppercase letters, lowercase letters, numbers and symbols

9.4 Emails containing personal information or business sensitive 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 It is always necessary to use the 'bcc' field rather than the 'cc' or 'to' fields 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 and/or password-protected before being transferred electronically. If personal data is to be sent by post a secure courier must be used. The recipient must be made aware as to when they should expect to receive the information and verification of safe receipt should be sought.

9.8 Personal data may be transferred outside the UK or the European Economic Area (EEA) in compliance with data protection laws. This may require the consent of the data subjects, or relying on transfer mechanisms including ensuring appropriate UK International Data Transfer Agreements (IDTA) and safeguards are in place to meet those data transfer rules such as UK-US Data Bridge, EU-US Data Privacy Framework. If unsure seek advice from the Law Department/DPO.

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 vulnerable adults who may be at risk and to be shared with the Church's Safeguarding Service or with statutory agencies.

10.2 We will only do so in compliance with the law and at all times respecting the rights and freedoms of the data subjects (individuals).

10.3 When sharing personal data with another organisation, there must be an appropriate data sharing agreement in place, following the ICO's Data Sharing Code of Practice.

10.4 If you are unsure of getting the appropriate data sharing agreement in place, please contact the DPO/Law Department for further advice and guidance.

11. How to deal with data security breaches

11.1 A security breach is broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data.

11.2 There are legal reporting requirements and it is therefore vital that should a potential personal data security breach occur, the congregation should notify the Presbytery Clerk **immediately** using the Breach Notification Form

11.3 If the breach is likely to result in a risk to the rights and freedoms of individuals then the UK Information Commissioner's Office (ICO) may require to be notified within 72 hours of the breach occurring.

11.4. Breaches will be handled by the Presbytery Clerk in accordance with the Presbytery's Data Protection Breach Incident Management Policy, working in conjunction with the National Office DPO.

11.5. It is important to note that the ICO can fine organisations in breach of data protection laws. This can include fines for breaches if they consider that the technical and organisational measures in place are not sufficient.

12. Subject access requests

12.1 Individuals (data subjects) have a number of rights, including the right to make a subject access request to find out what information is held about them by us. This request can be made orally or in writing. If oral, it will be necessary to confirm in writing the scope of the request and also, if necessary, verify the identity of the individual. 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 (one calendar month).

12.2 The timescale for response can be extended but that is only in extenuating circumstances. The Presbytery Clerk will seek advice from the DPO/Law Department as to whether such an extension could be applied.

12.3 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 The right to obtain information about your personal data is a fundamental right under data protection law, unless prohibited by law. As well as the right to be informed (privacy notices) and the right of access, individuals also have the following rights:

13.1.1 Right to rectification – this means that if data held is inaccurate or incomplete an individual can request that this is resolved.

13.1.2 Right to erasure, commonly known as the right to be forgotten, which means an individual can request an organisation to delete all of their data.

13.1.3 The right to restrict processing – this right links with some of the other rights and provides that if there is an issue in relation to processing it can be restricted until a resolution is found

13.1.4 The right to data portability – this means that an individual has the right to request that we provide data in a machine-readable format, for example a .csv file and transfer it to another organisation the individual has identified

13.1.5 The right to object – this means an individual can object to the processing and we would have to stop processing unless we can prove a legitimate lawful purpose for the processing. The right to object is absolute in relation to marketing.

13.1.6 Rights in relation to automated individual decision-making including profiling – this right is in relation to data being processed entirely by computers, with no human input, with outcomes of decisions which could potentially impact the individual, (e.g. pre-programmed algorithms and criteria). The right means that a data subject can request that there is human intervention and that the decision is considered by a human rather than computer algorithms.

13.2 All data subject requests (DSRs) should be passed to the Session Clerk 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 in data protection legislation will be included in the agreement or contract. There will also be appropriate due diligence checks to ensure the third party has all necessary safeguards in place, including, but not limited to, appropriate security controls, meeting cyber standards and ensuring the supplier's staff are fully trained on data protection. Please

seek advice from the DPO/Law Department to ensure the appropriate contract/ agreements are in place.

15. Responsibilities

Data Protection Officer (DPO)

The DPO is responsible for reviewing this policy from time to time.

Kirk Session

The Kirk Session is responsible for updating the congregation in relation to its data protection responsibilities and any risks in relation to the processing of data. It is also responsible for ensuring that all congregational staff and volunteers who process personal data are familiar with this policy, comply with it and take advantage of all available training opportunities relating to good data protection practice.