Data Security Policy for the Methodist Church (GDPR)

Last updated 24.05.2018

The Methodist Church in Great Britain uses personal information all the time to fulfil its calling and is committed to protecting the privacy of its members, ministers, volunteers, lay workers, supporters and all those whose personal information it holds.

As a Connexional Church we work together to ensure that all personal information is handled safely and in accordance with the General Data Protection Regulation and UK data protection legislation.

1. Definitions

This section sets out definitions of key terms referred to in this policy. Definitions used in particular sections are included at the head of such sections for ease of reference:

"**You**" "Your" are all those volunteers, ministers and staff within the Methodist Church who handle **personal data**.

"**We**" are the Connexional Team (registered under the name of the Methodist Church in Great Britain) and Trustees for Methodist Church Purposes (TMCP) as **controller**s.

"controller": the person or organisation that determines when, why and how to **process**, **personal data**. It is responsible for establishing practices and policies in line with the GDPR and UK data protection legislation.

Trustees for Methodist Church Purposes are **controller** for **personal data** used by staff and volunteers at Local Church, Circuit and District level. This is for routine, day to day data protection matters.

The Methodist Church in Great Britain is the **controller** responsible for all data protection matters concerning safeguarding and, complaints and discipline issues for the whole Methodist Church and other data protection matters for which the Connexional Team are solely responsible.

the "**appropriate controller**" is the **controller** for the matter in hand.

Criminal Offence Data: personal data relating to criminal offences and convictions.

Data Protection Policy: the data protection policy setting out the responsibilities of the **controller** and you in relation to privacy within the Methodist Church.

"data subject": a living, identified or identifiable individual about whom **personal data** is held. e.g. our

members, volunteers, lay employees, those who join us in worship and/or those who are interested in and supportive of the work of the Methodist Church, third parties such as community groups who use our buildings and other third parties.

ICO: Information Commissioner's Office.

GDPR: the General Data Protection Regulation ((EU) 2016/679). **Personal data** is subject to the safeguards specified in the GDPR.

Methodist Church or Church refers to the united church or denomination known as the Methodist Church formed under the provisions of the Methodist Church Union Act 1929 and a deed of union on 20 September 1932.

"personal data": any information identifying a living individual or information relating to an individual that can be identified from that information/data (alone or in combination with other information in your hands or that can reasonably be accessed). **Personal data** can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour. Personal information includes an individual's name, address, date of birth, telephone number, email address, a photograph or disability, health or ethnicity data.

"personal data breach" is: any act or omission that compromises the security, confidentiality, integrity or availability of **personal data** or the physical, technical, administrative or organisational safeguards that we as a Church have put in place to protect it. The loss, or unauthorised access, disclosure (sharing) or acquisition, of **personal data** is a **personal data** e.g. emailing **personal data** to the wrong person; or leaving **personal data** in a public place where others can access it.

"processing" or "processed" or "process": any activity that involves the use of **personal data**. It includes obtaining, recording or holding the data, or carrying out any activity or set of activities on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. **Processing** also includes transmitting or transferring **personal data** to third parties. E.g. sharing member information by email and shredding when information is no longer required.

Special Category Personal Data: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data.

Working Party: the data protection working party comprising members of the Connexional Team and Trustees for Methodist Church Purposes (TMCP).

2. INTRODUCTION AND SCOPE

Protecting the security, confidentiality and integrity of **personal data** (personal information) is a critical responsibility that we take seriously at all times. This policy sets out how we work together to do achieve this in accordance with applicable law and respecting the principles set out in Part II of the Data Protection Policy.

This policy sets out the organisational measures put in place by the **controllers** and provides guidelines on the

steps you need to take and good practice to keep information safe.

This policy must be followed by all volunteers, ministers and staff who handle **personal data** relating to the Methodist Church.

If you handle **personal data** as part of your role, in order to keep that **personal data** secure, you will:

- make sure that data security is maintained in line with this policy and any associated guidelines or procedures that may be issued by the **controllers** from time to time;
- implement reasonable and appropriate security measures at Local Church, Circuit and District level against unlawful or unauthorised **processing** of **personal data** and against the accidental loss of, or damage to, **personal data** in accordance with the guidelines and good practice outlined in this policy;
- exercise particular care in protecting Special Category Data and Criminal Offence Data from loss and unauthorised access, use or disclosure;
- take part in available data security training that is appropriate to your role including but not limited to any face to face and web-based training sessions offered by the **controllers**; and
- keep up-to-date with the guidance and policies produced or signposted by the **controllers**.

