Stratfield Mortimer Benefice
Data Protection Policy

About this Document

Contents

1 Introduction

The protection of personal data is enshrined in UK law, but it is also a moral responsibility that The Stratfield Mortimer Benefice takes seriously. Embedding data protection within the organisation benefits the Stratfield Mortimer Benefice, the Church and all individuals who interact with us, by enabling uniform and consistent decision making, building a culture of awareness and responsibility, making personal data management and infrastructure more resilient; and, through transparency and accountability, instilling trust and confidence in individuals when they provide us with their data, and ensuring their rights and freedoms are upheld.

1.1 Purpose

The purpose of this policy is to describe the steps that the Stratfield Mortimer Benefice are taking to comply with data protection legislation, to ensure that our compliance with the relevant legislation is clear and demonstrable.

This policy is also intended to provide us with measures for ensuring that risks to individuals through misuse of personal data are minimised, such as:

- personal data being used by unauthorised individuals through poor security or inappropriate disclosure;
- individuals being harmed by decisions made using inaccurate or insufficient data;
- individuals being uninformed by lack of transparency leading to unlawful practice;
- the invasion of privacy due to over-collection or over-retention of data.

1.2 Scope

This policy applies to the Stratfield Mortimer Benefice, which includes the Incumbent and the PCC's of St. Mary and St. John, Stratfield Mortimer, St. John the Baptist, Padworth and St. Saviour, Mortimer West End.

We expect all those processing personal data on behalf of the Stratfield Mortimer Benefice to act in accordance with this policy when engaged in the business of the Stratfield Mortimer Benefice.

Joint Data Controllers

The incumbent and PCCs have agreed to work as joint data controllers for data protection purposes

1.3 Definitions

- **Personal Data** - Any information that relates to an identifiable living individual.
- **Special Categories of Personal Data** (also known as sensitive personal data) - Specific types of data that require additional care being taken when processing. The categories are: race; ethnic origin; politics; religion; trade union membership; genetics; biometrics (where used for ID purposes); health; sex life; or sexual orientation. Data relating to Safeguarding are considered to be Special Category under the Data Protection Act 2018 where the processing of this data is necessary for the purposes of:
  - protecting an individual from neglect or physical, mental or emotional harm, or
  - protecting the physical, mental or emotional well-being of an individual,

- where the individual is aged under 18, or
- aged 18 or over and at risk.

- **Data processing** – Any activity relating to the collection, recording, organising, structuring, use, amendment, storage, access, retrieval, transfer, analysis, disclosure, dissemination, combination, restriction, erasure or disposal of personal data.
- **Data Protection Impact Assessment (DPIA)** - A process designed to help systematically analyse, identify and minimise the data protection risks of a project or activity.
- **Data Subject** - The individual to whom the data being processed relates.
- **Data Controller** - A body or organisation that makes decisions on how personal data is being processed. Data Controllers almost always also process data.
- **Data breach** - any occasion when personal data is: accidentally or unlawfully lost, destroyed, corrupted or disclosed; accessed or passed on without proper authorisation; or made unavailable (through being hacked or by accidental loss/destruction.
- **3rd Party Data Processors** – Other legal entities that process data on behalf of a Data Controller and under instruction from the Data Controller. Data Processors do not have the ability to make decisions about *how* the data should be processed, there should be documented instructions from the Data Controller about what the processor can and cannot do with the data (known as a Data Processing/Sharing Agreement).

2 Policy Statement

Personal data that the Stratfield Mortimer Benefice collects, uses, stores, transfers, shares and disposes of must be handled in line with the following policy.

2.1 Data Protection Lead

The Incumbent and Churchwardens of the Stratfield Mortimer Benefice are based at The Benefice Office, St. John's church, The Street, Mortimer Common, Berks, RG7 3SY and who may also be contacted by emailing admin@mortimerbenefice.co.uk or by phoning: 01189 333704.

They are responsible for assisting the Stratfield Mortimer Benefice to monitor internal compliance and to inform and advise on data protection obligations.

They will monitor data sharing agreements, data breaches, information risk, subject access requests and compliance with data protection policies and procedures. They will report to the Incumbent / PCC / Area Dean or whoever is deemed the responsible person or body.

2.2 Principles of data protection

Personal data is processed according to the following principles:

1. **Data is processed lawfully, fairly and in a transparent manner** in relation to the data subject, through the provision of clear and transparent privacy notices and responses to individual rights requests.
2. **Data is collected for specified, explicit and legitimate reasons** and not further processed for different reasons incompatible with these purposes. The Stratfield Mortimer Benefice will

maintain an Information Asset Register (Appendix 2) and Register of Processing Activities (Appendix 3) for the Stratfield Mortimer Benefice, that will be regularly and consistently reviewed and updated. Data that is stored and used for archiving purposes in the public interest, scientific or historical research or statistical purposes will be managed by the Stratfield Mortimer Benefice and stored at the local records office.

