



DATA PROTECTION POLICY

THE CONGREGATION OF BUCCLEUCH OF THE FREE CHURCH OF SCOTLAND IN THE PRESBYTERY OF EDINBURGH AND PERTH

1 Purpose and scope

- 1.1 We (the congregation) process personal information (also called personal data) about individuals. These include, but are not limited to, office holders, employees, volunteers, members, former members, adherents, contractors, suppliers, and others who are in contact with us for a variety of reasons.
- 1.2 **Personal data** is any information from which a person can be identified, directly or indirectly. In addition to basic personal information such as names, contact details etc. etc., it includes opinions expressed about a person and information regarding the intentions of the data controller and third parties about a person. It does not include information which has been appropriately anonymised.
- 1.3 **Processing** means anything we do with personal information - for example, collecting, editing, storing, holding, disclosing, sharing, viewing, recording, listening, erasing, deleting etc. We are committed to processing personal information appropriately and lawfully, in terms of the Data Protection Act 2018 (the "2018 Act") and the General Data Protection Regulation ("GDPR").
- 1.4 This document sets out our data protection policy. It provides some basic information about data protection, including the 7 data protection principles,

information regarding special categories of personal data, how we process personal information (including our legal bases for processing), how we keep it secure and where appropriate share it, and how we would deal with any data security breach. It also provides information on the rights of "data subjects" (individuals about whom we hold personal information). It applies to all those involved in processing personal information on our behalf, who must comply with this policy in all respects.

- 1.5 We have a separate **Privacy Notice** which outlines the way in which we process personal information provided to us, and a **Data Retention Policy** which outlines how long various categories of personal information are retained by us. In general terms, personal information should only be retained for as long as is necessary for the purposes for which it was obtained. Copies of our Privacy Notice and Data Retention Policy are available on the church noticeboard or by emailing our administrator on admin@buccleuchfreechurch.co.uk
- 1.6 This policy does not form part of any contract of employment or contract to provide services. It will be reviewed from time to time to ensure compliance with data protection laws and will be updated as required.
- 1.7 We take compliance with this policy very seriously. Any deliberate or negligent breach of this policy by an employee may result in disciplinary action being taken and may result in dismissal for gross misconduct.

2 Data Protection Principles

- 2.1 Personal information will be processed by us in accordance with the 7 GDPR Data Protection Principles, which stipulate that personal information must be:
 - processed lawfully, fairly and in a transparent manner;
 - collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with these purposes;
 - adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;
 - accurate and, where necessary, kept up to date;
 - kept in a form which permits identification of individuals for no longer than is necessary for the purposes for which it is processed;
 - processed securely, with protection against unauthorised or unlawful processing and against accidental loss or damage, using appropriate technical or organisational measures;

and, in accordance with the seventh principle, we are responsible for, and must be able to demonstrate compliance with, the first 6 principles as listed above.

3 Special categories of personal data

3.1 These are categories of personal information that are deemed to be more sensitive than others. Additional rules (see under paragraph 4 below) apply to the processing of personal information which falls under any of these categories, which are defined in the GDPR as being *"Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation."*

3.2 A significant amount of personal information held by us will be classed as special category personal data, either specifically or by implication (the mere fact of us holding the information being potentially indicative of a person's religious beliefs).

4. Legal Bases for processing personal information and special categories of personal information

4.1 We process personal information on one or more of the following legal bases, which are also set out in our Privacy Notice, where:

4.1.1 you have given consent to the processing for one or more specific purpose;

4.1.2 processing is necessary for the purposes of the congregation's legitimate interests, and such interests are not overridden by your interests or fundamental rights and freedoms;

4.1.3 processing is necessary for the performance of a contract with you; or

4.1.4 processing is necessary for compliance with a legal obligation.

4.2 Where we process any special category data (and this will be most of the data we process) we will, **in addition** to meeting a minimum of one of the legal bases listed in paragraph 4.1 hereof, ensure that one or more of the following applies:

4.2.1 processing is carried out in the course of our legitimate activities with appropriate safeguards by us as a not-for-profit body with a religious aim and on condition that the processing relates solely to our members, or to former members, or to

people who have regular contact with us in connection with our purposes, and that the personal information is not disclosed outside the Free Church of Scotland without your consent; or

4.2.2 you have given explicit consent to the processing of your personal information for one or more specified purpose; or

4.2.3 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 is unable to protect themselves).

