DATA PROTECTION
POLICY AND PROCESS

Name of Church: St John the Evangelist

Address: Church Way
Hurst Green
Oxted
Surrey RH8 9EA

Date: May 2018
Review Date: May 2019

This policy and process was reviewed in January 2020 by Adrian Hardingham (Data Compliance Officer) and Cathy Booth (Churchwarden) and it was agreed no changes were required. It will be further reviewed in January 2021.

Contents

1. Introduction

In order to operate, St John's needs to gather, store and use certain forms of information about individuals.

These can include members of the church community, employees, volunteers, contractors, suppliers, business contacts and other people the church has a relationship with or regularly needs to contact.

This policy explains how this data should be collected, stored and used to meet St John's data protection standards and comply with the General Data Protection Regulations (GDPR).

This policy ensures that St John's:

- Protects the rights of our members, employees, volunteers and supporters
- Complies with data protection law and follows good practice
- Protects itself from the risks of a data breach

2. Roles and responsibilities

Members of Standing Committee will determine what data is collected and how it is used. They, together with the PCC, are responsible for the secure, fair and transparent collection and use of data by St John's. Any questions relating to the collection or use of data should be directed to the Data Compliance Officer.

Everyone who has access to data as part of St John's has a responsibility to ensure that they adhere to this policy.

St John's uses third part Data Processors (e.g. Mail Chimp) to process data on its behalf. St John's will ensure all Data Processors are compliant with GDPR.

3. Data protection principles

a) We fairly and lawfully process personal data in a transparent way

St John's will only collect data where lawful and where it is necessary for the legitimate purposes of the church. St John's will collect personal data of church members including:

- Name
- Address
- Email Address
- Telephone numbers (landline and mobile)
- Taxpayer (if gift aiding)

The information is obtained directly from the individual and a consent form to use the data is completed.

The name and contact details of volunteers, employees and contractors will be collected when they take up a position and will be used to contact them regarding any administration related to their role.

Further information, including personal financial information and criminal records information may also be collected in specific circumstances where lawful and necessary (in order to process payment to the person or in order to carry out a DBS check).

An individual's name and contact details will be collected if they make a booking for an event which is being managed by St John's. This will be used to contact them about their booking and to allow them entry to the event.

b) We only collect and use personal data for specific, explicit and legitimate purposes and will only use the data for those specified purposes.

When collecting data, St John's will always provide a clear and specific privacy statement explaining to the subject why the data is required and what it will be used for.

c) We ensure any data collected is relevant and not excessive

St John's will not collect or store more data than the minimum information required for its intended purpose. E.g. we will need to collect telephone numbers in order to be able to contact them about church activities, but data on their marital status or sexuality will not be collected, since it is unnecessary and excessive for the purposes of St John's administration.

d) We ensure data is accurate and up to date

Any individual will be able to update their data at any point by contacting the Data Compliance Officer. The data will be reviewed at regular intervals e.g. at the time of completing the Annual Parish Returns.

e) We ensure data is not kept longer than necessary

St John's will keep records for no longer than is necessary in order to meet the intended use for which it is gathered. Safeguarding and financial records will be retained in accordance with legal requirements. The storage and intended use of data will be reviewed in line with St John's data retention policy. When the intended use is no longer applicable (e.g. contact details for a member of the congregation who has moved away), the data will be deleted within a year.

f) We keep personal data secure

St John's will ensure that data held by us is kept secure.

- Electronically-held data will be held within a secure environment
- Physically-held data will be stored in a locked cupboard
- Keys for locks securing physical data files should be collected by the Data Compliance Officer from any individual with access if they leave their role/position
- Access to data will only be given to relevant PCC members/contractors/employees where it is clearly necessary for the running of St John's.

g) Transfer to countries outside the EEA

St John's will not transfer data to countries outside the European Economic Area (EEA) unless the country has adequate protection for the individual's data privacy rights.

4. Individual rights

When St John's collects, holds and uses an individual's personal data that individual has the following rights over that data. St John's will ensure its data processes comply with those rights and will make all reasonable efforts to fulfil requests from an individual in relation to those rights.

