General Data Protection Policy

1. Introduction

This Policy sets out the obligations of Mothers' Union Diocese of St Edmundsbury and Ipswich ("charity" or "MU") regarding data protection and the rights of customers and suppliers ("data subjects") in respect of their personal data under the General Data Protection Regulation ("the Regulation").

The Regulation defines "personal data" as any information relating to an identified or identifiable natural person (a 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.

This Policy sets out the procedures that are to be followed when dealing with personal data. The procedures and principles set out herein must be followed at all times by the charity, its employees, members, volunteers, agents, contractors, or other parties working on behalf of the charity.

The charity is committed not only to the letter of the law, but also to the spirit of the law and places high importance on the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy, and trust of all individuals with whom it deals.

2. The Data Protection Principles

This Policy aims to ensure compliance with the Regulation. The Regulation sets out the following principles with which any party handling personal data must comply. All personal data must be:

a) processed lawfully, fairly, and in a transparent manner in relation to the data subject;

b) collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;

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

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the Regulation in order to safeguard the rights and freedoms of the data subject;

f) 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.

3. **Data Processing by External Suppliers**

It is the responsibility of the nominated 'Data Owner' (for each activity a person is logged as responsible for the handling of personal data) within the Diocese to approve all subcontractors used by MU to process personal data on its behalf, according to the requirements of this procedure. It is the responsibility of the owners of third-party relationships to ensure that all data processing by third parties are carried out according to the requirements of this procedure. Regular audits of third-party compliance shall be carried out by the Data Owner, who shall be responsible for them.

4. **Consent**

4.1 Consent is not required for members' data to be held by the charity, or for the charity to communicate with members – this is 'legitimate interest'. The charity will not engage in marketing appeals or products, as the primary purpose of the communication, with any individual unless consent is obtained first.

4.2 Consent explicitly is required when collecting images, video and other material for external marketing purposes (this includes use on the website, social media and any publication intended for the general public). Consent will also be sought when non-members seek information or to be added to mailing lists.

4.3 Consent is defined as any indication on the part of the data subject that he or she agrees that their personal data may be processed. Consent must be given freely, without any duress, it must be specific, informed and without ambiguity and shall be granted by the data subject either by way of a statement or through clear, affirmative action on his or her part.

4.4 In relation to the processing of personal data of children under the age of 16, MU requires additional consent from the person who has parental responsibility over the child and MU must be able to demonstrate that this additional consent has been provided, as per Parental Consent Form and that it has taken reasonable efforts to ensure that the claim of parental responsibility is authentic and true, including the use of available technology.

5. **Retention Procedure**

Role	**Responsibility**
Data Owner	To ensure that the collection, retention and destruction of all personal data by each department is carried out according to the requirements of the GDPR.
Treasurer	To ensure that all financial records, including accounting and tax records are retained for no longer than 7 years.
Diocesan President	To ensure that all HR records are retained no longer than 6 years in total.
Health and Safety Officer	To ensure that all Health and Safety records are retained in accordance to MU's Public Liability Insurance policy (normally 40 years).
Treasurer	To ensure that all relevant statutory and regulatory records are retained for statutory limitation periods. (with the exception of the aforementioned records listed above).
Treasurer	Donor's data if lapsed should not be kept beyond the 7 years tax audit.
Communications Coordinator	Consent to receive communication is advised to be refreshed every 2 years other than the consent already obtained to use photographs and video footages.

6. Data Breach

MU is required to provide the following to the supervisory authority in case of a data breach:

- A description of the nature of the personal data breach;
- The categories of personal data that have been affected by the breach;
- The number, which may be approximated if necessary, of data subjects affected by the breach;
- The number, which may be approximated if necessary, of personal data records affected by the breach;
- The name and contact details of the Data Owner (individual nominated within the Diocese as responsible for the security of that data);
- The likely outcomes of the personal data breach;
- Any measures taken by MU to address and/or mitigate the breach; and
- All other information regarding the data breach.

7. General Training

MU is responsible for ensuring that all of its employees, members and volunteers are aware of their personal responsibilities in relation to personal data, ensuring that it is properly protected at all times and is processed only in line with MU's procedures.

To this end, MU shall ensure that all of its employees, members and volunteers are given appropriate and relevant training.

8. Privacy Impact Assessment

A subsequent PIA may be carried out in the following circumstances:

- When setting up a new IT system;
- When new legislation, policies or related matters affecting privacy, are developed;
- When launching a data sharing initiative; and/or
- When personal data is used for new purposes.

9. Fair Processing Procedure and the Data Subjects Rights

Information regarding the rights of data subjects in respect of their personal data, including but not limited to must be included in the Fair Processing Notice:

- The right to access personal information;
- The right to withdraw consent;
- The right to amend personal data;
- The right to request that personal data be permanently deleted;
- The right to strict processing; and
- The right to raise an official complaint with the relevant authority.

