Faughanvale Presbyterian Church

DATA PROTECTION POLICY

Introduction

We, Faughanvale 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.

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

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.
- 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 should also be considered:

- Data should be protected by strong passwords that are changed regularly and 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.
- Data should never be saved directly to laptops or other mobile devices like tablets or smart phones. In exceptional cases where it is necessary to temporarily save data to a laptop, pen drive, or other mobile device then

equivalent measures such as password protection, encryption etc. as appropriate should be adopted.

- 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, individuals 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/Data Protection Commissioner (as is applicable) 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: Trevor Evans Position: Data protection Lead Date: 9 February 2022   Review Date: February 2023

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.

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.

DATA RETENTION POLICY

Faughanvale Presbyterian Church

(Reviewed February 2022)

INTRODUCTION

The law does not specify minimum or maximum periods for retaining personal data but rather gives the general principle:

'Personal data processed for any purpose or purposes shall not be kept for longer than necessary for that purpose or purposes.'

In practice this means that we need to:

- review the length of time we keep personal data
- consider the purposes for which we hold the information, as a guide to determining whether, and for how long, we retain it
- securely delete or destroy information that is no longer needed for those purposes; and
- update, archive or securely delete or destroy information if it goes out of date

PURPOSE

This Policy is to be read in conjunction with the Data Protection Policy and is designed to outline the time period for which we, Faughanvale Presbyterian Church, will hold certain types of data. As noted in the Data Protection Policy, it is a legal requirement that personal data is not be kept for longer than is necessary.

We are required by law to keep certain records, usually for a specific amount of time. The accidental or intentional destruction of these records during their specified retention periods could result in the following consequences for the congregation including:

- Fines and penalties.
- Civil action.
- Criminal action.
- Reputational damage.

Therefore, we prohibit the inappropriate destruction of any records, files, documents, samples, and other forms of information. This Policy is part of a congregation-wide system for the review, retention, and destruction of records we create or receive in connection with the activities we conduct.

TYPES OF DOCUMENTS

This Policy explains the differences among records, disposable information, and confidential information belonging to others.

Records. A record is any type of information created, received, or transmitted in the transaction of our activities, regardless of physical format. Examples of where the various types of information are located include:

- Appointment books and calendars.
- Audio and video recordings.
- Computer programs.
- Contracts.
- Electronic files.
- Emails.
- Handwritten notes.
- Invoices.
- Letters and other correspondence.
- Memory in mobile phones, tablets, laptops and any other portable electronic device.
- Online postings.
- Performance reviews.
- Test samples.
- Voicemails.

Therefore, any paper records and electronic files, including any records of donations made online, that are part of any of the categories listed in the Records Retention Schedule contained in the Appendix to this Policy, are be retained for the amount of time indicated in the Records Retention Schedule or such other time as is necessary in the circumstances. A record must not be retained beyond the period indicated in the Record Retention Schedule**, unless a valid reason (or there is potential for litigation or other special situation) or specific legal requirement calls for its continued retention**. If you are unsure whether to retain a certain record, contact the Data Protection Lead.

Disposable Information. Disposable information consists of data that may be discarded or deleted at the discretion of the user once it has served its temporary useful purpose and/or data that may be safely destroyed because it is not a record as defined by this Policy. Examples may include:

- Duplicates of originals that have not been annotated.
- Preliminary drafts of letters, memoranda, reports, worksheets, and informal notes that do not represent significant steps or decisions in the preparation of an official record.
- Books, periodicals, manuals, training binders, and other printed materials obtained from sources outside of the Organisation and retained primarily for reference purposes.
- Spam and junk mail.

Confidential Information Belonging to Others. Any confidential information that an employee may have obtained from a source outside of the congregation, such as a previous employer, must not, so long as such information remains confidential, be disclosed to or used by us. Unsolicited confidential information submitted to us should be refused, returned to the sender where possible, and deleted, if received via the internet.

MANDATORY COMPLIANCE

Responsibility of All Employees and Volunteers. We strive to comply with the laws, rules, and regulations that govern compliance and with recognised compliance practices. All congregation employees and volunteers must comply with this Policy and the Records Retention Schedule. Failure to do so may subject the congregation, its employees, contract staff and volunteers to serious civil and/or criminal liability. An employee's failure to comply with this Policy may result in disciplinary sanctions, including suspension or termination.

Reporting Policy Violations. We are committed to enforcing this Policy as it applies to all forms of records. The effectiveness of our efforts, however, depends largely on employees and volunteers. If you feel that you or someone else may have violated this Policy, you should report the incident immediately to the Data Protection Lead.

