Data Protection

Contact Name and Details	Louise Wilkins, Conference Officer for Legal and Constitutional Practice wilkinsl@methodisthchurch.org.uk
Status of Paper	Final
Action Required	Decision
Resolutions	39/1. The Council receives the report. 39/2. The Council adopts the Data Protection Policy for the Connexional Team. 39/3. The Council agrees to the principle of a requirement being included within Standing Orders for managing trustees to adopt the precedent policies and notices of the Trustees for Methodist Church Purposes as the data controller.

Summary of Content

Subject and Aims	To provide the Council with an update on the work undertaken to date on preparations for the forthcoming General Data Protection Regulation (GDPR) and the Data Protection Bill. To inform the Council of its responsibilities as the body responsible for ensuring the Team complies with the requirements of the new data protection legislation. To present the Council with an updated Data Protection Policy for the Connexional Team
Main Points	• Working group formed between Trustees for Methodist Church Purposes (TMCP) and the Connexional Team to consider GDPR compliance across the Connexion. An existing member of staff has been seconded to the role of Data Protection Implementation Officer to support the working group. • The Methodist Church in Great Britain has been registered as the data controller for the Connexional Team. • An overview of steps taken to ensure compliance with data protection legislation and preparations for the GDPR within the Team. A Data Protection Policy for the Connexional Team is presented to the Council for adoption.
Background Context	SRC/17/27 Data Protection SRC/18/02 Data Protection Update
Consultations	Trustees for Methodist Church Purposes

Summary of Impact

Standing Orders	It is anticipated that changes will need to be made to SO 019
Financial	The budget for 2017/18 and 2018/19 includes additional resource for preparation for and compliance with GDPR.
Legal, including impact on other jurisdictions	None (on the basis that the Connexional Team and wider Connexion are able to demonstrate compliance with GDPR).
Wider Connexional	Compliance required across the Connexion
External (eg ecumenical)	Conversations are being held with ecumenical partners particularly around Local Ecumenical Partnerships
Risk	A breach of the new regulations and legislation could result in significant fines and reputational damage.

Data Protection

1. This paper provides the Council with an update on work required to ensure compliance with current data protection legislation and preparations for compliance with the General Data Protection Regulation that come into force in May 2018, and the responsibilities of the Council as the trustee body that will need to ensure the Team complies with its responsibilities.

2. The Methodist Church has been registered as the data controller for the Connexional Team on the basis this is the national charity so the body that has to register with the Information Commissioner's Officer (ICO). Until now the Trustees for Methodist Church Purposes (TMCP) has been registered as the data controller for local churches, circuits and districts and the Team. However, it was evident following discussions that TMCP has no control over personal data held by the Team and therefore it was necessary to amend the registration. TMCP continues to be the data controller for local churches, circuits and districts and is therefore leading on the advice being provided to the wider Connexion regarding preparation for and compliance with GDPR.

Preparations for the GDPR within the Connexional Team

3. A working group of the Connexional Team meets regularly to ensure the necessary steps are being taken to prepare for May 2018. Data mapping has been completed by the Lead Staff providing the working group with a clearer picture of the personal data processed in each of the Team's activities. The mapping has been used to determine the legal basis for processing in each area of the Team and shape the updated privacy notice that will be uploaded to the website before the GDPR deadline on 25 May 2018.

4. Training has been provided to all members of the Team and basic training now forms part of the induction process. By the time the Council meets, additional training will have been provided to the Lead Staff group as to the implications of GDPR on each area of work and the steps lead staff need to take. It is being stressed within such meetings that compliance with data protection requirements is everyone's responsibility not just the Data Protection Officer. The Connexional Team Data Protection Policy has been updated in accordance with GDPR requirements and is supplied to the Council for adoption.

5. Guidance is currently being produced for the chairs of connexional committees and working parties on steps to be taken in respect of the personal data held processed by these committees and working parties. This work includes the Connexional Complaints Panel and Discipline Committees.

