

**St Stephen's Church, Canonbury**  
**17 Canonbury Road, London. N1 2DE**

**General Data Protection Regulation (GDPR)**  
**Policy statement**

Adopted May 2018, due for revision December 2018

The General Data Protection Regulations govern all aspects of the storage and processing of personal data by which a person could be identified. It is designed to minimise the amount of data that can be held, limit the time for which data can be retained and limit the use, or processing, of that data to only uses which can be justified and for which there is a lawful basis.

At St Stephen's we are committed to comply with the requirements of the GDPR and to monitor our systems for continuing compliance.

We recognise the grounds ( the legal basis) on which data can be held and processed

- Legitimate interest
- Legal obligation
- Performance of a contract
- Consent

Data will only be held or processed if one of these conditions has been met.

We will

- Only hold data if it is held on a lawful basis.
- Only process data if it is done on a lawful basis.
- Ensure that parental/guardian consent is obtained for the retention of data concerning children under 13.
- Make all people for who we hold data aware of their rights under the GDPR by displaying and making available a privacy notice.
- Make all employees and role-holders aware of their rights and consent they are giving by virtue of their contracts of employment or volunteer/role agreements with us, by displaying a 'role-holders' privacy notice.
- Regularly train staff, role-holders and volunteers in GDPR requirements.
- Carry out an annual Data Audit across the organisation.
- Destroy/delete all data for which there is no longer a lawful basis for retention or processing.

**Individual rights**

We will respect the rights of all individuals enshrined in the GDPR.

- To be informed what data we hold
- To access personal data (Subject Access Request)
- To rectify mistakes
- To have data erased ('be forgotten')
- To restrict processing
- To make data portable
- To object to processing
- To object to automated decision-making

We will ensure that all our processes for data retention and processing allow these rights to be exercised.

**Data Controller**

The PCC is the Data Controller for the Church, the PCC will appoint 2 people as 'Data Compliance Officers' (the vicar and one other) to enable it to carry out its responsibilities under GDPR.

**Data storage**

All data will be stored securely in locked filing cabinets or on password protected digital systems. We will have policies and protocols for the moving of data and for data kept on portable devices.

### **Data retention**

We will only hold data for as long as it is required and only as long as there is a lawful basis or as we are otherwise permitted to do so.

### **Data disposal**

We will put in place a 6 monthly process of data cleansing during which all data will be checked for current usefulness and data that there is no longer a lawful basis or justification for us to hold will be destroyed or deleted. Paper will be shredded and digital information deleted so it cannot be retrieved.

### **Data sharing**

We will only share data with consent or if there is a legal basis by virtue of a contract, employment or any particular role. We will ensure that any organisation/system with which data is shared is compliant with the GDPR. We will ensure that any contractors with whom data is shared comply with their obligations as contractors under the GDPR.

### **Data subject requests**

If we receive a request by an individual to disclose all data we hold on them we will comply with this request within the 30 day period set down in the GDPR. If a request is received to delete data we will comply subject to any exemptions regarding safeguarding or other issues.

### **Data breaches**

All staff and volunteers who may process data will be regularly trained and updated on how to identify a data breach. We recognise that these can occur in many different ways – emails sent to the wrong person, phone messages overheard by others, computer screens left open for others to see, Cyber-attacks, loss of memory sticks, theft of equipment, loss of paper records etc etc. All data breaches will be reported to the Data Compliance Officers' who will decide if they warrant reporting to the Information Commissioners Office. If so, they will be reported within 72 hours of the breach being notified. All notified data breaches will be recorded.

### **Display of privacy notices**

Privacy notices will be displayed on noticeboards in the Church and halls and will be posted on the church website – [www.ststephenscanonbury.org.uk](http://www.ststephenscanonbury.org.uk)

### **New systems and projects**

Data protection will be at the heart of the development of new projects and systems. We will adopt the principle of 'Privacy by Design' across the organisation.