GDPR Checklist guidance questions

CHECK 1

Review the personal information of the Local Church, Circuit or District holds (known as Data Mapping)
This can seem a daunting task at first. TMCP have provided a template to record all the data lists as a table in Word or Excel.
There is a simple form (Data Mapping – Individual record) which can be used to record each type of documents/lists.

- Do you have an up-to-date record of what personal information is held by each of the people who are entitled to and need to hold data, as a consequence of the job that they do in the church or circuit? (e.g. treasurer, pastoral visitors, Sunday School or Youth leaders)?
- Are you satisfied that they only keep the minimum of personal information that they need to do their job?
- Do you know how they keep that information? (On a computer, manual records?)
- Do you know how they keep that information secure? (Computer passworded files, computer backups, manual records in a safe place?) Note that the level of security necessary does depend on how "personal" the Information that is being held is.
- Do you have a "handover" procedure for when one person stops doing a job and it passes to someone else?

CHECK 2

Conduct a "Data Cleansing" exercise to destroy any information that is no longer required.

- Have you checked that all the data being held has been kept up to date?
- Are you satisfied that, when a "handover" has taken place, that the person ceasing to do the job has deleted or destroyed all the relevant records?
- Are records being cleansed after the recommended retention period (such as financial records after 7 years)?

CHECK 3

Review the Managing Trustees' Privacy Notice

- The Managing Trustees' Privacy Notice is provided by TMCP. A copy should be displayed in each church. Is the copy that you have displayed the latest one?
- Do any directories or any other lists that you publish for your members have the detail of where people can find the Privacy Notice (either online or in the church)?

CHECK 4

Ensure your contact information is correct

- Is the information that is being held, by all that are holding it, being kept up to date (addresses, phone numbers, email addresses etc.)?
- Do you keep a record of when it was last checked?

CHECK 5

Review & Renew Consents

- The two most common reasons where consent is required are:
    - Sharing contact details in a directory (or other document) where there information will be shared with third parties (eg where the directory is available to read in church foyers)
    - Publicising details about members or church activities including personal information **publicly** on church websites, social media pages or in newsletters.
- For those situations where you have asked for, and received, consent (consent can be given verbally as well

as written, depending on the circumstances)
    - have you kept a record of how and when the consent was given
    - have you renewed that consent?
- Is your Consents Recording up to date?

CHECK 6

Review the "Processor Record" of the Local Church, Circuit or District

- Only the parts in white need to be completed. The rest is held by TMCP as the Data Controllers.
- The Processor Record shows where the various records are held.
    - 10. Consents Record – Ideally there should be a single document where all the consents are recorded, but in some cases it may be more appropriate to have more than one version. Does everyone know where/how they record Consent (for example – a prayer request).
      Do you know where the Consents Record is held?
    - 11. Categories of Processing: This is the data mapping form. As with Consents, the ideal would be a single document which can be easily checked, but it may be more appropriate to hold different ones relating to the role.
      Do you know where the Data Mapping record is held?
    - 12. Breach record – Are you prepared to deal with a data breach? All instances of a personal Data breach, regardless of how small (eg an email sent to the wrong recipient) should be recorded.
      Does everyone know how to report a breach?
      Do you know where this record is?
    - 13. Transfer of information overseas: In some cases you may be sending personal information overseas – for example, to a partner church for prayer request. If this is the case, a separate record is required on the Annex to the Processor Record.
- Is this information recorded on the Template Processor Record for Managing Trustees? (sections 10-12)
- Do you know where the Processor Record is stored?

CHECK 7

Review your Data Security

- This section is asking that you make sure that the data is kept as secure as possible. Whilst this may be fairly straight forward in the church office, it is not as easy when people hold data at home.
- Things to be looked at might include:
    - ◊ Are all computers kept on the latest level of software update?
    - ◊ Do all computers have virus protection software?
    - ◊ Is the information on the computer either backed up regularly or kept on the cloud?
    - ◊ If a printed directory is produced, are those who hold a copy reminded to keep it where a member of the public cannot access it (for example, in a drawer rather than on a table by the phone)? Are they also reminded of what they can and cannot do with this information?
- Do you have job specific email addresses that are only used for that job and are used by successive job holders?

Ensure Managing Trustees are aware of their Data Protection Obligations

- Membership of church councils and circuit meetings changes on a continuing basis. Are new members (especially people new to a managing trustee role) given any induction? (It maybe that the induction is just being given a pamphlet that outlines the responsibilities to read)
- Does that include their responsibilities with regard to GDPR?