DATA PROTECTION POLICY

Fitzroy Presbyterian Church

Introduction

We, Fitzroy Presbyterian Church, need to gather and use certain information about individuals.

This can include information about members and adherents, employees, volunteers, suppliers, service users, facilities users, residents, business contacts, and other people we have a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet data protection standards and to comply with the law.

Why this policy exists

This data protection policy ensures that we:

- Comply with data protection law and follows good practice.
- Protect the rights of members and adherents, staff, volunteers and other people we have a relationship with or may need to contact.
- Are open about how we store and process individuals' data.
- Protect ourselves from the risks of a data breach

Data protection law

The General Data Protection Regulation (EU 2016/679) (GDPR) regulates how organisations collect, handle and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or on other materials. To comply with the law, personal information must be collected and used fairly, stored and disposed of safely and not disclosed unlawfully. The GDPR is underpinned by six important principles to which we will adhere. These say that personal data shall be:

1. Processed lawfully, fairly and in a transparent manner in relation to individuals;

2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

4. Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

5. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

6. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Policy scope

This policy applies to us and all staff, post-holders, volunteers, contractors, suppliers and other people processing personal data on behalf of us.

It applies to all data that we hold relating to identifiable individuals. This can include for example:

- Names of individuals, postal/email addresses, telephone numbers, bank details.

- Sensitive personal data such as information in relation to physical or mental health conditions, religious beliefs, ethnic origin, sexual orientation.

However, we consider that membership of the church community implies a willingness to be included in church events and to receive information, invitations, updates, and pastoral care from the church community. Contact details are therefore widely shared within the church community by its members, and without the involvement of church officers and staff. We consider that Fitzroy's obligation in

relation to the use of 'basic contact data' – limited here to names, addresses, email addresses and phone numbers – on a peer to peer basis within the church community is limited to ensuring that the centrally held records are accurate. We cannot be responsible for the peer to peer sharing of such data among the church community

Data Protection Risks

This policy helps to protect us from some very real data security risks, including:

- Breaches of confidentiality – for instance, information being given out inappropriately about our members, volunteers or staff.
- Failing to offer choice – for instance, all individuals should be free to choose how we use data relating to them.
- Reputational damage – for instance, we could suffer if hackers or thieves successfully gained access to personal data.

Responsibilities

Everyone who works for or with us has some responsibility for ensuring personal data is collected, stored and handled appropriately.

Everyone who handles personal data must ensure that it is handled and processed in line with this policy and data protection principles. Failure to comply with the data protection policy and principles is a serious offence and in the case of staff could result in disciplinary action.

However, the following have key areas of responsibility:

- The Kirk Session is ultimately responsible for ensuring that we meet our legal obligations.
- The Data Protection Lead is responsible for:
    - Keeping the Kirk Session and Committee updated about data protection responsibilities, risks and issues.
    - Reviewing all data protection procedures and related policies, in line with an agreed schedule.
    - Arranging data protection training and advice for the people covered by this policy.

- Dealing with requests from individuals to see the data we hold about them (also called “subject access requests”).

- Checking and approving any contracts or agreements with third parties that may handle the company’s sensitive data.

General Staff Guidelines

- The only people able to access data covered by this policy should be those who need it for their work.

- Data should not be shared informally.

- We will provide guidance to all staff, leaders and volunteers to help them understand their responsibilities when handling data.

- Staff, leaders and volunteers should keep all data secure, by taking sensible precautions and following the guidelines below.

- In particular, strong passwords must be used and changed regularly; they should never be shared.

- Personal data should not be disclosed to unauthorised people, either internally or externally.

- When receiving telephone enquiries, we will only disclose personal data we hold on our systems if the following conditions are met:

  a) We will check the caller's identity to make sure that information is only given to a person who is entitled to it.

  b) We will suggest that the caller put their request in writing if we are not sure about the caller’s identity and where their identity cannot be checked.

  Our staff, leaders and volunteers will refer a request to the Minister or Clerk of Session for assistance in difficult situations. Individuals should not be pressurised into disclosing personal information.

- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.

- Staff, leaders and volunteers should request help from the Data Protection Lead if they are unsure about any aspect of data protection.

Data Collection

In accordance with data protection legislation the main legal basis for collecting personal data on our members and those affiliated with us will be on the basis that it is necessary for us to hold said data for the purposes of legitimate interests which are not overridden by the interests of the data subject. In respect of certain types of sensitive data (and in particular data revealing religious beliefs of the data subject) this data will be held on the basis that it is processed in the course of the legitimate activities of a not-for-profit religious body and will not be disclosed outside of that body without the consent of the data subject.