This policy will be updated from time to time and while we will give notice via TMCP's News Hub and other communication methods deemed appropriate by the **controllers** from time to time the onus is on you to check back regularly to obtain the latest copy of this policy. This policy was first published on 24 May 2018 and was last revised on the date stated on the front page.

3. INFORMATION SECURITY

3.1 Security principle

The Methodist Church is committed to ensuring **personal data** is handled and managed appropriately. Together we adhere to the principles relating to the **processing** of **personal data** set out in the GDPR and UK data protection legislation which in relation to security require **personal data** to be:

> *"**processed** in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful **processing** and against accidental loss, destruction or damage, using appropriate technical or organisational measures"* (Article 5(1)(f) of the GDPR) (**security principle**).

You will adhere to organisational measures put forward by us and implement reasonable and appropriate organisational measures (see Section 4) and technical measures (see Section 5) against unlawful or unauthorised **processing** of **personal data** and against the accidental loss of, or damage to, **personal data** in accordance with good practice outlined in this policy.

This means you must ensure that you have appropriate **personal data** security (sometimes referred to as "information security") to prevent **personal data** being compromised.

3.2 Confidentiality, integrity and availability

You will maintain data security by protecting the confidentiality, integrity and availability of **personal data.** This means that:

(a) only people who have a need to know and are authorised to use the **personal data** can access it (Confidentiality). People who are not authorised should not be able to access the **personal data** you hold or alter, disclose or delete it.

Ensure that **personal data** is only shared amongst those ministers, volunteers and staff members who have a need to know the information to fulfil a specific task. Decide who needs to know what and stick to this so that you can keep an eye on who can amend, disclose or delete records. Protect databases and work stations with passwords and lock information away as appropriate in accordance with the good practice points outlined in the Security Responsibilities ABC in Annex 1.

You must also comply with Section 5 of the Privacy Notice in relation to non-disclosure of **personal data** and treat all personal data as strictly confidential, except where consent has been provided for it to appear in publications available to general members of the public. Stop and think – does the information you intend to share need to be shared? Can you be an open Local Church and encourage participation in **Church** life by the wider community by using generic email addresses that do not identify individuals e.g. stjohnsmc-bookingsecretary@[EMAIL PROVIDER].uk? Can you invite people to get in touch using office contact addresses and telephone numbers or "work" mobile phones rather than putting **personal data** on Local Church noticeboards?

(b) **personal data** is accurate and suitable for the purpose for which it is **processed** in accordance with principle 4 of GDPR (see Section 4.4. of the Data Protection Policy) e.g. **personal data** is kept up to date and can only be updated by authorised volunteers, ministers and other staff members (Integrity).

(c) the **personal data** you hold is accessible and usable by authorised users when they need it for authorised purposes (Availability) e.g. you can restore access to **personal data** in the event of incidents occurring by routinely backing up data and implementing other measures necessary to ensure continued access in accordance with the good practice points outlined in the Security Responsibilities ABC in Annex 1.

Whilst not compromising the security of **personal data**, make sure a sufficient number of authorised Local Church, Circuit or District officers or ministers know where "**Church**" **personal data** is kept should they need to. Avoid a situation where if you became ill for example nobody would know where to find the **personal data** you hold e.g. it was not "accessible".

3.3 Appropriate measures

You will decide what level of information security is appropriate and reasonable by assessing and keeping under review your "information risk". This means the impact of a **personal data breach** affecting **data subjects** and the damage and distress likely to be caused given the amount and type of **personal data** you are **processing** and what you are doing with it (purpose).

The more **personal data** there is to protect, the more sensitive that **personal data** is (e.g. if it includes Special Category Data and/or Criminal Offence Data) and the riskier the intended use (**processing**) e.g. the risk of the personal information falling into the wrong hands, the tighter the security measures will need to be.

You are expected to take a common sense approach with the emphasis on the time, sophistication and expense of security measures being proportionate to the risk to **personal data**. However, you do need to ensure that you can justify the security choices you make. E.g. A list of luncheon club members' contact telephone numbers kept to enable one another to operate the Local Church luncheon club would not need to be under as tight security measures as an email being sent to HMRC including details of lay workers' dates of birth and National Insurance Numbers.

The data mapping exercise carried out in accordance with Step 2 of the **9 Steps for Methodist Managing Trustees to Take Now to Comply with GDPR** will help you to assess the risk to **personal data**.

