Presbyterian
CHURCH IN IRELAND

SECOND DROMARA PRESBYTERIAN CHURCH

DATA PROTECTION POLICY

1. Introduction

1.1 In Second Dromara Presbyterian Church, we need to gather and use certain information about people. This can include information about members and their families, employees, volunteers, suppliers, service users, users of our facilities, local residents, business contacts, and other people with whom we have a relationship or may need to contact. This policy describes how this information, which constitutes personal data, will be collected, handled and stored to meet data protection standards and to comply with the law.

2. Why this policy exists

2.1 This Data Protection Policy seeks to ensure that we:

- comply with data protection law and follow good practice
- protect the rights of those people with whom we have a relationship or may need to contact
- are open about how we store and process personal data; and
- minimise the potential for a data breach.

3. Data Protection Law

3.1 The General Data Protection Regulation (GDPR) (EU 2016/679) regulates how organisations collect, handle and store personal information. The law applies regardless of whether the data is stored electronically, on paper, or on other materials.

3.2 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 state that personal information shall be:

- processed lawfully, fairly and in a transparent manner in relation to individuals
- 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 is not considered incompatible with the initial 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 data subjects for no longer than is necessary; and
- 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.

4. Policy scope

4.1 This policy applies to the members of the Kirk Session and Congregational Committee as well as employees, post-holders, volunteers, contractors and suppliers and any other people processing personal data on behalf of Second Dromara Presbyterian Church or its associated organisations.

4.2 The policy relates to all personal data that we hold in respect of individuals. This may include, for example:

- names of individuals, postal/email addresses, dates of birth, telephone numbers, National Insurance Numbers
- sensitive personal data such as information in relation to physical or mental health conditions, disability, religious or political beliefs, race, ethnic origin or sexual orientation.

5. Data Protection Risks

5.1 Failure to act in accordance with the provisions of this policy increases the potential for risks associated with collecting, holding and processing personal data to be realised. These include:

- 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 decide which personal data they wish to share with us and how we use data relating to them
- reputational damage – for instance, if personal data was stolen or lost and then used by others.

6. Responsibilities

6.1 Everyone who works for, or with, us, whether in a paid or voluntary capacity, has some responsibility for ensuring personal data is collected, stored and processed appropriately, in line with this policy and the data protection principles set out in paragraph 3.2 above. Failure to comply with the Data Protection Policy and the principles is a serious offence and in the case of employees could result in disciplinary action.

6.2 The following people have key areas of responsibility:

- ultimately the Kirk Session is responsible for ensuring that we meet our legal obligations.
- the Data Protection Lead is responsible for:
  - keeping the Kirk Session and Congregational 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 for, and providing advice to, the Kirk Session, Congregational Committee, employees, leaders and volunteers 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 sensitive data on behalf of Second Dromara church.

7. General Guidelines for Employees and Volunteers

7.1 The only people able to access personal data covered by this policy should be those who need it because of their role within Second Dromara Presbyterian Church (e.g. as a member of the Kirk Session or Congregational Committee, as an employee or as a leader/volunteer within an organisation).

7.2 Every effort must be made to keep all personal data secure, by taking sensible precautions and following the guidelines below:

- where information is stored on computer, strong passwords must be used and changed regularly; they should never be shared with others
- personal data should never be disclosed to unauthorised people, either internally or externally
- personal data should never be shared informally e.g. during a casual conversation or while other people are present who are not covered by this policy
- when receiving telephone enquiries, personal data should only be disclosed if the caller's identity can be checked to make sure that information is only given to a person who is entitled to it
- where there is uncertainty about the caller's identity or it cannot be checked he/she should be asked to put their request in writing.

7.3 Where a member of staff, a leader or a volunteer is uncertain about the validity of a request or what to do in respect of a particular request he/ she should refer

it to the Data Protection Lead and / or the Minister or Clerk of Kirk Session. No-one should feel pressurised into disclosing personal information.

7.4 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 / or disposed of in a secure manner (e.g. shredding).

7.5 Anyone who is unsure about any aspect of data protection should contact the Data Protection Lead (details available at the end of this policy statement).

8. Data Collection

8.1 In accordance with data protection legislation the main legal basis for collecting personal data on our members and those affiliated with us will be that it is necessary for us to hold that data for the purposes of legitimate interests which are not overridden by the interests of the data subject. Sensitive data (and, in particular, data revealing the religious beliefs of the data subject) 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

8.2 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 an individual's consent to process their personal data, particularly if it is outside of normal day-to-day activities or it would involve sharing personal data with a third party. If this is necessary, then the individual's consent will be informed consent.

8.3 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.

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

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

- has received sufficient information on why their personal data is needed and how it will be used

- is made aware what the personal data will be used for and what the consequences are should the individual decide not to give consent to processing;
- where necessary, grants explicit consent, either written or verbal for data to be processed;
- is, as far as reasonably practicable, competent enough to give consent and has given so freely without any duress; and
- 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.

9. Processing in line with Data Subject's Rights

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

- request access to data held about them
- prevent the processing of their data for direct-marketing purposes
- ask to have inaccurate data corrected or erased
- prevent processing that is likely to cause damage or distress to themselves or anyone else.

10. Data Storage

10.1 Regardless of how personal data is collected and held (electronically or in print format) it must be stored safely and securely.

Information held in print format

10.2 When personal data is stored in print format, it should be kept in a locked filing cabinet where unauthorised people cannot access it. All personal data stored on paper should be returned to the appropriate locked drawer or filing cabinet when no longer required and no papers should be unnecessarily left unattended. Paper and printouts must not be not left where unauthorised people could see them, e.g. on a printer or photocopier.

10.3 Print documents containing personal data should be shredded and disposed of in a secure manner when no longer required or when they are out of date.

Information held electronically

10.4 Computers, laptops and mobile phones which hold personal data must be password protected and, where appropriate, have approved security software and a firewall installed.

10.5 Members of Kirk Session and the Congregational Committee, staff and volunteer leaders may use their own electronic devices to retain personal data relevant to the work in which they are engaged. Where this is the case, however it is essential that particular care is taken to ensure that this personal data is protected from unauthorised access, accidental deletion and malicious hacking attempts.

10.6 Security measures must be applied to personal devices, consistent with those that are applied to centrally held equipment and should include the following:

- appropriate security software and firewalls
- personal data must be protected by strong passwords that are changed regularly
- if personal data is stored on removable media (like a CD, DVD, memory stick / flash drive etc.), these should be password protected / encrypted and be stored securely when not being used.
- personal data should be backed up frequently.

11 Data Retention and Secure Destruction

11.1 Personal data will not be retained longer than is 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 the confidential destruction of data when no longer required.

12 Data Use

12.1 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 will adopt the following additional security measures:

- personal data should not be shared informally. In particular, care will be taken when sending personal data by e-mail as this form of communication is <u>not secure</u>
- 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 if an adequate level of protection can be guaranteed.
- consideration will be given to the anonymization of personal data to promote the safe use or sharing of data with other authorised people within the congregation.

Presbyterian
CHURCH IN IRELAND

13. Data Accuracy

13.1 The law requires us to take reasonable steps to ensure personal data is kept accurate and up to date. It is the responsibility of everyone who collects / processes personal data to take reasonable steps to ensure data is kept as accurate and up to date as possible. Data should be updated as soon as inaccuracies are discovered.

13.2 Anyone who wishes to update their personal information should pass that information in a sealed envelope to the Minister, the Clerk of Kirk Session, the Data Protection Lead or the recognised leader of a relevant organisation. The information can also be emailed to the Data Protection Lead who will pass it on to the relevant people.

14. Providing information to Data Subjects

14.1 We aim to ensure that individuals are aware of how their personal data is being processed and that they understand how to exercise their rights in relation to that data.

14.2 We will issue privacy notices as appropriate to members and those affiliated with our congregation, employees, customers, suppliers, business contacts, and other individuals with whom we have a relationship 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 that data; and
- how to raise a complaint.

A Privacy Statement will also be available on our website.

15. Subject Access Requests

15.1 Anyone who is the subject of personal data held by us is 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; and
- be informed how we are meeting our data protection obligations.

15.2 When a person contacts us requesting this information, this is called a Subject Access Request. Subject Access Requests from individuals may be made by e-mail or in writing and should be addressed to the Data Protection Lead. The identity of anyone making a Subject Access Request will be verified before any personal data is released to them.

Presbyterian
CHURCH IN IRELAND

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

16. Disclosing data for other reasons

16.1 We regard the lawful and correct treatment of personal data as very important to successful working and to maintaining the confidence of the people with whom we work. We will seek to ensure that individuals who share their personal data with us are made aware how, and with whom, their information will be shared.

16.2 There are certain circumstances, however, when the law allows us to disclose data (including sensitive personal data) without the individual's consent e.g. to local authorities, law enforcement and statutory agencies. 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 Kirk Session where necessary.

17. Security Breach Management

17.1 An incident response procedure is 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 be made, within 72 hours, to the Information Commissioner's Office as well as to those affected, providing details of the nature of the breach, the likely consequences and mitigations being taken to address identified issues.

18. Review

18.1 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.

19. Data Protection Lead

19.1 The Data Protection Lead person is Irene Burrows. She can be contacted at the following email address:
seconddromaragdpr@btinternet.com

Signed: Kenneth Hann

Position: Minister

Date: 26/9/18

Presbyterian
CHURCH IN IRELAND

Glossary of Key Terms

Personal Data
Any information relating to a living person (a Data Subject) who may be identified, directly or indirectly, by reference to such factors as name, date of birth, national insurance number, postal address, workplace, or email address or to a physical, physiological, genetic, mental, economic, cultural or social characteristic.

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.

Data Subject
A living individual who is the subject of personal data.

Data Processing
The operation or set of operations performed on 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
The person who has agreed to take on responsibility for ensuring that we abide by our data protection policies and to act as a point of contact for anyone with concerns as to how their information is being handled.

Data Controller
The organisation which, alone or jointly with others, determines the purposes and means of processing the data.

Data Processor
A person or organisation which processes personal data on behalf of the Data Controller.