Data Protection – Quick reference guide for trustees

This guidance 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.

DO's

- 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 District Data Championr in the first instance. They will then contact TMCP regarding general data protection matters and the Conference Office for queries specifically relating to safeguarding or complaints and discipline matters if necessary.

DONT's

- 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.

Thanks to Adwick-le-Street Methodist Church for their work on this