4. ORGANISATIONAL MEASURES

4.1 Risk assessment

The Working Party has carried out a data mapping exercise and risk assessment to assess the information risk.

We have put in place this data security policy (including the good practice guidelines set out in the Security Responsibilities ABC in Annex 1) together with associated guidelines to help you to address the risks identified and keep information safe.

We will keep this policy under review, test its effectiveness and make adjustments to address any weaknesses discovered and respond to new security threats that may develop over time.

4.2 Awareness

The **controllers** recognise the importance of those ministers, volunteers and staff members who handle **personal data** being aware of data security good practice and their responsibilities. We raise awareness of data security good practice by:

- Putting in place this data security policy and keeping it under review (Section 4.1);
- Arranging a combination of face to face and web based training sessions for those handling **personal**

data across the **Methodist Church** to complete;

- Working with the Districts to put in place and train "data champions" who can promote good practice at District level down to Circuit and Local Church level and provide support and guidance to you on the practical application of this policy and accompanying guidelines and procedures;
- Being a point of contact to answer questions that you may have on data security and GDPR in general (see Section 8); and
- Making detailed guidance available to you on data security and GDPR in general.

4.3 Data minimisation

In accordance with Section 4.3 of the Data Security Policy you will minimise the **personal data** that you **process** to reduce the amount of **personal data** for which you are responsible under data protection legislation and which you must keep safe (and the risk of a **personal data breach**).

As far as is reasonably appropriate (and depending on the type and volume of **personal data** and the purposes it is being put to) you will:

- Carry out a **personal data** cleanse e.g. destroy any personal information that is no longer required in accordance with the Methodist Retention Schedules.
- Only record **personal data** when required e.g. under the Constitutional Practice and Discipline of the Methodist Church or to carry out a specific task related to your role with the **Church**. E.g. if somebody is giving you more **personal data** than you require e.g. medical information when you are calling them to arrange a pastoral visit, only note down the information you actually need to arrange that visit.

This means that as Church we need to stop and think before collecting **personal data** from people however willing they are to give it. With **personal data** come responsibilities to keep it safe. In some cases you can protect the people you care about by simply not collecting their personal information. What information is required to fulfil the task you are trying to fulfil? When you collect personal information be aware of the responsibilities on you to keep that information safe and destroy that personal information as soon as you can in accordance with the Methodist Retention Schedules so that it cannot inadvertently fall into the wrong hands.

5. TECHNICAL MEASURES – PHYSICAL AND TECHNICAL/CYBER SECURITY

You will put in place physical and technical security measures that are reasonable and appropriate given the risk assessment in Section 3.3 and in accordance with the good practice set out in the Security Responsibilities ABC in Annex 1.

5.1 Physical measures

You will put in place reasonable and appropriate physical measures to minimise the risk of security incidents arising due to equipment being lost or stolen, incorrectly disposed of equipment (see Section 6.2 Safe disposal of personal data) and electronic devices or hard-copy records being lost or stolen.

Good practice is to take steps including but not limited to:

- Ensuring the physical security of the premises in which **personal data** is stored (whether that is Local Church, Circuit or District premises or your home etc.) including the quality of doors and locks, and the use of alarms, security lighting , CCTV or other security mechanisms where appropriate;
- Controlling access to Local Church, Circuit or District premises and supervision of visitors to prevent unauthorised access to equipment holding **personal data** and hardcopy records;
- Protecting the security of your IT equipment and mobile devices e.g. take good care of devices;
- Not leaving **personal data** unattended;
- Operating a "clean desk" policy e.g. not leaving papers containing **personal data** lying about unattended;
- Keeping paper records (particularly those containing sensitive **personal data**) in locked filing cabinets or cupboards or in other secure locations;

Think about how you secure your own passport, paper driving licence and bank correspondence etc. and ensure "**Church**" **personal data** is similarly secured, especially if you are handling "**Church**" **personal data** at home.

- Not leaving paper records containing **personal data** on public transport;
- Doing whatever is reasonable and appropriate to recover lost items e.g. retracing your steps or ringing the bus company or library to see if they have found your lost papers or electronic device etc.

5.2 Technical controls/ cyber security

You will implement cybersecurity measures appropriate to the size and use of your networks and information systems in line with this policy and the ICO and UK Government guidance from time to time.

5.2.1 Practical steps

Good practice is to take practical steps including but not limited to:

- Taking care when typing email addresses;
- Considering whether to use the BCC field for general correspondence e.g. mailshots;

Use your judgment as to when it is appropriate to use the BCC field e.g. it may not be necessary where emails are sent to members of a particular group such as between youth leaders or members of the Local Church's women's fellowship group but would be appropriate for general correspondence e.g. sending out a Local Church newsletter. Would the recipients mind the others knowing their email address? Do they know each other's contact details already?

- Regularly backing-up computer files;
- Not leaving devices unattended and if so make use of the screensaver function requiring a password to log back into the session you were in; (use the *WIN* + L shortcut *key* combination);
- Not printing information unless you really need to and if you do store it somewhere safe;
- Ensuring live and back-up files are secure e.g. password protected (see Section 5.2.2); and
- Storing computer files on a password protected machine; (see Section 5.2.2).

5.2.2 Cyber essentials scheme

Ensure that the electronic device(s) you use and give others to use for **Methodist Church** related activities operate in line with the Government's cyber essentials scheme; https://www.cyberessentials.ncsc.gov.uk/. Use the Use the Cyber Essential's checklist to help check this.

Good practice is to ensure that the recommendations in the Government's cyber essentials scheme are put in place including but not limited to:

- The use of passwords;
- Checking the security settings of devices rather than staying with the often lower security pre-installed settings;
- Installing suitable firewalls;
- Installing malware software;
- Controlling access through the use of different login accounts particularly where devices are shared with other family members or used for both Church roles and private use.

5.2.3 Encryption

"encryption": a mathematical function using a secret value known as; "the key" which encodes data so that only users with access to that key can read the information.

You will use **encryption** when appropriate (see box below) and particularly when sending sensitive information (Special Category or Criminal Offence Data) by email. This includes sending such information in the body of an email or as an attachment. You will assess the need for this based on the assessment carried out under Section 3.3.

Refer to the ICO's guidance on **encryption** including: https://ico.org.uk/for-organisations/guide-to-data-protection/encryption/

Refer back to Section 3.3 for the points to take into consideration when assessing what measures are appropriate to take and remember that the assessment takes into consideration the time, sophistication and expense of security measures being proportionate to the risk to **personal data**.

5.2.4 Pseudonymisation

Pseudonymisation or Pseudonymised: means replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.

Although Pseudonymisation is unlikely to be a reasonable and appropriate data security tool in respect of day to day **processing** by Local Churches, Circuits and Districts, you will review its suitability on an ongoing basis and use this method when appropriate. You should consider Pseudonymisation in situations such as embarking on a new project involving new IT systems, the transfer of particularly sensitive information onto new systems perhaps in the event of a Circuit merger or archiving sensitive information. (Note that you continue to be responsible for the security of archived (as opposed to deleted/destroyed) material.)

In such cases follow the requirements to carry out a Data Protection Impact Assessment (DPIA) under Section 7 of the Data Protection Policy.

Further guidance on Pseudonymisation will be provided in due course.

5.4 Review

You will keep the security measures at Local Church, Circuit and District level under review and update the same as required to ensure that they continue to be reasonable and appropriate.

You will review this policy for any updates and update your security measures appropriately as and when required.

You must keep and maintain accurate records reflecting your **processing** activities in accordance with the Methodist Church's record keeping guidelines. These include a description of security measures put in place in the Data Mapping Form.

6. STORAGE LIMITATION AND SAFE DISPOSAL OF PERSONAL DATA

6.1 Storage limitation

You will not keep **personal data**, in a form which would permit the **data subject** to be identified, for longer than

is necessary for the purposes you originally collected it for. (Please see Section 4.5 of the Data Protection Policy in relation to storage limitation and the Methodist Retention Schedules.)

6.2 Safe disposal of personal data

You will take all reasonable steps to destroy and erase all physical and electronic **personal data** that you no longer require in accordance with the **Methodist Church's** guidelines, retention schedules and policies from time to time and best practice guidance from the ICO including their guidance on "deleting your data" (https://ico.org.uk/for-the-public/online/deleting-your-data.aspx).

The "reasonable and appropriate" steps that you need to take depend on the type and volume of **personal data** you are dealing with and the damage and distress likely to be caused to the **data subject** in the event of a **personal data breach** (see Section 3.3). Take a common sense approach.

Good practice to dispose of **personal data** safely includes taking measures such as:

- Shredding hardcopy documents

It is recommended that a shredder (e.g. a "cross cut" shredder) is used to shred documents containing **personal data**. Depending on the sensitivity and volume of the **personal data** you are destroying you may decide to invest in an office grade shredder, use an external shredding company or purchase an inexpensive shredder for domestic use. Manual shredding can be used as a last resort if you deem that this is appropriate in the particular circumstances at your Local Church, Circuit or District (see Section 3.3).

