## GDPR guidance for the Kirk Session

**Introduction**

GDPR became law on 25 May 2018. The documents below explain our responsibilities towards our church members and adherents who have entrusted their personal data to us.

**General points**

1. Members and adherents give their personal data such as names addresses to the church as an organisation and that data must be used only for purposes which we clearly define and must be disclosed only to those who carry out those processes. The data is not given to all the members of our church.
2. We need to be clear about the circumstances when a data breach has occurred. Most breaches occur by sending personal data by email post of fax to the wrong person. See pages 14 and 15 of the “General Guidance for congregations” below and at <http://www.churchofscotland.org.uk/resources/law_circulars#data_protection> see “Breach Notification Form” and “Data Security Breach Management for Presbyteries”.
3. All personal data that the church holds must be kept securely. If held electronically, it should be encrypted and password protected. Data should only be shared with those who need to have the data. Personal data includes data such as membership data, rotas, financial and employment data.
4. Be aware that someone could request access to the data we hold about them. We need to contact Presbytery in the first instance.
5. We all need to understand the Privacy Notice, Data Protection Policy, Information Security Policy and Data Retention Policy.
6. We should control the use of removable media by ensuring that personal data on such media is kept securely on media which is church property and used only for the purpose intended. We should avoid attaching memory sticks to church IT property.
7. When emailing groups of members, use “bcc” rather than “to” to protect the identity of individuals. Avoid including personal data in emails as much as possible as email messages are inherently unsecure unless encrypted.
8. When group photographs are taken, people should be warned beforehand that a photo is to be taken and will be published. Individual consent is not required.

**Training materials**

Webinar guide to GDPR: http://www.churchofscotland.org.uk/resources/law\_circulars
 section: Data Protection – GDPR Resources

Brief Guide for congregations: <http://www.churchofscotland.org.uk/__data/assets/pdf_file/0003/50943/Brief_Guide_to_congregational_Resources.pdf>

General Guidance for congregations: <http://www.churchofscotland.org.uk/__data/assets/pdf_file/0003/49251/General_Guidance_for_Congregations.pdf>

Hints and Tips: <https://urc.org.uk/images/Human-Resources/GDPR/Hints_and_tips.pdf>

**Introduction to GDPR compliance**

The starting point is to create a data model and audit. The data model should all the significant processing that we do and shows the data coming in and going out of those processes. It defines the data into component parts such as name and address. The data audit looks a each set of data components flowing into and out of each process and documents why the data is held and what it is used for, who holds the data and who can access it, what security controls are in place, how long the data is kept for, is the data updated, is it disclosed and it is covered by our Privacy Notice?

Next, we document what data do we hold, where it come from, who we share it with and what we do with it. We then need to remember that our data falls into the category of “special category data” because it relates to religious beliefs by implication because we are a church. We can only process such data if we have consent or processing is carried out in the course of its **legitimate activities** with **appropriate safeguards** by a foundation, association or any other not-for-profit body with a political, philosophical, **religious** or trade union aim and on condition that the processing relates solely to the **members or to former members of the body or to persons who have regular contact with it in connection with its purposes** and that the **personal data are not disclosed outside that body** **without the consent** of the data subjects;”.

We now decide on the lawful basis for each process in turn. The Church of Scotland has advised us to use “legitimate interests” as our lawful basis wherever possible. Legitimate interests means that we must undertake a three part test to consider whether the way that we use the personal data entrusted to us by our congregation is a) for a specific purpose, b) necessary to fulfil that purpose and c) balances the need for us to carry out the processing against the rights of the individual. A legitimate interest assessment is done for each process and covers all three tests. The alternative to legitimate interests is consent. This needs the agreement of each member or adherent and it must clearly specify exactly what processing the person is giving us their consent to carry out. Consent also needs to be renewed, possibly every 5 years. Most of our processing should therefore be done on the basis of legitimate interests. When we use legitimate interests as our lawful basis, we as a church need to ensure that the rights of our members and adherents are being considered when we process their data. Members and adherents can still opt out of such processing. When members and adherents give their consent, they are explicitly exercising their right to opt in to our processing.

However, there are processes that we carry out that cannot be done on the basis of legitimate interests. For example, the publishing of a person’s photograph in the Link or displaying the phone number of a person in the order of service requires consent. Therefore 4 consent forms have been created to capture the consent of members and adherents. Our members and adherents are under no obligation to complete these forms and if they do not do so, we must respect their wishes and take care when including personal data in orders or service, the Link, publishing data on our website or passing information out-with the church.

All our documents should be reviewed once a year to ensure compliance and to make any necessary amendments.

### Explanation of church GDPR documents (shown in bold)

The documents are based on information taken from the Information Commissioner’s Office (ICO) website:-

Checklists for data controllers, information security and records management (see document **checklists**):

<https://ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/>

The links down the left hand side of the following pages give detailed explanations of the various aspects of the regulations:

<https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/>

#### Policies and Consent forms publicly available

**Consent forms 1-4** – these are needed because consent is necessary for collecting certain types of data

**Privacy Notice** – this is a public document which describes what data we hold and why we do so.

**Data Protection Policy** – this is a public document which provides an overview of the responsibilities required for GDPR compliance – this is from the C of S website

**Data Retention Policy** – how long to keep certain documents – this is from the C of S website

#### Policies for internal use only

**Information Security Policy** – this covers physical, computer and network security

**Records Management Policy** – a reminder of the need to consider business continuity in the event of a disaster

#### Documents describing our data

**Data Model and Audit** – this is the starting point and describes the flow of personal information into and out of the church. This needs to be updated if we engage in new processing.

**Data controller documentation 1** – this describes all our processes and suggested justification for lawful bases chosen for each one. It includes legitimate interests assessments. Note that the lawful bases should not be changed.

#### Documents based on the ICO’s checklists

**Data controller documentation** **2** – this is a description of an individual’s rights. Note however that a subject access request should be referred the Presbytery in the first instance

**Data controller documentation 3** – this is needed to meet data protection criteria – how data is collected eg lawfully, fairly etc

**Data controller documentation 4** – this is needed to meet information security criteria – how data is kept secure – physically and electronically

**Data Protection Principles** – this describes the 6 principles a) to f) and provides checklists to ensure compliance

**Information Security documentation** – provides a checklist and a reminder of our legal obligation to carry out testing of the security of our systems

#### Documents describing our risks and recurring action points

**Information Risk Assessment** – these are the risks which must be reviewed periodically by the KS to ensure that we are taking adequate steps to mitigate the risks to the church

**Schedule of tasks** –periodic tasks to be completed to ensure the integrity of our systems and premises are maintained