Data Protection Policy for the Methodist Church (GDPR)

Last updated 24.05.2018

The Methodist Connexion 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.

Part I – This Data Protection Policy

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 **controllers**.

"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 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.

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

Methodist Church in Great Britain, 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.

Privacy Notices (also referred to as **"fair processing notices"** or **"privacy policies"**)**:** separate notices setting out information that may be provided to data subjects when you collect information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, employee privacy notices or the website privacy policy) or they may be stand-alone, one time privacy statements covering **processing** related to a specific purpose. A general **Managing Trustee Privacy Notice** will be included in the Data Protection Toolkit for your use together with more specific template notices and wording for fair processing notices.

"processing, 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. P**rocessing** 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 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

Protecting the 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 all work together to protect the privacy of all those who are part of the Methodist Church or are associated with it by handling **personal data** in accordance with applicable law and respecting the principles set out in Part II of this policy.

This policy sets out what is expected from you. Amongst other things it outlines the other policies and guidelines that have been put in place to help you keep information safe, maintain proper records and uphold the rights of individuals.

This policy must be followed by all volunteers, ministers and staff who handle **personal data** relating to the Methodist Church. In order to protect people's privacy you will:

- read, understand and comply with this policy when handling **personal data**;
- take part in available training that is appropriate to your role; and
- keep up-to-date with the guidance produced or signposted by the **controllers**.

The **controllers** have produced a number of related policies and privacy guidelines available to help you interpret and act in accordance with this policy. You shall adopt and comply with all such related policies and privacy guidelines that may be introduced and notified to you from time to time.

3. SCOPE

Why does the Methodist Church need to handle personal data?

The Methodist Church holds personal information about its members, volunteers, ministers, staff, supporters, third party users and others in order to:

- Fulfil the Methodist Church's calling and more specifically to:
    - Respond to the gospel of God's love in Christ through Worship, Learning and Caring, Service and Evangelism as expressed in *Our Calling*
    - Provide pastoral support and care to its members
    - Further the purposes of the Methodist Church as defined in s.4 of the Methodist Church Act 1976
    - Provide activities and support for its members and the wider community
- Fulfil the Church's responsibilities to safeguard young people and vulnerable adults including safely recruiting and training volunteers and employees
- Fulfil its obligations and due diligence as an employer
- Enable the Church to fulfil the obligations placed on it under statute such as taxation and gift aid requirements and landlord and tenant obligations.

Who is accountable for this policy in the Methodist Church, and responsible for it being followed across the Connexion?

TMCP acts as the **controller** for all Local Churches, Circuits and Districts (who are deemed to be the "Data Processors" i.e. the people who deal with data/ information on behalf of the Methodist Church). This is for routine, day to day data protection matters. The Methodist Church in Great Britain (whose responsibility is delegated by Conference to the Methodist Council with the work being carried out by the Connexional Team) now acts as **controller** to cover those **processing** activities 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 Board of TMCP and the Methodist Council are responsible for overseeing this policy. These bodies will be the point of contact with the Information Commissioner's Office (ICO) and for any queries arising in respect of their corresponding registrations and about the policy for staff, members, volunteers and the public. As applicable, the **controllers** will develop related policies and privacy guidelines.

Pursuant to Standing Order 019 the District Synod, Circuit Meeting and Local Church Council are ultimately accountable for compliance with the Data Protection Acts, regulations and orders in force from time to time.

This means that all District Synods, Circuit Meetings, Local Church Councils or other responsible authorities of each body registered under TMCP's and the Methodist Church in Great Britain's notifications are responsible for ensuring those within their District, Circuit or Local Church who handle Personal Data comply with this policy and need to implement appropriate practices, processes, controls and training to ensure such compliance. Appropriate guidance and support to help them do this will be provided by the **controllers**.

