

**Agenda item 8**

**DATA PROTECTION AND THE CHURCH COUNCIL**

**Background**

Local churches, Circuits and Districts find themselves holding a variety of personal data including details of members and employees. There are legal obligations imposed on Church Councils as managing trustees in relation to this data under Data Protection legislation.

The Trustees for Methodist Church Purpose (TMCP) who in law own all our property, have produced guidance about the action needed to meet the requirement of the European General Data Protection Regulations (GDPR) 2016/679 which are in force from 25 May 2018. These regulations will replace the Data Protection Act 1988. Managing Trustees need to be aware of the changes brought about by GDPR and how it will affect local church life.

TMCP, with the connexional team, are producing guidance and there is a working party which will oversee the transition from the current legislation to the new laws. A wide range of policies and procedures have already been identified which will be made available to all managing trustees over the coming months to ensure compliance with GDPR.

**Definition of personal data**

The Regulations cover the storage and use of personal data. This means information (1) about a living individual which is capable of identifying that individual, called the Data Subject.The Controller is the legal entity that is responsible for ensuring compliance. For the Methodist Church this is TMCP. The Processor is any person who processes data on behalf of the Controller. For the Methodist Church this is the local churches, circuits and districts.

**Consent**

Consent by an individual to process data must be freely given and can no longer be implied from silence or inaction.  It must be unambiguous and in clear plain English. Managing Trustees must also provide clear information on how an individual can withdraw consent and prevent the processing of their data for any given purpose. A form of consent is being drafted for local use.

**Rights of the individual and Access to data**

Information must be provided to individuals about their rights. Guidance is being produced to explain what is involved. Individuals also have a right of access to their personal data and Controllers will no longer be able to charge a fee for providing data to the individual. There is also a right to have inaccurate or incomplete information corrected.

**Essential reading**

Below is further information which provides more details about this complicated subject:

## TMCP : Guidance notes : 9 Steps for Methodist Managing Trustees to take now to comply with GDPR;

## TMCP : Technical Updates : Local Church, Circuit and District Directories – Data Collection

* TMCP: Focus Note : Date Protection Do's and Don'ts.

**More reading**

For those who want to read more, the following websites have further information:

* Trustees for Methodist Church Purposes : www.tmcp.org.uk
* Methodist connexional website : www.methodist .org.uk
* Information Commissioner's Office: www.ico.org.uk

**Finally .....**

One of the main changes will be a greater requirement for security in holding and transmitting personal data, whether electronically or on paper. However, it is not necessary to have everything in place by 25 May 2018. What is important is that there are plans being put in place to meet the requirements of the Regulations.

**Advice**

Church Council members are asked to note this information and await further guidance.

**Chris Kitchin, Church Council Secretary, March 2018**

(1) *The type of information a church holds would include:*

*Church membership database, Sunday Club records, Fellowship and House Group membership lists, Rotas, Babies & Toddlers Group records, Pastoral lists, Prayer Diary, Community Roll, Trustee Declarations, Church Council and other committee membership. Minutes of meetings, Annual Reports, Safeguarding documentation, Baptismal , Marriage and Funeral records, Room bookings, Financial records, Church website, and so the list goes on...*

## TMCP 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.



Only print expanded Guidance Notes

Print

#### 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.

**There are 9 steps recommended to implement the Regulations, with detailed guidance:**

#### 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.

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

#### Step 3 – Ensure clear and accessible information is provided to individuals about how their data will be used (use of a Privacy Notice).

#### Step 4 – Understand the [rights](https://www.tmcp.org.uk/about/data-protection/resources/guidenotes/gdpr#c) of the people whose personal information Managing Trustees hold (Data Subjects) and work out what Managing Trustees need to do to accommodate these rights.

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

#### Step 6 – Review how Managing Trustees obtain, record and manage [consent](https://www.tmcp.org.uk/about/data-protection/resources/guidenotes/gdpr#d) – one of the legal reasons (lawful bases) discussed in Step 5.

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

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

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

## TMCP : Technical Updates : Local Church, Circuit and District Directories – Data Collection

We are approaching the time of year when the Methodist Church is preparing for the new Connexional year and many Managing Trustees are starting to collect data for inclusion in their members directories; whether that is for a local church, circuit or district.

In May 2018, the Data Protection Act 1998 will be replaced with the new European General Data Protection Regulation (GDPR).  The GDPR makes several changes to existing Data Protection laws, details of which we will imminently be providing guidance upon and you will find the same on our website. One of those changes, however, is in relation to ‘Consent’.

Under the Data Protection Act 1998, Consent for inclusion of personal details in the local church, circuit and district directory may be given implicitly. This means that provided an individual knows that their personal data is being collected and why and how it is used, then written Consent is not required.

This will not be the case, however, under the GDPR as explicit Consent must be obtained.  Explicit Consent does not necessarily mean that consent must be in writing, but it cannot be obtained by implication or assumed that it is ok to use the personal data and the Consent must be freely given.