Other legal bases will also apply such as employment law, contract law, etc. There are particular provisions under the General Data Protection Regulation when the legal basis being relied upon is consent. In certain circumstances we may need to seek your consent to process your personal data, particularly if it is outside of our normal day to day activities or it would involve sharing your personal data with a third party. If this is necessary then your consent will be informed consent.

Informed consent is when

- An Individual clearly understands why their information is needed, who it will be shared with, the possible consequences of them agreeing or refusing the proposed use of the data
- And then gives their informed and unambiguous consent.

We will ensure that data is collected within the boundaries defined in this policy. This applies to data that is collected in person, or by completing a form.

When collecting data, we will ensure that the Individual (Data Subject):

a) Has received sufficient information on why their data is needed and how it will be used;

b) Is made aware what the data will be used for and what the consequences are should the Individual/Service User decide not to give consent to processing;

c) Where necessary, grants explicit consent, either written or verbal for data to be processed;

d) Is, as far as reasonably practicable, competent enough to give consent and has given so freely without any duress; and

e) In the absence of valid consent (that which is freely given, specific, informed and unambiguous) or where consent is deemed unnecessary i.e. another legal basis applies, has received information as to the lawful basis for processing their information.

Processing in line with Data Subject's Rights

We will process all personal data in line with data subjects' rights, in particular their right to:

a) Request access to data held about them by a data controller.

b) Prevent the processing of their data for direct-marketing purposes.

c) Ask to have inaccurate data corrected or erased.

d) Prevent processing that is likely to cause damage or distress to themselves or anyone else.

Data Storage

These rules describe how and where data should be safely stored and the security measures implemented by us. Questions about storing data safely can be directed to the Data Protection Lead.

When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it. These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept in a locked drawer or filing cabinet.

- Staff, leaders and volunteers should make sure paper and printouts are not left where unauthorised people could see them, like on a printer.

- Data printouts should be shredded and disposed of securely when no longer required.

- With regards to personal data, a “clear desk” policy is in effect. All data stored on paper should be returned to the appropriate drawer or filing cabinet at the end of the day and no papers should be unnecessarily left unattended on desks during the day.

- Where personal data is recorded in a notebook (for example for the purposes of pastoral visitation) consideration should be given to anonymization or pseudonymising of personal data so as to reduce the risk of damage to the data subject should the notebook be lost or stolen.

When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts. It must be password protected and encryption may also be considered, if felt necessary:

- Data should be protected by strong passwords that are never shared between staff, leaders and volunteers.

- If data is stored on removable media (like a CD, DVD, flash drive etc.), these should be secured when not being used.

- Data should only be stored on designated drives and servers and should only be uploaded to an approved cloud computing service. When using services such as these you must be satisfied that the supplier will hold the data in a manner which is compliant with data protection legislation. To do this you should review their terms and conditions or other contractual information to ensure that these matters are addressed.

- Servers containing personal data should be sited in a secure location, away from general office space.

- Data is backed up frequently.

- Personal data – other than basic contact data - should never be saved directly to mobile devices like tablets or smart phones. In exceptional cases where it is necessary to temporarily save data to a pen drive, or other mobile device then equivalent measures such as password protection, encryption etc. as appropriate should be adopted.
- Where data is saved to laptops, it will be password protected and encrypted.

- All servers and computers containing data are protected by approved security software and a firewall.

- Personal data collected by us should not be stored exclusively on a personal computer as this may prevent legitimate access to and use of that data by us.

- Security measures must be applied to personal devices consistent with those applied to our equipment.

Data Retention and Secure Destruction

Personal data will not be retained longer than necessary, in relation to the purpose for which such data is processed. We will ensure that secure storage/archiving periods are clearly defined for each type of data and ensure confidential destruction of data when no longer required.

Data Use

Personal data is of no value to us unless we can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft and as such we adopt the following additional security measures:

- When working with personal data, staff, leaders and volunteers should ensure the screens of their computers are always locked when left unattended.

- Personal data should not be shared informally. In particular, employees should be particularly vigilant when sending data by e-mail as this form of communication is not secure.

- Financial Data, and in particular bank details must not be transferred electronically. Bank details should only be transferred by letter and/or confirmed by telephone.

- Personal data should never be transferred outside of the European Economic Area without the approval of the Data Protection Lead/Clerk of Session and will only be permitted in the event that an adequate level of protection can be guaranteed. Some suppliers (e.g. cloud storage, survey software etc.) may operate outside of the EEA in terms of the processing they carry out and we will only use suppliers that can demonstrate GDPR compliance and have agreed to this in their terms and conditions.