District Synods are strongly encouraged to nominate an individual or individuals to act as "Data Champion". Such Data Champions will be responsible for encouraging good practice, promoting the merits of protecting privacy and assisting the **controllers** with compliance. Circuits and Local Churches will consider whether they need to nominate individuals at a local level to help volunteers and staff to comply.

Where to go for help?

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

You must always contact the **appropriate controller** (the Connexional Team – Data Protection for issues relating to safeguarding, complaints and discipline and TMCP Data Protection for all other data protection matters) in the following circumstances:

- if there has been a **personal data** Breach (*Section 4.6.2* below);
- if you receive any requests from individuals relating to their **personal data** rights such as a subject access request (SAR) (see *Section 4.8*); and

- whenever you are engaging in a significant new, or change in, **processing** activity which is likely to require a data protection impact assessment (DPIA) (see *Section 7* below) or plan to use **personal data** for purposes other than what it was collected for.

You should also contact the **appropriate controller** if you are unsure what to do so that further guidance can be provided including but not limited to:

(a) if you are unsure of the lawful basis which you are relying on to **process personal data** (including the legitimate interests used by the Church) (see *Section 4.1* below);

(b) if you need to rely on Consent and/or need to capture Explicit Consent (see *Section 6* below);

(c) if you need to draft Fair Processing Notices (see *Section 4.1.1* below);

(d) if you are unsure about the retention period for the **personal data** being **processed** (see *Section 4.5* below);

(e) if you are unsure about what security or other measures you need to implement to protect **personal data** (see *Section 4.6.1* below);

(f) if there has been a **personal data** Breach (*Section 4.6.2* below);

(g) if you are unsure on what basis to transfer **personal data** outside the EEA (see *Section 4.7* below);

(h) if you need any assistance dealing with any rights invoked by a data subject (see *Section 4.8*);

(i) whenever you are engaging in a significant new, or change in, **processing** activity which is likely to require a Data Protection Impact Assessment (DPIA) (see *Section 7* below) or plan to use **personal data** for purposes others than what it was collected for;

(j) if you need help complying with applicable law when carrying out direct marketing activities (see *Section 8* below); or

(k) if you need help with any contracts or other areas in relation to sharing **personal data** with third parties (including our vendors) (see *Section 9* below).

Part II – Data Protection Principles

4. PERSONAL DATA PROTECTION PRINCIPLES

The Methodist Church is committed to ensuring that **personal data** is used and managed appropriately. Together we adhere to the principles relating to **processing** of **personal data** set out in the GDPR which require **personal data** to be:

- **Processed** lawfully, fairly and in a transparent manner (**Lawfulness, Fairness and Transparency**). See 4.1.
- Collected only for specified, explicit and legitimate purposes (**Purpose Limitation**). See 4.2.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which it is **processed** (**Data Minimisation**). See 4.3.
- Accurate and where necessary kept up to date (**Accuracy**). See 4.4.
- Not kept in a form which permits identification of **data subjects** for longer than is necessary for the purposes for which the data is **processed** (**Storage Limitation**). See 4.5.
- **Processed** in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful **processing** and against accidental loss, destruction or damage (**Security, Integrity and Confidentiality**). See 4.6.
- Not transferred to another country without appropriate safeguards being in place (**Transfer Limitation**). See 4.7.
- Made available to **data subjects** and **data subjects** allowed to exercise certain rights in relation to their **personal data** (**Data Subject's Rights and Requests**). See 4.8.

You must be able to demonstrate compliance with the data protection principles listed above (this is known as "Accountability").

4.1. LAWFULNESS, FAIRNESS, TRANSPARENCY

4.1.1 LAWFULNESS AND FAIRNESS

The Methodist Church is committed to ensuring that **personal data** is **processed** lawfully, fairly and in a transparent manner in relation to the **data subject**.

The Methodist Church makes use of the most appropriate legal basis when **processing** different categories of **personal data** for different purposes. The [Methodist Privacy Policy] states which of the six lawful bases should be used in different circumstances to ensure that **personal data** is **processed** fairly and without adversely affecting the **data subject**.

