St Thomas of Canterbury Woodford (STOC) Data Protection Act Policy

Aims of the Data Protection Act

The Data Protection Act obliges everybody to process personal data in accordance with the law. Its aim is to balance the rights of individuals with regard to how their information is processed with the legitimate need of organisations to use information.

Certain not-for-profit organisations are exempt from registration provided that:-

1. The processing of personal data is only for the following purposes

- Establishing or maintaining membership
- Providing or administering activities for individuals who are members.
- The persons about whom the data is held are current or prospective members of the organisation.
- The type of data held is only that necessary to undertake the purposes above i.e. names, addresses, identification

Obligations under the Act.

Even though STOC does not need to register, we must still comply with the other requirements of the Act and remain subject to penalties if offences occur. Most importantly the processing should be in Compliance with the Eight Data Protection Principles. These determine how personal data should be processed in order to Comply with the Act and give rights to individuals regarding this processing.

The Eight Data Protection Principles

1. Personal data shall be processed fairly and lawfully.

2. Personal data shall be obtained for one or more specified and lawful purposes and shall not be further processed in any matter incompatible with that purpose or those purposes.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4. Personal data shall be accurate and where necessary kept up to date.

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6. Personal data shall be processed in accordance with the rights of data subjects under this Act.

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction or damage to personal data.

8. Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection for the rights and freedoms of data Subjects in relation to the processing of personal data.

Data protection requirements

1. Do the people whose information is held know what it is going to be used for?

The best way is to put a statement on your relevant forms that the supplied data will be held and maintained on a computer for the purposes of correspondence/contact. If you haven't done this in the past, you would be advised to mention it in your newsletter and other communications.

2. Is it accurate and up to date?

You must ensure that you make changes quickly to all copies.

3. Is it deleted and destroyed if the person leaves?

4. Is it held on a strict need to know basis?

Ensure that you limit the number of persons holding the full database to the absolute minimum. If there are other members who need contact details just supply them with minimal information necessary to do their job.

5. Is it held securely?

Password protect any databases and avoid issuing hard copies unless you have no choice

Paper copies of information must not be made available publicly (e.g. they must not be displayed at the back of the church).

Paper copies should only be distributed on an absolute need basis.

Recipients of paper copies must treat the information confidentially and must keep it secure. They must ensure it is never left unprotected or unsecured so that it would be available to unauthorised third parties.

Electronic devices (e.g. Desktop computers and mobile devices etc.) should be password protected. If it is necessary for a desktop computer to be taken off site for any reason (e.g. to work from home or for upgrade or repair) the data must be secured by passwords, encryption or other such methods so as to prevent unauthorised access. Additionally any third party must protect and, where they have access to data, maintain the same principles of confidentiality and data protection as those with which members of the church are expected to comply.

Any data accessible via mobile devices must adhere to the same principles as laid down in the preceding paragraph.

Data must never be left unprotected so that it would be available to unauthorised third

parties. (This is particularly relevant in the case of shared computer access or shared mobile devices).

Confidential data must never be shared with any unauthorised parties either electronically or in hard copy. This includes, but is not limited to paper, the parish website, social media, mobile or any electronic devices or by word of mouth.

A QUICK 'HOW TO COMPLY' CHECKLIST

This short checklist will help you comply with the Data Protection Act (the Act). Being able to answer 'yes' to every question does not guarantee compliance, but it should mean that you are heading in the right direction. At the end is a list of guidance on particular areas where you may need more help as well as telephone helpline numbers.

Do I really need this information about an individual? Do I know what I'm going to use it for?

Do the people whose information I hold know that I've got it, and are they likely to understand what it will be used for?

Am I satisfied the information is being held securely, whether it's on paper or on computer? And what about my website? Is it secure?

Am I sure the personal information is accurate and up to date?

Do I delete/destroy personal information as soon as I have no more need for it?

Is access to personal information limited only to those with a strict need to know?

If I want to put people's details on our website have I consulted with them about this?

Do we have a policy for dealing with data protection issues?

Do I need to notify the Information Commissioner?

If I have already notified, is my notification up to date, or does it need removing or amending?

If you need any more information about this or any other aspect of data protection, please see website www.ico.org.uk

Other useful publications

You can find all these publications on the website www.ico.org.uk

Aimed particularly at small businesses:

• Employment Practices Code – A Quick Guide (PDF)

General guidance:

• CCTV Code of Practice

• Guide to the Privacy and Electronic Communications Regulations

- Subject Access Request Checklist
- Disclosing information about tenants
- Electronic mail marketing
- Outsourcing: a guide for small and medium-sized businesses
- Using the crime and taxation exemptions
- Good Practice Note – Tied agents and independent financial advisers.