STORAGEE AND DESTRUCTION OF RECORDS

Storage. Our records must be stored in a safe, secure, and accessible manner. Any documents and financial files that are essential to our purpose and activities during an emergency must be duplicated and/or backed up at regular intervals.

Destruction. The Data Protection Lead is responsible for the continuing process of identifying the records that have met their required retention period and supervising their destruction. The destruction of confidential, financial, and personnel-related

records must be conducted by shredding if possible. Non-confidential records may be destroyed by recycling. The destruction of electronic records must be undertaken with appropriate expert advice and oversight.

The destruction of records must stop immediately upon notification that litigation to which the said documents would be relevant is likely to occur.

INTERNAL REVIEW

The Data Protection Lead will periodically review this Policy and its procedures to ensure that the congregation is in full compliance with relevant new or amended regulations.

Presbyterian
CHURCH IN IRELAND

APPENDIX – RECORDS RETENTION SCHEDULE

TYPE OF RECORD	RECOMMENDED RETENTION PERIOD	BASIS
Property and Equipment		
Title deeds and other documents of title	Indefinitely	Recommended
Service contracts and certificates, warranty documents	Retain for 3 years after expiry	Recommended
Financial		
Annual examined/audited	Indefinitely	Recommended
All financial records in support of examined/audited accounts	Current year + 6 years history	Legal requirement
Gift Aid declarations	Keep as long as they are valid + 6	Legal requirement
Capital expenditure, guarantees, invoices, receipts etc.	Last action + 5 years dependant on the nature of the expenditure and the length of the guarantee. After that review for possible retention or destroy	Recommended
Insurance policies – employers' liability	Current year + 40 years	Recommended
Insurance policies – other than employers' liability	Current year + 6 years	Recommended
Church Copyright Licence information	Current year + 6 years	Recommended
Church Services		
Baptism, Marriage records	Permanent	Recommended
Orders of Service	2 years	Recommended
General Church Administration		
Minutes of Session and General Committee	Indefinitely	Recommended
Electoral Rolls	Retain last complete review then destroy previous roll.	Recommended
Voicemail	Until transcribed or acted upon + 1	Recommended
Application and Consent forms for Events and Organisations		
In respect of children: for events such as Holiday Bible Club, Church weekends OR forms to register for organisations such as BB, GB, Youth Club, etc.	For membership records and registration forms - up to 6 years after the event or the child has left the organisation	In accordance with Taking Care guidance

In respect of adult leadership	In the case of an event or organisation pertaining to children – up to 6 years after they have left their position. Otherwise: Current year +1	In accordance with Taking Care guidance / otherwise as recommended.
In respect of adult events or organisations	For events – up to 1 year For organisations – up to 1 year	Recommended

TYPE OF RECORD	RECOMMENDED RETENTION PERIOD	BASIS
Recruitment and Employment		
Application forms, CVs and other records from unsuccessful	One year after applicant is informed of outcome.	Recommended
Application forms, CVs and other records from successful applicants.	3 years from the date of recruitment.	Recommended
Appraisal records, performance reviews etc.	5 years after the employee has left the Organisation.	Recommended
Details of injuries or accident reports	5 years from the date of the incident.	Recommended
Employment records, details of terms and conditions and	5 years after the employee has left the Organisation.	Recommended
Health and Safety Assessments	40 years from the date of the assessment.	Recommended
Pay and benefits information	5 years after the employee has left the Organisation.	Recommended
Training records	5 years after the employee has left the Organisation.	Recommended
Pastoral Care, Safeguarding and Health and Safety		
Pastoral visitation notes and records	3 years after the member has left the congregation	Recommended
Accident reporting sheets or book – if relating to adults	Date of incident + 15 years	Recommended - in case of need to review and also re potential
Accident reporting sheets or book – if relating to children	Date of incident + 15 years or until the child turns 21 (whichever is the later)	Recommended - in case of need to review and also re potential
Records of other safeguarding adult or child protection incidents either within the parish or within a family/ by an individual where the Parish was the reporting body or involved in care or monitoring plans.	50 years after the conclusion of the matter	Recommended

Records of any children's activities and related general safety risk assessments. Any communication from parents or other parties in relation to the above.	Current year + 20 years	Recommended

SUBJECT ACCESS POLICY

Faughanvale Presbyterian Church

(Reviewed February 2022)

Faughanvale Presbyterian Church is committed to complying with data protection legislation. Under the legislation individuals can access the personal data that an organisation holds about them. The individual is entitled to be:

- told whether any personal data is being processed;
- given a description of the personal data, the reasons it is being processed, and whether it will be given to any other organisations or people;
- given a copy of the information comprising the data; and given details of the source of the data (where this is available).