3. **Data is adequate, relevant and not more than is necessary** to complete the task for which it was collected and will be subject to regular review of data collection and processing needs.
4. **Data is accurate and up-to-date** and reasonable steps will be taken to ensure this through regular data quality checks.
5. **Data is not kept for longer than is necessary** to complete the task for which it was collected, by the implementation of a retention schedule (Appendix 4) and a regular data cleansing programme.
6. **Data is kept secure**, with appropriate technical and organisational measures to protect against unauthorised or illegal processing, accidental corruption, loss or disclosure of personal data. This will include:
    - storing paper copies of personal data in locked cabinets;
    - maintaining password protection of electronic data held on computers and online storage;
    - ensuring access to paper and electronic media is restricted only to those individuals authorised to access the data;
    - ensuring that extra precautions are taken when personal data is carried in public places, to keep the risk of data breaches to an acceptable level.

    To maintain appropriate data security, we will undertake regular risk assessments of our practices and provide awareness and training to all those processing personal data on behalf of the Stratfield Mortimer Benefice.
7. **Data that is transferred outside the United Kingdom** will only take place with appropriate safeguards to protect the rights of individuals.
8. **Accountability**. The Stratfield Mortimer Benefice are responsible for, and will demonstrate, compliance with the principles by:
    - Adopting and implementing this data protection policy;
    - Publish privacy notices to explain our data protection practices to those whose personal data we process
    - Put in place written contracts with 3rd party Data Processors that process personal data on our behalf;
    - Implementing annual reviews, to update the measures we have put in place.

2.3 Collecting personal data

Data protection legislation requires that the collection and use of personal data is fair and transparent. If we acquire any personal data related to an individual (including employees, officer

holders, volunteers, suppliers, supporters or other external contacts), either directly from the data subject or from a third party, we must do so in line with the above 'Principles of Data Protection'.

If we acquire data in error (that is, data we should not have access to), by whatever means, we must inform the Data Protection Lead who will assess whether the data should be retained and if so, arrange for it to be given to the appropriate individual.

2.4 Privacy Notices

Individuals have the right to be informed about the collection and use of their personal data and the Stratfield Mortimer Benefice will be open and transparent about our use of personal data in line with this Policy. Our current privacy notice can be found on the benefice website: www.mortimerbenefice.org.uk.

We shall create and maintain one or more privacy notices, covering our data processing activities relating to personal data. Privacy notice(s) will be published on our website and in church and we will provide this to individuals at the time we collect or significantly amend their personal data.

If our data processing practices change, causing a Privacy Notice to be updated, we will reissue the notice to the affected data subjects, by email.

2.5 Lawful bases

Personal data must only be processed once we have identified an appropriate lawful reason to do so. There are six available lawful bases for processing (Appendix 1). No single basis is 'better' or more important than the others, we must decide which basis is most appropriate depending on our purpose and relationship with the individual.

The Lawful basis for different areas of our data processing will be included in [Appendix 3] of this policy and indicated in the relevant Privacy Notice.

2.6 Individual rights

Data protection legislation gives individuals specific rights regarding their personal data:

1. The right to be informed
2. The right to access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability (unlikely to be relevant to parishes or deaneries)
7. The right to object
8. Rights in relation to automated decision making and profiling (unlikely to be relevant to parishes or deaneries)

2.7 Data Protection Impact Assessment

The Stratfield Mortimer Benefice has adopted the principle of privacy by design. All new projects, updated processes or significantly changed systems that require the use of personal data and may

pose a high risk to data subjects, will be subject to a Data Protection Impact Assessment (DPIA). A DPIA template is available here: https://ico.org.uk/media/about-the-ico/consultations/2258461/dpia-template-v04-post-comms-review-20180308.pdf.

2.8 Data Sharing

As a data controller, we recognise that when we share personal data with third parties, we are responsible for:

- ensuring the third party complies with GDPR, and
- stating any constraints or requirements about what the third party can or cannot do with our data.

When sharing or disclosing personal data we shall ensure that:

- We consider the benefits and risks, either to individuals or the Church, of sharing the data, along with the potential results of not sharing the data;
- We are clear about with whom we can share the data. If we are unsure, we check with the data owner, or our Data Protection Lead person.
- We do not disclose personal data about an individual to an external organisation without first checking that we have a legitimate reason to do so (see above 'Lawful bases' section).
- If we must transfer or share data, we do so using appropriate security measures;
- If we are sharing data outside of the UK, we take particular care to ensure that the destination country meets all the necessary requirements to protect the data.

If we are unsure whether or not we can share information, we will contact our Data Protection Lead person.

Data Sharing statements

We may state any constraints or requirements on the use of data shared with third parties in the following ways, depending on the level of risk:

- Through the use of disclaimer-type statements in emails or on contractor job sheets
- By the inclusion of a 'Data Protection' section of a contract with a third party (such as a leasing agreement)
- By a standalone 'Data Sharing Agreement'

2.9 Storing and disposing of data

We will ensure that we use the most appropriate and secure methods available for both storage and disposal of personal data. We will ensure that:

- In so far as we are able, all personal data in our possession is kept secure from unauthorised access;
- We lock physical files containing personal data in a secure cabinet;

- We are vigilant of our surroundings, in particular when working outside of normal office locations, being careful not to place any personal data in a position where it can be viewed, stolen or lost;
- All devices used to handle personal data are password protected and we do not share passwords;
- Desks are kept clear of personal data when not occupied.

