# GDPR Policy

## Purpose

The purpose of this policy is to uphold and protect the rights on living individuals concerning information about them (known as ‘personal data’).

All aspects of the GDPR legislation will be complied with as outlined in this policy. Specifically, personal data that is obtained, held or disclosed by St Peter’s will be:

* Processed fairly and lawfully
* Only used for specific and lawful purposes. Individuals will be informed as to these purposes
* Adequate information, relevant and not excessive in relation to what is being used for
* Not be kept longer than necessary for the purpose
* Securely kept
* Not disclosed to third-parties other than in line with the stated purpose or in specific circumstances as outlined below.

## Data processing purposes

St Peters Church processes and stores date for legitimate interests of the organisation.

These interests are for the provision of Christian services, events and activities at or through this church.

All data collected will only be used for purposes falling within these legitimate interests.

If data is required for purposes outside of these interests, the data subject will be informed of the different purpose at the point of data collection, in a clear and succinct notice.

## Datasets processed

The following sets of data are processed and stored as part of the operations of St Peter’s. This list is indicative rather than exhaustive and additional relevant data may also be processed and stored.

### Employees and interns:

* **Personal details**: name, address, date of birth, contact phone & email, marital status
* **Financial details**: bank account, tax code, NI, Student grant status
* **Employment details**: CV, references, annual appraisals, work permit, leave taken, sickness leave taken
* **Health information**: any disabilities, any other health-related matters which require support
* Sensitive information: information relating to criminal convictions as returned by a DBS check

### Church Members:

* **Personal details**: name, address, date of birth, contact phone & email
* Activities: history of church-related activities including group memberships and volunteering

### Children and Youth:

* Names, gender, dates of birth, parent name and number, medical information, emergency contact

### Volunteers:

* Name, and contact details.
* In specific ministries, details of references given in connection with their recruitment to the voluntary role
* In specific ministries, information relating to criminal convictions as returned through a DBS check

### Donors

* **Personal details**: name, address, date of birth, contact phone & email
* **Financial details**: bank account, Gift Aid status, amount donated

### Beneficiaries of church activities

* Contact details
* Many ministries collect further personal details including sensitive information regarding the person’s life situation and history

### Members of the public:

* Name, address and phone details
* Details of enquiry
* In cases of baptisms, weddings and funerals, information relating to life situations and family relationships

### Contractors:

* **Contact details:** Names, addresses, phone, email
* **Financial details:** cost of their services, bank account details

## Types of data processed

The following data types are processed by the different areas of our organisation:

* **Operations**: personal, financial, some sensitive data (employment references)
* **Youth/Kids:** personal, data relating to children, some sensitive data (DBS)
* **Relationships**: personal, some data relating to marital and family situation
* **Pastoral**: personal, some sensitive data (relating to pastoral situations)
* **Giving**: personal and financial data
* **Finance**: personal and financial data
* **Vulnerable Persons ministries:** personal data, some sensitive data (relating to life situations)

## Those responsible for processing

Data is processed at St Peter’s by:

* Staff members
* Interns
* Volunteers
* Third-party processors with whom St Peter’s has a contractual relationship

## Significant data risks

We have identified the following main data risks to our organisation:

* Unauthorised access to our third-party processors via former staff or volunteers
* Hacking into our ChurchSuite database
* Data being stored on local hard drives (laptops)
  + being taken out of building for working at home
  + being lost or stolen
  + old data remaining on private laptops and being forgotten and therefore left insecure
* Paper-based data being stored or left out in unlocked locations (pigeonholes, on desks, in recycling)

## Key precautions undertaken to protect data

We have undertaken to address these risks by the following actions and procedures:

* Office volunteers sign a declaration that they have been informed of their responsibilities with respect to data processing and confidentiality
* All staff are issued with passworded work credentials for accessing their work devices and the Office 365 cloud-based work environment
* Staff are further set up with multi-factor authentication for their work logins
* We uphold a clear-desk policy: all work materials are cleared away into staff drawers at the end of each working day
* We uphold a policy of shredding discarded paper containing any personal data
* All sensitive and financial data is kept in locked locations
* Staff access to sensitive and pastoral data is restricted to only those staff who are responsible for the appropriate ministry area

## Data storage and backup

All data is kept on cloud-based environments with inbuilt backup and data-restore functions.

Any financial information recorded on paper is kept in a locked cabinet to which only the Finance and Leadership teams have access

Any paper-based information relating to sensitive data, such as personnel records, DBS applications, details of guests at the church nightshelter, are kept in locked cabinets to which only restricted staff members have access

## Data accuracy and deletion

Team managers are responsible for the accuracy of the data they hold. Data accuracy checks are to be carried out in line with data deletion procedures.

