GDPR Policy
St Mary the Virgin, Whickham

I. Purpose

For the purposes of the Data Protection Act 1998 and the General Data Protection Regulation (GDPR), **St Mary the Virgin, Whickham. PCC Officers, Trustees, Office employees** ("we", "us" or "our"), are a 'Data Controller'. This means that we are responsible for, and control the processing of, your personal information. As the Data Controller, we are responsible for implementing appropriate technical and organisational measures through the issue of this policy to be able to demonstrate that data processing is performed in accordance with the GDPR.

Definitions of Key Terms

Data Controller – means a body which, alone or jointly with others, determines the purposes and means of the processing of personal data. They must be able to demonstrate compliance with the data protection principles and take appropriate technical and organisational measures to ensure their processing is carried out in line with the UK GDPR.

Data Processor – means a body which processes personal data on behalf of the controller. In doing so, they serve the controller's interests rather than their own.

Data Subject – This is an end user whose personal data can be collected.

II. Scope

This policy applies to all our employees regardless of full time, part time, casual or temporary employment or level and to comply with the laws and regulations of the countries in which we operate. The GDPR's requirements apply to personal information gathered by us and anyone in our organisation who processes that data.

The GDPR applies to two types of data as detailed below:

- **Personal Data** – This is any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. This can include a name, identification number, location data or online identifier. The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria.
- **Sensitive Personal Data** – This is referred by the GDPR as "special categories of personal data" and can include the following: o Race
  - Ethnicity
  - Political views
  - Religion, spiritual or philosophical beliefs
  - Biometric data for ID purposes
  - Health data
  - Sex data

- Sexual orientation
- Genetic data

III. Responsibility

All PCC Members of the trust and employees are required to read, understand and adhere to the Code and the policies it refers to.

The responsibility of the implementation of the GDPR policy will be with the PCC. Any queries relating to requests or GDPR breaches must be sent to the St Mary the Virgin, Whickham PCC in the first instance.

Any changes to this policy will be made by the Data Controller with approval of St Mary the Virgin, Whickham PCC who are responsible for contents of this policy.

Principles The UK GDPR sets out six key principles which lie at the heart of the regulation:

a) **Lawfulness, Fairness and Transparency** – Data processed lawfully, fairly and in a transparent manner in relation to individuals.

b) **Purpose Limitation** – Data collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

c) **Data Minimisation** – Data is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

d) **Accuracy** – Data is accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

e) **Storage Limitation** – Data kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

f) **Integrity and Confidentiality** – Data is processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

St Mary the Virgin, Whickham is committed to meeting these principles as set out in this policy.

IV. Data Subject Rights

GDPR gives individuals eight rights relating to their personal data, which are detailed below. In order to process any of the requests listed below, we may need to verify your identity for your security. In such cases your response will be necessary for you to exercise this right.

1. **The right to be informed**

Organisations need to tell individuals what data is being collected, how it's being used, how long it will be kept and whether it will be shared with any third parties. This information must be communicated concisely and in plain language.

2. **The right of access**

Individuals can submit subject access requests, which oblige organisations to provide a copy of any personal data they hold concerning the individual. There are exceptions for requests that are manifestly unfounded, repetitive or excessive.

3. **The right to rectification**

If an individual discovers that the information an organisation holds on them is inaccurate or incomplete, they can request that it be updated. As with the right of access, organisations have one month to do this, and the same exceptions apply.

4. **The right to erasure**

Individuals can request that organisations erase their data in certain circumstances – for example, when the data is no longer necessary, the data was unlawfully processed, or it no longer meets the lawful ground for which it was collected. This includes instances where the individual withdraws consent.

5. **The right to restrict processing**

Individuals can request that an organisation limits the way it uses personal data. It's an alternative to requesting the erasure of data and might be used when an individual contests the accuracy of their personal data. An individual can also exercise this right when they no longer use the product or service for which it was originally collected, but the organisation needs it to establish, exercise or defend a legal claim.

