



Data Protection Policy

Introduction

Shirley Parish is committed to protecting the rights and freedoms of its parishioners and safely and securely processing their data in accordance with all of our legal obligations.

We hold personal data about our employees, parishioners, suppliers and other individuals for a variety of purposes.

This policy sets out how we seek to protect personal data and ensure that the Parish Administrators, Clergy and Volunteers all understand the rules governing their use of the personal data to which they have access in the course of their work. In particular, this policy requires everyone to ensure that the Data Protection Assistant (DPA) is consulted before any significant new data processing activity is initiated in order to ensure that relevant compliance steps are addressed.

Definitions

Personal data	‘Personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. <i>Personal data we gather may include: names, postal addresses, individuals’ phone number, email address, financial and pay details,</i>
Special categories of personal data	Special categories of data include information about an individual’s racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, criminal offences, or related proceedings, and genetic and biometric information —any use of special categories of personal data should be strictly controlled in accordance with this policy.
Data controller	‘Data controller’ means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by law.
Data processor	‘Processor’ means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
Processing	‘Processing’ means any operation or set of operations which is/are performed on personal data or on sets of personal data, whether or not by automated means, such as 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.
Supervisory authority	This is the national body responsible for data protection. The supervisory authority for Shirley Parish is the Information Commissioners Office (ICO).

Scope

This policy applies to all employees and volunteers. All of whom must be familiar with this policy and comply with all of its terms.

We may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be circulated before being adopted.

Who is responsible for this policy?

As our Data Protection Assistant (DPA), Belinda Piasecki has overall responsibility for the day-to-day implementation of this policy. You should contact the DPA for further information about this policy if necessary.

Phone – 0121 244 9637, email – Belinda.piasecki@hotmail.co.uk

The principles

Shirley Parish shall comply with the principles of data protection (the Principles) enumerated in the EU General Data Protection Regulation. We will make every effort possible in everything we do to comply with these principles. The Principles are:

1. Lawful, fair and transparent

Data collection must be fair, for a legal purpose and we must be open and transparent as to how the data will be used.

2. Limited for its purpose

Data can only be collected for a specific purpose.

3. Data minimisation

Any data collected must be necessary and not excessive for its purpose.

4. Accurate

The data we hold must be accurate and kept up to date.

5. Retention

We cannot store data longer than necessary.

6. Integrity and confidentiality

The data we hold must be kept safe and secure.

Accountability and transparency

We must ensure accountability and transparency in all of our use of personal data. We must show how we comply with each Principle. The Parish Office will hold documentation demonstrating how all the data processing activities comply with each of the Principles.

To comply with data protection laws and the accountability and transparency principle of GDPR, we must demonstrate compliance. You are responsible for understanding your particular responsibilities to ensure we meet the following data protection obligations:

- Fully implement all appropriate technical and organisational measures
- Maintain up to date and relevant documentation on all processing activities
- Conducting Data Protection Impact Assessments
- Implement measures to ensure privacy by design and default, including:
 - Data minimisation
 - Pseudonymisation
 - Transparency
 - Allowing individuals to monitor processing
 - Creating and improving security and enhanced privacy procedures on an ongoing basis

Our procedures

Fair and lawful processing

We must process personal data fairly and lawfully in accordance with individuals' rights under the first Principle. This generally means that we should not process personal data unless the individual whose details we are processing has consented to this happening.

If we cannot apply a lawful basis (explained below), our processing does not conform to the first principle and will be unlawful. Data subjects have the right to have any data unlawfully processed deleted.

Controlling vs. processing data

The Parochial Church Council (PCC) of Shirley Parish and the Clergy are classified as the data controllers.

The diocese needs to be reassured that the PCC and the Clergy understand their responsibilities.

[For data processors] As a data processor, you must comply with our contractual obligations and act only on the documented instructions of the data controller. As a data processor, you must:

- Not use a sub-processor without written authorisation of the data controller
- Co-operate fully with the ICO or other supervisory authority
- Ensure the security of the processing
- Keep accurate records of processing activities
- Notify the data controller of any personal data breaches

If you are in any doubt about how we handle data, contact the DPA for clarification.

Lawful basis for processing data

We must establish a lawful basis for processing data. Ensure that any data you are responsible for managing has a lawful basis. It is your responsibility to check the lawful basis for any data you are working with and ensure all of your actions comply with the lawful basis. At least one of the following conditions must apply whenever we process personal data:

Consent

We hold recent, clear, explicit, and defined consent for the individual's data to be processed for a specific purpose.