Team managers are to organise an annual review of the personal data they hold, carrying out appropriate checks on its accuracy, by contacting data subjects or otherwise.

They will select data for deletion and inform data subjects if required.

Data is selected for deletion as follows:

**Membership database**: those who during the previous 2 calendar years have not engaged in any aspect of church life, for example groups, teams, courses, giving, attending events.

**Finance**:   
- paper records of financial data are kept for 6 years as required by relevant legislation   
- electronic records are kept in perpetuity for statistical and analytical purposes

**Nightshelter**   
- For guests who have been housed, records are deleted at the latest one calendar year later. For other guests, records are deleted at the end of the NightShelter period.

In all cases, if team managers wish to retain data as part of an archive for statistical purposes, they shall take measures to anonymise the personal data.

## Subject Access Request

Staff have a legal duty to provide details of information held about a data subject when this is requested. This must be provided in a form which is accessible to the data subject, free of charge and within one month of the request.

Subject Access Requests should be directed to the Data Manager, who will act as coordinator.

The data manager will take measures to confirm the identity of the data subject requesting subject access.

The data manager will then contact all staff with the request. Staff will send details of data held on the subject within 2 weeks.

The data manager will collate the data and ensure it is presented as electronic documents in a commonly used format, and/or paper records, sending or presenting the records to the data subject within one month of the subject access request.

## Subject Erasure Request

Staff have a legal duty to remove all information held about a data subject from all systems when this is requested, when this is a valid request given our relationship with the data subject, and within our responsibilities relating to other relevant legislation.

Subject Erasure Requests should be directed to the Data Manager, who will act as coordinator.

The data manager will take measures to confirm the identity of the data subject requesting subject erasure and liaise with that person to clarify any queries. This may include stating where we are obligated to maintain personal data for longer periods, such as in the case of safeguarding incident reports; financial data; records of baptisms, marriages and funerals. It may also include clarifying that removing the data will mean the person will no longer be able to participate in particular activities where data collection/processing is required, such as small groups.

The data manager will then contact all staff with the request. Staff will take any measures required to remove details of the data subject from their files and records, or to anonymise such records to ensure the person is no longer identifiable.

## Data disclosure

We provide details of the data held on an individual to that person in response to a Subject Access Request.

In the event of issues relating to safeguarding, data may be disclosed to our Parish Safeguarding Officer as part of our Safeguarding policy.

Safeguarding officers may disclose data to third party agencies to ensure the safety and well-being of those involved.

We conform to the duty of care in the case of individuals who inform us of intentionality to self-harm or endanger others. In such cases we will contact the appropriate statutory agencies.

## Provision of information to data subjects

Our privacy notice is kept in an accessible location on our website and as a hard copy at the Connect point in our church building.

Brief privacy notices are added to forms where we collect people’s data, informing them of the purposes of the data collection.

## Data breaches

The Information Commissioner’s Office (ICO) defines as a data breach as follows:

*A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on individuals.*

Staff, volunteers and third party data processors are informed through training of their responsibility to report any possible data breaches to the data manager.

The data manager has responsibility to assess the likelihood and extent of the data breach and of the resulting risk to people’s rights and freedoms.

In the event of serious risk, the data manager shall report the breach to the ICO within 72 hours. This section of the GDPR legislation shall apply:

*A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned.*

In the event of a third-party data processor reporting a data breach to us, the data manager shall inform the ICO within 72 hours.

In all cases of a notifiable breach, the individuals concerned shall be notified as soon as possible, including information on the name and contact details of the data protection officer, a description of the likely consequences of the personal data breach; and a description of the measures taken, or proposed to be taken, to deal with the personal data breach, and where appropriate, the measures taken to mitigate any possible adverse effects

In all cases, including of breaches which do not require notification, a record shall be kept of the breach.

The data manager shall lead investigations into data breaches and make recommendations to the leadership team to reduce the risk of future breaches.

## Staff training

Trustees of St Peters Brighton (the Parochial Church Council) will be required to undergo suitable training with respect to their duties and responsibilities as data controllers.

On a regular basis, staff team shall undergo training in their responsibilities with respect to the GDPR. This training will also form an integral part of staff induction.

Failure to comply with the provisions of this policy may constitute a disciplinary matter.

Any failure to comply with the provisions of this policy which results directly and demonstrably in a data breach shall always constitute a disciplinary matter.