St Peter's Church
ROPLEY
Discovering and sharing the generous love of God

GENERAL DATA PROTECTION REGULATION (GDPR) POLICY

1.0 Introduction

St Peter's Church Parochial Church Council (PCC and all subcommittees) needs to gather and use certain information (described as "personal data") about individuals. These individuals can include members of the PCC, church congregation, family and friends of church members, business contacts, contractors, purchasers of tickets for events held at the church, sponsors and other people the PCC has a relationship with or may need to contact.

St Peter's Church Parochial Church Council (PCC) is the "data controller". 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 the data controller's possession or likely to come into such possession. The processing of personal data is governed by UK General Data Protection Regulation ("GDPR").

This policy and the accompanying privacy notice describes how this personal data must be collected, handled and stored to meet UK GDPR.

2.0 Why this policy exists

This data protection policy ensures that the PCC:

- Complies with the GDPR and follows good practice
- Is open about how it stores and processes an individual's data
- Manages and minimises the risks of a data breach
- Specifies individual rights and how an individual can request access to their personal data

GDPR describes how an organisation, including the PCC collects, handles and stores personal data.

- http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted
- https://www.gov.uk/government/publications/guide-to-the-general-data-protection-regulation

These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal data must be collected and used fairly, stored safely and not disclosed unlawfully.

The PCC must ensure that personal data is:

- Processed fairly and lawfully
- Obtained only for specified, lawful purposes

- Adequate, relevant and not excessive
- Accurate and kept up to date
- Not to be held for any longer than necessary
- Processed in accordance with the rights of data subjects
- Protected in appropriate ways
- Not to be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection.

As part of this policy, the PCC has developed a privacy notice for public use which explains how it uses personal data. This privacy notice is based on a Church of England template which is compliant with the GDPR. The PCC will confirm annually that this is up to date and will ensure that the policy is provided to all those within the policy scope.

3.0 Policy scope

This policy applies to all St Peter's, Ropley staff and volunteers who process personal data, including clergy, church administrators, PCC members, volunteers handling membership lists, and those involved in children's or vulnerable adults' work.

It applies to all data held relating to identifiable individuals (ie, living individuals, who are identified or identifiable).

4.0 Data protection risks

This policy helps to protect the PCC, and the individuals whose personal information we handle, from some very real data security risks, including:

- **Breaches of confidentiality** eg, information being given out inappropriately.

- **Failing to offer choice** eg, all individuals should be free to choose how the data relating to them is used.

- **Reputational damage** eg, the PCC members and Events Team could suffer if hackers successfully gained access to sensitive data.

5.0 Responsibilities

The PCC has the responsibility for ensuring that data is collected, stored and handled appropriately. Each person responsible for personal data must ensure that it is handled and processed in line with this policy and the GDPR principles. The PCC is ultimately responsible for ensuring that it meets its legal obligations relating to data protection.

Though not mandated for individual churches, it is good practice to appoint a **Data Protection Lead (DPL). The DPL** for St Peter's, Ropley PCC is: Elizabeth Barley.

While all PCC members, church staff and volunteers are responsible for the GDPR, the DPL will be responsible for:

- Keeping the PCC updated about data protection responsibilities, risks and issues
- Reviewing all data protection procedures and related policies
- Handling data protection questions from PCC and anyone else covered by this policy

- Ensuring that requests from individuals to see the data that the PCC holds about them are dealt with in a timely manner.
- Checking and approving any contracts or agreements with third parties that may handle the PCC's data.
- Ensuring that data breaches are reported to the ICO in a timely manner when necessary. Though, it should be noted that all staff and volunteers also have a duty to do this.
- Ensuring those processing personal data (including vicar, church wardens, PCC secretary, parish administrator, safeguarding officer, GDPR lead, musical director, events committee lead, youth group leads, stewardship lead, social media lead and others on the events committee who access 'squarespace') are trained in the GDPR and that all those within the scope of this policy have a copy of the privacy notice.

6.0 General guidelines

The only people able to access data as defined above should be those who need it to progress the business of the PCC and anyone else covered by this policy.

- Data should not be shared informally. When access to confidential information is required, this should be done through the Vicar, PCC Data Protection Officer, PCC Secretary, Treasurer or subcommittee leads.
- Those who handle data should keep all data secure, by taking sensible precautions and following the guidelines below.
- In particular, strong passwords must be used for email accounts and any electronic device that stores personal data, and passwords should never be shared.
- Personal data should not be disclosed to unauthorised people, either within the PCC or externally.
- It should be noted however that, in relation to matters of Safeguarding, there sometimes is a legitimate need, i.e. a compelling reason, to share information with law enforcement authorities which over-rides the need for consent.

7.0 Data storage

These rules describe how and where data should be safely stored.

When data is **stored on paper** it should be kept in a secure place where unauthorised people cannot see it. These guidelines also apply to data that are usually stored electronically but have been printed out for some reason:

- When not required, the paper or files should be kept under lock and key.
- PCC members and anyone else covered by this policy should make sure paper and printouts are not left where unauthorised people could see them.
- Data printouts should be shredded and disposed of securely when no longer required.

When data is **stored electronically**, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data should be **protected by strong passwords** that are changed regularly and never shared between employees.
- If data are **stored on removable media** (like a CD, DVD, flash drive), these should be encrypted.
- Data should be **backed up frequently**.
- This policy equally applies to where **data is saved to mobile devices** like smart phones and tablets

- All computers and mobile devices containing data should be protected by **approved security software and a firewall**.

8.0 Data Use

When personal data is accessed and used it can be at the greatest risk of loss, corruption or theft:

- When working with personal data PCC and anyone else covered by this policy must ensure that **the screens of their computers are always locked** when left unattended.
- Personal data should **not be shared informally,** in particular it should never be sent by email, as this form of communication is not secure. Google Drive links should be used where sharing is necessary.
- Personal data must be **encrypted before being transferred electronically.**
- At the time of completing Electoral Roll Application Forms, permission must also be sought for personal data to be used in order that members may be informed about church events and the like.

Data will be destroyed when it is no longer needed. Data will be keep in accordance with the guidance set out in the guide "Keep or Bin: The Care of Your Parish Records": Records management guides | The Church of England.

Details of how we process personal data are given in our privacy notice.

12.0 Data Breaches

Any breaches of data must be logged by the Data Protection Officer within 72 hours and all PCC members notified. A record must be kept of the nature of the breach and the actions taken.

13.0 Making contact

In the first instance the Data Protection Office can be contacted via the Ropley Benefice Administrator at admin@ropleybenefice.church, phone number 07544 970166

Signed:

Rev'd Amber Beresford – Vicar & PCC Chair

Date: