For more information on what Personal Data is, what constitutes Personal Sensitive Data, who is a Data Subject and a general overview on Data Protection legislation then please refer to the Data Protection page on the TMCP website.

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.
Generally, only use personal data where you have received consent by the Data Subject to hold and use the data for a particular purpose.	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.
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 data that you hold on 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.
Once an electronic device has come to the end of its shelf life, ensure that ALL data is erased and	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.

DO's	DONT's
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.	
Always remember that a Data Subject has the right to see the 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 a Data Subject Access Request being received.	Don't amend or destroy personal data that you know is subject to 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-	Don't write passwords down and ensure you change them at least every 60 days.

DO's	DONT's
European keyboards don’t have them.	
All communications sent electronically which contains personal data, especially sensitive 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.	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.
Keep a record of any data breach: further guidance will be provided on what constitutes a data breach.	Don’t pass on personal data to a third party without consent.
Be safe; if you’re not sure ask for advice.	Don’t assume that data protection doesn’t matter – IT DOES.