a

The Ashburton & Moorland Mission Community

Data Protection Policy and Procedures

Policy summary

The Churches of The Ashburton and Moorland Mission Community, collects and uses personal information to carry out the mission and ministry of the Church of England in Devon. We therefore collect a wide range of personal data required for or incidental to the discharge of our functions, involving clergy, church officers, employees, parishioners, etc. The Ashburton and Moorland Mission Community will endeavour to ensure that it uses personal information in line with the expectations and interests of those with whom they come into contact for the benefit of the Church and wider society and in compliance with data protection legislation, namely the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA 2018).

This policy provides guidance on the processing of personal data, (collection, use, storage, sharing and disposal), in accordance with data protection legislation. It applies to data that relates to identifiable living individuals stored and used either electronically or on paper.

Scope

This policy applies to The Ashburton and Moorland Mission Community, which includes the Rector, Vicars and the Parochial Church Councils (PCCs). All personal data processed by the Team Administrator is within the scope of this policy, as such we expect all those processing personal data on behalf of The Ashburton and Moorland Mission Community to act in accordance with this policy.

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

The guidance identifies some of the key issues and gives advice on what you need to do.
If you have any questions or queries about this policy or specific questions on what you should do please contact:

admin@moorlandteam.org.uk | dataprotection@exeter.anglican.org

Contents

Appendices

Policy

The protection of personal data is enshrined in UK law, but it is also a moral responsibility that The Ashburton & Moorland Mission Community (AMMC) takes seriously. Embedding data protection within the organisation benefits 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.

The Ashburton & Moorland Mission Community is committed to conducting its business in accordance with all applicable
legislation, including:

a. **Data Protection Act 2018**
b. **General Data Protection Regulation 2016**
c. **Human Rights Act 1998, Article 8**
d. **The Common Law Duty of Confidence**
e. **Privacy and Electronic Communications Regulations 2003**
f. **Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011**
g. **and other regulatory requirements and applicable guidance.**

Purpose

The purpose of this policy is to describe the steps that The Ashburton & Moorland Mission Community is taking to comply with data protection legislation. It is our policy to ensure that our compliance with the relevant legislation is clear and demonstrable at all times.

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.

Definition of Data Protection Terms

Data Breach - Any occasion where personal data is: accidentally or unlawfully lost, destroyed, corrupted, all disclosed; accessed or passed on without proper authorisation; or made unavailable through being hacked or by accidental loss /destruction.

Data Controller - A 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.

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 Processor - A natural or legal person, Public Authority, Agency or other body which Processes Personal Data on behalf of a Data Controller.

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 identified or Identifiable Natural Person to which the data refers.

Personal Data - Any information which relates to an identified or Identifiable Natural Person.

Special Categories of 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; health; sex life; sexual orientation; genetic data; or biometric data (where used for ID purposes)

Third Party - An external organisation which processes data on behalf of the Data Controller. They do not have the ability to make any decisions about how the data should be processed. Instructions from the Data Controller about what the processor can and cannot do with the data should be documented through a contract or a Data Processing/Sharing Agreement.

Governance

AMMC has a Data Protection Lead Person (DPL) Name, who may be contacted by emailing: francis@moorlandteam.org.uk.

- They are responsible for assisting AMMC 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 incumbents and the PCC as joint data controllers.

Data Protection Principles

Personal data is processed according to the following principles:

Principle 1: Lawfulness, Fairness and Transparency

Personal data shall be 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.

Principle 2: Purpose Limitation

Personal Data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

Personal data may only be processed for the specific purposes notified to the data subject when the data was first collected or for any other purposes specifically permitted by the GDPR and the DPA 2018. This means that personal data must not be collected for one purpose and then used for another.

Principle 3: Data Minimisation

Personal Data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed.

Personal data will only be collected for the specific purpose notified to the data subject. Any data which is not necessary for that purpose will not be collected.

Principle 4: Accuracy

Data is accurate and up-to-date and reasonable steps will be taken to ensure this through regular data quality checks.

Principle 5: Storage Limitation

Data is not kept for longer than is necessary in relation to the purposes for which it was originally collected, or for which it was further processed. The length of time personal data may be retained is in accordance with the Church of England Records Management Guidelines: "Keep or Bin…? The Care of Your Parish Records": C of E - Keep or Bin. Any Personal Data processed for the purposes of Safeguarding will be kept in accordance with our legal requirements and can be found in the guidance, "Data Protection and Safeguarding in the Diocese of Exeter", which is available from the Diocese of Exeter website: https://exeter.anglican.org/resources/safeguarding/resources/exeter-safeguarding-guidance/

Principle 6: Integrity and Confidentiality

Confidentiality *means that only people who are authorised to use the data can access it.*

Integrity *means that personal data should be accurate and suitable for the purpose for which it is processed.*

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 Ashburton and Moorland Mission Community.

Principle 7: Accountability

The joint data controllers shall be responsible for, and be able to demonstrate, compliance with the principles by:

- Adopting and implementing this data protection policy;
- Publishing 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.

How we collect 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, either directly from the data subject or from a third party, we must do so in line with the above Principles.

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

- *The nature of the purpose necessitates collection of the personal data from other persons or bodies*
- *The collection needs to 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*

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 applies:

- *The data subject has received the required information by other means*
- *The collection of the information must remain confidential due to a professional secrecy obligation*
- *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*

If we acquire data in error, *i.e. that we should not have access to*, by whatever means, we will inform the DPL who will assess whether the data should be retained and if so, arrange for it to be processed appropriately.

