Personal Data Breach Policy (Interim)

In this interim policy:

"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.

"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**

A **personal data breach** could include, for example, emailing **personal data** to the wrong person; or leaving **personal data** in a public place where others can access it or losing a laptop or USB stick.

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

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

Preventative measures, training and record

In accordance with Step 8 of the 9 Steps for Methodist Managing Trustees to Take Now to Comply with GDPR and pending finalisation of the full Personal Data Breach Policy, **you** need to follow the guidance in this interim policy.

You need to be prepared to deal with any **personal data breaches**:

- Consider what systems can be put in place to minimise any potential **personal data breach** in accordance with the Data Security Policy. These include:
    - Ensuring electronic files are kept securely (e.g. pass worded, encrypted and appropriate virus, malware, anti-phishing software is loaded to protect electronic data);
    - Ensuring manual files are held in locked filing cabinets or other suitably secure cupboards;
    - Operating a "clear desk policy"

  and other such measures to prevent unauthorised access to data or even its loss.
- Ensure those handling **personal data** are trained in appropriate security measures so that they can help to look after the personal data of those involved in church life and using church premises.

- Use the model Managing Trustees' Personal Data Breach Register to record all instances of a **personal data breach** regardless of how small e.g. an email being sent to the wrong recipient.
- Review and provide training (further to the training being provided by the Working Party) to all those who deal with **personal data** in a Local Church, Circuit or District so that they know what has to be recorded and what has to happen in the event of a **personal data breach**.

What happens if **you know or suspect that a Personal Data Breach has occurred e.g.** ***personal information is lost or stolen?***