6. **The right to data portability**

Individuals are permitted to obtain and reuse their personal data for their own purposes across different services. This right only applies to personal data that an individual has provided to data controllers by way of a contract or consent.

7. **The right to object**

Individuals can object to the processing of personal data that is collected on the grounds of legitimate interests or the performance of a task in the interest/exercise of official authority.

8. **Rights related to automated decision-making including profiling**

The GDPR includes provisions for decisions made with no human involvement, such as profiling, which uses personal data to make calculated assumptions about individuals. There are strict rules about this kind of processing, and individuals are permitted to challenge and request a review of the processing if they believe the rules aren't being followed.

We take your privacy very seriously and will make every effort to ensure the above rights are met under the GDPR. To protect your information, we have policies and procedures in place to make sure that only authorised personnel can access the information, that information is handled and stored in a secure and sensible manner and all systems that can access the information have the necessary security measures in place.

To accomplish this, all our employees, contractors and sub-contractors have roles and responsibilities defined. In addition to these operational measures, we also use a range of technologies and security systems to reinforce the policies.

To make sure that these measures are suitable audits to identify areas of weakness and non-compliance are scheduled.

To ensure that all data protection requirements are identified and addressed when designing new systems or processes or services and/or when reviewing or expanding existing systems or processes or services, each of them must go through an approval process before continuing. Each Parish Office/Church service/entity must ensure that a Data Protection Impact Assessment (DPIA) is conducted, in cooperation with the Data Protection Officer, for all new and/or revised systems or processes for which it has responsibility. The subsequent findings of the DPIA must then be submitted to the PCC for review and approval. Where applicable, the any Information Technology (IT) contractors, as part of St Mary the Virgin, Whickham's IT system and application design review process, will cooperate with the Data Protection Officer to assess the impact of any new technology uses on the security of personal data.

V. Data Protection Principles

St Mary the Virgin, Whickham has adopted the principles to govern its collection, use, retention, transfer, disclosure and destruction of personal data in section IV.

VI. Data Collection

Data Sources

Personal data should be collected only from the data subject unless one of the following apply:

- The nature of the business purpose necessitates collection of the personal data from other persons or bodies. **(E.g: Ministry, Planned Giving, Magazine Subscribers, Electoral Roll and Outreach).**
- The collection must be carried out under emergency circumstances in order to protect the vital interests of the data subject or to prevent serious loss or injury to another person. (**E.g. Safeguarding and Health & Safety).**

If personal data is collected from someone other than the data subject, the data subject must be informed of the collection unless one of the following apply:

- The data subject has received the required information by other means.
- The information must remain confidential due to safeguarding issues.
- A national law expressly provides for the collection, processing or transfer of the personal data.

Where it has been determined that notification to a data subject is required, notification should occur promptly, but in no case later than:

- One calendar month from the first collection or recording of the personal data
- At the time of first communication if used for communication with the data subject
- At the time of disclosure if disclosed to another recipient.

Data subject consent

Each Parish Office/Church service/entity will obtain personal data only by lawful and fair means and, where appropriate, with the knowledge and consent of the individual concerned.

Where a need exists to request and receive the consent of an individual prior to the collection, use or disclosure of their personal data, St Mary the Virgin, Whickham is committed to seeking such consent. The Data Protection Officer, in cooperation with other relevant representatives, will maintain a system for obtaining and documenting data subject consent for the collection, processing, and/or transfer of their personal data.

Data subject Notification

Each **Parish Office/Church** service/entity will, when required by applicable law or contract, or where it considers that it is reasonably appropriate to do so, provide data subjects with information as to the purpose of the processing of their personal data. When the data subject is asked to give consent to the processing of personal data and when any personal data is collected from the data subject, all appropriate disclosures will be made, in a manner that draws attention to them, unless one of the following apply:

- The data subject already has the information;
- A legal exemption applies to the requirements for disclosure and/or consent. The disclosures may be given orally, electronically or in writing. If given orally, the person making the disclosures should use a suitable script or form approved in advance by the Data Protection Officer. The associated receipt or form should be retained, along with a record of the facts, date, content, and method of disclosure.