Individual's rights

- *Right to be informed:* whenever St John's collects data it will provide a clear and specific privacy statement explaining why it is being collected and how it will be used.
- *Right of access:* individuals can request to see the data St John's holds on them and confirmation of how it is being used. Requests should be made in writing to the Data Compliance Officer and will be complied with free of charge and within one month. Where requests are complex or numerous this may be extended to two months.
- *Right to rectification:* individuals can request that their data be updated where it is inaccurate or incomplete. Any requests for data to be updated will be processed within one month.
- *Right to object:* individuals can object to their data being used for a particular purpose. St John's will always provide a way for an individual to withdraw consent in any form of communication. Where we receive a request to stop using data we will comply unless we have a lawful reason to use the data for legitimate interests or contractual obligation.
- *Right to erasure:* individuals can request for all data held on them to be deleted. St John's data retention policy will ensure data is not held for longer than is reasonably necessary in relation to the purpose it was originally collected. If a request for deletion is made, we will comply with the request unless:
    - There is a lawful reason to keep and use the data for legitimate interests or contractual obligation.
    - There is a legal requirement to keep the data.
- *Right to restrict processing:* individuals can request that their personal data be 'restricted' – that is, retained and stored but not processed further (e.g. if they have contested the accuracy of any of their data, St John's will restrict the data while it is verified).

Though unlikely to apply to the data processed by St John's, we will also ensure that rights related to portability and automated decision making (including profiling) are complied with where appropriate.

5. How we get consent

St John's will collect data from consenting individuals so that they can be contacted and updated on church activities.

We will provide:

- A method for users to show their positive and active consent to receive these communications (e.g. a 'tick box')
- A clear and specific explanation of what the data will be used for

Data collected will only ever be used in the way described and consented to (e.g. we will not use email data in order to market 3rd-party products).

Communications will contain a method through which a recipient can withdraw their consent (e.g. an 'unsubscribe' link in an email). Opt-out requests such as this will be processed within 14 days.

6. Member-to-member contact

As a church community, St John's encourages communication between members.

To facilitate this:

- Members can request the personal contact data of other members in writing via the Data Compliance Officer. These details will be given, as long as they are for the purposes of contacting the subject (e.g. an email address, not financial or health data) and the subject has consented to their data being shared with other members in this way.

7. Data retention

A regular review of all data will take place to establish if St John's still has good reason to keep and use the data held at the time of the review. As a general rule, a data review will be held every two years and no more than 27 calendar months after the last review. The first review took place in March 2018.

The data which will be reviewed includes:

- Digital documents in Dropbox
- Data stored on third party online services e.g. Mail Chimp
- Physical data stored in filing cabinets

The review will be conducted by the Data Compliance Officer with other members of the PCC to be decided on at the time of the review.

Physical data will be destroyed safely and securely, including shredding.

All reasonable and practical efforts will be made to remove data stored digitally.

The following criteria will be used to make a decision about what data to keep and what to delete:

Question	Action	
	Yes	**No**
Is the data stored securely?	No action necessary	Update storage protocol in line with Data Protection policy
Does the original reason for having the data still apply?	Continue to use	Delete or remove data
Is the data being used for its original intention?	Continue to use	Either delete/remove or record lawful basis for use and get consent if necessary
Is there a statutory requirement to keep the data?	Keep the data at least until the statutory minimum no longer applies	Delete or remove the data unless we have reason to keep the data under other criteria.
Is the data accurate?	Continue to use	Ask the subject to confirm/update details
Where appropriate do we have consent to use the data. This consent could be implied by previous use and engagement by the individual	Continue to use	Get consent
Can the data be anonymised	Anonymise data	Continue to use

Statutory Requirements

Date stored by St John's may be retained based in statutory requirements for storing data other than data protection regulations. This might include but is not limited to:

- Gift Aid declarations records
- Details of payments made and received (e.g. in bank statements and accounting records)
- PCC meeting minutes
- Contracts and agreements with suppliers/customers
- Insurance details
- Tax and employment records

8. Data breach

If a personal data breach were to occur, the Data Compliance Officer will notify the Diocesan Registrar without delay and seek advice. The Information Commissioner's Office (ICO) will be notified within 72 hours. The potential scope, cause of the breach, mitigation actions and how the problem will be addressed are to be identified.

9. Data protection impact assessments

St John's will complete a data protection impact assessment if any proposed processing operation if going to use personal data. It will include:

- A description of the processing activity and its purpose
- An assessment of the need for and the proportionality of the processing
- The risks arising and measures adopted to try and prevent any risks, in particular any safeguarding or security measures to protect data and comply with GDPR.

10. CCTV

Signs will be in place to ensure that visitors to the church are aware that CCTV is being used and for what purpose.