This means that you may only collect, **process** and share **personal data** fairly and lawfully and for specified purposes. The six lawful bases or specific purposes that you are most likely to use in the context of the Methodist Church are set out below:

- the **processing** is necessary for the performance of a contract with the **data subject** e.g. pay employees

and make pension contributions under an employment contract – refer to Lawful Basis Fact Sheet 1 - Contractual;

- to meet legal compliance obligations e.g. keeping records of marriages – refer to Lawful Basis Fact Sheet 2 - Legal Obligation;

- to pursue legitimate interests for purposes providing they are not overridden because the interests or fundamental rights and freedoms of **data subjects** are prejudiced. The purposes for which **personal data** is **processed** for legitimate interests need to be set out in applicable Privacy Notices or Fair Processing Notices e.g. collecting and sharing membership information amongst members - refer to Lawful Basis Fact Sheet 3 - Legitimate Interests; or

- the **data subject** has given his or her Consent e.g. sharing details about members with third parties – refer to Lawful Basis Fact Sheet 4 - Consent;

and in rare cases:

- to perform a task in the public interest e.g. a safeguarding situation where information needs to be shared outside of the Methodist Church.

- to protect the **data subject**'s vital interests e.g. where information is shared with the emergency services in a life or death situation;

You must identify and document the legal ground being relied on for each **processing** activity in accordance with the guidelines on **Lawful Bases for Processing Personal Data**.

4.1.2 TRANSPARENCY (NOTIFYING DATA SUBJECTS)

The Methodist Church is committed to ensuring that **data subjects** are provided with the detailed, specific information required under GDPR.

You must provide the specific information required under GDPR using appropriate Privacy Notices to ensure that the required information is provided in a form that is concise, transparent, intelligible, easily accessible, and in clear and plain language so that a **data subject** can easily understand.

You must use the **Methodist Church's Template Privacy Notice** (or similar comparable templates) and comply with the **controllers**' guidelines on drafting and use of Privacy Notices.

4.2. PURPOSE LIMITATION

You must only collect **personal data** for explicit and legitimate purposes explained to the **data subject** in an appropriate Privacy Notice (see 3.1.2).

You must not use **personal data** for new, different or incompatible purposes unless you first inform the **data subject** of the new purposes and if necessary obtain their consent.

This means that if a member gives you their photograph for one purpose (to put in the Local Church newsletter for example), you would not be able to use this photograph for another purpose without informing the individual and explaining what you now intend to do with it. If the new purpose included sharing the information with a third party e.g. an article in the local paper then consent may be required.

4.3. DATA MINIMISATION

The Methodist Church is committed to ensuring that **personal data** is adequate, relevant and limited to what is necessary in relation to the purposes for which it is **processed**. You will only collect **personal data** that you require for a specific task (relevant and necessary data). You will not collect more information than you actually need (not collect excessive data).

You must ensure that when **personal data** is no longer needed for specified purposes, it is deleted or anonymised in accordance with the Methodist Church's guidelines on data retention.

This means that if you are arranging a pastoral visit, you only need to collect sufficient personal information to enable the pastoral visitor to provide pastoral support. You are meeting the spiritual needs of the church member rather than providing medical care requiring detailed medical information.

4.4. ACCURACY

You will ensure that the **personal data** you use and hold is accurate, complete, kept up to date and relevant to the purpose for which it was collected. You must check the accuracy of any **personal data** when you first collect it and at regular intervals afterwards e.g. annually in the case of Circuit and District Directories or quarterly in the case of Circuit plans. You must take all reasonable steps to destroy or amend inaccurate or out-of-date **personal data**.

You will notify those responsible for central databases and directories of any changes without delay so that these can be updated promptly. This would include databases held by the Connexional Team and TMCP including the Connexional Database and the Trust Information System (TIS) respectively.

4.5. 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.