Responsibilities of the Council

6. All organisations that process personal data must have a data controller registered with the ICO and for the Team this is now the Methodist Church as the national charity. The Council, as the employing/appointing body of the Team and body that fulfils the responsibilities of the Conference between its meetings, must ensure the Team is complying with GDPR and is able to demonstrate this compliance. One of the new requirements in terms of data protection that the GDPR introduces is the need for accountability. The accountability requirement means that the data controller must be able to provide evidence of steps it has taken to protect data and ensure the principles of data protection are complied with eg evidence of consent is held or a record of the conclusion as to why the processing of personal data without consent was considered to be a legitimate interest.

7. Members of the Council are likely to want to consider the guidance produced by TMCP that has been drafted to ensure it is directly applicable to the life of a Local Church, Circuit and District. However in order to assist members of the Council in beginning to understand GDPR requirements, an overview is provided as an annex to this paper.

8. The Connexional Data Protection Policy before the Council also outlines the control measures in place in the Team, and the reporting mechanisms in place to ensure accountability and oversight by the Council. The adoption of a new Data Protection Policy by the Council for the Team that is compliant with GDPR is a vital step towards ensuring compliance from 25 May 2018.

GDPR compliance across the Connexion

9. A working group has been established between members of staff from TMCP and the Connexional Team to ensure appropriate guidance and precedent documentation is available to the wider Connexion in advance of May 2018. To support the working group in the delivery of this task, a Data Protection Implementation Officer is now in post. This post reports to the Conference Officer for Legal and Constitutional Practice and has been filled by an existing member of staff being seconded to this role.

10. TMCP now has various guidance notes available on their website and is sending updates to District Chairs and Superintendents and others who have signed up for updates. Guidance available include 9 Steps for Managing Trustees, Dos and Don'ts, GDPR Guidance Note and FAQs. Updates will continue to be circulated as additional guidance for areas specific to Methodist Churches is produced.

11. A presentation covering the key compliance areas was made to the District Chairs in March 2018 and other opportunities are being sought for TMCP staff to offer face to face training although it is anticipated that the majority of the training will be provided through webinars to be available on the TMCP website.

12. The Working Party is suggesting that Districts should nominate someone to hold the role of Data Protection Champion to assist with compliance across the District and to point managing trustees in the direction of guidance and the webinars.

GDPR standards for Managing Trustees

13. Standing Order 019 will be reviewed and any amendments taken to the Conference in 2018 by the Law and Polity Committee. The Standing Order currently states:-

> **019 Data Protection.** (1) All connexional, district, circuit, local and other Methodist bodies, and all societies, institutions and other organizations subsidiary or ancillary to the Methodist Church shall comply with the Data Protection Acts for the time being in force and with any regulations or orders made or having effect under such legislation.
> (2) In particular, every such body shall be registered, where required to do so, with the relevant Commissioner or other authority, as specified in clause (3) below.
> (3) In England and Wales, and in Scotland, any such body may be registered separately by giving the required notification directly to the relevant authority (the Information Commissioner's Office), and shall do so if the notification by the Trustees for Methodist Church Purposes ('the Board') is not sufficiently comprehensive for its purposes. Every such body which is thus registered directly with the Commissioner shall notify the Board in writing of that fact. Every such body which has not so notified the Board will be registered under the

Board's notification. In other jurisdictions, any such body must register separately with the appropriate authority as required by the relevant legislation.
(4) The Synod, Circuit Meeting, Church Council or other responsible authority of each body registered under the Board's notification shall indemnify the Board, as Data Controller, against the consequences of any breach of the Data Protection legislation, regulations or orders committed by any officer (ministerial or lay), meeting or committee of that body or by any other person or persons holding data relating to its affairs.