External Privacy Notices

Each external website provided by **St Mary the Virgin, Whickham** includes an online **'Privacy Notice'** which explains personal data, who we are, how we process personal data, the legal basis, sharing

data, how long data is kept, rights of data subjects, further processing, contact details and an online **Cookie Notice** is included within this document fulfilling the requirements of applicable law.

VII. Data Use

Data processing

St Mary the Virgin, Whickham uses the personal data of its contacts for the following broad purposes:

- The general running and business administration of **the Parish Office/Church** services/entities.
- To provide services to **St Mary the Virgin, Whickham's** membership.
- The ongoing administration and management of services operations.

The use of a contact's information should always be considered from their perspective and whether the use will be within their expectations or if they are likely to object. For example, it would clearly be within a contact's expectations that their details will be used by **St Mary the Virgin, Whickham** to respond to a contact request for information about the products and services on offer. However, it will not be within their reasonable expectations that **the Parish Office/Church** would then provide their details to third parties for marketing purposes and **St Mary the Virgin, Whickham** will not send any information to a third party except those necessitated by law or convention (EG: PCC Officers to the Diocese). The Parish will process personal data in accordance with all applicable laws and applicable contractual obligations. More specifically, **the Parish Office/Church** will not process personal data unless at least one of the following requirements are met:

- The data subject has given **consent** to the processing of their personal data for one or more specific purposes.
- Processing is necessary for the performance of a **contract** to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.
- Processing is necessary for compliance with a **legal obligation** to which the Data Controller is subject.
- Processing is necessary in order to protect the **vital interests** of the data subject or of another natural person.
- Processing is necessary for the performance of a task carried out in the **public interest** or in the exercise of official authority vested in the Data Controller.
- Processing is necessary for the purposes of the **legitimate interests** pursued by the Data Controller/Processor or by a third party (except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject, in particular where the data subject is a child).

There are some circumstances in which personal data may be further processed for purposes that go beyond the original purpose for which the personal data was collected. When making a determination as to the compatibility of the new reason for processing, guidance and approval must be obtained from the Data Protection Officer before any such processing may commence.

In any circumstance where consent has not been gained for the specific processing in question, **the Parish Office/Church** will address the following additional conditions to determine the fairness and transparency of any processing beyond the original purpose for which the personal data was collected: Any link between the purpose for which the personal data was collected and the reasons for intended further processing.

- The context in which the personal data has been collected, in particular regarding the relationship between data subject and the Data Controller.
- The nature of the personal data, in particular whether special categories of data are being processed, or whether personal data related to criminal convictions and offences are being processed.
- The possible consequences of the intended further processing for the data subject.

- The existence of appropriate safeguards pertaining to further processing, which may include encryption, anonymization or pseudonymisation.

IX. Special Categories of Data

St Mary the Virgin, Whickham will only process special categories of data (also known as sensitive data) where the data subject **expressly consents** to such processing or where one of the following conditions apply:

- The processing relates to personal data which has already been made public by the data subject.
- The processing is necessary for the establishment, exercise or defence of legal claims.
- The processing is specifically authorised or required by law.
- The 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.
- Further conditions, including limitations, based upon national law related to the processing of genetic data, biometric data or data concerning health.

In any situation where, special categories of data are to be processed, prior approval must be obtained from the Data Protection Officer, and the basis for the processing clearly recorded with the personal data in question. Where special categories of data are being processed, **St Mary the Virgin, Whickham** will adopt additional protection measures.

Children's Data

Children under the age of 18 are unable to consent to the processing of personal data for information society services (any service normally provided for payment, by electronic means and at the individual request of a recipient of services). Consent must be sought from the person who holds parental responsibility over the child. However, it should be noted that where processing is lawful under other grounds, consent need not be obtained from the child or the holder of parental responsibility.

