## GDPR guidance for staff and members with access to church data

**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.

**Specific guidance**

1. Please read though the “Training materials” and all the ”Policies and Consent forms publicly available” at least once.
2. The Church of Scotland has suggested that everyone with responsibility for personal data in our church should watch the webinar (first item in training materials below) once a year to refresh their knowledge of GDPR. The data protection officer is required to keep a log of those who have completed the webinar each year.

**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>

#### 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