- Deleting **personal data** held electronically so that the information is put "beyond use".

Remember that simply deleting an entry from a current Excel spreadsheet, deleting a document or email does not remove information completely. Permanent deletion can be technically very difficult. A simple google search may give you some ideas for basic IT systems but exercise caution in using and relying on any free downloadable applications as they may carry their own security concerns or not be as effective as they suggest.

Consider what reasonable practical steps can be taken at your specific Local Church, Circuit or District depending on the systems that you use and the information risk identified in accordance with Section 3.3. Practical steps could include simply emptying email inboxes and recycling folders, deleting information from backups or getting specialist assistance.

Ensure that "deleted" information is not accessed and does not continue to be used in practice.

- Disposing of old electronic devices safely and deleting **personal data** before recycling devices or disposing of them so that data is not accessible to others after the device has left your ownership.

Think about what **personal data** may be leaving the Methodist Church along with the device it is stored on whether the device belongs to the Local Church, Circuit, District or you personally.

As a practical step you should record what devices – Church owned or personal – are used to handle personal

data. Remember that this can include not only PCs, laptops, tablets, notebooks etc. but also faxes, printers, servers, back-up storage and USB stick. When any such devices are disposed of, recycled or given to a relative etc. make a written record, of who you are handing the devices and what steps you took to erase/delete the **personal data** on them.

Refer to the ICO's guidance on "deleting your data" (https://ico.org.uk/for-the-public/online/deleting-your-data.aspx) for practical steps to take including restoring devices to factory settings, using overwriting software or physical destruction.

- Returning rented electronic devices to the supplier safely and wiping any hard drives so that data is not accessible to others after the device has left your ownership.

Remember that photocopiers and other electronic devices you may hire have hard drives which store **personal data** and need to be wiped before they go back to the supplier.

8. WHERE TO GO FOR HELP?

Please contact the **appropriate controller** with any questions about the operation of this policy, the GDPR, UK data protection legislation or if you have any concerns that this policy is not being or has not been adhered to.

The **controller** for routine, day to day data protection matters for Methodist Local Churches, Circuits and Districts is:

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

Title of contact: Laura Carnall, legal manager
Tel: 0161 235 6770
Email: dataprotection@tmcp.methodist.org.uk
Web: https://www.tmcp.org.uk/about/data-protection

The **controller** for matters relating to safeguarding matters or complaints and discipline for Methodist Local Churches, Circuits and Districts is:

The Methodist Church in Great Britain
The Conference Office
Methodist Church House
25 Marylebone Road
London
NW1 5JR

Title of contact: Sarah Wadman, Internal Services Manager
Tel: 0207 486 5502
Email: dataprotection@methodistchurch.org.uk
Web: www.methodist.org.uk

Refer to the ICO's guidance on data security and government backed sources of information.

Annex 1

SECURITY RESPONSIBILITIES ABC – GOOD PRACTICE

C

CCTV

- Refer to the ICO's guidance on the use of CCTV.
  Link: https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf

Circuit Plan

- See **Directories**.
- It is good practice to have two versions of the Plan:
  - one version without **personal data** (except relating to Ministers in Full Connexion, probationers and those office holders whose details need to be in the public domain to fulfil their function within the Methodist Church and who would expect their details to be public); and
  - one for Church members only with the **personal data** (for everybody whose personal information you have decided needs to be included in the Plan) to enable the Local Church or Circuit to function as a membership organisation e.g. so that members can contact each other to arrange services and other Church activities.

Contact details

- See Circuit Plan and Noticeboards
- Use a different contact email address for "Church" business where appropriate to help you to split up information that you know in your official capacity e.g. as a Local Church or Circuit steward and information that somebody tells you as a friend. Ask somebody how their poorly relation is using your personal email and find out whether the Local Church hall is free using the email address you use for "Church" business. Splitting the two may be tricky and take time getting used to but will reduce the amount of **personal data** you deal with and are responsible for in your Local Church, Circuit or District role.