Going forward, if you obtain the personal data of an individual by way of a manual data collection form then the individual must sign and date the form.

If the personal data is obtained electronically, e.g. by email then, by the very fact that the individual has provided their details, this may be taken to mean that consent has been given freely and explicitly. Although Managing Trustees should be aware that however the data is collected they must provide the individual with the following information:

* What personal data you require? e.g. name, address, email address etc.
* What the personal data is required for? e.g. circuit directory
	+ For what purpose is the directory used? Is it merely a contact list? How will the individual’s contact details be used?  Who are likely recipients of such personal data?
	+ Could it be used for any other purpose?
* Who will have access to the personal data, e.g. the directory?  Is it published online?
* How the personal data is stored, e.g. computer/laptop/USB storage drive.  To whom do the devices belong?
* That the individual may withdraw their consent at any time in writing
* That the individual is entitled to complain to the Information Commission should their personal data be used in an unauthorised way.

This should also be linked to a more detailed Privacy Policy or Privacy Notice, and TMCP will provide an example for Managing Trustees to refer to in due course.  Briefly, the Privacy Policy/Notice will include, but is not limited to, detailed explanation on the above bullet points, how the personal data is kept up to date, how it is destroyed when it is no longer required and details of how an individual can request details of their personal data.

TMCP are in the process of making detailed guidance on the changes to data protection law available to Managing Trustees as well as providing example policies and procedures. We will notify you when then guidance is available through these updates and by contacting your Circuit Superintendent and District Property Secretary/Chair. In the meantime if you have any queries then please contact [TMCP Legal](http://tmcp.org.uk/contact) for further assistance.

**TMCP: Focus Note : Date Protection Do's and Don'ts**

|  |  |
| --- | --- |
| **Do's** | **Don'ts** |
| Only collect personal data for the purpose for which it is required. e.g. for Gift Aid purposes and the reclaiming of tax from HMRC. | Don’t use personal data for a different purpose or store it indefinitely because Managing Trustees think it might be useful in the future. |
| Generally, only use personal data where you have received consent by the Data Subject to hold and use the data for a particular purpose. | Don’t assume that a Data Subject’s consent will last forever.  They have the right to withdraw their consent for the processing of their data. |
| Once the purpose for which Managing Trustees hold personal data has expired, ensure that all records are securely deleted or destroyed preferably by shredding paper documents and then disposing of them in a confidential waste bin. | Don’t keep inaccurate data as this is a breach of data protection legislation. |
| Review the data that you hold on any individual at least once a year.  This will ensure that records held by Managing Trustees are accurate and up to date. | Don’t store or send personal data on removable media, such as a USB pen drive as these are easily lost or stolen. |
| Once an electronic device has come to the end of its shelf life, ensure that ALL data is erased and that the hard drive is wiped.  Ideally the device should be disposed of using professional services but the only real way to guarantee erasure is to destroy the device completely. | Don’t encourage the use of personal devices for church business. Wherever possible issue phones, laptops etc to individuals for official business and ensure that these are returned at the end of that person’s role or stationing. |
| Always remember that a Data Subject has the right to see the data Managing Trustees are holding about them.  Managing Trustees need to be careful as to what information is held and ensure that it can be retrieved quickly. | Don’t write any comment about an individual that Managing Trustees cannot defend if challenged.  Personal opinions are classified as personal data and Managing Trustees should assume that everything may be read by the Data Subject. |
| Managing Trustees should ensure that personal data is held in such a way that it can be accessed quickly in the event of a Data Subject Access Request being received. | Don’t amend or destroy personal data that you know is subject to a Data Subject Access Request. |
| Managing Trustees should ensure that all computers, screensavers and documents are password protected.  Passwords should be at least 8 characters long and include upper and lower characters as well as symbols and numbers.**Hint:** replace an ‘E’ for a ‘£’ symbol.  Non- European keyboards don’t have them. | Don’t write passwords down and ensure you change them at least every 60 days. |
| All communications sent electronically which contains personal data, especially sensitive personal data should always be encrypted. | Don’t send confidential communications by email if possible but at the very least such communications should be encrypted. |
| Managing Trustees should ensure everyone is familiar with all data protection policies and procedures.  Keep a record so Managing Trustees can demonstrate this requirement has been complied with. | Don’t open emails from unknown sources. If the email appears suspicious, check with the sender by phone before reading and opening any attachments. |
| For Managing Trustees that have offices, ensure that all visitors are escorted out of the office/building to ensure that there is no access to unauthorised areas. | Don’t ignore software security updates on devices.  Failure to do so can leave devices open to hackers and cyber-theft. |
| Keep a record of any data breach: further guidance will be provided on what constitutes a data breach. | Don’t pass on personal data to a third party without consent. |
| Be safe; if you’re not sure ask for advice. | Don’t assume that data protection doesn’t matter – IT DOES. |

**Remember to keep all personal data secure, confidential and**

**treat it as if it were your own.**