****

**Section 1: The Data Protection Act**

All parishes collect personal information. Mostly this is names and addresses of parishioners and the information on the electoral roll. It may be stored on a computer or in card index or similar. However it is recorded it is subject to the Data Protection Act 1998.

The Data Protection Act 1998 (“the 1998 Act”) gave individuals the right to know what information is held about them and provides a frame work to ensure that personal information is handled properly. It also states that organisations need to uphold 8 principles of good information handling:

1. Personal data shall be processed fairly and lawfully.
2. Personal data shall be obtained only for specified and lawful purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose for which they are processed.
4. Personal data shall be accurate and 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 individuals.
7. Data is kept securely.
8. Personal data is not transferred to any other country without adequate protection in situ.

**NB: Personal data** is anything that identifies an individual; either on its own or by reference to other information. It can include expressions of opinion. Data can be electronic, or paper and includes photographs.

**Section 2: St Peter’s Church requirement for Data Protection**

As with all churches, staff and volunteers are required to continually process personal data on behalf of St Peter’s Church. Examples of personal data processed at St Peter’s include:

1. Electoral Roll
2. Church giving and Gift Aid
3. CRB applicants
4. Registration forms for children’s groups
5. Baptisms, weddings, funerals
6. Employment records of paid staff and volunteers
7. Registration for occasional or one-off events
8. Jethro

Data is processed on behalf of St Peter’s Church by clergy, staff, and appointed volunteers. This means that data may be processed on church premises (rectory, vestry, office) or in individual’s own homes.

St Peter’s Church is a small, non-for-profit organisation and as such is exempt from notification with the Information Commissioner’s Office (ICO). However we are obliged to comply with the remainder of the Data Protection Act.

**NB:** Jethro is a database managed from the Hub, containing contact details for the St Peter’s congregation and other relevant contacts. The data is held on a secure server and user access is password protected. Individual users of the database are given restricted access according to their specific need eg Minnows leader can view only contacts for Minnows children and their parent/carer. User access is withdrawn as soon as it is no longer needed. The Hub Team are trained in data protection and how to deal with requests for information. Jethro is only updated with express permission from the contact, usually using Jethro data collection forms. Completed forms are stored in a locked cabinet.

**Section 3: Data protection policy for St Peter’s Church**

In the following policy “**St Peter’s**” is taken to be the staff member, clergy or volunteer that is acting on behalf of St Peter’s Church.

1. Personal data shall be processed fairly and lawfully.
	1. St Peter’s will ensure that everyone managing and handling data about individuals is aware of the data protection principles and the steps St Peter’s is taking to process data fairly. Users of Jethro will be asked to sign a User Agreement – see Appendix 1.
	2. St Peter’s will endeavour to ensure that individuals are aware of any information collected, processed, stored or used with respect to them.
	3. Should any photos be taken for the use of St Peter’s Church, consent from the individuals concerned or their parents (if under the age of 18) will be sought. In practice, if we are taking photographs of the congregation at worship we will advise members of the congregation as they enter the church (by notice). They will also be advised that a section of the church will not be photographed and members of the congregation may choose to sit there.
2. Personal data shall be obtained only for specified and lawful purposes.
	1. St Peter’s will be clear from the outset why it is collecting personal data and what it intends to do with it.
	2. Privacy notices:

A privacy notice is an oral or written statement that gives our identity, the purposes for requesting the information, and any usage that is not obvious.

As St Peter’s is exempt from notification then we only need to give a “privacy notice” when the usage of the data collected could go beyond the obvious purpose for which it was taken. For example First Steps all have registration forms and these would not need a privacy notice. However to enable St Peter’s to communicate with the families about activities outside of First Steps all parents should be also asked to complete a Jethro contact form.

Where a privacy notice is required, then the following paragraph should be included, with appropriate amendments depending on the nature and purpose of the data to be collected:

*In completing this form, you agree that St Peter’s Church may collect, process, store and use any personal information which you may provide us with, for the purposes of providing you with information about our current and future programme of activities and facilitating church administration. St Peter’s Church aims to comply with the requirements of the Data Protection Act.*

