Due for revision: May 2027

DATA PRIVACY NOTICE

The Parochial Church Council (PCC) of Southbourne with West Thorney

Introduction

St. John the Evangelist Church, Southbourne and St Nicholas West Thorney (referred to as 'us' and 'we') are Church of England churches in the Diocese of Chichester, which exists to know Jesus Christ and to make him known.

We believe in God the Father, God the Son and God the Holy Spirit; we believe what the Bible says, and we believe that God's love is for everyone who seeks it. As a church, we believe that everyone is important. We aim to be accessible and inclusive and seek to be a community which cares for, supports and serves each other. For more information on our church, please see our website: www.stjohnssouthbourne.com.

Information

We believe that everyone should be given the opportunity to hear about the Kingdom of God and the good news of Jesus Christ. We value everyone who is in contact with us, by whatever means, and we do all we can to protect your privacy and to make sure shared personal data is kept safe.

This policy explains how we collect data, how we use and store this information and what it means for you. We also have specific Terms and Conditions for the use of our website, which you should read as well.

We treat everyone who contacts us in line with our beliefs and we welcome any feedback on any of our actions. Just call us on **01243 375576** or email **admin@stjohnssouthbourne.com**

1. Your personal data – what is it?

Personal data relates to a living individual who can be identified from that data. Identification can be by the information alone or in conjunction with any other information in our possession. The processing of personal data is governed by the General Data Protection Regulation (the "GDPR"). Examples of personal data we hold include our electoral roll and our parish directory.

2. Who are we?

The Parochial Church Council of Southbourne with West Thorney (the PCC) is the governing body of St. John the Evangelist Church, Southbourne (also known as St. John's Church, Southbourne) and St. Nicholas, West Thorney. The PCC is registered with the Charity Commission for England and Wales (number 1130876) and our contact address is St. John's Church Centre, Stein Road, Southbourne, Hampshire PO10 8LB.

3. How do we process your personal data?

We comply with our obligations under the "GDPR" by:

- keeping your personal data up to date;
- storing and destroying it securely;
- maintaining and applying appropriate retention periods (see Section 8); •

not collecting or retaining excessive amounts of data;

- protecting personal data from loss, misuse, unauthorised access and disclosure: and •

ensuring that appropriate technical measures are in place to protect personal data.

We use your personal data for the following purposes: -

- to enable us to provide a voluntary service for the benefit of the public within the parish and diocese;
- to administer membership records;
- to fundraise and promote the interests of the PCC;
- to manage our employees and volunteers;
- to abide by all legislation regarding safeguarding and record keeping, including the mandatory collection and storage of checked documents for the purposes of DBS checks for a minimum of two years.
- to maintain our own accounts and records (including the processing of gift aid applications);
- to inform you of news, events, activities and services running at St John's and St. Nicholas churches;
- to safeguard the interests of children and vulnerable adults in the church family;
- to hold information about trustees (PCC members) and some selected leadership roles, as legally required
- to share your contact details with the Diocesan office so they can keep you informed about news in the diocese and events, activities and services that will be occurring in the diocese and in which you may be interested.

4. How we hold your personal (sensitive) data

The definition of personal data is given in Section 1 of this document. These data are subject to rigorous controls as defined below. More detailed explanations of these security protocols which we require those church members with responsibility for processing and storing your data to follow are given in **Appendix A Control of Sensitive Data.**

4.1 Office Security Protocols

All paper records containing personal data will be held securely in the church office within a locked cabinet with access restricted to designated people within the church who have

legitimate requirements to view and/or process the data. They are subject to stringent confidentiality rules and data will not be shared with others except as permitted by you. We use separate WiFi networks for public and internal use to reduce the risk of unauthorised access.

4.2 Personal Security in Handling Sensitive Data

Detailed security protocols for handling sensitive data are given in **Appendix A Control of Sensitive Data.** In summary these include:

- use of secure passwords on any computer holding such data which limit access to authorised person(s);
- installation of appropriate anti-virus and firewall protection on these computers; •
- use of secure methods to transfer personal data from computer to computer; •
- careful handling of paper records to minimise risk of loss / unauthorised disclosure

5. What is the legal basis for processing your personal data?

There are 3 main foundations for our data processing, namely:

- Explicit consent from you so that we can keep you informed about news, events, activities and services and process your gift aid donations and keep you informed about diocesan events. We always obtain consent for contacting to you by email, in line with the Privacy and Electronic Communications Regulations.
- Where you have contacted us before we may from time to time contact you where we believe this to be in our mutual legitimate interest to do so. For example, if you have a child baptised at St John's we may send you an invitation to our Toddlers group.
- Where required by law or by a regulatory body we may need to pass on information. For example, to HMRC regarding payments to employees and Gift Aid.

