

THE GDPR – 10 PREPARATORY STEPS FOR CONGREGATIONAL CHARITY TRUSTEES TO TAKE NOW

1. In general, ensure that all those who “process” (collect, hold, use, etc.) personal information (data) on behalf of the congregation are aware of the principles of the GDPR. A guidance note is available on the Free Church website.
2. Carry out a review of the categories of personal information processed by the congregation (called a “data audit” – a template form for this is available on the website for use). Check where the information came from, and who it is shared with.
3. For each category of personal information held, decide which lawful bases you are relying on for processing this information. Remember that most personal information processed by congregations will come under the “special categories” of personal data, and that for such data you must identify 2 legal bases for processing – one from the general bases and one from the additional bases for special categories of personal data. Document this as evidence of compliance.
4. Prepare and adopt a Privacy Notice for the congregation. A template is available on the website.
5. Review whether consent is required for any personal information already held and obtain consents where appropriate. Retain consents as evidence of compliance. Several template forms are available on the website. **Remember that more than one consent form may be required from the same person for separate categories of data processing.**
6. Ensure that you are aware of each of the rights of individuals under the GDPR, as referred to in the guidance note.
7. Review data relating to children. Consent may not always be the most appropriate legal basis for processing, but, where it is, ensure that it has been appropriately obtained.
8. Review security, especially around access and the use of hard copy and electronic records.
9. Ensure that you have processes or systems in place to enable you to comply with any possible subject access request within 30 days of receipt.
10. Ensure that you have processes or systems in place to detect, report and investigate any personal data breach.