14. One matter that the Data Protection Working Party has considered is the question of how far TMCP as the registered data controller can ever have absolute control over the personal data being processed by managing trustees. Consideration has therefore been given as to whether managing trustees will be asked to provide evidence to TMCP as the data controller that the managing trustee body has adopted the precedent data protection policy and privacy notice. This might be considered necessary in light of the accountability requirement in GDPR meaning TMCP as data controller needs to be able to demonstrate compliance. GDPR will also mean that both data controllers and data processors can be fined by the ICO and therefore it seems prudent for TMCP to be able to demonstrate that it, as controllers has done all that can be expected of it through the issuing of precedent documents and guidance.

15. The Council is asked whether it would in principle agree to a proposal being made to the Conference that managing trustees are required to adopt the precedent policies and notices necessary for compliance with GDPR. If the Council is content to agree to this principle then further consideration will be given to exactly what it would be necessary adopt and any Standing Order amendments to reflect a requirement for adoption of particular precedent policies or notices would be taken to the Conference in 2018. Consideration will also need to be given to the question of what should happen if a managing trustee body has a legitimate reason for wanting to adopt a different policy or notice. There is clearly further work to be undertaken to explore the implications of having such a requirement and this will be referred to the working party.

*****RESOLUTIONS**

39/1. The Council receives the report.

39/2. The Council adopts the Data Protection Policy for the Connexional Team.

39/3. The Council agrees to the principle of a requirement being included within Standing Orders for managing trustees to adopt the precedent policies and notices of the Trustees for Methodist Church Purposes as the data controller.

Data Protection Policy – Connexional Team

1. Aim

The Connexional Team (hereafter "the Team") holds a large amount of personal data in order to resource the wider connexion and fulfil its functions. The Methodist Council as the employer and appointing body of the Connexional Team has ultimate responsibility for ensuring that the Team is compliant with the requirements of data protection legislation. Data is held on a number of individuals ranging from ministers, volunteers, staff, church members and officeholders and those who are interested in and supportive of the work of the Methodist Church.

This policy aims to ensure the operations carried out by the Connexional Team comply with the Data Protection Act 1998 and subsequent legislation including the General Data Protection Regulations (GDPR) (hereafter "data protection legislation") and respects the principles and rights of individuals. This policy outlines the control measures and procedures and structures in place for monitoring compliance.

2. Principles

Under the GDPR, the data protection principles set out the main responsibilities for organisations. Article 5 of the GDPR requires that personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;
b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
f) 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(2) requires that:
"the controller shall be responsible for, and be able to demonstrate, compliance with the principles."

3. Responsibility for Compliance

A framework for data protection compliance has been developed to demonstrate the controls measures in place to ensure the Council is holding the Connexional Team accountable for complying with data protection legislation

Within the Team each Lead Staff member holds the role of Data Protection Champion with responsibility for promoting and ensuring good data protection practice to their staff. The Data Protection Officer for the Team shall ensure that compliance with the principles can be demonstrated. Any legal queries or subject access requests made to the Team will be overseen by the Conference Officer for Legal and Constitutional Practice who shall obtain external legal advice as required. The Connexional Secretary as Risk Champion for the Team holds the role of Data

Protection Champion on the Senior Leadership Group to ensure that all decisions taken by the Senior Leadership Group consider the implications for data protection and the risks associated with a breach of the data protection principles are mitigated as far as possible. An annual report shall be made to the Strategy and Resources Committee and the Council on compliance with the data protection principles and any concerns about compliance shall be raised with the Strategy and Resources Committee and the Methodist Council as considered necessary by the Data Protection Officer.

The data controller for the Connexional Team is the Methodist Church whose notification with the Information Commissioner can be found here: https://ico.org.uk/ESDWebPages/Entry/ZA303456

All Team members will adhere to the Data Protection Policy and any policies referred to in this document. Failure to do so will result in disciplinary action.

Monitoring
It is the responsibility of all line managers in the Connexional Team to monitor compliance with the policy with any concerns or queries referred to the Team's Data Protection Officer.

Staff Training
All staff are required to carry out data protection training. This is included in the induction process for new staff members.