2.10 Fact versus Opinion

When using personal data, it is our policy not to write comments about any individual that are unfair, untrue or offensive and that you would not be able to defend if challenged. In general we:

- Express facts, not opinions
- Work on the basis that anything written about an individual might be seen by that individual.

This includes emails. Although a certain amount of informality attaches to email writing, it should not be overlooked that these can provide a written record of our comments and, in the event of a Subject Access Request, they are subject to disclosure if they contain personal data.

2.11 Data Breaches

A personal data breach means the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes.

There will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

Any data breach, as described above, is to be reported to the Data Protection Lead person.

Where a breach is known to have occurred which is likely to result in a high risk to the rights and freedoms of individuals, our Data Protection Lead person will report this to the ICO within 72 hours and will co-operate with any subsequent investigation. We will contact the affected data subject(s) where it is necessary to do so.

2.12 Training

We will provide appropriate support and training to all those involved in the benefice in the safe and lawful processing of personal data.

3 Approval and review

Approved by	PCC
Policy owner	PCC
Policy author	PCC
Date	April 2024

Review date	April 2025

4 Revision History

Version No	Revision Date	Previous revision date	Summary of Changes
1	April 2024	.	.

5 APPENDIX 1 – Lawful bases (from GDPR Article 6)

Legitimate interest

The processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

Processing Safeguarding data will usually be considered as being included under this heading.

The Data Protection Act allows all organisations to process data for safeguarding purposes lawfully and without consent where necessary for the purposes of:

- protecting an individual from neglect or physical and emotional harm; or
- protecting the physical, mental or emotional wellbeing of an individual.

However, this only applies to the extent that complying with these provisions would be likely to *prejudice* the proper discharge of your functions. If you can comply with these provisions and discharge your functions as normal, you must do so.

Legitimate Interest Assessment. When can you rely on legitimate interests?

- When processing is not required by law but is of benefit to you
- When there is a limited privacy impact on the data subject
- When the data subject would reasonably expect your processing to take place

In order to use legitimate interests as your lawful basis for processing, your processing must therefore meet all of the following criteria:

- Have a specific purpose with a defined benefit
- Be necessary – if your defined benefit can be achieved without processing personal data then legitimate interests is not appropriate
- Be balanced against, and not override, the interests, rights and freedoms of data subjects

Contract

The processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

Legal obligation

The processing is necessary for you to comply with the law (not including contractual obligations).

Consent

The individual has given clear consent for you to process their personal data for a specific purpose.

If Consent is used it must be valid (freely given, unambiguous, actively selected, can easily be withdrawn); Both giving and withdrawing consent must be recorded.

For consent to be valid, i.e. the correct basis, it must be a choice - so if the data subject refuses to give consent, does that mean that the service can't be provided? If it is an essential service (e.g.

pension, payroll etc) then the data controller cannot refuse the service, so there is effectively no choice, so consent is not valid.

Vital interests

The processing is necessary to protect someone's life.

Public Task

The processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

For further information and assistance seek advice from [the DPO or Data Protection Lead or local registrar as appropriate].

6 APPENDIX 2 - Information Asset Register

Here you should list the areas of personal data which your parish, benefice or deanery process (e.g. your contact/distribution lists, electoral roll, gift aid information, etc. The final column allows you to record the level of sensitivity (and associated risk) of the data, to help you identify those assets which might require particular attention from a data security perspective. Add rows to the table as needed.

No.	Title and description	Storage: location and format	Sensitivity of data (risk)
1			
2			
3			
4			

7 APPENDIX 3 – Register of Processing Activities

Here list all of the *main* areas of personal data processing which you regularly undertake, together with key information as indicated by the seven numbered paragraphs. You may also wish to include data processing that is relatively infrequent but highly sensitive (and therefore carries a high risk). You might simply list them, as in the paragraphs below, or turn the information into a table, as you prefer.

Data processing Activity #1

1. Reason/purpose: What are you trying to do & why?
2. Data Categories: What kind of data is involved. Is it sensitive? Special category?
3. Collection Point: Where does the data come from?
4. Processing Justification: What are you doing with this data, and why, including the lawful basis for processing
5. Database, Location & Access: What, where, who can access & how maintained. Secure?
6. Data Sharing: which, if any, other organisations (legal entities) do you share this data with?
7. Retention Policy: How long do you keep the data and how is it deleted/destroyed?

Data processing Activity #2

1. Reason/purpose: What are you trying to do & why?
2. Data Categories: What kind of data is involved. Is it sensitive? Special category?
3. Collection Point: Where does the data come from?
4. Processing Justification: What are you doing with this data, and why, including the lawful basis for processing
5. Database, Location & Access: What, where, who can access & how maintained. Secure?
6. Data Sharing: which, if any, other organisations (legal entities) do you share this data with?
7. Retention Policy: How long do you keep the data and how is it deleted/destroyed?

Data processing Activity #3

… etc

8 APPENDIX 4 – Retention schedule

A summary of all the paragraph 7s from Appendix 3