

ST JOHN & ST LUKE


✠

CLAY HILL

PCC of St John & St Luke, Clay Hill

The Parochial Church Council of the Ecclesiastical Parish of
St John the Baptist and St Luke the Evangelist, Clay Hill, Enfield
Registered Charity number 1151418

Data Protection Policy

Prepared by:	John Wright
This version:	2.1
Date of Issue:	9 May 2023
Date of review:	29 June 2023
Signed by:	

PARISH OF ST JOHN & ST LUKE: DATA PROTECTION POLICY

Contents

1. Introduction.....	2
2. Definitions.....	2
3. Organisation and Responsibilities.....	3
3.1 General Guidelines	3
3.2 Responsibility of the Vicar	3
3.3 Parochial Church Council.....	3
3.4 Data Protection Compliance Officer	4
3.5 Responsibility of members of the PCC, Role Holders and voluntary workers	4
3.6 Further Information.....	4
3.7 Detailed Procedures and Guidelines	4
4. Provisions of the General Data Protection Regulation	5
4.1 Underlying Principles	5
4.2 The Rights of Individuals (Data Subjects).....	5
4.3 Lawful Bases for Processing Data.....	6
5. Policy Statements.....	6
5.1 Privacy Notices	6
5.2 Data Subject Access Requests	7
5.3 Personal Data Breaches	7
5.4 Request to Erase or Stop Processing Personal Data	7
5.5 Data Maintenance.....	8

PARISH OF ST JOHN & ST LUKE: DATA PROTECTION POLICY

1. Introduction

The Parochial Church Council (PCC) of the Parish of St John & St Luke, Clay Hill is committed to a policy of protecting the rights and privacy of individuals. The PCC needs to collect and use certain types of data about individual in order to carry on its work. This personal information must be collected and dealt with appropriately.

The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR) which controls how personal information is used by organisations, businesses or the government. It governs the use of information about people ie personal data. Personal data can be held on computers, laptops and mobile devices or on paper in a manual file and includes emails, letters, minutes of meetings and photographs.

For the parish, the PCC is the Data Controller for the information held. The Vicar, members of the PCC, Role Holders and volunteers will be personally responsible for processing and using personal information for parish purposes in accordance with GDPR and will be expected to read and comply with this policy.

The PCC intends to ensure that personal information is treated lawfully and correctly which the PCC regards as very important to successful working and to maintaining the confidence of those with whom it deals with.

The purpose of this policy is to set out the commitment and procedures for protecting personal data. It describes how personal data must be collected, handled and stored to comply with GDPR, how the rights of individuals are protected and how the PCC protects itself from the risk of a data breach.

This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments made to GDPR. To achieve this, the policy and the way in which it has operated will be reviewed regularly and the appropriate changes made.

2. Definitions

Consent is any freely given, specific, informed and unambiguous indication of an individual's wishes – either by a statement or by a clear affirmative action.

Data Controller is the person or organisation with overall responsibility for personal data, how and why it is processed and making sure an organisation adheres to the GDPR. For the Parish of St John and St Luke Clay Hill, this is the Parochial Church Council (PCC).

Data Protection is the process of safeguarding Personal Data from unauthorised or unlawful disclosure, access, alteration, processing, transfer or destruction.

Data Protection Compliance Officer (DPCO) is responsible for overseeing and implementing the PCC's data protection strategy to make sure it complies with the GDPR.

Data Subject is the individual about whom personal data is processed.

General Data Protection Regulation (GDPR) was implemented in the UK on 25 May 2018 within the Data Protection Act 2018 which replaced the Data Protection Act 1998.

Information Commissioner's Office (ICO) – The UK Information Commissioner responsible for implementing and overseeing GDPR.

Personal Data is any information about a living person which can identify them. This is not just an individual's name and address but any ID information, for example a phone number or email address. Any other contact information or an individual's employment history, medical conditions, criminal record or credit history are all personal data.

PARISH OF ST JOHN & ST LUKE: DATA PROTECTION POLICY

Processing personal data means storing or deleting any personal data on a computer, database or some manual files (e.g. HR personnel files). "Processing" also covers selecting a name for a mailing list as well as transferring or altering data. Indeed, practically anything done to personal data constitutes processing.

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.

Search Access Request (SAR) is a request for personal information that the PCC may hold about an individual.

Sensitive Personal or 'Special Category Data' means information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health, sexual life, criminal history and allegations, genetic data, biometric data and sexual orientation.

3. Organisation and Responsibilities

3.1 General Guidelines

- The only people able to access data covered by this policy should be those who need it for their work on behalf of the PCC.
- Data should not be shared informally.
- The PCC has and will provide training to all PCC members, Role Holders and volunteers to help them understand their responsibilities when handling data.
- Data holders should keep all data secure by taking sensible precautions and following guidelines published by the PCC below.
- When storing data on electronic system, strong passwords must be used and they should never be shared.
- Personal data should not be disclosed to unauthorised people, either within the parish or externally.
- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Data holders should request help from the Vicar or the Data Protection Compliance Officer if they are unsure about any aspect of data protection.

3.2 Responsibility of the Vicar

The Vicar is vested with overall accountability for compliance with data protection regulations by the PCC.

3.3 Parochial Church Council

The Parochial Church Council (PCC) as "Data Controller" will determine what purposes personal information held will be used for and ensure that appropriate codes of practice are in place.

The PCC will take into account legal requirements and ensure that they are properly implemented. Through appropriate management, strict application of criteria and controls, the PCC will:

- fully observe conditions regarding the fair collection and use of information;
- meet its legal obligations to specify the purposes for which information is used;
- collect and process appropriate information and only to the extent that it is needed to fulfil its operational needs or to comply with any legal requirements;
- ensure the quality of information used;
- ensure that the rights of individuals about whom information is held, can be fully exercised under GDPR.

3.4 Data Protection Compliance Officer

The Data Protection Compliance Officer (DPCO) will be responsible to the PCC for ensuring that the policy is implemented and will have overall responsibility for:

- ensuring everyone processing personal information understands that they are contractually responsible for following good data protection practice;
- ensuring everyone processing personal information is appropriately trained to do so;
- ensuring anybody wanting to make enquiries about handling personal information knows what to do;
- dealing promptly and courteously with any enquiries about handling personal information;
- describing clearly how the PCC handles personal information;
- regularly reviewing and auditing the ways the PCC holds, manages and uses personal information;
- regularly assessing and evaluating the PCC's methods and performance in relation to handling personal information;
- provide reports to the PCC about data protection matters.

3.5 Responsibility of members of the PCC, Role Holders and voluntary workers

All members of the PCC, Role Holders and voluntary workers have a responsibility to co-operate in the implementation of this policy and must therefore:

- comply with all operating instructions and working procedures;
- report any data breach (however minor) immediately to the Vicar or the Data Protection Compliance Officer.

3.6 Further Information

In case of any queries or questions in relation to this policy please contact the Data Protection Compliance Officer.

The Information Commissioner's Office website (www.ico.gov.uk) is another source of useful information

The ICO personal data breach helpline can offer advice about what to do after a personal data breach has been experienced, including how to contain it and how stop it happening again. It can also offer advice about whether individuals involved should be notified. The ICO operates a chatbot service which allows site visitors to ask and get answers to, questions from an automated service. The ICO may also be contacted by e-mail on icocasework@ico.org.uk. The ICO's normal opening hours are Monday to Friday between 9am and 5pm (excluding bank holidays).

0303 123 1113

3.7 Detailed Procedures and Guidelines

The PCC has prepared the following procedures and guidelines that provide detailed instructions to implement the policy statements in section 5.

- Clay Hill Search Access Request Procedure (see section 5.2)
- Clay Hill Personal Data Breach Procedure (see section 5.3)
- Clay Hill Data Subject Maintenance Requests Procedure (see section 5.4)
- Clay Hill Data Maintenance Guidelines (see also section 5.5)

4. Provisions of the General Data Protection Regulation

4.1 Underlying Principles

The GDPR has a number of underlying principles which include that personal data:

1. must be processed lawfully, fairly and transparently.
2. may only be used for a specific processing purpose that the individual has been made aware of and no other, without further consent.
3. should be adequate, relevant and limited, i.e. only the minimum amount of data should be kept for specific processing.
4. must be accurate and where necessary kept up to date.
5. should not be stored for longer than is necessary and stored safely and securely.
6. should be processed in a manner that ensures appropriate security and protection.

Parental consent will be required for the processing of personal data of children under age 13.

4.2 The Rights of Individuals (Data Subjects)

1. Right to be informed

Individuals continue to have a right to be given "fair processing information", usually through a privacy notice. Under the GDPR there is additional information that the PCC will need to supply.

Example: The PCC will have to explain the lawful basis for the processing of their data; how long the PCC will keep it and that individuals have a right to complain to the ICO if they think that there is a problem in the way that the PCC deals with their personal data.

2. Right to access (includes subject access requests)

Individuals have the right to request information about the personal data held and processed by the PCC and to request a copy of that information. The PCC must respond without undue delay and in any case within one month of receipt of the request.

3. Right to rectification (correction)

Individuals have the right to have their personal data corrected (rectified) if it is inaccurate or incomplete. The PCC has one month to do this after receipt of the request.

4. Right to erasure (also known as the right to be forgotten)

Individuals have the right to request the removal or erasure of their personal data in certain circumstances.

Example: If it is no longer necessary to process their data, the individual objects to such processing and/or the individual withdraws consent.

However, consent may not be the appropriate lawful basis for data processing.

Example: Safeguarding information about an individual cannot be deleted if retention is still necessary, reasonable and proportionate to protect members of the public from significant harm or if some financial information, such as that relating to Gift Aid, cannot be deleted immediately due to financial auditing regulations.

5. Right to restrict processing

Individuals have the right to restrict processing of their personal data in certain circumstances.

Example: If a person believes his/her personal data is inaccurate or he/she objects to the processing. If processing is restricted, data can still be stored but cannot otherwise be used.

6. Right to data portability

Individuals have the right to request that their personal data be provided to them (or a third party) in a machine-readable portable format free of charge. The PCC would have to consider how and where the personal data is held and if such data can be easily transferred in a safe, secure manner without impacting the usability of such data by the Individual. The PCC will need to comply with such requests without undue delay and in any event within one month.

PARISH OF ST JOHN & ST LUKE: DATA PROTECTION POLICY

7. Right to object

Individuals have the right to object to processing in certain circumstances

Example: If the PCC has relied on a legitimate interest to process data without consent and an individual is not happy with this then they have the right to object to the PCC processing their data.

8. Right not to be subject to automated decision-making including profiling

The GDPR provides protection against the risk that a potentially damaging decision is taken without human intervention.

4.3 Lawful Bases for Processing Data

The six lawful bases for processing personal data under the GDPR are:

1. Consent

The PCC must be able to demonstrate that consent was freely and clearly given by an Individual. Consents given in written declarations which also cover other matters must be clearly distinguishable, must be intelligible, easily accessible and in clear and plain language.

2. Legitimate interests

This is a processing activity that an Individual would normally expect the PCC to do with their personal data. This involves balancing between the PCC's legitimate interests and the interests or fundamental rights and freedoms of the Individual – in particular where the Individual is a child. The privacy policy must inform Individuals about the legitimate interests that are the basis for the balancing of interests.

3. Contractual necessity

Personal data may be processed if the processing is necessary in order to enter into or perform a contract with the Individual or to take steps prior to entering into a contract. *(Unlikely for a PCC.)*

4. Compliance with legal obligations

Personal data may be processed if the PCC is legally required to perform such processing.

Examples: To comply with the provisions of the Church Representation Rules, preparing claims for recovery of Gift Aid or reporting of race or ethnic origin or gender.

5. Vital interests

Personal data may be processed to protect the vital interests of an Individual. *(Rare)*

Example: In a life or death situation it is permissible to use a person's medical or emergency contact information without their consent.

6. Public interest

Personal data may be processed if the processing is necessary for the performance of tasks carried out in the public interest or for a function that has a clear basis in law. *(Unlikely for a PCC)*

5. Policy Statements

5.1 Privacy Notices

The PCC is required to provide individuals with extensive information about how their personal data is collected, stored and used by the PCC. This information is published in a General Privacy Notice that may be viewed electronically on the parish website <http://www.clayhillparish.org.uk> or on paper copies appended to the noticeboards in the porch of both churches.

The General Privacy Notice explains:

- why the information is needed – the tasks for which it may be used;
- the legal basis for processing personal data;
- the conditions under which personal data may be shared;
- how long data will be retained;
- the rights of an Individual regarding their personal data.

5.2 Data Subject Access Requests

The PCC will respond within one month to a Data Subject Access Request (SAR) from an Individual to ascertain what personal information about the Individual is held by the PCC and why the PCC holds that information. Under GDPR, there is no charge for a SAR unless the request is “*manifestly unfounded or excessive*”.

In responding to a SAR, the PCC will need to advise the Individual of:

- the purposes of the processing;
- the categories of personal data concerned;
- who are the recipients to whom the PCC discloses the information;
- where possible, how long the PCC will hold onto the information or what categories the PCC uses to decide how long the personal information will be held for;
- the right to request rectification, erasure or restriction of the processing;
- the right to lodge a complaint to the ICO;
- where the personal data is not collected from the Individual, the source from where the PCC obtained the data.

Under GDPR, the PCC can withhold personal data if disclosing it would “*adversely affect the rights and freedoms of others*”. Some of the exemptions apply to:

- crime prevention and detection;
- negotiations with the requester;
- confidential references given by an organisation;
- information used for research, historical or statistical purposes.

The PCC will take advice if it is proposing to withhold information on this basis as its applicability will need to be carefully considered and its use should not act to result in a refusal to provide all information.

The PCC has established a procedure for dealing with SARs.

5.3 Personal Data Breaches

All actual or suspected Personal Data Breaches involving personal information held on behalf of the PCC must be reported immediately to the Vicar or Data Protection Compliance Officer, either by the person who holds the personal information held on behalf of the PCC or the Individual.

The PCC will seek the advice of the London Diocesan Registrar about any suspected breaches without delay and will maintain a log detailing all actions taken.

The PCC will inform the ICO and all Individuals concerned within 72 hours in certain circumstances. *Example:* Where there is a high risk to the individual(s) involved such as through identity theft.

The PCC has established a procedure for responding to and dealing with all Personal Data Breaches including recording details of all actions taken.

5.4 Request to Erase or Stop Processing Personal Data

An Individual may request that the PCC:

- corrects and updates any inaccuracies in the personal data held about the Individual;
- erases all personal data held about the Individual;
- restricts processing the personal data held about the Individual;
- stops processing the personal data held about the Individual.

However, an Individual should be aware that the PCC is sometimes unable to delete or stop processing personal data:

Example: When the PCC needs it for legitimate interests or regulatory purpose(s) or to comply with other rights of the Individual or to bring or defend legal claims.

PARISH OF ST JOHN & ST LUKE: DATA PROTECTION POLICY

The PCC has established a Data Subject Maintenance Requests Procedure for responding to requests from Individuals to correct, erase, restrict processing or stop processing personal data.

5.5 Data Maintenance

The PCC has established a set of guidelines for:

- managing and controlling personal data during telephone and email communications;
- ensuring that personal data records including emails, computer files and paper documents are carefully named and organised to facilitate easy and speedy location during a search;
- ensuring that personal data held either electronically or on paper is securely stored to prevent access by an unauthorised person;
- ensuring that personal data is securely destroyed or deleted as soon as it is no longer needed.

All people who hold and process personal data on behalf of the PCC will be expected to adhere to these guidelines.