Individuals also have a number of other rights which we must comply with including the rights to:

- rectify personal data which is incomplete or inaccurate and if necessary inform third parties that this has been done.
- be informed of how personal data is processed in a transparent manner.
- have their personal data deleted unless if there is a valid reason not to do this.
- restrict processing of personal data for certain purposes.
- object to the processing of personal data in a certain way.
- have data transferred to a third party so it can be reused (data portability).
- have a say in whether automated decisions are being made using the personal data and insist on an actual person intervening.

Children also have the same rights as adults in this regard. In the case of young children, these rights are usually exercised through their parents. However, if we are satisfied that the child in question is mature enough to understand their rights, then we will respond to the child directly. We will encourage the child to discuss the matter with his or her parents. When responding to a request from a child, we will take particular care to ensure that the response is given in a way which the child can understand.

There is no set fashion in which the individual has to make these requests and if such a request is made we will always seek advice from the Data Protection Lead.

Faughanvale Presbyterian Church will aim to provide the relevant data within 14 days and in any event within 1 month of receipt of the request. If the nature of the request is particularly complex, then we may need an extension of time to comply with the request. We will inform the individual if this is the case and the reasons why this is necessary. Also, we may need to ask for information that we reasonably need to find the personal data covered by the request.

Previously, we had the right to charge a fee for these requests. Now this is no longer usually permitted. Individuals will not have to pay a fee to access their personal information (or to exercise any of the other rights). However, we may charge a reasonable fee if their request for access is clearly unfounded or excessive. Alternatively, we may refuse to

comply with the request in such circumstances.

Appendix A contains a precedent Subject Access Request form. We suggest (but do not insist) that individuals complete this form so that we can process their request more easily. **We must always ensure that we know who is making the request and what they are requesting before providing any information, otherwise we may be in breach of data protection law**.

Appendix A

Data Subject Access Request Form

How to apply for personal held about you by Faughanvale Presbyterian Church

Under data protection law you can ask for copies of paper and computer records that an organisation holds, shares or uses about you. In order to deal with your request we can ask for proof of identity and enough information to enable us to locate the personal data that you request. Please complete this form and return it to us with proof of your identity to [Insert appropriate correspondence address of Presbytery or Congregation]. We will acknowledge safe receipt and respond within one month.

Part 1: Person that the request relates to (the Data Subject)

Title: Mr / Mrs / Miss / Ms / Other

Surname:

Forenames:

Any other names that you are known by that may assist in the search:

Address:

Postcode:

Telephone:

E-mail:

Date of birth:

If you are an employee or former employee of Faughanvale Presbyterian Church please provide your staff number:

Part 2: Proof of identity

To help us establish your identity your application must be accompanied by **two** pieces of identification that between them clearly show your name, date of birth and current address.

Please enclose a photocopy of **one** of the following as proof of identity:

- passport,
- photocard driving licence,
- birth or adoption certificate

and a copy of a bank statement or utility bill dated within the last three months.

This is to ensure that we are only sending information to the data subject and not to a third party. If none of these are available, please contact [Insert contact details for Data Protection Lead] for advice on other acceptable forms of identification.

Part 3: Information requested

To help us to deal with your request quickly and efficiently please provide as much detail as possible about the information you want. Please include time frames, dates, names or types of documents, any file or incident reference and any other information that may enable us to locate your data, for example, for e-mails, the names of senders and recipients and approximate dates.

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Please continue on a separate sheet of paper, if necessary.

I, _____, confirm that the information provided on this form is correct and that I am the data subject whose name appears on this form. I understand that Faughanvale Presbyterian Church must confirm proof of identity and that it may be necessary to contact me again for further information to locate the personal data I want. I also understand that my request will not be valid until all of the information requested is received by Faughanvale Presbyterian Church.

Signature: _____ **Date**: _____

Faughanvale Presbyterian Church

DATA BREACH POLICY

Faughanvale Presbyterian Church is committed to complying with data protection legislation and will take appropriate technical and organisational measures against unauthorised or unlawful processing and against accidental loss or destruction of or damage to personal data:

If, despite the technical and organisational measures that we have put in place to protect personal data, a data security breach occurs, it is important to manage and respond to it effectively. A data security breach covers more than the simple misappropriation of data and may occur through incidents, such as:

- Loss or theft of data or equipment.
- People gaining inappropriate access.
- A deliberate attack on systems.
- Equipment failure.
- Human error.
- Catastrophic events, (for example, fire or flood).
- Malicious acts such as hacking, viruses or deception.