Review
This policy and accompanying procedures will be reviewed every two years by the Data Protection Officer and the Methodist Council will be required to adopt an amended policy. The review will ensure that the policy and procedures comply with all current legislation, regulatory guidance and recommended good practice.

4. Privacy Notice

The Connexional Team is committed to informing individuals of their rights and how and why the Team processes personal data, which is documented in the Team's Privacy Notice available on www.methodist.org.uk.

This notice provides individuals with information about the purposes of processing personal data with the Connexional Team, including lawful basis, security measures and retention and destruction of personal data.

This notice is made available at the point of data collection where required in both electronic and paper format.

5. Information Categorisation, Recording and Review

Information processed by the Connexional Team will be suitably categorised to determine where processing of sensitive data occurs and to enable suitable security measures are put in place for each category. This is reflected in the *Practice Guidelines for Information Management in the Connexional Team*.

Data processing activities including the legal basis for processing will be documented and reviewed every two years.

6. Sharing Data

Data will not be shared outside of the Methodist Church, except where required to do so by law, or with trusted third parties where necessary to communicate with our members, office holders and

volunteers (such as mailing companies for postal communications or through small email campaigns or newsletters), and only once satisfied that any such use of data will accord with this policy. Explicit, informed consent will be sought from individuals whenever and wherever required in accordance with data protection legislation.

Procurement/ Outsourcing

When entering into contracts with third parties that necessitate sharing personal data suitable data sharing agreements and security arrangements are put in place to in accordance with the Team's outsourcing procedures and Procurement Policy.

7. Data Accuracy

Databases used by the Connexional Team are developed to comply with data protection legislation. The accuracy of data held by the Connexional Team supplied from local churches, circuits and districts is dependent upon information being shared to the Team from local areas.

Staff in the Team will update the database promptly when information is shared to them, including the regular review of connexional mailing lists.

8. Security

Electronic format

Users of Connexional Team IT systems must comply with the security measures specified in the Team's *Information Security Policy*. These measures include the back-up all computer files that are created or updated. Both live and back-up copies of files are kept safe and secure when not actually in use.

Specific instructions regarding the use of IT equipment including the use of secure passwords is contained within the Team's *Use of Computers and other Office Equipment Policy*.

Paper format

Personal data of any description should not be left unattended and on open view in accordance with the Team's *Clean Desk Guidance*.

Sensitive data retained in paper-based systems will, when not in use be securely stored in locked cupboards and filing drawers.

Remote Working/ Working from home

The aforementioned provisions of the policy relating to security in both electronic and paper format apply to staff when working remotely or working from home.

9. Retention and Disposal of Data

The Connexional Team will only retain personal data for as long as necessary. Retention Schedules for the Connexional Team outline the periods that each category of data is retained for. The schedules are set in accordance with statutory requirements as well those set out in the *Constitutional Practice and Discipline of the Methodist Church*. The retention schedules will be reviewed regularly and are available on the staff intranet site.

Guidance on managing and disposing of data is included within the *Practice Guidelines for Information Management in the Connexional Team*. Confidential information that is no longer required will be securely disposed of and shredded.

10. Rights of individuals

Unless subject to an exemption under the GDPR, individuals have the following rights with respect to their personal data:

- The right to request a copy of personal data which the Methodist Council holds about an individual;
- The right to request that the Methodist Council corrects any personal data if it is found to be inaccurate or out of date;
- The right to request personal data is erased where it is no longer necessary for the Methodist Council to retain such data;
- The right to withdraw consent to the processing at any time
- The right to request that the data controller provide the data subject with his/her personal data and where possible, to transmit that data directly to another data controller, (known as the right to data portability), (where applicable) [*Only applies where the processing is based on consent or is necessary for the performance of a contract with the data subject and in either case the data controller processes the data by automated means*].
- The right, where there is a dispute in relation to the accuracy or processing of personal data, to request a restriction is placed on further processing;
- The right to object to the processing of personal data, (where applicable) [*Only applies where processing is based on legitimate interests (or the performance of a task in the public interest/exercise of official authority); direct marketing and processing for the purposes of scientific/historical research and statistics*]
- The right to lodge a complaint with the Information Commissioners Office.

