St Mary's Ewell
www.stmarysewell.com

THE PAROCHIAL CHURCH COUNCIL OF THE ECCLESIASTICAL PARISH OF EWELL

Registered Charity No: 1128409

DATA PROTECTION POLICY

Version 2.00

13 February 2024

1 Introduction

1.1 The PCC is committed to protecting personal data and respecting the rights of our data subjects; the people whose personal data we collect and use. We value the personal information entrusted to us and we respect that trust, by complying with the law governing the control and use of personal data as set out in the Data Protection Act 2018 which is the UK's implementation of the General Data Protection Regulation (the "GDPR") and other legislation relating to personal data and rights such as the Human Rights Act 1998.

1.2 The PCC is thus committed to protecting personal data from being misused, getting into the wrong hands as a result of poor security, being shared carelessly or being inaccurate.

1.3 This policy sets out the measures we take as an organisation and what we expect each of our role holders or members to do in order to ensure we comply with the relevant legislation. It applies to:
a) all role holders and members and to any third party who provide a service to the PCC
b) all personal data and special categories of data stored on paper or on computer.

1.4 Version 2.00 of this policy was approved by the PCC on 13 February 2024. Minor revisions are approved by the Incumbent and Data Protection Compliance Officer. The policy is due a full revision in 2027

2 Terminology

The Data Protection Regulations use various terms as follows

2.1 **Data subject.** This is any identified or identifiable living person to whom personal data relates**.** The data subjects for whom we hold personal data include our role holders (for example church officers, volunteers, employees, contractors, agents, staff, retirees, beneficiaries) and other members of our church.

2.2 **Personal data**. This means any information relating to an identified or identifiable living person ('data subject'). Section 4 considers the personal data we may hold.

2.3 **Data controller**. This is the legal entity that alone or jointly with others determines the purposes and means of processing personal data. In our case the PCC and the incumbent are joint data controllers.

2.4 **Processing.** This means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means. This includes collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.

2.5 **Processor.** Any person or body that processes data on behalf of the data controller.

2.6 **Special categories of personal data.** These are personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

3 Data protection obligations

In accordance with the Data Protection Regulations we will ensure that all personal data are:

(a) processed lawfully, fairly and in a transparent manner;

(b) processed for specified, explicit and legitimate purposes and not in a manner that is incompatible with those purposes;

(c) adequate, relevant and limited to what is necessary for the purposes for which it is being processed;

(d) accurate and, where necessary, up to date;

(e) not kept longer than necessary for the purposes for which it is being processed;

(f) processed in a secure manner, by using appropriate technical and organisational means;

(g) processed in keeping with the rights of data subjects regarding their personal data.

4 Personal data

4.1 The personal data we may process are detailed in our data privacy notices and are:

- Names, titles, and aliases, photographs and videos;
- Contact details such as telephone numbers, addresses, and email addresses;
- Where they are relevant to our mission, or where you provide them to us, we may process demographic information such as gender, age, date of birth, marital status, nationality, education/work histories, academic/professional qualifications, hobbies, family composition, and dependants;
- Non-financial identifiers such as passport numbers, driving license numbers, vehicle registration numbers, taxpayer identification numbers, employee identification numbers, tax reference codes, and national insurance numbers.
- Financial identifiers such as bank account numbers, payment card numbers, payment/transaction identifiers, policy numbers, and claim numbers.
- Financial information such as salary, bonus, record of earnings, tax code, tax and benefits contributions, expenses claimed, creditworthiness, car allowance (if applicable), amounts insured and amounts claimed, donations or payments for activities such as the use of the church hall.
- Other operational personal data created, obtained, or otherwise processed in the course of carrying out our activities, including but not limited to, CCTV, records of access to the church buildings including Ewell Hall, recordings of telephone conversations, IP addresses and website visit histories, logs of visitors, and logs of accidents, injuries, insurance claims and booking details for the use of the church or Ewell Hall.
- Other employee data (not covered above) relating to Role Holders including emergency contact information; gender, birth date, referral source (e.g. agency, employee referral); level, performance management information, languages and proficiency; licences/certificates, citizenship, immigration status; employment status, retirement date; billing rates, office location, practice and speciality; publication and awards for articles, books etc.; prior job history, employment references and personal biographies.