If such an incident occurs, it is imperative that we act immediately. The following steps will be taken:

A. The Data Protection Lead, the Minister, and the Clerk of Session (the "Security Breach Team") will be informed immediately.
B. An investigation will be undertaken to determine:
   i. The nature and cause of the breach; and
   ii. The extent and nature of harm that has or could arise from the breach.

If there is no risk of harm, then no further action is required (for example if papers are temporarily lost due to being incorrectly filed but are then promptly found and no disclosure has occurred or harm likely to occur, then no further action is required).

If there is considered to be a risk of harm, then the following steps must be undertaken:

1. Information Commissioner's Office must be informed within 72 hours. If we do not have all of the information by then a report should be made within the 72 hours on the basis of what is known while investigations continue.
2. If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, we must also inform those individuals

without undue delay. Examples of this could include where there is a high risk of reputational damage, embarrassment or putting the individual's property at risk.

3. If necessary, a number of third parties will be informed which may include:
   a. PCI
   b. the Organisation's insurers;
   c. the police;
4. Following notification, we will continue to liaise and cooperate with ICO.
5. All reasonable steps to mitigate the damage arising from the breach will be taken.

A record of all data protection breaches will be maintained regardless of whether or not notification is required. Detailed records of the investigation will be maintained as well.

Following a breach, if necessary, it must be considered whether any of the below is required:

- Disciplinary action;
- Legal action;
- Internal review of security procedures.

NOTE:

A number of precedent documents have been prepared which may be of use. Please note that, where possible, legal advice should always be sought in the case of a data breach prior to sending these correspondences.

Appendix A contains a precedent letter which can be sent to a data subject on discovery of a data breach which is likely to result in a high risk of harm to the data subject and or the presbytery/congregation (could be significant reputational damage or embarrassment or putting person(s) or property at risk).

Appendix B contains a precedent letter informing the ICO upon a data breach for which there is a risk of harm.

Appendix A

[On headed notepaper of Data Controller i.e. Congregation]
[ADDRESSEE]
[ADDRESS LINE 1]
[ADDRESS LINE 2]
[POSTCODE]
[DATE]

Reference: PERSONAL DATA BREACH NOTIFICATION

We are sorry to inform you of a breach of security that has resulted in the [loss OR unauthorised disclosure OR destruction OR corruption – DELETE AS APPROPRIATE] of your personal data.

The breach was discovered on [DATE] and is likely to have taken place on [DATE].

As a result of our investigation of the breach, we have concluded that:

The breach affects the following types of information:
[TYPES OF INFORMATION. FOR EXAMPLE, FINANCIAL, SENSITIVE PERSONAL DATA].
The information has been [accidentally or unlawfully destroyed OR lost OR altered OR disclosed without authorisation OR accessed by [[Name or Description of Organisation] OR an unauthorised person]]. [DELETE AS APPROPRIATE]

The breach occurred under the following circumstances and for the following reasons:
[CIRCUMSTANCES].
[REASONS].

We have taken the following steps to mitigate any adverse effects of the breach:
[MEASURES].

We recommend that you take the following measures to mitigate possible adverse effects of the breach:
[MEASURES].

[We informed the Information Commissioner's Office/Data Protection Commissioner's Office [DELETE AS APPROPRIATE] of the breach on [DATE]].

You can obtain more information about the breach from any of the following contact points:
[NAME OF CONGREGATION].
[CONGREGATION POSTAL ADDRESS].
[CONGREGATION E-MAIL ADDRESS].
[CONGREGATION TELEPHONE NUMBER OR HELPLINE NUMBER].

[CONGREGATION WEBSITE ADDRESS].

We apologise for any inconvenience this breach may cause you.
Yours sincerely,

.....

[NAME OF SENDER – printed under signature]

For and on behalf of [Insert name of Congregation]

Appendix B

[On headed notepaper of Data Controller i.e. Congregation]
[ADDRESSEE]
[ADDRESS LINE 1]
[ADDRESS LINE 2]
[POSTCODE]
[DATE]

Reference: PERSONAL DATA BREACH NOTIFICATION

I am writing to notify you of a [breach of security that resulted in the [loss OR unauthorised disclosure OR corruption OR destruction– DELETE AS APPROPRIATE] of personal data. We consider this to be a serious data security breach.