1. Personal data shall be adequate, relevant and not excessive in relation to the purpose for which they are processed.
	1. Before requesting data St Peter’s will consider its intended purpose and ensure that data collected is adequate, relevant and not excessive.
2. Personal data shall be accurate and kept up to date.
	1. Within church groups, registers and team member details will be updated at appropriate regular intervals. For example, registration to children’s groups annually and electoral roll and Jethro every 6 years. Changes of personal details such as address or phone number will be updated as data is given to St Peter’s.
3. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
	1. St Peter’s will not store any data longer than is reasonable with respect to the purpose for which the data was collected. Data no longer needed will be deleted, shredded or securely disposed of. People that move away from St Peter’s or are deceased will be removed from Jethro.
4. Personal data shall be processed in accordance with the rights of individuals.
	1. Individuals are able to request access to information held about them. They may request at any time access to, or amendment of, any of their personal information that we hold by contacting us by email at thehub@stpeters-woolton.org.uk. We will respond within 40 days of the request. Where the person managing the access procedure does not know the individual personally they will check their identity before handing over any information. Depending on the sensitivity of the information requested, this may include requesting photographic proof of identity, and collecting the information in person from the Hub.
5. Data is kept securely.
	1. All information on paper should be kept in a locked cabinet, with restricted access.
	2. Files containing personal data must be locked away when not in use, and computers must have adequate password protection to prevent access by unauthorised individuals, and must be kept in a secure location.
	3. Any computer on which personal data is stored must have access to that data controlled by means of a personal password that is known only to persons authorised to use that data for a legitimate purpose.
	4. To minimize the risk of loss of personal data through transfer between computers the following security tips should be undertaken
		1. Regularly check your computer for viruses and malware by installing a reputable antivrus program and make sure it is kept up to date.
		2. Use a spam filter and scan all email attachments for viruses.
		3. Consider whether you should have instant messaging protection or a firewall on the computer that you use for sending personal data.
		4. Consider using email encryption; particularly for sensitive data, or if you have had previous security issues on your computer. To do this check if you can add an email encryption plug-in to your email hosting service or use a provider such as hushmail.com.
		5. Do not open emails from unreliable sources and NEVER click on a link in an email that you cannot trust for sure.
		6. Always use bcc when sending emails to a large number of people.
		7. Ensure your email and computer passwords are strong and not easy for a human or computer to guess. Aim to change the password twice a year.
		8. Always update your operating system, browsers and software as soon as they are available as they often contain important security fixes.
		9. Be careful of suspicious websites, offers or emails – even if it looks like they are from friends.
		10. Never enter your personal details or password into a website from following a link in an email. Instead go to the real website directly by typing in the proper web address.
	5. If you suspect or know that personal data relating to St Peter’s church has been taken from your email or computer then contact a Church Warden immediately.
	6. Data transfer must also not be transferred by means of physical electronic means, e.g. memory stick or CD.
6. Personal data is not transferred to any other country without adequate protection in situ.

**Approved and Adopted at the PCC meeting held on 12 February 2013**

**Review Date:** This Policy will be reviewed bi-annually.

**Appendix 1: Jethro User Agreement**

The Jethro database has been set up to support the smooth running of St Peter’s church and all its activities. We hope that Jethro will make your role easier; providing you with accurate information quickly, and assisting easy communication within the church community.

Whether data is held on paper, or in a database, we have duties under the Data Protection Act and restrictions on how we can use personal data. This data protection policy outlines the duties and the procedures identified for proper use of personal data held in Jethro.

Access

Access to data in Jethro will be restricted to what is relevant to the individual’s role. For example group leaders will only be given access to data of members of their own groups.

Permission to make changes or add new contacts to the database is restricted to a small number of users, located in The Hub within the Simon Peter Centre.

Usage

Data should only be used strictly for the purpose that it has been provided for. Information held in Jethro should never be given to an external party, even upon request.

Security

Your password should be kept secure; never tell anyone else your password and make it easy to remember so you don’t need to write it down. Never allow a computer or device to store the password.

Always log out when you have finished using Jethro. You will be automatically logged out after a period of inactivity.

Always keep your computer protected with antivirus software. Avast and Norton are reputable antivirus software packages that can be downloaded for free.

Updating Jethro

Completed and signed contact data sheets should be given in at Hub or handed in person to a Warden, the Verger, or the Parish Coordinator.

Data misuse

It is the responsibility of every individual to protect personal data. It should be noted that any individual that deliberately tries to access, or to disclose information without authority may be committing a criminal offence.

If you become aware of misuse of data, of unauthorised access, or of loss of data then you should contact the parish coordinator or a church warden immediately. Action will need to be taken to assess the potential impact, minimise damage and to review data protection procedures.

Agreement

I have read and agree to the data protection policy relating to the access and use of data held in Jethro:

Print name: Role:

Sign: Date: