LEGACURRY PRESBYTERIAN CHURCH

DATA PROTECTION GUIDANCE

1. Introduction

The General Data Protection Regulation (EU 2016/679) (GDPR) regulates how we collect, handle, store and dispose of 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.

2. Scope

This guidance describes how personal data must be collected, handled, stored and disposed of in order to comply with data protection law and follow good practice.

It applies to all data that is held relating to identifiable individuals.

The GDPR is underpinned by six important principles and everyone who handles personal data must ensure that it is handled and processed in line with these principles. 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.

3. Key Responsibility Areas

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;

    - Providing advice for the people covered by the data protection policy;

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

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

4. Guidelines - Staff/Volunteer/Leaders

All leaders, staff, and volunteers are required to:

- respect the confidentiality of personal data;

- take all reasonable measures to ensure its security while in their position; and

- return or securely destroy/delete personal data held on the congregation’s behalf when they leave their position.

5. Data Accuracy

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

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; and

- Staff, leaders and volunteers should not create any unnecessary additional data sets.

6. Data Security

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

- The only people able to access data should be those who need it;

- Personal data must not be disclosed to unauthorised people, either internally or externally;

- Personal data should not be shared informally;
- When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts. It must be password protected and encrypted;

- Data should be regularly reviewed and updated if it is found to be out of date.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

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

7. Data Storage

These rules describe how and where data should be safely stored and the security measures. 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 put away securely;

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

- Data printouts should be shredded/disposed of securely when no longer required;

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

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

- Data should only be uploaded to the approved cloud computing service. This service is fully compliant with the GDPR legislation. If there is a need to store data on another cloud provider you must ensure that the service provider is fully compliant with the GDPR legislation and receive permission from the data protection officer.

8. Data Retention and Secure Destruction

Personal data must not be retained longer than necessary, in relation to the purpose for which such data is processed. Please refer to the Data Retention Policy for retention/disposal details.

9. 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; and

- 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 which will be dealt with by the Data Protection Lead who will aim to provide the relevant data within 14 days and in any event within 1 month.

10. Security Breach Management

If a breach occurs, it should be reported immediately to the Data Protection Lead who will be responsible for the investigation and reporting procedure.