

<b>Title</b>	Data Protection Policy
<b>Approved by</b>	PCC
<b>Date approved</b>	November 2020
<b>Review date</b>	November 2022
<b>Owner</b>	Janet Norris
<b>Where to be published</b>	website , policy folder in parish office

*As the Leadership (Vicar, Churchwardens and PCC of St George & St Paul’s) we recognise the need to comply with all relevant legislation concerning the treatment of personal information held by us. We will ensure that all personal information held by St George and St Paul’s, Tiverton (hereafter referred to as ‘our church’ in this policy) whether it is held on paper, computer or other media will be dealt with in accordance with the provisions of the 2018 Data Protection Act (DPA).*

*All staff & volunteers will be made aware of this policy and any training and support required will be provided.*

**This policy should be considered in conjunction with the policies listed at the end of this document.**

All data we process is in accordance with the rules as laid down in statute, including the General Data Protection Regulations and the provisions of the Data Protection Act 2018. The following principles apply to all employees and any others who obtain, handle, process, transport and store personal data for our church and they must adhere to them

**The Key Principles**

- Individuals retain rights over their data
- Data should be collected fairly and lawfully processed
- Data will be processed for limited purposes - and not in any manner incompatible with those purposes
- Data will be kept up-to-date and accurate, also adequate, relevant and not excessive.
- Data should only be kept as long as is necessary
- Data integrity and security is paramount
- Data governance will be actively managed at all levels of the organisation, to minimise risks to both the individual and the organisation
- All collection and use of data will be open and honest

This policy will help ensure that we respect the rights of all individuals whose data it collects. It encompasses legal responsibilities and best practice. Routine application of these principles will also help protect our church from the risk of data breaches and unauthorised access to personal information.

**Data Protection Law and Principles**

The use of personal data is governed by EU and UK law. The General Data Protection Regulations (GDPR) set out how data should be obtained stored and handled. These regulations set out six principles that underpin lawful use of data. These provide the foundation for good data governance. These principles are enhanced by a range of powers for individuals to control how their data is processed and stored.

## **Responsibilities Under This Policy**

### **Maintaining Confidentiality**

Everyone who is employed or serves within our church has some responsibility for ensuring that data is handled safely, securely and appropriately. Our Church will treat all personal information as private and confidential and not disclose any data about individuals to anyone other than the leadership and ministry overseers/co-coordinators of the church in order to facilitate the administration and day-to-day ministry of the church.

**All our Church staff and those who serve within our church who have access to Personal Data will be required to sign to say they have read the Data Protection policy.**

### **What is Personal Data?**

Personal data is information about a person – anything that would allow someone to identify a living individual. Processing that data means obtaining, using and transferring data, and storing it in any system that allows it to be found again, such as a computer database or filing system.

### **Our Privacy Notice**

Our church will take all reasonable steps to ensure that individuals are aware their data is being processed. This will include telling individuals what is being used, how it is being used, how long it will be kept for, and how they can exercise their rights in respect of that data.

Our Privacy Notice sets out how we collect data, what data we collect, and the lawful basis for that and how long we retain it. It includes information on who we share data with and the lawful basis for such sharing. It also sets out how people can request copies of data we hold about them. The notice will be included in our literature and on our website and available on request.

### **There are four exceptional circumstances to the above permitted by law:**

- Where we are legally compelled to do so.
- Where there is a duty to the public to disclose.
- Where disclosure is required to protect your interest.
- Where disclosure is made at your request or with your consent.

### **Use of Personal Data**

Our church will use your data for three main purposes:

- The day-to-day administration of the church; e.g. pastoral care and oversight including calls and visits, preparation of ministry rotas, maintaining financial records of giving for audit and tax purposes.
- Contacting you to keep you informed of church activities and events.
- Statistical analysis; gaining a better understanding of church demographics. N.B. although collated church data may be passed to a third party, such as number of small groups or small group's attendance, no personal data will be disclosed.

### **The Leadership will ensure that:**

- Staff & servers within the church understand their responsibilities with regard to the proper handling of data and that training will be provided if required.
- Staff & servers within the church are aware of how to deal with enquiries about handling personal data
- The requirements of the DPA are considered in key decision-making processes, such as the development and implementation of information systems and evaluation.
- The way personal information is handled and managed is regularly reviewed.

### **Data Use and Transfer**

Anyone has the right to ask to see a copy of any information we hold about them. This is known as a Subject Access Request (SAR). To do this the request can be made in writing (including by electronic means) to the leadership via the Parish Office, where initially this will be referred to a churchwarden. An individual is entitled within 30 calendar days of making the request:

- to be told whether any personal data is being processed

- to be given a description of the personal data, the reasons it is being processed, and whether it will be given to any other organisations or people
- to be given a copy of the information comprising the data; and given details of the source of the data (where this is available).

### **Sharing Data:**

Subject Consent: The need to process data for normal purposes has been communicated to all data subjects. In some cases if the data is sensitive, for example, information about health, race or gender, express consent to process the data must be obtained. Information contained on the database will not be used for any other purposes than set out in this section. The database is accessed through the cloud and, therefore, can be accessed through any computer or smart device with internet access. The server for the ChurchSuite database is in the UK and hosted by Churchapp, and Windows 365 is based in EU.

- Access to the database is strictly controlled through the use of name specific passwords, which are selected by the individual.
- Those authorised to use the database only have access to their specific area of use within the database. This is controlled by the Data Controller and other specified administrators. These are the only people who can access and set these security parameters.
- People who will have secure and authorised access to the database include Church Staff, Ministry Team Leaders, Churchwardens and treasurer
- All access and activity on the database is logged and maybe viewed by the [vicar/churchwarden/treasurer]
- No personal data will be shared outside of the Leadership of the Parish of St George's & St Paul's unless written consent is obtained from the individual concerned.
- The only exceptions will be where we are required by law to do so as can be seen above.

### **Data Storage:**

In order to keep personal data secure the following controls will be followed:

- Personal data will usually be stored securely on church premises.
- Personal data may be held at the home of staff and volunteers but they must ensure this is held securely.
- Any computer on which personal data is stored must have access to that data controlled by means of a strong personal password.

### **File Destruction Policy:**

All information held regarding staff and volunteer appointment that are not shortlisted will be destroyed once an appointment has been made. Shortlisted applicants' information will be destroyed after 6 months.

The staff and volunteer privacy notice, i.e. the personal data policy, gives more information about retention periods.

These records are kept secure within the parish office and the churchwardens are responsible for identifying the records and destroying all records specified in the staff personal data policy.

When files are destroyed care will be taken that all paper files together with associated documents and correspondence are shredded in-house and the electronic data is permanently deleted from the database along with all associated computer files.

Reviewed Nov 2020

Amended Nov 2019

Approved January 2016

### **Related Policies and Procedures:**

Acceptable Use of IT Equipment Policy

Staff and Volunteer Privacy Notice, Personal Data Policy