X. Data Quality

Each **Parish Office/Church** service/entity will adopt all necessary measures to ensure that the personal data it collects, and processes is complete and accurate in the first instance and is updated to reflect the current situation of the data subject. The measures adopted by **St Mary the Virgin, Whickham** to ensure data quality include

- Correcting personal data known to be incorrect, inaccurate, incomplete, ambiguous, misleading or outdated, even if the data subject does not request rectification.
- Keeping personal data only for the period necessary to satisfy the permitted uses or applicable statutory retention period.
- The removal of personal data if in violation of any of the data protection principles or if the personal data is no longer required.
- Restriction, rather than deletion of personal data, insofar as:
    - a law prohibits erasure.
    - erasure would impair legitimate interests of the data subject.
    - the data subject disputes that their personal data is correct and it cannot be clearly ascertained whether their information is correct or incorrect.

XI Profiling & Automated Decision Making

St Mary the Virgin, Whickham does not currently engage in in profiling and automated decision making. However, if St Mary the Virgin Whickham engages it is necessary to enter into, or to perform, a contract with the data subject or where it is authorised by law. Where a **Parish Office/Church** service/entity utilises profiling and automated decision-making, this will be disclosed to the relevant data subjects. In such cases the data subject will be given the opportunity to:

- Express their point of view.
- Obtain an explanation for the automated decision.

- Review the logic used by the automated system.
- Supplement the automated system with additional data.
- Have a human carry out a review of the automated decision.
- Contest the automated decision.
- Object to the automated decision-making being carried out. Each **Parish Office/Church** service/entity must also ensure that all profiling and automated decision-making relating to a data subject is based on accurate data.

XII Digital Marketing

As a rule, **St Mary the Virgin, Whickham** will not send promotional or direct marketing material to a parish church contact through digital channels such as mobile phones, email and the Internet, without first obtaining their consent. Any **Parish Office/Church** service/entity wishing to carry out a digital marketing campaign without obtaining prior Consent from the data subject must first have it approved by the Data Protection Officer. Where **personal data** (e.g. case studies or photographs on the website) processing is approved for digital marketing purposes, the data subject must be informed at the point of first contact that they have the right to object, at any stage, to having their data processed for such purposes. If the data subject puts forward an objection at any time digital marketing related processing of their personal data must cease immediately and, if necessary, their details should be kept on ***a suppression list*** with a record of their opt-out decision, rather than being completely deleted. It should be noted that where digital marketing is carried out in a 'business to business' context, there is no legal requirement to obtain an indication of Consent to carry out digital marketing to individuals provided that they are given the opportunity to opt-out

XIV. Data Retention

To ensure fair processing, personal data will not be retained by **St Mary the Virgin, Whickham** for longer than necessary in relation to the purposes for which it was originally collected, or for which it was further processed. The length of time for which **Parish Office/ Church** services/entities need to retain personal data will be according to the type of Data kept. This considers the legal and contractual requirements, both minimum and maximum, that influence the retention periods set forth in the schedule. All personal data should be deleted or destroyed as soon as possible where it has been confirmed that there is no longer a need to retain it.

XV. Data Protection

Each **Parish Office/church** service/entity will adopt physical, technical, and organisational measures to ensure the security of personal data. This includes the prevention of loss or damage, unauthorised alteration, access or processing, and other risks to which it may be exposed by virtue of human action or the physical or natural environment. A summary of the
personal data related security measures are provided below:

- Prevent unauthorised persons from gaining access to data processing systems in which personal data are processed.
- Prevent persons entitled to use a data processing system from accessing personal data beyond their needs and authorisations.
- Ensure all personal data stored on computers is password protected.
- Ensure that personal data in the course of electronic transmission during transport cannot be read, copied, modified or removed without authorisation.
- Any sensitive documents sent by email should be "read only" and in PDF format.
- Ensure that access logs are in place to establish whether, and by whom, the personal data was entered into, modified on or removed from a data processing system.
- Ensure that in the case where processing is carried out by a Data Processor, the data can be processed only in accordance with the instructions of the Data Controller.
- Ensure that personal data is protected against undesired destruction or loss.
- Ensure that personal data collected for different purposes can and is processed separately.

