Guidance notes

9 Steps for Methodist Managing Trustees to Take Now to Comply with GDPR

Practical steps for Managing Trustees to take now to prepare for the arrival of the General Data Protection Regulations (GDPR) on 25 May 2018.

Updated Feb 26th 2018

Section A - Introduction

The new European General Data Protection Regulation (GDPR) comes into force on 25th May 2018.

The Information Commission's Office (ICO) has produced guidance on steps that can be taken now to prepare for the arrival of GDPR. This Focus Note tailors the steps for Methodist Managing Trustees setting out specific practical steps for Local Churches, Circuits and Districts to take **immediately** to help them look after the personal information they collect and use (Steps). After each Step there is a "help box" highlighting the practical support available to assist Managing Trustees in fulfilling that Step. Whether the information (data) belongs to Church members, their families, employees or third parties who use church premises it is in everybody's interests to ensure that the information is looked after carefully and kept safe. Taking the steps in this Focus Note will help Managing Trustees to do that.

Please read this Focus Note together with the suite of data protection guidance being produced by the Data Protection Working Party (Working Party) to help Managing Trustees understand how to practically comply with the requirements of GDPR.

Step 1 - Ensure that those people in the Local Church, Circuit or District who collect and/or use (process) personal information (personal data) are aware of the requirements under GDPR.

- Ensure those who deal with personal data (whether compiling the Local Church or Circuit directory or organising lifts for guests to a local church's luncheon club) read the data protection guidance that has been made available via TMCP's website and understand how this applies to what they do.
- Promote use of the data protection guidance and model documents being produced by the Working Party (the data protection "tool kit") as well as the handpicked external guidance accessible from the TMCP website.
- Complete the data protection training that will be offered by TMCP, in conjunction with the Working Party. In addition to the online guidance notes there will be webinars available to view on the TMCP website.

Going forward:-

- Ensure that the Managing Trustees implement the data protection policies and best practice that is being developed and promoted by the Working Party.

To help with this:

The best way for Managing Trustees to keep abreast of new Methodist specific guidance on data protection issues and bespoke training is to sign up to receive email alerts via the TMCP website. Look out for the “Stay Updated” heading at the foot of each TMCP webpage and insert your email address.

Step 2 – Carry out a review of the personal information (data) the Local Church, Circuit or District holds (known as a “data mapping” exercise).

- Nominate members of the local Church Council, Circuit Meeting or District to review what personal information (data) the managing trustee body holds such as lists of members, contact details for third party users of church premises (licensees or tenants) and right to rent documents that Managing Trustees may hold for residential tenants living in Local Church, Circuit or District property.
- Managing Trustees need to question what the personal information is, where it came from, why it is held (what purpose?), who actually holds the data e.g. the Minister or church administrator, who has access to it and who it is shared with?
- Record the results using the Template Data Mapping Form for Managing Trustees produced by the Working Party and the Non-Exhaustive List of Examples. Completing the form will help Managing Trustees evaluate the personal information they hold, how it is used and provide the records required under GDPR.
- Use the information collated to pinpoint what further action is required – What action can the Managing Trustees take to ensure the data held is secure? Can the number of people with access to the records be limited e.g. on a need to know basis? Is all the data Managing Trustees currently collect actually necessary? Can less personal information be collected? Is it necessary to record youth fellowship member’s postal addresses if contact is only ever made by telephone or email? Is it necessary to record dates of birth for the Local Church’s men’s and women’s fellowships?

To help with this:

The Working Party has appointed a Data Protection Implementation Officer (DPIO) to assist the wider Methodist Church in identifying what data is held by Managing Trustees and how it is collected, stored and used. This work has been carried out using a representative sample of Local Churches and Circuits through “data mapping” exercises coordinated by the DPIO. The information produced will provide Managing Trustees with a comprehensive and practical list of situations in which personal data is processed by Methodist Managing Trustees. As well as providing valuable information to help the Working Party shape policies and guidance specific to the Methodist Church and the way it deals with (processes) personal information, it will also assist Managing Trustees to complete their own data mapping exercises (audits). In turn this will be a useful tool for Managing Trustees in maintaining records of their data processing activities and help demonstrate compliance with the GDPR. This is all part of the new “accountability” principle, which confirms the need to ensure proper systems are in place to manage the security of personal data.