The Methodist Church will maintain guidelines and procedures on data retention to ensure **personal data** is deleted after a reasonable time for the purposes for which it was being held, unless a law requires such data to be kept for a minimum time. Different categories of data will be kept for different periods of time and you must comply with the Methodist Church's guidelines on data retention.

You will take all reasonable steps to destroy or erase from your computer systems all **personal data** that you no

longer require in accordance with all the Methodist Church's guidelines, retention schedules and policies from time to time.

4.6. SECURITY INTEGRITY AND CONFIDENTIALITY

4.6.1 PROTECTING PERSONAL DATA

You are responsible for protecting the **personal data** you hold and making sure that data security is maintained, in line with the [Methodist Data Security Policy] and any associated guidelines or procedures that may be issued by the **controller** from time to time.

You must implement reasonable and appropriate security measures against unlawful or unauthorised **processing** of **personal data** and against the accidental loss of, or damage to, **personal data** in accordance with the **Data Security Policy**. You must exercise particular care in protecting Special Category Data and Criminal Offence Data from loss and unauthorised access, use or disclosure.

You must maintain data security by protecting the confidentiality, integrity and availability of the **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).

(b) **Personal data** is accurate and suitable for the purpose for which it is **processed** (Integrity).

(c) authorised users are able to access the **personal data** when they need it for authorised purposes (Availability).

You will need to take practical steps to protect **personal data** in accordance with the Data Security Policy. Examples of best practice include:

- Regularly backing-up computer files;
- Ensuring live and back-up files are secure e.g. password protected;
- Operating a "clean desk" policy;
- Keeping paper records and USB sticks (particularly those containing Special Category Data and Criminal Offence Data) in locked filing cabinets or cupboards or in other secure locations;
- Not leaving paper records or electronic devices such as laptops, USB sticks and work phones on public transport;
- Disposing of **personal data** safely e.g. by shredding documents and emptying email recycling folders.

4.6.2 REPORTING A PERSONAL DATA BREACH

A **"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 breach** e.g. emailing **personal data** to the wrong person; or leaving **personal data** in a public place where others can access it.

If you know or suspect that a **personal data breach** has occurred, immediately contact the **appropriate controller** (when directed by the Data Breach Policy) so that they can help you to investigate the matter and take appropriate steps in line with the Data Breach Policy and any accompanying guidelines and procedures. You will record all **personal data breaches** on your local Data Breach Record. The **appropriate controller** will notify d**ata subjects** or any applicable regulator where there is a legal requirement to do so. You should preserve all evidence relating to the potential **personal data breach**.

4.7. TRANSFER LIMITATION

EEA: the 28 countries in the EU, and Iceland, Liechtenstein and Norway.
Safe List: the list of countries outside the EEA from time to time that the European Commission has decided possess an adequate level of protection for **personal data**. Refer to the *European Commission's data protection website* [https://ec.europa.eu/info/law/law-topic/data-protection_en] for an up-to-date list. Note that Guernsey, the Isle of Man and Jersey appear on the Safe List.

If you intend to transfer **personal data** outside the EEA, and unless the country appears on the Safe List, additional safeguards will need to be followed in order to ensure that the level of data protection afforded to individuals by the GDPR is not undermined. You will transfer **personal data** originating in one country across borders when you transmit, send, view or access that data in or to a different country e.g. if a presbyter or volunteer is to go on an exchange programme.

You must comply with any guidelines that the Methodist Church issues from time to time on cross border data transfers.

