Data Protection Policy

Contents of this policy

1. Introduction

2. Key Terms

3. Our Data Protection Obligations

4. Personal Data We Process

- **4.1 Personal data**
- **4.2 Special Category Data**

5. How We Process and Share Personal Data

- **5.1 Sharing Personal Data**
- **5.2 Lawful Processing**
- **5.3 Special Category Data**
- **5.4 Legitimate Interests**
- **5.5 Consent**
- **5.6 Data Sharing**
- **5.7 Data Processors**

6. Rights of Data Subjects

7. Data Breaches

8. Data Protection Impact Assessments (DPIAs)

9. Transferring Data Outside the UK

10. Ensuring Compliance and Good Practice

- **10.1 Management**
- **10.2 Review**
- **10.3 Training**
- **10.4 Documentation**
- **10.5 Data Security**

10.6 Data Retention

10.7 Email Use

10.8 CCTV and Access control

10.9 Website

10.10 Ewell Parish News

10.11 Social Media

11. Review of Policy

1. Introduction

St Mary's PCC is committed to protecting personal data and respecting the rights of all individuals whose information we hold. We value the trust placed in us and comply with all relevant legislation, including the Data Protection Act 2018 (the UK implementation of GDPR) and the Human Rights Act 1998.

We take active steps to ensure personal data is not misused, lost, accessed without permission, shared inappropriately, or kept inaccurately.

This policy explains the measures we take as a PCC and the responsibilities of all role holders, volunteers, staff, and contractors. It applies to:

- Everyone who holds a role or membership within St Mary's, and any third party providing services to the PCC.
- All personal data and special category data, whether stored on paper or electronically.

Minor revisions may be approved by the Incumbent and the Data Protection Compliance Officer (DPCO). Full review is scheduled for 2027.

2. Key Terms

Data Subject Any living person whose personal data we hold. This includes role holders, volunteers, employees, contractors, agents, staff, retirees, beneficiaries, and church members.

Personal Data Any information relating to an identifiable living person.

Data Controller The PCC and the Incumbent jointly determine how and why personal data is processed.

Processing Any action involving personal data, including collecting, storing, organising, altering, retrieving, sharing, restricting, or deleting it.

Processor Any person or organisation processing data on behalf of the PCC.

Special Category Data Sensitive data such as racial/ethnic origin, religious beliefs, health information, biometric data, sexual orientation, and similar categories requiring additional protection.

3. Our Data Protection Obligations

We ensure that all personal data is:

- Processed lawfully, fairly, and transparently.
- Used only for specific, legitimate purposes.
- Adequate, relevant, and limited to what is necessary.
- Accurate and kept up to date.
- Retained only as long as necessary.
- Kept secure using appropriate technical and organisational measures.
- Processed in accordance with the rights of data subjects.

4. Personal Data We Process

4.1 Personal Data

We may process:

- Names, titles, aliases, photographs, videos.
- Contact details (addresses, phone numbers, email addresses).
- Demographic information relevant to our mission (gender, age, marital status, nationality, education, hobbies, dependants).
- Non-financial identifiers (passport numbers, driving licence numbers, vehicle registration, tax identifiers, NI numbers).
- Financial identifiers (bank account numbers, card numbers, policy numbers).
- Financial information (salary, tax details, expenses, donations, payments for hall hire).
- Operational data (CCTV, access logs, visitor logs, accident records, insurance claims, booking details, IP addresses, website logs).
- Employee/role holder data (emergency contacts, performance information, qualifications, immigration status, employment history, publications, awards).

4.2 Special Category Data

As a church, some of the data we process may indicate religious belief. We may also process sensitive data such as racial/ethnic origin, health information, injuries, treatment, political beliefs, union membership, genetic/biometric data, sexual orientation, and criminal records.

5. How We Process and Share Personal Data

5.1 Sharing Personal Data

We treat personal data as confidential. We share it only:

- With other church members when necessary for ministry or church activities.
- With third parties when the data subject has given consent or when required by law.
- In accordance with the ICO's Data Sharing Code of Practice.

5.2 Lawful Processing

We process personal data only when at least one lawful basis applies:

- Necessary for a contract.
- Necessary to comply with a legal obligation.
- Necessary to protect someone's life (vital interests).
- Necessary for a public task with a legal basis.
- Necessary for legitimate interests that do not override the rights of the individual.
- Or, where none of the above apply, with explicit consent.