Contract

The processing is necessary to fulfil or prepare a contract for the individual.

Legal obligation

We have a legal obligation to process the data (excluding a contract).

Vital interests

Processing the data is necessary to protect a person's life or in a medical situation.

Public function

Processing necessary to carry out a public function, a task of public interest or the function has a clear basis in law.

Legitimate interest

The processing is necessary for our legitimate interests. This condition does not apply if there is a good reason to protect the individual's personal data which overrides the legitimate interest.

Deciding which condition to rely on

If you are making an assessment of the lawful basis, you must first establish that the processing is necessary. This means the processing must be a targeted, appropriate way of achieving the stated purpose. You cannot rely on a lawful basis if you can reasonably achieve the same purpose by some other means.

Remember that more than one basis may apply, and you should rely on what will best fit the purpose, not what is the easiest to deal with.

Consider the following factors and document your answers:

- What is the purpose for processing the data?
- Can it reasonably be done in a different way?
- Is there a choice as to whether or not to process the data?
- Who does the processing benefit?
- After selecting the lawful basis, is this the same as the lawful basis the data subject would expect?
- What is the impact of the processing on the individual?
- Are you in a position of power over them?
- Are they a vulnerable person?
- Would they be likely to object to the processing?
- Are you able to stop the processing at any time on request, and have you factored in how to do this?

We must ensure that individuals whose data is being processed by us are informed of the lawful basis for processing their data, as well as the intended purpose. This occurs via a privacy notice. This applies whether we have collected the data directly from the individual, or from another source. The privacy notice is available on our website or a paper copy from the Parish Office.

Special categories of personal data

What are special categories of personal data?

Previously known as sensitive personal data, this means data about an individual which is more sensitive, so requires more protection. This type of data could create more significant risks to a person's fundamental rights and freedoms, for example by putting them at risk of unlawful discrimination. The special categories include information about an individual's:

- race
- ethnic origin
- politics
- religion
- trade union membership
- genetics
- biometrics (where used for ID purposes)
- health
- sexual orientation

In most cases where we process special categories of personal data we will require the data subject's *explicit* consent to do this unless exceptional circumstances apply or we are required to do this by law (e.g. to comply with legal obligations to ensure health and safety at work). Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

The condition for processing special categories of personal data must comply with the law. If we do not have a lawful basis for processing special categories of data that processing activity must cease.

Responsibilities

DPA and Clergy

- Analysing and documenting the type of personal data we hold
- Reviewing and checking all data protection procedures and policies on a regular basis
- Identify the lawful basis for processing data
- Ensuring consent procedures are lawful
- Implementing and reviewing procedures to detect, report and investigate personal data breaches
- Store data in safe and secure ways
- Identifying any risks and issues
- Assess the risk that could be posed to individual rights and freedoms should data be compromised
- Arranging data protection training and advice for all employees and volunteers
- Answering questions on data protection from employees and volunteers
- Responding to individuals such as parishioners and employees/volunteers who wish to know what data is being held on them by us
- Checking and approving with third parties that handle the parish's data any contracts or agreement regarding data processing

Employee and volunteer responsibilities

- Fully understand your data protection obligations
- Check that any data processing activities you are dealing with comply with our policy and are justified
- Do not use data in any unlawful way
- Do not store data incorrectly, be careless with it or otherwise cause us to breach data protection laws and our policies through your actions
- Comply with this policy at all times
- Raise any concerns, notify any breaches or errors, and report anything suspicious or contradictory to this policy or our legal obligations without delay

Accuracy and relevance

We must ensure that any personal data we process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. We will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

Individuals may ask that we correct inaccurate personal data relating to them. If you believe that information is inaccurate you should record the fact that the accuracy of the information is disputed and inform the DPO.

Data security

You must keep personal data secure against loss or misuse. Where other organisations process personal data as a service on our behalf, the DPO will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third party organisations.

Storing data securely

- In cases where data is stored on printed paper, it should be kept in a secure place where unauthorised personnel cannot access it
- Printed data should be shredded when it is no longer needed
- Data stored on a computer should be protected by strong passwords that are changed regularly
- Data stored on CDs or memory sticks must be encrypted or password protected and locked away securely when they are not being used
- Data should not be stored on any cloud based storage
- Data should be regularly backed up
- All possible technical measures must be put in place to keep data secure
- Data should not be removed from secure storage onto a cd/memory stick

Data retention

We must retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained, but should be determined in a manner consistent with our data retention guidelines. Please refer to the booklet - 'Keep or Bin...?' The Care of Your Parish Records.

Transferring data internationally

There are restrictions on international transfers of personal data. You must not transfer personal data abroad, or anywhere else outside of normal rules and procedures.

Rights of individuals

Individuals have rights to their data which we must respect and comply with to the best of our ability. We must ensure individuals can exercise their rights in the following ways:

1. Right to be informed

- Providing privacy notices which are concise, transparent, intelligible, easily accessible and free of charge, that are written in clear and plain language, particularly if aimed at children.
- Keeping a record of how we use personal data to demonstrate compliance with the need for accountability and transparency.

2. Right of access

- Enabling individuals to access their personal data and supplementary information
- Allowing individuals to be aware of and verify the lawfulness of the processing activities

3. Right to rectification

- We must rectify or amend the personal data of the individual if requested where it is found to be inaccurate or incomplete.
- This must be done without delay and no later than one month after any request has been made.

4. Right to erasure

- We must delete or remove an individual's data if requested and where there is no compelling reason for its continued processing.

5. Right to restrict processing

- We must comply with any request to restrict, block, or otherwise suppress the processing of personal data.
- We are permitted to store personal data if it has been restricted, but not process it further. We must retain enough data to ensure the right to restriction is respected in the future.

6. Right to data portability

- We must provide individuals with their data so that they can reuse it for their own purposes or across different services.
- We must provide it in a commonly used, machine-readable format, and send it directly to another controller if requested.

7. Right to object

- We must respect the right of an individual to object to data processing based on legitimate interest or the performance of a public interest task.
- We must respect the right of an individual to object to direct marketing, including profiling.
- We must respect the right of an individual to object to processing their data for scientific and historical research and statistics.

8. Rights in relation to automated decision making and profiling

- We must respect the rights of individuals in relation to automated decision making and profiling.
- Individuals retain their right to object to such automated processing, have the rationale explained to them, and request human intervention.

Privacy notices

When to supply a privacy notice

A privacy notice must be supplied at the time the data is obtained if obtained directly from the data subject. If the data is not obtained directly from the data subject, the privacy notice must be provided within one month of having obtained the data.

If the data is being used to communicate with the individual, then the privacy notice must be supplied at the latest when the first communication takes place.

If disclosure to another recipient is envisaged, then the privacy notice must be supplied prior to the data being disclosed.

What to include in a privacy notice

Privacy notices must be concise, transparent, intelligible and easily accessible. They are provided free of charge and must be written in clear and plain language, particularly if aimed at children

The following information must be included in a privacy notice to all data subjects:

- Identification and contact information of the data controller and the DPA
- The purpose of processing the data and the lawful basis for doing so
- The legitimate interests of the controller or third party
- The right to withdraw consent at any time
- The category of the personal data (only for data not obtained directly from the data subject)
- Any recipient or categories of recipients of the personal data
- Detailed information of any transfers to third parties/countries and safeguards in place
- The retention period of the data or the criteria used to determine the retention period, including details for the data disposal after the retention period
- The right to lodge a complaint with the ICO, and internal complaint procedures
- The source of the personal data, and whether it came from publicly available sources (only for data not obtained directly from the data subject)
- Any existence of automated decision making, including profiling and information about how those decisions are made, their significances and consequences for the data subject
- Whether the provision of personal data is part of a statutory or contractual requirement or obligation and possible consequences for any failure to provide the data (only for data obtained directly from the data subject)

Subject Access Requests

What is a subject access request?

An individual has the right to receive confirmation that their data is being processed. They can also have access to their personal data and any supplementary information.

How we deal with subject access requests

We must provide an individual with a copy of the information they request, free of charge. This must occur within one month of receipt.

If complying with the request is complex or numerous, the deadline can be extended by two months, but the individual must be informed within one month. You must ensure that the Clergy and DPO have been made aware of this request at the initial contact.

Once a subject access request has been made, you must not change or amend any of the data that has been requested. **Doing so is a criminal offence.**

Data portability requests

We may not be able to meet this type of request, if one is received please refer to Clergy and DPA ASAP, as guidance will need to be sought.