[We have investigated the breach by [DETAILS OF HOW THE BREACH WAS INVESTIGATED] and provide you with the following information.]
[We are in the process of investigating the breach and we anticipate completing our investigation by [DATE], when we will provide you with the further information required. We can provide you with the following details at this stage [PROVIDE ALL THAT IS KNOWN].]

[Insert name of Congregation] is the data controller in respect of the data breach.

The breach was discovered on [DATE] and is likely to have taken place on [DATE].

The information has been [accidentally or unlawfully destroyed OR lost OR altered OR disclosed without authorisation OR accessed by [[Name or Description of Organisation] OR an unauthorised person]]. [DELETE AS APPROPRIATE]

The breach occurred under the following circumstances and for the following reasons:
[CIRCUMSTANCES].
[REASONS].

<u>Measures in place</u>

We had the following measures in place to prevent an incident of this nature occurring:
[MEASURES].

We enclose extracts of policies and procedures that we consider to be relevant to the breach:
[EXTRACTS OF POLICES AND PROCEDURES AND DATE IMPLEMENTED].

The following were in existence at the time of the breach:
[LIST OF POLICIES AND PROCEDURES AND DATE IMPLEMENTED].

Personal data placed at risk

The breach affects the following types of information:
[TYPES OF INFORMATION, FOR EXAMPLE, FINANCIAL OR SENSITIVE PERSONAL DATA AND DETAILS OF THE EXTENT].

It is likely that the breach affects around [NUMBER] data subjects.
[We have [not] informed the individuals affected by the breach because [REASONS FOR DECISION] OR The individuals are [aware OR unaware] that the incident has occurred].

The breach may have the following consequences and adverse effects on the affected data subjects:
[CONSEQUENCES].
[ADVERSE EFFECTS].
We have [received [NUMBER] of complaints OR not received any complaints] from the affected individuals.

Containment and recovery

We [have taken OR propose to take] the following measures to address the breach and to minimise and mitigate its effects on the affected individuals:
[MEASURES].

The information has [not] been recovered [and the details are as follows:
[DETAILS OF HOW AND WHEN IT WAS RECOVERED]
We have also taken the following steps to prevent future occurrences of the breach:
[REMEDIAL ACTION TAKEN].

[The facts surrounding the breach, the effects of that breach and the remedial action taken have been recorded in a data breach inventory maintained by the [Presbytery OR Congregation]

Training and guidance

We provide staff/volunteers/leaders with training on the requirements of data protection legislation [and the details are as follows:

[DETAILS OR EXTRACTS FROM TRAINING RELEVANT TO THIS DATA BREACH]

We provide detailed guidance to staff/volunteers/leaders on the handling of personal data in relation to this incident [and the details are as follows:

[DETAILS OR EXTRACTS OF ANY DETAILED GUIDANCE GIVEN TO STAFF/ VOLUNTEERS/LEADERS ON THE HANDLING OF PERSONAL DATA IN RELATION TO THE DATA BREACH]
We confirm that training on the requirements under the data protection legislation is mandatory for all staff/volunteers/leaders [and that the staff members involved in this incident received training on [DATE]].

Previous contact with the Information Commissioner's Office

We have [not] reported [any] previous incidents to you within the last two years [and the details and reference numbers are as follows:
[DETAILS OF INCIDENT(S)].
[DATE(S) ON WHICH THE INCIDENT(S) WAS [WERE] REPORTED].
[THE INFORMATION COMMISSIONER'S REFERENCE NUMBER(S), IF KNOWN].

Miscellaneous

We have [not] notified any other (overseas) data protection authorities about this data breach [and the details are as follows:
[DETAILS OF DATA PROTECTION AUTHORITIES].

We have [not] informed the police about this data breach [and the details are as follows:
[DETAILS AND NAME OF POLICE FORCE].

We have [not] informed any other regulatory bodies about this data breach [and the details are as follows:
[NAME AND DETAILS OF REGULATORY BODIES].

There has [not] been [any] media coverage [and the details are as follows:
[DETAILS OF MEDIA COVERAGE].

In addition, we consider that the following information would be of interest to you:
[DETAILS].

Contact details:
If you require any further information about the breach, please contact:
[CONTACT NAME]
[INSERT NAME OF CONGREGATION]
[POSTAL ADDRESS]
[TELEPHONE NUMBER]
[E-MAIL ADDRESS]
[WEBSITE ADDRESS].