6. Sharing your personal data

Your personal data will be treated as strictly confidential and it will only be shared with other members of the church in order to enable them to carry out effective services within the church, or for legitimate purposes connected with the church. We will not share your data with a third party without your explicit consent.

7. St John's Church use of cookies on our website

Cookies are very small text files that are stored on your computer when you visit a website. You may find more information about cookies at http://www.allaboutcookies.org and at http://aboutcookies.org.

We may collect data from cookies to customise the content on our website and to help to analyse our visitors' future needs and to aid internal administration and analysis.

St John's church may work with a number of third party suppliers who may set cookies on our

website to enable them to provide us with services e.g. YouTube and Vimeo to embed videos. Some of these services may be based outside of the UK and EU and may not fall under the jurisdiction of UK courts.

Most browsers will allow you to turn off the cookie function, see the help function on your browser. To opt out of being tracked by Google Analytics across all websites visit **http://tools.google.com/dlpage/gaoptout**.

8. How long do we keep your personal data?

We keep data in accordance with our Record Retention Guidelines, which are based on the guidance set out in the guide "Keep or Bin: Care of Your Parish Records" which is available from the Church of England website [1].

[1] Details about retention periods can currently be found in the Record Management Guides located on the Church of England website at: - https://www.churchofengland.org/sites/default/files/2017-11/care_of_parish_records_keep_or_bin_-_2009_edition.pdf

9. Your rights and your personal data

Unless subject to an exemption under the GDPR, you have the following rights with respect to your personal data: -

- The right to request a copy of your personal data which the PCC holds about you;
- The right to request that we correct any personal data if they are found to be inaccurate or out of date;
- The right to request your personal data are erased where it is no longer necessary for us to retain such data;
- The right to withdraw your consent to us processing your data at any time
- The right to request that we provide you with a copy of your personal data
- The right, where there is a dispute in relation to the accuracy or processing of your personal data, to request a restriction is placed on further processing;
- The right to object to the processing of personal data.
- The right to lodge a complaint with the Information Commissioner's Office.

10. Further processing

If we wish to use your personal data for a new purpose, not covered by this Data Privacy Notice, then we will provide you with a new notice explaining this new use prior to commencing the processing and setting out the relevant purposes and processing conditions. Where and whenever necessary, we will seek your prior consent to the new processing.

11. Contact Details

To exercise all relevant rights, queries or complaints please in the first instance contact the St John's Parish Office at **admin@stjohnssouthbourne.com** and **01243 375576**

You can contact the Information Commissioner's Office on **0303 123 1113** or via email https://ico.org.uk/global/contact-us/email/ or at the **Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF**.

Appendix A Control of Sensitive Data (Guidance for holders)

Password protocol

To ensure that access to any personal data you hold is secure, your password must:

• be **at least eight characters long;**

• Use one of these **special characters** ! ( ) - , . ? [ ] _ ~ ; : ' @ # $ % ^ & * + = •

Include **both upper and lower case letters;**

• **not include spaces.**

It is also important to:

• Avoid words or phrases that are easy for people to guess, like your surname or pet's name;

• Change your password on a regular basis;

• Avoid letting your browser store passwords for you. It may save you time but if anyone has access to your computer they will have an easy job accessing your accounts.

• Avoid writing your password down;

and, where the computer is shared:

• Create a separate user partition with its own password for any sensitive data held.

N.B. Any suspected breach of your data security should be reported immediately to the PCC

Appropriate anti-virus and firewall protection

Any computer holding sensitive data must have an installed firewall and anti-virus software. Most computers come pre-installed with firewalls but anti-virus software is usually an extra. A minimum expectation is that reputable robust, free anti-virus software (such as AVG or AVAST) is installed and regularly updated and run alongside a good firewall which is made active.

Physical protection of sensitive data

Holders of personal data must limit exposure of paper copies to security risks through use of:

- Locked cabinets for stored/archived data and ensuring that any keys are not on open access and that cabinets remain locked when unattended;
- Sealed envelopes and confidentiality marking with appropriate care taken to avoid theft e.g. not leaving data in cars or in open access areas such as an unlocked office;
- Private rooms for essential discussion of any personal data e.g. where safeguarding issues arise;
- Face to face transfer of paper copies of sensitive data to minimise the risk of third party access.

Closed Transfer Systems

It is recognised that there will be occasions when personal data must be shared between computers but it is imperative that this is done as securely as possible. Use of email with all its inherent security weaknesses is to be avoided. We have decided to adopt the use of Google Drives when moving personal or confidential data from computer to computer. This will ensure that only authorised people will have access to such data as each drive can be limited to a defined audience. Training on the installation, set-up and use of Google Drives will be given to all potential holders of sensitive data to ensure smooth implementation of this policy. The training will also include a briefing on general data security protocols.