4.8. DATA SUBJECT'S RIGHTS AND REQUESTS

The Methodist Church respects the rights of individuals (**data subjects**) under GDPR including to:

(a) withdraw Consent to **processing** at any time where consent is relied upon as the sole lawful basis;

(b) receive certain information about the **controller's**, **processing** activities;

(c) request access to their **personal data** held by a District, Circuit or Local Church (known as a subject access request or SAR);

(d) prevent use of their **personal data** for direct marketing purposes;

(e) ask for their **personal data** to be erased (right to be forgotten) if it is no longer necessary in relation to the purposes for which it was collected or **processed** or to rectify inaccurate data or to complete incomplete data;

This means the individual has the right to ask for their **personal data** to be erased. However, this is not an "absolute" right and you need to ensure that such requests are considered carefully. You do not need to erase **personal data** in circumstances including where the **processing** is necessary to:

- comply with a legal obligation;
- perform a task carried out in the public interest;
- establish, exercise or defend legal claims; or
- where an individual objects to the **processing** of their **personal data** on the basis of legitimate interests but you can show that there is an overriding legitimate interest to continue this processing.

(f) restrict **processing** in specific circumstances e.g. pending the outcome of a dispute about the accuracy of **personal data** or challenge to **processing** g on the basis of legitimate interests;

(g) challenge **processing** which has been justified on the basis of our legitimate interests;

(h) prevent **processing** that is likely to cause damage or distress to the **data subject** or anyone else;

(i) be notified of a **personal data** Breach which is likely to result in high risk to their rights and freedoms; and

(j) make a complaint to the supervisory authority (at the date of this policy this is the Information Commissioner's Office (ICO)); and

You must verify the identity of an individual requesting data under any of the rights listed above (do not allow third parties to persuade you into disclosing personal data without proper authorisation). If in doubt you must contact the appropriate controller.

You must immediately forward any Data Subject Access request (SAR) you receive to the **appropriate controller** and comply with the SAR's Policy and any other guidelines and procedures that are in place from time to time.

Part III
Accountability – Your responsibilities and those of TMCP and the Connexional Team

5. ACCOUNTABILITY

The Methodist Church has established a framework for data protection compliance comprising the provision of guidance, policies and procedures, template documents, integrating data protection into internal documents, data championing, training volunteers, ministers and staff, monitoring the privacy measures and conducting periodic review to assess compliance.

5.1 What are TMCP and the Connexional Team's responsibilities as controller?

The **controllers** commit to:

Compliance

- Implement this policy and make sure it complies with data protection legislation.
- Co-operate with the relevant regulatory bodies and be a point of contact.
- Ensure this policy is up to date.
- Regularly test systems and processes to assess compliance.

Training

- Ensure volunteers and staff have access to appropriate training and guidance to enable them to comply with data privacy laws and help you to comply with this policy.

Record keeping

- Facilitate the keeping of full and accurate records of all your data **processing** activities by providing you with the template registers and guidelines to keep records

Security and retention

- Keep the Methodist Church's Data Retention Schedule up-to-date.

Breach

- Provide guidance and support to you in the event of a suspected **personal data breach** to enable you to deal with the suspected **personal data breach** in accordance with the Breach Policy and contact the **data subject** or ICO as required.

Rights

- Provide guidance and support to you in the event of you notifying us about any data protection requests or complaints which may arise.

Risk-based approach to processing

- Use a risk-based approach to **processing** activities where you notify us about them including the use of data protection impact assessments (DPIAs) for high-risk **processing** activities where necessary e.g. the transfer of **personal data** onto a new computer system.

5.2 What are your responsibilities?

As a volunteer, minister or member of staff within a Local Church, Circuit or District, if you handle **personal data** as part of your role you must:

Compliance

- Follow this policy and relevant procedures whenever **personal data** is being used for planning and delivering Church activities.
- Follow the procedures, guidance and codes of practice introduced by the **controllers** about the collection and use of **personal data**.
- Think about why you need to handle **personal data** and make sure you use as little data as you need to carry out your task.

Training

- You must undergo the data privacy related training that is made available to you and ensure those within your Local Church, Circuit or District who handle **personal data** undergo similar training.
- You must regularly review all the systems and processes under your control to ensure they comply with this policy and check that adequate governance controls and resources are in place to ensure proper use and protection of **personal data**.