Managing Trustees need to start making their own records now. They can then use the results of the Working Party’s data mapping exercise to check and maintain these records. These results will be made available once the task has been completed. Managing Trustees can ensure they find out when those results are available by signing up to receive TMCP’s email notifications. Please refer to Step 1 for details of how to do this.

Step 3 – Ensure clear and accessible information is provided to individuals about how

their data will be used (use of a Privacy Notice).

- Check what privacy information Managing Trustees currently give to individuals when they collect their personal information (data). The information that needs to be provided to individuals (see help box below) is contained in a "**Privacy Notice**". A **Privacy Notice** should be included on any online or paper forms used to collect such data e.g. permission slips for the youth church trip or a form for volunteers to carry out hospital visits. Behind the Privacy Notice sits a more detailed "**Privacy Policy**".
- Explain to members, employees and third party users etc. in the **Privacy Notice** why Managing Trustees are asking for and retaining their personal information, what they will use it for, who if anybody they will share it with and how they will protect an individual's personal information.
- Ensure that the information given in the **Privacy Notice** is clear, transparent and readily accessible.
- Update any notices that Managing Trustees currently use to include the additional information required under the GDPR.
- Put in place a **Privacy Policy** and ensure individuals are aware of the existence of the policy.

To help with this:

TMCP in conjunction with the Working Party is working on a model Privacy Notice and Policy for Managing Trustees to adapt for their own use. These will soon be available via the TMCP website together with a "how to" guide.

The results of the Working Party's data mapping exercise referred to in Step 2 will assist Managing Trustees in adapting the model **Privacy Notice** and Policy for their own use.

More information

Managing Trustees complying with existing data protection legislation will already be ensuring that they let their members, employees, third party users etc. (data subjects) know what information they hold about them, how it will be used and who it will be shared with. GDPR will require Managing Trustees to provide additional privacy information such as details of the legal reason (lawful basis) for using their personal information and the rights of the people whose data is being collected (Data Subjects) including the right to complain to the ICO and how and when the data will be destroyed.

Step 4 – Understand the rights of the people whose personal information Managing Trustees hold (Data Subjects) and work out what Managing Trustees need to do to accommodate these rights.

- Bear in mind the **rights** of those people Managing Trustees hold personal information about set out in Section C of the **GDPR Guidance Note** e.g. the right to be informed (through the **Privacy Notice** for example), the right of individuals to access their data or request that it is corrected or erased.
- Work out how the Managing Trustees will be able to deal with requests to exercise these rights and check that existing procedures are adequate or put in place new procedures:
  - Note that the timescales for dealing with a request are short and should be dealt with without undue delay.
  - Who is going to be responsible for updating or deleting personal information and with whose authority?
- Work out how the Managing Trustees will deal with requests for details of exactly what data they hold about an individual (data subject access requests) known as **SARs**:
  - Details of exactly what data Managing Trustees hold about an individual must be given within 30 calendar days.
  - Can Managing Trustees access all the records they hold to process **SARs** quickly enough?

    - Who will be responsible for accessing this information?
- Put in place the policy for dealing with requests including **SARs** (that will be available from the Working Party in due course) and ensure everybody is aware of how to react if they receive such a request. In the meantime Managing Trustees can refer to the current SARs Policy in Sections (8) to (11) of the Data Protection Booklet and the checklist in Section (11).
- Forward any **SARs** to the appropriate Data Controller :
    - the Conference Office (if it relates to Safeguarding or Complaints and Discipline) or
    - TMCP Data Protection if it relates to anything else

at the earliest opportunity.

To help with this:

Tackling Step 2 and getting to grips with what data Managing Trustees hold will go a long way in assisting Managing Trustees in complying with any requests received by people wanting to exercise their rights as "Data Subjects". If the Managing Trustees have a record of what data they hold and where it is kept, they will be able to quickly help an individual who wants to have their personal data corrected or deleted or simply wants to know what data the managing trustee body holds about them.

TMCP (or the Connexional Team in relation to Safeguarding or Complaints and Discipline matters) will help Managing Trustees to deal with **SARs** and other requests from individuals regarding their **rights**.

The Working Party will be producing a step by step guidance note on how to deal with SARs and updated **SARs Policy** in the near future. Managing Trustees will be notified when this is available if they sign up to receive updates via TMCP's News Hub alerts.