4.2 Special categories of personal data

In addition to the data listed in section 4.1 above, some of the data we process are likely to fall within the special category of personal data, often referred to sensitive data. As a church, the fact that we process some data at all may be suggestive of personal religious beliefs. Where this information is provided, we may also process other categories of sensitive personal data: racial or ethnic origin, sex life, mental and physical health, details of injuries, medication/treatment received, political beliefs, labour union affiliation, genetic data, biometric data, data concerning sexual orientation and criminal records, fines and other similar judicial records.

4.3 Sharing personal data

We will treat personal data as strictly confidential and will only share it with other members of the church in order to carry out a service to other church members or for purposes connected with the church and its activities were permitted to do so by data protection law. This is explained in our data privacy notices. We will only share personal data with third parties with the consent of the data subject and where appropriate keep records of any such record sharing. However, we recognise that this may not be possible in all cases, for example, if disclosure is required by law. We will follow the ICO's statutory Data Sharing Code of Practice (or any replacement code of practice) when sharing personal data with other data controllers. Legal advice will be sought as required.

5 Data processing

5.1 Our data processing is described in our Data Privacy Notices for non-role holders and for role holders.

5.2 We will ensure that the processing of personal data is fair and lawful.

This means that there must be a legal basis for the processing and the processing must be transparent. By publishing our data privacy notices on the church website and placing a link on Ewell Hall website, we will provide people with an explanation of how and why we process their personal data at the point we collect their data.

We will therefore ensure that our processing of personal data meets at least one of the following legal conditions as detailed in the Data Protection Regulations:

- the processing is necessary for a contract with the data subject;
- the processing is necessary for us to comply with a legal obligation;
- the processing is necessary to protect someone's life (this is called "vital interests");
- the processing is necessary for us to perform a task in the public interest, and the task has a clear basis in law;
- the processing is necessary for legitimate interests pursued by ourselves or another organisation, unless these are overridden by the interests, rights and freedoms of the data subject.

If none of these legal conditions apply, the processing will only be lawful if the data subject has given their explicit consent and we will therefore seek explicit consent in this case.

We will only process personal data for the specific purposes explained in our privacy notice or for other purposes specifically permitted by law. We will explain these purposes to data subjects unless there are lawful reasons for not so doing.

5.3 Processing special categories of personal data

Processing of 'special categories' of personal data is only lawful when, in addition to the conditions above, one of the extra conditions, as listed in the Data Protection Regulations is met. We will ensure that as least one of these conditions is met. The conditions include:

- the data subject has given explicit consent to the processing of those personal data for one or more specified purposes;
- processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law;
- processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
- processing is carried out in the course of its legitimate activities with appropriate safeguards by a not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;
- processing relates to personal data which are manifestly made public by the data subject;
- processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
- processing is necessary for reasons of substantial public interest on the basis of the Data Protection Regulations;
- processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

Where personal data are collected directly from the data subject, we will inform the data subject whether he or she is obliged to provide the personal data and the consequences, if he/she does not provide the data

We note that other data may be considered as sensitive, such as bank details, but are not subject to the same legal protection as the above listed special categories of data.

5.4 Legitimate interests

When we use legitimate interests as the legal basis for processing we will:

- understand our responsibility to protect the individual's interests;
- check that legitimate interests is the most appropriate basis;
- conduct a legitimate interests assessment (LIA) and keep a record of it, to ensure that we can justify our decision;
- identify the relevant legitimate interests;
- check that the processing is necessary and there is no less intrusive way to achieve the same result;

- perform a balancing test, so that we are confident that the individual's interests do not override our legitimate interests;
- only use individuals' data in ways they would reasonably expect, unless we have a very good reason;
- not use people's data in ways they would find intrusive or which could cause them harm, unless we have a very good reason;
- when we process children's data, take extra care to make sure we protect their interests;
- have considered safeguards to reduce the impact where possible;
- have considered whether we can offer an opt out;
- if our LIA identifies a significant privacy impact, consider whether we also need to conduct a data protection impact assessment.

We will keep our LIAs under review, and repeat them if circumstances change.

The bases for our legitimate interests are given in our data controllers register.

