Berkshire & Hampshire Borders Methodist Circuit

Data Protection Policy

Introduction

The Methodist Church cares about the people whose data it holds and as a Connexional Church we need to work together to protect privacy.

The Trustees for Methodist Church Purposes (TMCP) have produced a "Data Protection Responsibilities in a Nutshell" leaflet - Data Protection Responsibilities in a Nutshell - Trustees for Methodist Church Purposes (tmcp.org.uk)

This leaflet summarises the steps that volunteers, ministers and staff within the Church need to take to protect each other's privacy and keep personal information safe and provides an overview of the responsibilities of those who handle personal information

It is important that everybody is aware of what they need to do to keep personal information safe and the resources that TMCP have made available to help them do that.

It is essential that TMCP's guidelines are followed.

On an annual basis in May there is a checklist that TMCP ask each church and the Circuit itself to complete to enable them to ensure them that the data protection procedures and policies are being followed.

Berkshire & Hampshire Borders Methodist Circuit

Data Protection – Quick reference guide for trustees

This guidance is a short overview of basic Dos and Don'ts when it comes to compliance. This is meant to be a list that Managing Trustees can quickly refer to and is not intended to be a detailed guidance note.

Dos

- Only collect personal data for the purpose for which it is required. e.g. name & email address of committee members to allow for communication.
- Once the purpose for which you hold personal data has expired, ensure that all records are securely deleted or destroyed. Paper documents should be cross-shredded and then disposed in a confidential waste bin. Electronic data should be permanently deleted.
- Review the information that you hold about any individual at least once a year. This will ensure that the information you hold is accurate and up to date.
- Always remember that a data subject has the right to see the information/data that is being held. You need to be careful as to what information is held and ensure that it can be retrieved quickly.
- You should ensure that all computers and other devices used to access personal data are password protected. It may be appropriate to password protect electronic documents for further security.
- Managing Trustees should ensure everyone is familiar with all data protection policies and procedures.
- Keep a record of any data breach using the Breach Record for Managing Trustees.
- Be safe; if you are not sure ask for advice from the Circuit Compliance Officer.

Don'ts

- Don't use **personal data** for a different purpose or store it indefinitely because you think it might be useful in the future.
- Don't keep inaccurate data as this is a breach of data protection legislation.
- Don't store or send personal data on removable media, such as a USB pen drive as these are easily lost or stolen.
- Don't write any comment about an individual that you cannot defend if challenged.
- Don't write passwords down and ideally change them at least every 60 days.
- Don't open emails from unknown sources. If the email appears suspicious, check with the sender by phone before reading and opening any attachments.
- Don't routinely pass on personal data to a third party without consent.
- Don't assume that a **data subject's** consent will last forever. They have the right to withdraw their consent for the processing of their data.

Remember to keep all personal data secure, confidential and treat it as if it were your own.