Encourage anybody wanting to make a SAR to use the template SAR Form produced by TMCP as this asks the person making the request to describe all the information they require and where Managing Trustees should find it. Note the standard £10 fee referred to in the template will be abandoned when GDPR comes into force.

Step 5 – Decide what legal reason (lawful basis) Managing Trustees have to use the personal information (data) they hold and record this.

- Consider the ways that the managing trustee body uses (processes) personal data (as revealed in Step 2) and decide in each case what legal reason(s) (see "help box" for details of the legal reasons that can be used) the Managing Trustees can rely on for doing so (these are the reasons that will need to be set out in the Privacy Notice dealt with as part of Step 3).
- Keep a record of the legal reason(s) that is/are being relied on for each "processing" activity e.g. using somebody's personal details to respond to a HMRC query over tax would be founded on a different legal reason to contacting them about upcoming church activities.

To help with this:

The legal reasons (lawful bases) for using personal data are discussed in more detail in Section D of the GDPR Guidance Note. Briefly, the lawful bases are the legal reasons as to 'why' Managing Trustees process data. In most day to day cases Managing Trustees will rely on one of 4 following possibilities (out of 6 in total):

- Consent from the person whose data is being held (data subject);
- Contractual obligations e.g. use is necessary to perform obligations under an employment contract or licence agreement;
- Legal obligation e.g. use of the data is necessary to comply with HMRC requirements or landlord and tenant legislation such as "right to rent";
- Legitimate interests e.g. after careful consideration weighing up the needs of the charity and the interests, rights and freedoms of the individual, the Managing Trustees are satisfied that they need to use the information for their own legitimate interests such as maintaining lists of members.

The Working Party is producing more guidance to help Managing Trustees identify the most appropriate lawful basis to use and how to record this and communicate the reasons to the people whose data is being held (data subjects). There will be a particular focus on **consent** and **legitimate interests** explaining what legitimate interests may be relevant to the data held by Methodist Managing Trustees.

Step 6 – Review how Managing Trustees obtain, record and manage consent – one of the legal reasons (lawful bases) discussed in Step 5.

- Look at areas where the Managing Trustees rely solely on the **consent** of individuals to use their data e.g. to contact a one-off donor about a new fundraising appeal or publish details of sickness in the Local Church newsletter.
- Check whether the **consent** being relied on is valid under the GDPR i.e. was it given freely, specifically for the purpose in question, unambiguously and was it informed?
- Was the **consent** in question given explicitly i.e. did the individual do something positive to provide their **consent** e.g. tick a box or confirm verbally that they wanted to receive information about upcoming fundraising events? Is this **consent** fully documented, i.e.do Managing Trustees have comprehensive records of when and how consent was given along with records of exactly what the individual was told at the time?
- Where **consent** is to be the lawful basis relied upon, use the information gained from carrying out the exercise in Step 2 (and the results of the Working Party's data mapping exercise) to plan how to ensure that valid **consent** is obtained where it is not already in place, and in the future.

To help with this:

The Working Party is producing further guidance on consent. In the meantime please refer to the GDPR Guidance Note, the News Hub Article Local Church, Circuit and District Directories – Data Collection and the wealth of guidance on the ICO's website including "What is meant by "consent""?.

Although the issue of **consent** has caught the imagination of the media, please remember that Managing Trustees do not need **consent** every time they use (process) personal information (data). As discussed at Step 5, Managing Trustees can base their use of personal information on one or more of a number of legal reasons. It is not all about **consent** and most of the time **consent** will not be the answer. Further guidance is on its way to help Managing Trustees identify when **consent** is an issue and how to ensure that they can rely on **consent** when they do need it.

Step 7 – Review data relating to children and systems for obtaining consent.

- Check whether the managing trustee body holds any data relating to children.
- Check what such data is used for/ how it is processed and whether the changes introduced by GDPR will be relevant e.g. have Managing Trustees developed commercial internet services such as social networking to promote youth services? Contact the Connexional Safeguarding Team if you have any such projects so that specific guidance can be given on the safeguarding and data protection aspects in this complex area.
- Ensure appropriate systems are in place to check ages and obtain consent from parents or legal guardians if required. The age limit under which children can freely give consent is expected to be 13 although this will not be confirmed until the Data Protection Bill has gone through parliament. The Bill was on its third reading in the House of Lords when this Focus Note went live on TMCP's website and is scheduled to come into law in time for GDPR coming into force on 25th May 2018.