Record keeping

You must keep and maintain accurate records reflecting your **processing** in accordance with the Methodist Church's record keeping guidelines. These include:

- Name and contact details of the **controller** (in the Privacy Notice)
- Purposes of the **processing** (in the Privacy Notice)
- Description of the categories of individuals and categories of **personal data** being **processed** (in the Privacy Notice or Data Mapping Form)
- Categories of recipients of **personal data** when disclosed (in the Privacy Notice or Data Mapping Form)

- Records of the lawful bases being relied upon for **processing** (through the Lawful Bases Register)
- Records of **data subjects'** Consents and procedures for obtaining Consents (through the Consent Record)
- Details of transfers to parties outside the EEA including documentation of the transfer mechanism safeguards in place
- Description of security measures put in place (in the Data Mapping Form)
- Retention periods (in the Privacy Notice, Retention Schedules and Data Mapping Form)

Security and retention

- reduce as much as possible the likelihood of a **personal data breach** by maintaining good data handling practices with adequate control measures in place i.e. following the Data Security Policy, guidelines and procedures.
- make sure that **personal data** is destroyed safely (in line with the Methodist Church's Data Retention Schedule

Breach

- report **personal data** Breaches (in accordance with Section 4.6.2 of this policy) to the **appropriate controller** immediately on discovery
- establish, maintain and follow guidance on effective systems for reporting, monitoring and responding to any emergencies that could arise in relation to **personal data**

Rights

- inform the **appropriate controller** immediately if you receive a request from a **data subject** for information held or used about them
- inform the **appropriate controller** immediately if you receive complaints from **data subjects** relating to the use of their **personal data** and follow the **controller's** directions.

Part IV – Specific Issues

6. CONSENT

"Consent" is an agreement which must be freely given, specific, informed and be an unambiguous indication of the **data subject's** wishes by which they, by a statement or by a clear positive action, signifies agreement to the **processing** of **personal data** relating to them.

"Explicit Consent" is consent which requires a very clear and specific statement (that is, not just action).

Consent is just one of the lawful bases set out in the GDPR on which **personal data** can be **processed**.

You will only rely on Consent if there are no other lawful bases on which you can rely following the guidelines on Lawful Bases for processing personal data.

If you need to rely on Consent you will ensure that you obtain the **data subject's** clear agreement either by a statement or positive action to the **processing** of their **personal data**. You recognise that Consent requires affirmative action so silence, pre-ticked boxes or inactivity are insufficient. Consent must be kept separate from any other matters set out in an agreement with the **data subject**.

Data subjects must be easily able to withdraw their Consent at any time and withdrawal must be promptly honoured. You should ask the **data subject** to reconfirm their Consent if you intend to **process** their **personal data** for a different and incompatible purpose which was not disclosed when the **data subject** first consented.

Unless you can rely on another legal basis of **processing**, Explicit Consent is usually required for Processing Special Category Data and for transferring personal information overseas e.g. if a volunteer is to work overseas and information about them is sent beforehand. Where Explicit Consent is required, you must issue a Privacy Notice to the **data subject** to capture Explicit Consent.

You will need to evidence Consent captured and keep records of all Consents to demonstrate compliance with Consent requirements.

7. PRIVACY BY DESIGN AND DATA PROTECTION IMPACT ASSESSMENT (DPIA)

Data Protection Impact Assessment (DPIA): tools and assessments used to identify and reduce risks of a data processing activity. DPIA can be carried out as part of "Privacy by Design" and should be conducted for all major system or business change programs involving the **processing** of **personal data**.

Privacy by Design: implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the GDPR.

Pseudonymisation or Pseudonymised: 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.

The Methodist Church is committed to implementing Privacy by Design measures in cases where the Church handles (**processes**) **personal data** by ensuring that appropriate measures (like Pseudonymisation) are implemented in an effective manner, to ensure compliance with the data privacy principles set out in Part II of this policy.

