Guidance notes

Data Protection Do's and Don'ts Focus Note

Summary of Do's and Don'ts to help Managing Trustees comply with Data Protection legislation.

Updated Nov 21st 2018

Section A – Introduction

These Do's and Don'ts are for use alongside the detailed guidance specific to the Methodist Church which TMCP, working together with the Connexional Team have produced. This is available from the Data Protection page of TMCP's website. As a starting point these are some very basic rules which, if followed, will go a long way in ensuring Managing Trustees are abiding by the Data Protection Act 2018 and the General Data Protection Regulation (GDPR).

This guidance, produced by TMCP and the Connexional Team is a short overview of basic Do's 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. For detailed and in-depth, Managing Trustee focused guidance which covers all the above issues in more detail, please refer to the Data Protection page on TMCP's website.

Section B - Terminology

In this guidance note:

- **personal data** is any information relating to an identified or identifiable natural person, the 'Data Subject ',
- a **data subject** is an individual about whom particular personal data is about.

Section C – Do's and Don'ts

DO's	DONT's
Only collect **personal data** for the purpose for which it is required. e.g. for Gift Aid purposes and the reclaiming of tax from HMRC.	Don't use **personal data** for a different purpose or store it indefinitely because Managing Trustees think it might be useful in the future.
Once the purpose for which Managing Trustees hold **personal data** has expired, ensure that all records are securely deleted or destroyed preferably by shredding paper documents and then disposing of it in a confidential waste bin.	Don't keep inaccurate data as this is a breach of data protection legislation.
Review the information that you hold about any individual at least once a year. This will ensure that records held by Managing Trustees are accurate and up to date.	Don't store or send personal data on removable media, such as a USB pen drive as these are easily lost or stolen.

DO's	DONT's
Once an electronic device has come to the end of its shelf life, ensure that ALL data/information is erased and that the hard drive is wiped. Ideally the device should be disposed of using professional services but the only real way to guarantee erasure is to destroy the device completely.	Don't encourage the use of personal devices for Church business. Wherever possible issue phones, laptops etc to individuals for official business and ensure that these are returned at the end of that person's role or stationing.
Always remember that a **data subject** has the right to see the information/data Managing Trustees are holding about them. Managing Trustees need to be careful as to what information is held and ensure that it can be retrieved quickly.	Don't write any comment about an individual that Managing Trustees cannot defend if challenged. Personal opinions are classified as **personal data** and Managing Trustees should assume that everything may be read by the **data subject**.
Managing Trustees should ensure that **personal data** is held in such a way that it can be accessed quickly in the event of an individual making a request to access their **personal information**, a "Data Subject Access Request".	Don't amend or destroy **personal data** that you know is subject to a request from an individual to access their **personal information**, a "Data Subject Access Request".
Managing Trustees should ensure that all computers, screensavers and documents are password protected. Passwords should be at least 8 characters long and include upper and lower characters as well as symbols and numbers. ***Hint:*** replace an 'E' for a '£' symbol. Non-European keyboards don't have them.	Don't write passwords down and ensure you change them at least every 60 days.
All communications sent electronically which contain **personal data**, especially sensitive (known as "special category") **personal data** should always be encrypted.	Don't send confidential communications by email if possible but at the very least such communications should be encrypted.
Managing Trustees should ensure everyone is familiar with all data protection policies and procedures. Keep a record so Managing Trustees can demonstrate this requirement has been complied with. Access the toolkit of data protection guidance, policies and best practice that continues to be developed by TMCP and the Connexional Team and is available from the Data Protection page on TMCP's website.	Don't open emails from unknown sources. If the email appears suspicious, check with the sender by phone before reading and opening any attachments.
For Managing Trustees that have offices, ensure that all visitors are escorted out of the office/building to ensure that there is no access to unauthorised areas.	Don't ignore software security updates on devices. Failure to do so can leave devices open to hackers and cyber-theft.

DO's	DONT's
Keep a record of any data breach using the Breach Record for Managing Trustees. For guidance on what constitutes a data breach, how to avoid breaches and what to do if one occurs refer to Step 8 of the 9 Steps for Methodist Managing Trustees to Take Now to Comply with GDPR, the A to Z at the end of the Security Policy and the Breach Policy (Interim).	Don't routinely pass on personal data to a third party without consent except in accordance with section 5 of the managing Trustees Privacy Notice. For guidance on consent and the limited times when consent is required please refer to the Lawful Bases Guidance Note and the Lawful Bases Fact Sheet 4 – Consent in particular 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.
Be safe; if you are not sure ask for advice from TMCP regarding general data protection matters and the Conference Office for queries specifically relating to safeguarding or complaints and discipline matters.	Don't assume that data protection doesn't matter – IT DOES.

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

If Managing Trustees have any queries then please contact TMCP (dataprotection@tmcp.org.uk) for further assistance regarding general data protection matters and the Conference Office for queries specifically relating to safeguarding or complaints and discipline matters (dataprotection@methodistchurch.org.uk).

v2.0

Disclaimer

Registered Charity No. 1136358
A body corporate established by
the Methodist Church Act 1939

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

Telephone: 0161 235 6770
Fax: 0161 236 0752