We explain our purposes in our privacy notices.

5.3 Special Category Data

Processing special category data requires an additional lawful condition, such as:

- Explicit consent.
- Employment/social protection obligations.
- Vital interests.
- Legitimate activities of a not-for-profit religious body.
- Data made public by the data subject.
- Legal claims.
- Substantial public interest.
- Archiving, research, or statistical purposes.

5.4 Legitimate Interests

Where we rely on legitimate interests, we:

- Conduct and record a Legitimate Interests Assessment (LIA).
- Ensure processing is necessary and proportionate.
- Consider safeguards and opt-outs.
- Avoid intrusive or unexpected uses of data.
- Take extra care with children's data.
- Review LIAs regularly.

5.5 Consent

Where consent is required:

- We explain clearly what we are asking for and why.
- Consent is specific and freely given.
- Consent can be withdrawn at any time.

5.6 Data Sharing

We share data only when legally permitted and record sharing where appropriate.

5.7 Data Processors

Processors must:

- Act only on PCC instructions.
- Maintain appropriate security.
- Report breaches immediately.
- Assist with investigations where needed.

6. Rights of Data Subjects

Individuals have the right to:

- Access their personal data.
- Correct inaccurate data.
- Request erasure.
- Object to processing.
- Request data portability.
- Request restriction of processing.
- Avoid automated decision-making.
- Withdraw consent.
- Lodge complaints with the ICO.

Requests must be submitted to the PCC Secretary, who informs the Vicar, Churchwardens, and DPCO within 24 hours. Identity checks may be required.

We will respond within one month. However, the law allows this one-month response deadline to be extended if any particular subject access request is 'complex'.

7. Data Breaches

A data breach includes accidental or unlawful loss, destruction, alteration, unauthorised disclosure, or access.

Any suspected breach must be reported immediately to the PCC Chair (or Vice-Chair).

The DPCO, Churchwardens, and Parish Administrator will:

- Assess the breach and risks.
- Report to the ICO within 72 hours, if required.
- Notify affected individuals promptly.
- Record all breaches.
- Inform the PCC.

8. Data Protection Impact Assessments (DPIAs)

We conduct DPIAs when processing may pose high risk, including work involving vulnerable people or new technology. Decisions not to conduct a DPIA are recorded. We consult the ICO if risks cannot be mitigated.

9. Transferring Data Outside the UK

Personal data is not transferred or stored outside the UK unless permitted by law.

10. Ensuring Compliance and Good Practice

10.1 Management

The PCC appoints a Data Protection Compliance Officer (DPCO). CCTV and access control systems are managed by the Security Officer and Security Manager.

10.2 Review

All processing activities are regularly reviewed for compliance.

10.3 Training

Role holders receive appropriate training; attendance is recorded.

10.4 Documentation

We maintain:

- Policies and procedures.
- Privacy notices.
- Registers of controllers and processors.
- DPIA records.
- Complaints records.
- Data access request logs.

- Breach records.
- Training records.
- Document control logs.

10.5 Data Security

We use appropriate technical and organisational measures, including:

- Secure storage (locked cabinets for sensitive data).
- Password-protected and up-to-date devices.
- Secure backups.
- Physical security.
- CCTV and access control.
- Regular testing of security measures.

10.6 Data Retention

We retain data only as long as necessary, following Church of England guidance (*Keep or Bin*). Financial records are kept for at least seven years. Event-related contact may continue for up to two years unless consent is renewed.

10.7 Email Use

Church email accounts are to be used for all church business. Sensitive or high-risk data must be sent using church-provided email accounts. Strong passwords must be used. Emails containing personal data must include the PCC privacy notice. “BCC” must be used when emailing non-members.

10.8 CCTV and Access Control

Separate policies govern these systems.

10.9 Website

Personal data is published only when legally justified. Sensitive documents are stored in password-protected areas.

10.10 Ewell Parish News

Personal data is included only when legally justified and in the public interest as part of t the historical record.

10.11 Social Media

Personal data is posted only when a lawful basis exists.

11. Review of Policy

This policy will be reviewed by the clergy and PCC annually.

Vicar, Churchwardens and PCC of St Mary's Ewell.

26th October 2026