- Ensure that personal data is not kept longer than necessary

XVI. Data subject Requests

The Data Protection Officer will establish a system to enable and facilitate the exercise of data subject rights related to:

- Information access.
- Objection to processing.
- Objection to automated decision-making and profiling.
- Restriction of processing.
- Data portability.
- Data rectification.
- Data erasure.

If an individual makes a request relating to any of the rights listed above**, St Mary the Virgin, Whickham** will consider each such request in accordance with all applicable data protection laws and regulations. No administration fee will be charged for considering and/or complying with such a request unless the request is deemed to be unnecessary or excessive in nature.

Data subjects are entitled to obtain, based upon a request made in writing/email to:

Data Protection Officer,
St Mary's Centre,
Church Chare,
Whickham,
Newcastle upon Tyne,
NE16 4SH
or **parishoffice@stmaryswhickham.com**

It should be noted that situations may arise where providing the information requested by a data subject would disclose personal data about another individual. In such cases, information must be redacted or withheld as may be necessary or appropriate to protect that person's rights. A data subject requiring details of information held about them will need to contact St Mary the Virgin's Data Protection Officer.

XVII. Law Enforcement Requests & Disclosures

In certain circumstances, it is permitted that personal data be shared without the knowledge or consent of a data subject. This is the case where the disclosure of the personal data is necessary for any of the following purposes:

- The prevention or detection of crime.
- The apprehension or prosecution of offenders.
- The assessment or collection of a tax or duty.
- By the order of a court or by any rule of law.

If a **Parish Office/Church** service/entity processes personal data for one of these purposes, then it may apply an exception to the processing rules outlined in this policy but only to the extent that not doing so would be likely to prejudice the case in question. If any **Parish Office/Church** service/entity receives a request from a court or any regulatory or law enforcement authority for information relating to an **St Mary the Virgin, Whickham** contact, you must immediately notify the Data Protection Officer who will provide comprehensive guidance and assistance.

XVIII. Data Protection Training

All **St Mary the Virgin, Whickham** employees and officers that have access to personal data will have their responsibilities under this policy outlined to them. In addition, each **Parish Office/Church** service/entity will receive Data Protection training and guidance.

XIX. Data Transfers

St Mary the Virgin, Whickham services/entities may transfer personal data to internal or third-party recipients located in another country where that country is recognised as having an adequate level of legal protection for the rights and freedoms of the relevant data subjects. Where transfers need to be made to countries lacking an adequate level of legal protection (i.e. third world countries), they

must be made in compliance with an approved transfer mechanism. **Parish Office/Church** services/entities may only transfer personal data where one of the transfer scenarios listed below applies:

- The data subject has given consent to the proposed transfer.
- The transfer is necessary for the performance of a contract with the data subject.
- The transfer is necessary for the implementation of pre-contractual measures taken in response to the data subject's request.
- The transfer is necessary for the conclusion or performance of a contract concluded with a third party in the interest of the data subject.
- The transfer is legally required on important public interest grounds.
- The transfer is necessary for the establishment, exercise or defence of legal claims.
- The transfer is necessary in order to protect the vital interests of the data subject

When any data information is transferred to a memory stick it must always be password protected and sent separately from the stick.

XX. Complaints handling

Data subjects with a complaint about the processing of their personal data, should put forward the matter in writing to the Data Protection Officer. An investigation of the complaint will be carried out to the extent that is appropriate based on the merits of the specific case.

The Data Protection Officer will inform the data subject of the progress and the outcome of the complaint within a reasonable twenty-eight working days. If the issue cannot be resolved through consultation between the data subject and the Data Protection Officer, then the data subject may, at their option, seek redress through mediation, binding arbitration, litigation, or via complaint to the Data Protection Authority within the applicable jurisdiction.

XXI. Breach Reporting

Any individual who suspects that a personal data breach has occurred due to the theft or exposure of personal data must immediately notify the Data Protection Officer providing a description of what occurred. Notification of the incident can be made via e-mail, by calling, or by using the independent ICO Data Concern line on: 0303 123 1113. The Data Protection Officer will investigate all reported incidents to confirm whether or not a personal data breach has occurred. If a personal data breach is confirmed, the Data Protection Officer will follow the relevant **St Mary the Virgin, Whickham Data Breach Notification Policy and Procedure** based on the criticality and quantity of the personal data involved. Where there is a severe data breach of personal information then **St Mary the Virgin, Whickham's** GDPR Group will co-ordinate and manage the personal data breach response.

XXII. ROLES AND RESPONSIBILITIES

The **PCC** of **St Mary the Virgin, Whickham** must ensure that all **Parish Office/Church** employees who are responsible for the processing of any personal data are made aware the contents of this policy and they must comply. In addition, each **St Mary the Virgin, Whickham's** service/entity will make sure all third parties engaged to process personal data on their behalf (i.e. their data controllers and processors) are aware of and comply with the contents of this policy. Assurance of such compliance must be obtained from all third parties, granting them access to personal data, controlled by **St Mary the Virgin, Whickham.**

For advice and support in relation to this policy, please contact Data Protection Officer at **parishoffice@stmaryswhickham.com**

XXIII. REVIEW

This policy will be reviewed by the Data Protection Officer/PCC every **three years**, unless there are any changes to regulations or legislation that would merit a review earlier.

XXIV. RECORDS MANAGEMENT

Staff must maintain all records relevant to administering this policy and procedure in a recognised **St Mary the Virgin, Whickham** record keeping system.

All records relevant to administering this policy and procedure will be maintained for a period of **five years**.

TERMS AND DEFINITIONS

General Data Protection Regulation (GDPR): The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU). It also addresses the export of personal data outside the EU.

Data Controller: the entity that determines the purposes, conditions and means of the processing of personal data.

Data Processor: the entity that processes data on behalf of the Data Controller.

Data Protection Authority: national authorities tasked with the protection of data and privacy as well as monitoring and enforcement of the data protection regulations within the Union.

Data Protection Officer (DPO): an expert on data privacy who works independently to ensure that an entity is adhering to the policies and procedures set forth in the GDPR.

Data subject: a natural person whose personal data is processed by a controller or processor.

Personal data: any information related to a natural person or 'data subject' that can be used to directly or indirectly identify the person.

PCC: Parochial Church Council.

Privacy Impact Assessment: a tool used to identify and reduce the privacy risks of entities by analysing the personal data that are processed and the policies in place to protect the data.

Processing: any operation performed on personal data, whether or not by automated means, including collection, use, recording, etc.

Profiling: any automated processing of personal data intended to evaluate, analyse, or predict data subject behaviour.

Regulation: a binding legislative act that must be applied in its entirety across the Union.

Subject Access Right: also known as the Right to Access, it entitles the data subject to have access to and information about the personal data that a controller has concerning them.

ADDENDUM:

Data Subject Access Rights Policy: A data subject requiring details of information held about them will need to contact St Mary the Virgin's Data Protection Officer.

Data Breach Notification Policy: Where there is a severe data breach of personal information, then St Mary the Virgin, Whickham's GDPR group will coordinate and manage the personal data breach response.

RELATED LEGISLATION AND DOCUMENTS

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
<https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

XXV. Document Clarification /Amendments / Errors:

In the event that any of the content within this document is unclear or inaccurate or any of the sections in the policy need to be changed as a result of planned business changes; please notify the document owner in section XVI.