The data must be provided in a structured, commonly used and machine-readable format. This would normally be a CSV file, although other formats are acceptable. We must provide this data either to the individual who has requested it, or to the data controller they have requested it be sent to. This must be done free of charge and within one month of receiving the request. This can be extended to two months for complex or numerous requests but, the individual must be informed of the extension within one month and you must receive express permission from the DPA first.

Right to erasure

What is the right to erasure?

Individuals have a right to have their data erased and for processing to cease in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected and / or processed
- Where consent is withdrawn
- Where the individual objects to processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed or otherwise breached data protection laws
- To comply with a legal obligation
- The processing relates to a child

How we deal with the right to erasure

We can only refuse to comply with a right to erasure in the following circumstances:

- To exercise the right of freedom of expression and information
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority
- For public health purposes in the public interest
- For archiving purposes in the public interest, scientific research, historical research or statistical purposes
- The exercise or defence of legal claims

If personal data that needs to be erased has been passed onto other parties or recipients, they must be contacted and informed of their obligation to erase the data. If the individual asks, we must inform them of those other parties or recipients.

The right to object

Individuals have the right to object to their data being used on grounds relating to their particular situation. We must cease processing unless:

We have legitimate grounds for processing which override the interests, rights and freedoms of the individual.

The processing relates to the establishment, exercise or defence of legal claims.

We must always inform the individual of their right to object at the first point of communication, i.e. in the privacy notice. We must offer a way for individuals to object online.

Third parties

Using third party controllers and processors

As a data controller and/or data processor, we must have written contracts in place with any third party [data controllers (and/or) data processors] that we use. The contract must contain specific clauses which set out our and their liabilities, obligations and responsibilities.

Contracts

Our contracts must comply with the standards set out by the ICO and, where possible, follow the standard contractual clauses which are available. Our contracts with [data controllers (and/or) data processors] must set out the subject matter and duration of the processing, the nature and stated purpose of the processing activities, the types of personal data and categories of data subject, and the obligations and rights of the controller.

At a minimum, our contracts must include terms that specify:

- Acting only on written instructions
- Those involved in processing the data are subject to a duty of confidence
- Appropriate measures will be taken to ensure the security of the processing
- Sub-processors will only be engaged with the prior consent of the controller and under a written contract
- The controller will assist the processor in dealing with subject access requests and allowing data subjects to exercise their rights under GDPR
- The processor will assist the controller in meeting its GDPR obligations in relation to the security of processing, notification of data breaches and implementation of Data Protection Impact Assessments
- Delete or return all personal data at the end of the contract
- Submit to regular audits and inspections, and provide whatever information necessary for the controller and processor to meet their legal obligations.
- Nothing will be done by either the controller or processor to infringe on GDPR.

Criminal offence data

Criminal record checks

Any criminal record checks are justified by law. Criminal record checks cannot be undertaken based solely on the consent of the subject. We cannot keep a comprehensive register of criminal offence data. All data relating to criminal offences is considered to be a special category of personal data and must be treated as such. You must have approval from the Clergy/DPO prior to carrying out a criminal record check.

Audits, monitoring and training

Data audits

Regular data audits to manage and mitigate risks will inform the data register. This contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant. A regular data audit will be carried out by the DPA.

Monitoring

Everyone must observe this policy. The DPA and Clergy have overall responsibility for this policy. Shirley PCC will keep this policy under review and amend or change it as required. You must notify the DPA of any breaches of this policy. You must comply with this policy fully and at all times.

Training

You will receive adequate training on GDPR and provisions of data protection law specific for your role. You must complete all training as requested.

If you require additional training on data protection matters, contact the DPA.

Reporting breaches

Any breach of this policy or of data protection laws must be reported immediately. This means as soon as you have become aware of a breach. Shirley PCC has a legal obligation to report any data breaches to the ICO and Birmingham Diocese within 72 hours.

All employees and volunteers have an obligation to report actual or potential data protection compliance failures. This allows us to:

- Investigate the failure and take remedial steps if necessary
- Maintain a register of compliance failures
- Notify the Diocese of any compliance failures that are material either in their own right or as part of a pattern of failures

Failure to comply

We take compliance with this policy very seriously. Failure to comply puts both you and the Parish at risk. The importance of this policy means that failure to comply with any requirement may lead to very serious repercussions for both the individual and the Parish.

If you have any questions or concerns about anything in this policy, do not hesitate to contact the DPA.

Policy created August 2018

Reviewed June 2021