5. Access to personal information and keeping it secure

5.1 Everyone who processes personal information on our behalf (including, but not limited to, the minister, office-bearers, employees, volunteers and service providers) must ensure that they do so in line with this policy, our Data Retention Policy and our Privacy Notice, and all in accordance with data protection law.

5.2 Personal information should only be accessed by those who need it in connection with the work they do for us.

5.3 In relation to minutes of meetings of the Kirk Session and Deacons' Courts only individuals specifically authorised by the Kirk Session and/or Deacons' Court are permitted to receive copies of such minutes and other records.

5.4 Personal information should be processed only for the purposes for which it was obtained.

5.5 Personal information should be accurate and, where necessary, updated.

5.6 Personal information 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, whether by letter, email communication, 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.

- 5.7 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.
- 5.8 Confidential paper waste should be disposed of securely by shredding.
- 5.9 Any computers being used in a shared area (including in the user's home) should be shut down, or the user should log off, when leaving them unattended.
- 5.10 Personal information being processed electronically should always be password protected. Passwords should be kept secure, should be strong, changed regularly and not written down or shared with others.
- 5.11 Joint or shared email addresses should not be used for processing personal information.
- 5.12 It is recommended that emails containing personal information should not be sent to or received at a work email address (other than an @freechurch.org address) as this might be accessed by third parties.
- 5.13 If personal devices have an @freechurch.org account linked to them these should not be accessed on a shared device for which someone else has the pin code.
- 5.14 Personal data should always be encrypted if being taken off premises.
- 5.15 Back-ups of personal data stored electronically should be kept.
- 5.16 Personal data should never be transferred outside the European Economic Area except in compliance with the law.

6. Sharing personal data

- 6.1 We will only share personal information where we have a legal basis to do so, including for our legitimate interests within the Free Church of Scotland (either within the Presbytery or to enable central databases held within the Church Offices at The Mound, 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 those within the Church who have designated roles in respect of Safeguarding, or with statutory agencies.

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

7. If there is a data security breach

7.1 A data breach is where there is accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This can happen in many different ways, for example:

- Loss or theft of data or equipment on which personal information is stored;
- Unauthorised access to or use of personal information by a member of staff, volunteer or third party;
- Loss of data resulting from an equipment or systems failure;
- Human error, such as accidental deletion, alteration or transfer of data;
- Unforeseen circumstances, such as fire or flooding;
- Deliberate attacks on IT systems, such as hacking, viruses or phishing scams;

7.2 Should a data security breach occur, and if the breach is likely to result in a risk to the rights and freedoms of individuals, then we will notify the Information Commissioner's Office without undue delay and, where possible, within 72 hours of the time we become aware of the breach. Notification will be made or coordinated by the Session Clerk.

8. Subject access requests

8.1 Individuals who are data subjects may ask us for copies of the personal information we hold about them. This request must be made in writing. Any such request received by the congregation should be forwarded immediately to the Session Clerk sessionclerk@bucleuchfreechurch.co.uk who will coordinate a response within the necessary time limit (maximum 30 days).

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

9. Rights of Data subjects

- 9.1 Data subjects have certain other rights under the GDPR and the 2018 Act. These include the right to know what personal data we are processing, the purposes of such processing, and the legal basis or bases for the processing.
- 9.2 Data subjects also have the right to request that we have any inaccurate or incomplete personal information rectified, and to have their personal data erased if we are not entitled by law to process it or it is no longer necessary for us to process it for the purpose for which it was collected. In situations where consent is the only legal basis which we have for processing then personal information should be erased if and when the individual revokes that consent.
- 9.3 All requests to have personal data corrected or erased should be passed to the Session Clerk John MacLeod on sessionclerk@bucleuchfreechurch.co.uk who will be responsible for responding to them.

10. Training

- 10.1 We will ensure that all those engaged in processing personal information for the congregation receive adequate training in their data protection responsibilities

11. Contracts

- 11.1 If any processing of personal information is outsourced to an external data processor we will enter into a contract with them to ensure compliance with data protection law.

12. Data Protection Policy Review

- 12.1 This policy will be reviewed and updated from time to time.

This Data Protection Policy was adopted on 25/05/2018. The charity trustees will be responsible for the implementation of this Policy in the Congregation.