You must assess what Privacy by Design measures can be implemented on all programs/systems/processes that **process, personal data** by taking into account matters including the cost of implementation, the nature, scope, context and purposes of **processing** and the risks of varying likelihood and severity for rights and freedoms of

data subjects posed by the **processing**.

You should conduct a DPIA and discuss your findings with the **controller** before implementing major changes in systems involving the **processing** of **personal data** e.g. use of new IT systems or large scale **processing** of Special Category Data and/or Criminal Offence Data.

A DPIA must include:

- a description of the **processing**, its purposes and the legitimate interests if appropriate;
- an assessment of the necessity and proportionality of the **processing** in relation to its purpose;
- an assessment of the risk to individuals; and
- the measures in place to mitigate risk and demonstrate compliance.

You must comply with the **controllers'** guidelines on DPIA and Privacy by Design.

8. FUNDRAISING

The Methodist Church commits to ensuring that any fundraising activities are carried out in accordance with the Methodist Church's guidelines on fundraising.

You must comply with the Church's guidelines on fundraising [http://www.methodist.org.uk/our-work/support-our-work/fundraise/].

Note that a **data subject's** prior Consent is required for electronic direct marketing (for example, by email, text or calls to telephone preference numbers). The rules catch any fundraising that a Local Church, Circuit or District may decide to undertake. Refer to the Lawful Bases Fact Sheet 8 - Privacy and Electronic Communications Regulations (PECR) 2003**.**

You must explicitly offer the **data subject** the right to object to receive such fundraising or other "direct marketing". You must make this offer in an intelligible manner so that it is clearly distinguishable from other information.

A **data subject's** objection to direct marketing must be promptly honoured. If anybody "opts out" at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences e.g. their objection, are respected in the future.

9. SHARING PERSONAL DATA

The Methodist Church acknowledges that sharing **personal data** with third parties is not permitted unless certain safeguards and contractual arrangements have been put in place.

You may only share the **personal data** in your possession with another volunteer, minister or staff member if the recipient has a "need to know" the information relate to their role (confidentiality).

You may only share the **personal data** you hold with third parties, such as other organisations or individuals who use Methodist premises, the local community or service providers if:

- they need to know the information e.g. to provide services to church members or allow the Church to further Mission by publicising events to the local community;

- sharing the **personal data** complies with the Privacy Notice provided to the **data subject** and, if required, the **data subject's** Consent has been obtained;
- In the case of a third party organisations (not the general public), the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures and

- if the third party is a contracted service provider, there is a fully executed written contract that contains the Template GDPR Third Party Clauses (to be provided from time to time).

Common examples of this within the Methodist Church are where Directories or Circuit Plans containing contact details i.e. **personal data** for Managing Trustees and other volunteers are left in the foyer or published on the Local Church's website. To do this you need to ensure that consent is in place. However, there is **no need for consent to be obtained from Ministers in Full Connexion, probationers** or **office holders** whose contact details would need to be in the public domain to fulfil specific Church functions e.g. the treasurer or bookings secretary.

You must comply with the **controller's** guidelines on sharing data with third parties.

Part V – Changes to and acceptance of this policy

10. CHANGES TO THIS PRIVACY STANDARD

This policy will be updated from time to time. We will try to give notice via TMCP's News Hub and other means of communication 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.

11. ACKNOWLEDGEMENT OF RECEIPT AND REVIEW

I, [NAME], acknowledge that on [DATE], I received and read a copy of the [Methodist Church's [policy] and understand that I am responsible for knowing and abiding by its terms and ensuring compliance by the members of my [Local Church] OR [Circuit] OR [District]. I understand that the information in this policy is intended to help volunteers and staff work together effectively and assist in the use and protection of **personal data**.

Signed …….

Printed Name …….

For and on behalf of the [Church Council] OR [Circuit Meeting] or [District Synod]

of …… *(name of managing trustee body)*
Date …….

END OF DOCUMENT