5.5 Consent

Where we are required to get consent from a data subject, we will clearly set out for what purpose we are asking consent, including why we are collecting the data and how we plan to use it. Consent will be specific to each process for which we request consent and we will only ask for consent when the data subject has a real choice whether or not to provide us with their data.

Consent can however be withdrawn at any time and if withdrawn, the processing will stop. Data subjects will be informed of their right to withdraw consent and how consent can be withdrawn.

5.6 Our data processing

The data processing that we undertake is listed in our data privacy notices.

5.7 Data sharing

We will only share personal data with other organisations or people when we have a legal basis to do so. We will inform the data subject beforehand unless there are legal exemptions which apply to informing the data subject. We will keep records of data sharing in our data processors register where appropriate.

5.8 Processing by appointed data processors/contractors

Companies who are appointed by us as data processors are detailed in our data controllers register. They are required to comply with the data protection and other appropriate regulations in relation to the data processing that they undertake for us.

- They may only undertake such data processing under instruction from the PCC and must implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk involved.
- They must inform the PCC immediately of any data breach and if appropriate, help the PCC to investigate the breach and mitigate its effects.

6 Data subject's rights

6.1 The Data Protection Regulations gives the following rights to individuals in respect of their personal data that we hold:

- The right to access and confirm their personal information that we hold
  At any point data subjects can contact us to request the information we hold on them as well as why we have that information, who has access to the information and from where we obtained the information.
- The right to correct and update information
  If the data subject informs us that the data we hold is out of date, incomplete or incorrect, we will update the data.
- The right to have information erased
  If the data subject feels that we should no longer be using their data or that we are illegally using their data, they can request that we erase the data that we hold.
- The right to object to processing of data
  Data subjects have the right to request that we stop processing their data.
- The right to data portability
  Data subjects have the right to request that we transfer some of their data to another controller.
- The right, where there is a dispute in relation to the accuracy or processing of personal information, to request that a restriction is placed on further processing
- The right not to be subject to a decision based solely on automated decision making
- The right at any time to withdraw consent to any processing of data for which consent was sought
  Consent can be withdrawn by email, or by post.
- The right to lodge a complaint with the Information Commissioner's Office

6.2 Requests from data subjects to exercise their rights

Requests from data subjects to exercise any of the rights detailed above should be submitted to the PCC secretary by email or in writing. The PCC secretary must inform the Vicar, Churchwardens and Data Protection Compliance Officer within 24hrs of reading the email or written Subject Access Request. For requests relating to building access or CCTV, the Security Manager and Security Officer must also be informed. Together these officers must take appropriate steps to comply with the subject data request. Before responding to the request, they must consider whether to first request proof of identity. If the information requested also includes information about another person, permission must be sought from that data subject before the information can be released

If we receive a request to access the personal information we hold on a data subject, to ask why we have that information, who has access to the information and from where we obtained the information, we will respond within one month. We will make no charges for the first request but additional requests for the same data may be subject to an administrative fee. If we are unable to comply we must give the reasons why this is so.

If we receive a request for erasure of data, we will confirm whether the data has been deleted or the reason why it cannot be deleted (for example because we need it for our legitimate interests or regulatory purpose(s)).

If we receive a request to stop processing data, we will inform the data subject whether we are able to comply or if we have legitimate grounds to continue to process their data. Even after this right has been exercised, we may continue to hold their data to comply with their other rights or to bring or defend legal claims.

We will communicate any rectification or erasure of personal data or restriction of processing carried out to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. We will also inform the data subject about those recipients if the data subject requests it.

If we receive a request to transfer data, we will comply with the request when it is feasible to do so within one month.

7 Data breaches

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

When role holders or members of the church or organisations that perform data processing for us know that there has been or may have been a data breach this must be reported immediately to the chair of the PCC, or in his/her absence to the vice-chair, who must immediately inform the data protection compliance officer, the churchwardens and if appropriate the parish administrator. Together these officers must:

- establish whether a breach has taken place and if so whether it is likely to result in a risk to the data subject(s);
- if such a risk is likely, the data breach must be reported to the Information Commissioner's Office (ICO) as soon as possible and no later than 72 hours after notification of the breach was received;
- notify the data subject(s) and others as appropriate and without undue delay. Informing data subjects can enable them to take steps to protect themselves and/or exercise their rights;
- keep a record of the breach whether or not the ICO was informed;
- inform the PCC of the nature of the breach and the assessment made of the risk to the data subjects.