To help with this:

The Connexional Safeguarding Team in conjunction with the Working Party is producing guidance on data protection issues relating to safeguarding.

Managing Trustees can contact the Connexional Team for help on issues regarding safeguarding.

Step 8 – Be prepared to deal with any data breaches.

- Use the model **Breach Register** being prepared by the Working Party to record all instances of a data breach (see "help box"), regardless of how small e.g. an email being sent to the wrong recipient.
- Review and provide training (further to the training being provided by the Working Party) to all those who deal with personal data in a Local Church, Circuit or District so that they know what has to be recorded.
- Consider what systems can be put in place to minimise any potential data breach such as ensuring electronic files are kept securely (e.g. pass worded, encrypted and appropriate virus, malware, anti-phishing software is loaded to protect electronic data). Ensure that manual files are held in locked filing cabinets and consider whether a "clear desk policy" and other such measures could prevent unauthorised access to data or even its loss.
- Ensure those handling personal data are trained in appropriate security measures so that they can help to look after the personal data of those involved in church life and using church premises.
- Contact TMCP if you believe that a breach needs to be reported to the ICO i.e. a breach leading to loss of confidentiality or reputational damage so that we can handle this for the Managing Trustees as Data Controller.
- Contact TMCP if you believe that a breach needs to be notified to individuals themselves i.e. where ID fraud or financial loss is a high probability. Further information will be produced by TMCP in due course.

It is important to contact TMCP as soon as possible to that help can be provided.

More information:

A “data breach” is where personal data is processed in a way that is not authorised by the individual whose data it is (the Data Subject) and includes, but is not limited to losing data, theft of the data, allowing unauthorised access to data or accidentally deleting the data.

To help with this:

The Working Party will be providing a model **Breach Register** shortly together with detailed guidance on avoiding and dealing with data breaches.

Managing Trustees can refer to the ICO’s guidance note on security in the interim.

Step 9 – Consider data protection implications when making key decisions.

- Ensure that the managing trustee body considers what it needs to do to protect the personal information of its members, their families and anybody else who has an association with the Church (and whose data they hold) whenever it starts a new project that could involve dealing with personal information in any way.
    - Such a new project could involve a Circuit office transferring its paper records onto a new computer programme – what will happen to the paper records? How can they be destroyed safely and completely? Is the new computer system secure? Is it password protected? Who will have access to it?
    - A project could also be something less obviously related to personal information such as opening negotiations with a potential new sharing partner – will information about the Local Church, its members and third party user groups be discussed?
- Before starting a new project that is likely to have a high impact on the rights and freedoms of individuals e.g. if a Church Council decided to employ an external group to take over the running of a local church’s youth club, consider carrying out a full risk assessment known as a **Privacy Impact Assessment**. This risk assessment will help the Managing Trustees identify any risk to individuals and how these can be overcome.

To help with this:

The Working Party will be providing further guidance on this topic in due course. Although formal Privacy Assessments will not be required by most Managing Trustees, Managing Trustees should consider and document whether or not any of the data being processed could be subject to a risk assessment. This means that Managing Trustees would need to consider whether the project exposed any data protection risks and if so, explain how these risks would be minimised.

Additional material to help Managing Trustees to take these steps will continue to appear on TMCP’s website. Sign up to receive the News Hub alerts to keep a pace with what is available. Alternatively, please do not hesitate to contact TMCP if you have any general data protection queries and the Conference Office for enquiries relating to safeguarding and complaints and discipline issues.

Disclaimer

Please note that this document is to provide guidance and assistance to Managing Trustees and their professional advisers. This guidance note is general in nature, may not reflect all recent legal developments and may not apply to the specific facts and circumstances of any particular matter.

Also note that nothing within the documents and guidance notes provided by TMCP nor any receipt or use of such information, should be construed or relied on as advertising or soliciting to provide any legal services. Nor does it create any solicitor-client relationship or provide any legal representation, advice or opinion whatsoever on behalf of TMCP or its employees.

Accordingly, neither TMCP nor its employees accept any responsibility for use of this document or action taken as a result of information provided in it.

Please remember that Managing Trustees need to take advice that is specific to the situation at hand. This document is not legal advice and is no substitute for such advice from Managing Trustees' own legal advisers.

Trustees For Methodist Church Purposes, Central Buildings
Oldham Street, Manchester, M1 1JQ

Telephone: 0161 235 6770
Fax: 0161 236 0752