D

Directories (Circuit and District Directories)

- See Sections 5.1 and 5.2 of this policy**.**
- Think about how you collect the **personal data** to go into the Directory or Circuit Plan. If you collect the information by email or written forms (Incoming Information) and then transfer that information onto the Directory or Circuit Plan document, destroy the Incoming Information safely to avoid duplication of **personal data** as part of the drive to minimise the amount of **personal data** that you hold.
- However, if the Incoming Information is on a consent form (because you make the Directory or Circuit Plan available to the general public), the consent form must be kept safe as part of your consent records.
- Shred or tear up Incoming Information handed to you in paper form and delete emails OR store the information securely only for so long as you need to. Keep in locked filing cabinets, locked cupboards or password protected files or anywhere that is considered safe and secure.
- If you have not obtained consent because you do not make the Directory or Circuit Plan available to third parties, ensure those members with a copy know they must keep the information confidential.

E

Email

- See Sections 5.1 and 5.2 of this policy in relation to the use of email generally and Section 5.2.3 in relation to **encryption**.
- There are no specific directions from the Methodist Church in relation to the use of certain email account providers but do keep under review in line with Government and ICO recommendations and use a provider that you have confidence in.
- It is generally accepted that as American email providers such as google and Microsoft have signed up to the so called "privacy shield" (an agreement between the US and EU about the transfer of **personal data** between the EU and America), there are no particular compliance concerns about using such providers. The situation is being kept under review in light of recent case law.

Employment details

- See Sections 5.1 and 5.2 of this policy**.**
- Remember that this **personal data** may include Special Category Data and/or Criminal Offence Data and take extra care of it.
- Bear in mind the disposal responsibilities and retention periods relating to unsuccessful applicants.

G

Gift Aid Records

- See Sections 5.1 and 5.2 of this policy**.**
- Refer to Section 5.2.3 (Encryption) if you are required to provide any information to HMRC.

L

Letters (outgoing)

- Make sure that they are correctly addressed.
- Send letters containing **personal data** safely. Use "signed for" delivery as a minimum and "special delivery" or even specialist couriers if the **personal data** is Special Category Data or relates to a number of **data subjects.**

Licensees - Licence agreement and records of licensees

- See "Third Party Users"

M

Membership Lists (also lists of group members)

- See Sections 5.1 and 5.2 of this policy**.**
- Consider how much information you really need to include and who should have access to the lists. Do lists of adult members need to include a date of birth or simply confirmation that the individual is over 18? Think about whether you have a legitimate reason for processing this information e.g. considerations under the Equality Act 2010.
- Bear in mind the need to keep **personal data** up to date, correct any mistakes and ensure the integrity of the information by controlling who can amend the lists.

N

Noticeboards

- Limit information on noticeboards outside the Local Church and those accessible to the general public inside the chapel to non-personal information wherever possible e.g. church office contact details and generic email addresses.
- Where **personal data** is required e.g. so people can contact the minister or office holders to talk about worship at the Local Church, marriage or use of Local Church premises, limit the information to Ministers in Full Connexion, probationers and office holders. Office holders may include the booking secretary or treasurer and/or other office holders who would expect their information to be in the public domain (to fulfil their function within the Methodist Church). But do consider the use of generic contact details as a first port of call.

P

Pastoral Records

- See Sections 5.1 and 5.2 of this policy**.**
- Think about what information you actually need to record. If you are calling somebody to arrange a pastoral visit, only note down the information you actually need to arrange that visit. Do you need to record all the information they may be telling you e.g. medical information? (See Section 4.3 (Minimisation).)
- If the information will include Special Category Information e.g. health data, take special care of it. Keep any paper records in a locked filing cabinet (or cupboard) if possible, keep any computer records password protected, do not leave the files unattended and follow the good practice guidance in this policy.
- Only share information with others involved in pastoral visits on a "need to know" basis.

R

Residential Tenancy Documents

- See Sections 5.1 and 5.2 of this policy**.**
- Remember that this **personal data** may include Special Category Data and take extra care of it.

Rotas (including flower arranging)

- See Sections 5.1 and 5.2 of this policy**.**
- Consider how much information you really need to include on the rota – is it just the names so that people know when it is their turn? Can first names be used?
- If you usually include contact numbers so that volunteers can contact each other, do you really need to? Can this additional **personal data** be held by a Church or Circuit Officer and not included in the rota itself or membership lists etc. used?
- Consider where the rota will be displayed e.g. is it in an area of the Local Church premises that is accessible by the general public.

T

Third Party Users

- See Sections 5.1 and 5.2 of this policy**.**
- If you keep a database of your third party users to help you to manage third party use of the Local

Church, Circuit or District premises ensure that the necessary privacy information has been served on the third party users and keep the information safe in accordance with this policy.

END OF DOCUMENT