The Team regularly reviews its processes regarding the processing of data to be in accordance with data protection legislation and to allow individuals to exercise their rights.

On receipt of a Subject Access Request (SAR), the Team's *SAR Procedures* must be followed.

11. Requests for information about children

Data protection legislation confers additional security measures to be in place regarding data held about children, and the Methodist Church's Safeguarding Policy and Practice include suitable measures to protect such data.

General Data Protection Regulations (GDPR) – overview of application in the Connexional Team

Introduction

The General Data Protection Regulation (GDPR) will take effect in the UK on 25 May 2018. It replaces the existing law on data protection (the Data Protection Act 1998) and gives individuals more rights and protection in how their personal data is used by organisations, and therefore the Connexional Team must comply with its requirements. This document provides an overview of what is needed to comply with the GDPR and includes and considers how it will be implemented within the Connexional Team.

A. Underlying Principles,

The law is complex, but there are a number of underlying principles, including that **personal data**:

1. will be **processed** lawfully, fairly and transparently.
2. is only used for a specific processing purpose that the **data subject** has been made aware of and no other, without further consent.
3. collected on a data subject should be "adequate, relevant and limited." i.e. only the minimum amount of data should be kept for specific processing.
4. must be "accurate and where necessary kept up to date"
5. should not be stored for longer than is necessary, and that storage is safe and secure.

Explaining the jargon:
Personal data is information relating to a living individual, who can be identified directly from that data or indirectly by reference to other data held.
Processing is anything done with/to personal data, including storing it.
The **data subject** is the person about whom personal data are processed.
The **data controller** is the person or organisation who determines the how and what of data processing. The Methodist Church in Britain is the data controller for the Connexional Team.

B. Key Areas for application in the Connexional Team

1. There are several **legal bases for processing data**, of which consent is one. Others include legal obligation (e.g. safeguarding, contracts of employment etc), contract (e.g. contracts with caterers, cleaners etc), or legitimate interest (routine administration including ministers contact information and lists of church, circuit and district officers etc). For each area of processing, it is important to be clear on the legal basis for carrying out that processing. A data mapping exercise has been carried out across the Connexional Team for this purposes and a record will be obtained.

2. **Consent** may have to be obtained from people for some data processing; e.g. some newsletters or marketing emails and fundraising activities. This will need to be clear and unambiguous – some form of positive action to 'opt-in'. An implementation plan is being produced for the areas of the Team that undertake such processing.
3. Data subjects have a number of **rights**, including that of knowing how data is used by the data controller, of knowing what data is held about them, of correcting any errors and generally the right 'to be forgotten'. The Connexional Team will make provision for people to exercise these rights, including developing a Privacy Notice which will be available on the Methodist Church website and other points of data collection.

4. The GDPR introduces a stronger requirement on **accountability** and **data controllers.** This means that controllers must be able to show they are complying with the principles by providing evidence. For example, where processing takes place on the basis of consent, evidence of consent must be stored. Since consent should be specific to a "purpose", separate consent may be required to cover different areas of data processing within the Connexional Team. This will be included in the implementation plan.

5. Where data "reveals religious belief" it becomes special category data – which requires additional care with regard to processing. We await further guidance from the ICO as to what this means in the context of processing activities in church organisations. Until then the Working Party is working on the basis that not all data held by the Team is special category and someone's belief cannot be assumed just because of their employer. Even where special category data is being processed, there is a second legal basis upon which an organization can process the data without needing explicit consent. GDPR allows membership bodies that are not-for-profit to process special category data without explicit consent as long as it relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent.

6. Information security and disposal – procedures have been developed for managing data in both electronic and paper format, including how data should be stored and disposed of securely.