10. Keeping Data Subjects Informed

MU shall ensure that the following information is provided - by reference to this Data Protection Policy - to every data subject when personal data is collected:

a) Details of the charity including, but not limited to, the identity of its Data Owner;

b) The purpose(s) for which the personal data is being collected and will be processed and the legal basis justifying that collection and processing;

c) Where applicable, the legitimate interests upon which MU is justifying its collection and processing of the personal data;

d) Where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed;

e) Where the personal data is to be transferred to one or more third parties, details of those parties;

f) Where the personal data is to be transferred to a third party that is located outside of the European Economic Area (the "EEA"), details of that transfer, including but not limited to the safeguards in place;

g) Details of the length of time the personal data will be held by MU (or, where there is no predetermined period, details of how that length of time will be determined);

g) Details of the data subject's rights under the Regulation;

h) Details of the data subject's right to withdraw their consent to the MU's processing of their personal data at any time;

i) Details of the data subject's right to complain to the Information Commissioner's Office (the 'supervisory authority' under the Regulation);

j) Where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data and details of any consequences of failing to provide it;

k) Details of any automated decision-making that will take place using the personal data (including but not limited to profiling), including information on how decisions will be made, the significance of those decisions and any consequences.

The information set out above in Part 10 shall be provided to the data subject at the following applicable time:

10.1 Where the personal data is obtained from the data subject directly, at the time of collection;

10.2 Where the personal data is not obtained from the data subject directly (i.e. from another party):

a) If the personal data is used to communicate with the data subject, at the time of the first communication; or

b) If the personal data is to be disclosed to another party, before the personal data is disclosed; or

c) In any event, not more than one month after the time at which the MU obtains the personal data.

11. **Data Protection Measures**

The Charity shall ensure that all its employees, members, volunteers, agents, contractors, or other parties working on its behalf comply with the following when working with personal data:

a) When the Diocese sends personal data by email, the personal data should not be in the body of the email but in an attachment (eg Word document) which should be password protected;

b) Where any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of. Hardcopies should be shredded, and the more sensitive of personal data be securely shredded with certificate provided by shredding agent;

c) It is preferable to transmit personal data via a wired connection rather than over a wireless network (ie use a LAN cable rather than wifi if possible);

d) If an email is received which contains personal data in the body of the email, then the data should be copied from the body of that email and stored securely. The email itself should be deleted, and the Deleted Items email folder emptied.

e) Where personal data is to be sent by facsimile transmission the recipient should be informed in advance of the transmission and should be waiting by the fax machine to receive the data;

f) Where personal data is to be transferred in hardcopy form it should be passed directly to the recipient or sent using Royal Mail or an equivalent postal service, preferably tracked;

g) No personal data may be shared informally and if an employee, member, volunteer, agent, sub-contractor, or other party working on behalf of the Charity requires access to any personal data that they do not already have access to, such access should be formally requested from the Data Owner;

h) All hardcopies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet or similar;

i) No personal data may be transferred to any employees, members, volunteers, agents, contractors, or other parties, whether such parties are working on behalf of the Charity or not, without the authorisation of the Data Controller;

j) Personal data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, members, volunteers, agents, sub-contractors or other parties at any time;

k) If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it;

l) No personal data should be stored on a memory stick, whether such device belongs to the Charity or otherwise without formal written approval from the Data Controller and, in the event of such approval, strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary;

m) All electronic copies of personal data should be stored securely using passwords and data encryption;

n) All passwords used to protect personal data should be changed regularly and should not use words or phrases that can be easily guessed or otherwise compromised. All passwords should contain a combination of uppercase and lowercase letters, numbers, and symbols;

o) Under no circumstances should any passwords be written down or shared between any employees, members, volunteers, agents, contractors, or other parties working on behalf of the Charity. If a password is forgotten, it must be reset using the applicable method.

12. **Organisational Measures**

MU shall ensure that the following measures are taken with respect to the collection, holding, and processing of personal data:

a) All employees, members, volunteers, agents, contractors, or other parties working on behalf of the Charity shall be made fully aware of both their individual responsibilities and the Charity's responsibilities under the Regulation and under this Policy, and shall be provided with a copy of this Policy;

b) Only employees, members, volunteers, agents, sub-contractors, or other parties working on behalf of MU that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data held by the Charity;

c) All employees, members, volunteers, agents, contractors, or other parties working on behalf of MU handling personal data will be appropriately trained to do so;

d) All employees, members, volunteers, agents, contractors, or other parties working on behalf of MU handling personal data will be appropriately supervised, particularly when handling sensitive personal data (eg AFIA beneficiaries);

e) Methods of collecting, holding and processing personal data shall be regularly evaluated and reviewed;

f) All employees, members, volunteers, agents, contractors, or other parties working on behalf of MU handling personal data will be bound to do so in accordance with the principles of the Regulation and this Policy by contract;

g) All volunteers, agents, contractors, or other parties working on behalf of MU handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees and volunteers of MU arising out of this Policy and the Regulation;

h) Where any volunteers, agent, contractor or other party working on behalf of MU handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless MU against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

13. **Implementation of Policy**

This Policy shall be deemed effective as of 18/3/2019. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

This Policy has been approved and authorised by:

Name: Position: Diocesan President

Signature: Date:

Due for Review by: 2025