8 Data Protection Impact Assessments

When we are planning to carry out any data processing which is likely to result in a high risk we will carry out a Data Protection Impact Assessment (DPIA). These include situations when we process data relating to vulnerable people or are, using new technology. Any decision not to conduct a DPIA will be recorded.

We may also conduct a DPIA in other cases when we consider it appropriate to do so. If we are unable to mitigate the identified risks such that a high risk remains we will consult with the ICO.

DPIAs will be conducted in accordance with the ICO's Code of Practice 'Conducting privacy impact assessments'.

9 Transferring data outside the UK

Personal data must not be transferred (or stored) outside of the UK unless this is permitted by the Data Protection Regulations.

10 Ensuring compliance and good practice

10.1 Management of data protection

As noted in section 1.1, the PCC is committed to protecting personal data and respecting the rights of our data subjects. It is responsible for compliance with the Data Protection Regulations and to facilitate this it appoints a Data Protection Compliance Officer (DPCO). (This is not the same as the Data Protection Officer referred to in the regulations to which specific conditions are attached. We are not required to appoint a Data Protection Officer).

The DPCO works with other church officers to monitor, audit or otherwise review the use and processing of personal data that we hold.

The PCC uses CCTV and access control systems for the security of the church and Ewell Hall and their contents i.e. to protect people and property. CCTV is also used to monitor compliance with the booking conditions for the hire of Ewell Hall. It appoints a Security Officer (SO) who is responsible for the overall management of our security systems. This person is usually a Churchwarden. The PCC also appoints a Security Manager who is responsible for defining, implementing and monitoring its systems for managing and recording secure access to the church premises and Ewell Hall as well as the use of CCTV.

The PCC meetings include data protection as a regular item.

The PCC, the DPCO, the SO and other church officers will seek legal advice where necessary. This may for example be from the ICO or the relevant officers of the Guildford Diocese.

10.2 Review

All personal data processing is reviewed by the DPCO and/or other church officers to ensure compliance with the regulations. This includes the legal basis for processing, whether all data are necessary, how data are collected, who has access to the data, how the data are stored and data retention periods.

10.3 Training

We will ensure that appropriate role holders receive in-house training. A register is kept of training courses and those attending.

10.4 Documentation

Our personal data processing activities are recorded in the following documentation:

- Policies and procedures (this document and *inter alia* our Email, Security Management and CCTV policies). Policies and procedures are reviewed every five years or more frequently as appropriate;
- Two data privacy statements (general and role holders). These are available on our websites and from the Parish Administrator. They are reviewed as necessary and at least every three years;
- Registers of Data Controllers and Data Processors. We are required to maintain records of the processing activities under our control. For this purpose we use registers based on templates provided by the ICO;
    - In the Data Controllers Register for each data processing activity we record inter alia the purpose of the processing, the categories of data, data subjects and recipients of the data, security measures, data retention schedules, the lawful basis and if appropriate details of our legitimate interest;
    - In the Data Controllers Register, we also note details of those organisations that perform data processing for us so that this also forms our Data Processors Register.
    - The registers are updated as appropriate and reviewed periodically.
- Records of Data Protection Impact Assessments;
- Records of complaints;
- Records of data access and other requests;
- Records of data breaches;
- Records of training;
- Document control records of version numbers, changes made and dates when revisions are made to policies and privacy notices

10.5 Data security

We will use appropriate measures to keep personal data secure at all points of the processing. Keeping data secure includes protecting it from unauthorised or unlawful processing, or from accidental loss, destruction or damage.

We will implement security measures which provide a level of security which is appropriate to the risks involved in the processing.

Measures will include technical and organisational security measures. In assessing what measures are the most appropriate we will take into account the following and anything else that is relevant:

- the quality of the security measure;
- the costs of implementation;
- the nature, scope, context and purpose of processing;
- the risk (of varying likelihood and severity) to the rights and freedoms of data subjects;
- the risk which could result from a data breach.