- Staff, leaders and volunteers should not save copies of personal data to their own computers. Always access and update the central copy of any data.

- Consideration will be given to the anonymization or pseudonymising of personal data to promote the safe use or sharing of data within the organisation

Data Accuracy

The law requires us to take reasonable steps to ensure data is kept accurate and up to date.

The more important it is that the personal data is accurate, the greater the effort we should put into ensuring its accuracy.

It is the responsibility of all staff, leaders and volunteers who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in as few places as necessary. Staff, leaders and volunteers should not create any unnecessary additional data sets.

- Staff, leaders and volunteers should take every opportunity to ensure data is updated.

- We will make it easy for data subjects to update the information we hold about them. For instance, via the website or through cards placed in the sanctuary.

- Data should be updated as inaccuracies are discovered.

Subject Access Requests

All individuals who are the subject of personal data held by us are entitled to:

- Ask what information we hold about them and why.
- Ask how to gain access to it and to have inaccurate data corrected or erased.
- Be informed as to how to keep it up to date.
- Be informed how we are meeting our data protection obligations.

If an individual contacts us requesting this information, this is called a subject access request.

Subject access requests from individuals should be made by e-mail or in writing and addressed to the Data Protection Lead. We can supply a standard request form, although individuals do not have to use this.

The Data Protection Lead will aim to provide the relevant data within 14 days and in any event within 1 month.

The Data Protection Lead will always verify the identity of anyone making a subject access request before handing over any information.

Disclosing data for other reasons

In certain circumstances, the GDPR allows personal data to be disclosed to local authorities, law enforcement and statutory agencies without the consent of the data subject. Under these circumstances, we will disclose the necessary data. However, the Data Protection Lead will ensure the request is legitimate, seeking assistance and approval from the Clerk of Session where necessary.

Service Users will be made aware in most circumstances how and with whom their information will be shared. There are circumstances where the law allows us to disclose data (including sensitive data) without the data subject's consent. These include carrying out a legal duty and protecting vital interests of a member or other individual.

We regard the lawful and correct treatment of personal information as very important to successful working, and to maintaining the confidence of those with whom we deal.

Providing information to Data Subjects

We aim to ensure that individuals are aware that their data is being processed and that they understand:

- How the data is being used.
- How to exercise their rights in relation to same.

To these ends, we will issue privacy notices as appropriate to members and those affiliated with our congregation, employees, customers, suppliers, business contacts, and other individuals we have a relationship with or may need to contact, setting out how data relating to an individual is used by us, how to exercise their rights in relation to same including options available and how to raise a complaint.

A version of this statement will also be available on our website.

Security Breach Management

We have an incident response procedure in place so that any breach of data protection can be acted upon immediately. The breach will be internally investigated with appropriate remedial taken and where required, notification will further be made within 72 hours to the Information Commissioner's Office and those affected providing details of the nature of the breach, likely consequences and mitigations being taken to address same.

Review

This policy and related data protection procedures will be reviewed on an annual basis by the Data Protection Lead to reflect best practice in data management, security and control and to ensure compliance with GDPR.

Signed: Position: Date: Review Date:

Glossary of Key Terms

Personal Data
Any information relating to an identifiable natural person 'data subject'; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as: a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Basic Contact Data

Names, addresses, email addresses and phone numbers, which is likely to be widely shared within the church community by its members, and without the involvement of Fitzroy staff.

Sensitive Personal Data
Any data relating to: racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health conditions, sexual life or sexual orientation, genetic data and/or biometric data. We process this data in respect of our both our service users and our staff.

A Data Subject
An individual who is the subject of personal data, not including deceased individuals or individuals who cannot be identified or distinguished from others – e.g. statistics.

Data Processing
The operation or set of operations performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Data Protection Lead
Is the person from time to time that has agreed with us to take on responsibility for ensuring that we abide by our data protection policies, to act as a point of contact for anyone with concerns as to how their information is being handled and generally to undertake the responsibilities as detailed in this policy.

Data Controller
The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of processing the data.

Data Processor
A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Pseudonymisation

Pseudonymisation takes the most identifying fields within a database and replaces them with artificial identifiers, or pseudonyms. For example a name is replaced with a unique number. The purpose is to render the data record less identifying and therefore reduce concerns with data sharing and data retention

Encryption

Encryption is a mathematical function using a secret value — the key — which encodes data so that only users with access to that key can read the information. In many cases encryption can provide an appropriate safeguard against the unauthorised or unlawful processing of personal data, especially in cases where it is not possible to implement alternative measures.