Privacy Notices

Individuals have the right to be informed about the collection and use of their personal data and we will be open and transparent about our use of personal data in line with this Policy.

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 we will provide this to individuals at the time we collect or significantly amend their personal data.

Our current privacy notice can be found here: https://ashburtonandmoor.org.uk/privacy-policy

Attention will be drawn to the availability of the privacy notice on all forms where personal data is collected, with an online link provided where applicable.

The privacy notices will be regularly reviewed and updated to reflect any changes in the processing of data.

Legal Basis for Processing

Personal data will be processed in accordance with all applicable laws and applicable contractual obligations. More specifically, we will not process personal data unless at least one of the following requirements is met:

1. The data subject has given **Consent** to the processing of their personal data for one or more specific purposes.
2. 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.
3. Processing is necessary for compliance with a **Legal Obligation** to which the data controller is subject.
4. Processing is necessary in order to protect the **Vital Interests** of the data Subject or of another natural person.
5. 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.
6. Processing is necessary for the purposes of the **Legitimate Interests** pursued by the data controller 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).

No single basis is 'better' or more important than the others and a decision will be made about which is most appropriate, depending on the purpose and relationship with the individual. Legal Bases are stated in the Privacy Notice.

Individual Rights

Under Data Protection legislation, data subjects have the following rights with regards to their personal information:

- the right to be informed about the collection and use of their personal data
- the right to access personal data
- the right to have inaccurate personal data rectified, or completed if it is incomplete
- the right to erasure (to be forgotten) in certain circumstances
- the right to stop or restrict processing of personal data
- the right to data portability, which allows the data subject to obtain and reuse their personal data for their own purposes across different services
- the right to object to processing in certain circumstances
- rights in relation to automated decision making and profiling

Data Protection Impact Assessment

The Ashburton and Moorland Mission Community 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).

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 the GDPR and the DPA 2018, 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 our Benefice, 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 DPL.
- 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 basis' section).
- If we must transfer or share data, we do so using appropriate security measures;
- If we are sharing data outside of the UK or the EU, 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 DPL.

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 we would not be able to defend if challenged. Although a certain amount of informality can be attached to email writing, these can provide a written record of our comments and they are potentially disclosable to a data subject if they contain personal data.

. In general we:

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

Data Subject Access Requests

If an individual makes a Data Subject Access Request (DSAR) relating to their personal data processed by the AMMC, the DPL 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.

Requests must be made in writing.

Data subjects are entitled to obtain, based upon a request made in writing to the DPL and upon successful verification of their identity, the following information about their own personal data:

- The purposes of the collection, processing, use and storage of their personal data.
- The source(s) of the personal data, if it was not obtained from the data subject.
- The categories of personal data stored for the data subject.
- The recipients or categories of recipients to whom the personal data has been or may be transmitted, along with the location of those recipients.
- The envisaged period of storage for the personal data or the rationale for determining the storage period.
- The use of any automated decision-making, including profiling.
- The right of the data subject to:
    - object to processing of their personal data.
    - lodge a complaint with the Data Protection Authority.
    - request rectification or erasure of their personal data.
    - request restriction of processing of their personal data.

All requests received for access to or rectification of personal data must be directed to the DPL, who will log each request as it is received. A response to each request will be provided within 30 days of the receipt of the written request from the data subject. Appropriate verification must be obtained to confirm that the requestor is the data subject or their authorised legal representative. Data subjects shall have the right to require the AMMC to correct or supplement erroneous, misleading, outdated, or incomplete personal data.

If The Ashburton and Moorland Mission Community cannot respond fully to the request within 30 days, the DPL shall nevertheless provide the following information to the data subject, or their authorised legal representative within the specified time:

- An acknowledgement of receipt of the request.
- Any personal data located to date.
- Details of any requested information or modifications which will not be provided to the data subject, the reason(s) for the refusal, and any procedures available for appealing the decision.
- An estimated date by which any remaining responses will be provided.
- An estimate of any costs to be paid by the data subject (e.g. where the request is excessive in nature).
- The name and contact information of the DPL

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.

Detailed guidance for dealing with requests from data subjects is available from the Diocese by emailing:

dataprotection@exeter.anglican.org

Data Breaches

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

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. Every effort should be made to contain the Breach to ensure no further data is lost, corrupted or accessed.

You must report suspected or actual personal data breaches to the DPL, who will then notify the Rector, Vicars and Churchwardens.

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

Training

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

Complaints

If an individual is dissatisfied with the way that The Ashburton and Moorland Mission Community has dealt with the processing of their Personal Data, they should be advised to contact the DPL in the first instance:

Francis Parffrey | francis@moorlandteam.org.uk

Should the DPL be unable to satisfy the complaint, individuals should be advised to put forward their complaint in writing to the Diocesan Data Protection Officer:

Annemarie Kendell, Operations Manager & Executive Assistant to the Diocesan Secretary
The Old Deanery, Exeter EX1 1HS
dataprotection@exeter.anglican.org
Tel: 01392 294901

If they are still dissatisfied, they can complain to the Information Commissioners Office, who can be contacted on 0303 123 1113 or via email https://ico.org.uk/global/contact-us/email/

or at the Information Commissioner's Office,
Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF

Approval and Review

Approved by	Cassie Long
Policy owner	AMMC
Policy author	Annemarie Kendell
Date	14/07/2023
Review date	14/07/2024

Revision History

Version No.	Revision Date	Summary of Changes	Author
1.0	18.02.2021	New policy	Annemarie Kendell
1.1	14.07.2023	Amended policy	Annemarie Kendell