Security measures may include:

- technical systems security;
- measures to restrict or minimise access to data;

- measures to ensure our systems and data remain available, or can be easily restored in the case of an incident;
- physical security of information and of our premises;
- CCTV monitoring and access control and monitoring;
- organisational measures, including policies, procedures, training and audits;
- regular testing and evaluating of the effectiveness of security measures.

The PCC has separate policies for CCTV monitoring and access control and monitoring.

The data that we store may be on paper, stored on local computers or in the cloud, and may be kept in the church or Ewell Hall and in the homes or offices of our role holders and members. As part of our review and audit procedures (section 10.2) we require:

Personal data shall be kept no longer than required (section 10.6)

When no longer required paper records should be shredded or similarly destroyed.

When no longer required computer based records should be deleted, including when possible computer back-ups.

Paper based records of personal data should be kept in a secure location. Whenever practicable they should be kept in a locked filing cabinet. For data considered sensitive, high risk or special category this is a requirement.

Computers and other devices storing personal data must be kept secure by requiring password-controlled or biometric login and must run up-to-date anti-virus software. Physical copies of back-ups must be kept in a secure location. Mobile phones should be kept secure in a similar way.

The PCC has a business Dropbox account.

Storage of bank details may only be in our authorised bank accounts and only when necessary to facilitate payments.

10.6 Data retention

We will aim to keep personal data for no longer than is reasonably necessary and in accordance with the guidance set out in the guide “Keep or Bin: Care of Your Parish Records” which is available from the Church of England website. We therefore review the content of all data collected, retention periods and use and delete it when it is no longer needed.

We keep some records permanently if we are legally required to do so. We may keep some other records for an extended period of time. For example, it is current best practice to keep financial records for a minimum period of 7 years to support HMRC audits.

Where we contact people about events that they have attended in the past, we may contact them for up to two years thereafter. We will not contact them after that unless we have their consent or we believe that the event will continue to be of interest to them.

10.7 Use of email

There is a separate policy for the use of email on Church business.

Email is used by our role holders and members and often a personal email account may be used for both personal and church business. Where it is likely that the personal data received or sent by role holders would be considered sensitive, high risk or special category an email

account provided by our email service provider must be used. A personal email account may not be used for this purpose.

Those sending emails on PCC business, whether using a church email address or a personal email address, must use a strong email password which is compliant with the church email policy and is not the same as that used for any other email or computer account held by the email user. They should also include the following email privacy notice at the end of all emails sent on church business that contain personal data (e.g. names and contact details of church members or members of the public).

> *This message contains information sent on behalf of the PCC of St Mary the Virgin Ewell (registered charity no 1128409), and may include privileged and confidential information. If you believe you are not the intended recipient you may not make any disclosure, distribution or use of the contents. If you have received this message in error please delete it and notify the sender immediately.*

Email software has a signature facility that can be used to add this this privacy notice to the bottom of emails. Help is provided where necessary to set-up email signatures.

Those sending emails on PCC business **should not**

- include any personal data that are not required for the purpose of the email
- or use "CC" when copying emails to non-members of St Mary's church. This shares all the email addresses in the "CC" list with everyone in the list, and if shared outside our church membership, could be a breach of the Data Protection Regulations. "BCC" should be used instead which provides a "blind carbon copy"

10.8 CCTV and access control and monitoring

As noted in section 10.1, the PCC uses CCTV and access control systems. There are separate documents that describes our policies and procedures for using and managing these facilities.

10.9 Website

There are separate public websites for the church and for Ewell Hall. Content published on these websites only includes personal data where there is an appropriate legal basis. Recent copies of the Weekly Notes and Ewell Parish News and other documents created for public consumption are posted to the church website. Rotas and other documents containing personal data are made available in the password-protected area of the church website. All material is reviewed before being posted on either website.

10.10 Ewell Parish News

Content published in the Ewell Parish News only includes personal data where there is an appropriate legal basis. EPN fulfils the role of an historical record of the public activities of St Mary's church, and personal data may be included in articles so that this record can be made in the public interest. Editorial control ensures that data protection decisions as to what content may be published are informed and proportionate and respect the rights of data subjects.

10.11 Social media

Content we publish on social media may only include personal data when there is an appropriate legal basis.