Yours faithfully,

.....
[NAME OF SENDER]
For and on behalf of [Insert name of Congregation]

Faughanvale Presbyterian Church

DATA PRIVACY NOTICE

1. Your personal data – what is it?
Personal data relates to a living individual who can be identified from that data. Identification can be by the information alone or in conjunction with any other information in the data controller's possession or likely to come into such possession. The processing of personal data is governed by the General Data Protection Regulation (the "GDPR").

2. Who are we?
We, Faughanvale Presbyterian Church, are the data controller (contact details below). This means that we decide how your personal data is processed and for what purposes.

3. How do we process your personal data?
We comply with our obligations under the "GDPR" by keeping personal data up to date; by storing and destroying it securely; by not collecting or retaining excessive amounts of data; by protecting personal data from loss, misuse, unauthorised access and disclosure and by ensuring that appropriate technical measures are in place to protect personal data.

We use your personal data for the following purposes: -

- To enable us to provide a voluntary service (pastoral care) for the benefit of the public in a particular geographical area;
- To administer membership records;
- To fundraise and promote the interests of the charity;
- To manage our employees and volunteers;
- To maintain our own accounts and records (including the processing of gift aid applications);
- To inform you of news, events, activities and services running at or run by us; and
- To share your contact details with the Presbyterian Church in Ireland so they can keep you informed about news and events, activities and services that will be occurring and in which you may be interested.

4. What is the legal basis for processing your personal data?
The legal basis for processing your personal data is dependent upon the data subject (individual) and the purpose of the data processing. For example: the data processing for an employee in terms of what data is collected and how it is further

processed is different from that of a member of our congregation. Legal bases we rely on will primarily consist of one or more of the following:

- Processing is necessary for the purposes of legitimate interests pursued by us or a third party except where such interests are overridden by the interests, rights or freedoms of the data subject. This is where we need to use your data to engage in our normal day to day activities e.g. keeping a record of your name and address on our membership list;
- Processing is carried out by us in our capacity as a not-for-profit body with a religious aim provided: -
    - the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes); and
    - there is no disclosure to a third party without consent.

  An example of this may be where a record of sensitive data may need to be kept by us so that effective pastoral care may be provided to members;
- Explicit consent of the data subject. An example of this would be your consent to joining a mailing list so that we can keep you informed about news, events, activities and services and process your gift aid donations and keep you informed about PCI events;
- Processing is necessary for us to comply with the law. Examples of this could be our legal obligations to maintain certain records so that we may carry out our obligations under employment, social security or social protection law, or a collective agreement; and
- Processing is necessary for us to protect the vital interests of a data subject that cannot physically or legally give consent. An example of this may be for us to run special needs activities.

5. Sharing your personal data

Your personal data will be treated as strictly confidential and will only be shared with other members of the church in order to carry out a service to other church members or for purposes connected with the church. We will not normally share your personal data with any third party and will only share your data with third parties outside of ourselves with your consent.

6. How long do we keep your personal data?

This can vary; we retain members' data while it is still current; gift aid declarations and associated paperwork for up to 6 years after the calendar year to which they relate; and presbytery or congregational registers (baptisms, marriages, funerals) permanently. Where consent has been obtained, for example – for membership of an organisation or to attend a one-off activity, we will normally retain this for one year.

7. Your rights and your personal data

Unless subject to an exemption under the GDPR, you have the following rights with respect to your personal data: -

- The right to request a copy of your personal data which we hold about you;

- The right to request that we correct any personal data if it is found to be inaccurate or out of date;
- The right to request your personal data is erased where it is no longer necessary for us to retain such data;
- The right to withdraw your consent to the processing at any time
- The right to request that the data controller provide the data subject with his/her personal data and where possible, to transmit that data directly to another data controller
- The right, where there is a dispute in relation to the accuracy or processing of your personal data, to request a restriction is placed on further processing;
- The right to object to the processing of personal data.
- The right to lodge a complaint with the Information Commissioner's Office.

8. Further processing

If we wish to use your personal data for a new purpose, not covered by this Data Privacy Notice, then we will provide you with a new notice explaining this new use prior to commencing the processing and setting out the relevant purposes and processing conditions. Where and whenever necessary, we will seek your prior consent to the new processing.

9. Contact Details

To exercise all relevant rights, queries of complaints, please, in the first instance contact the Data Protection Lead, Trevor Evans at evans341@btinternet.com.

You can contact the Information Commissioners Office on 0303 123 1113 or via email https://ico.org.uk/global/contact-us/email/ or at the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire. SK9 5AF