



Carlisle Diocese Mothers' Union

Data Protection Policy

June 2020

Carlisle Diocese Mothers' Union
Data Protection Policy
June 2020

1. Introduction

1.1 This Policy sets out the obligations of Carlisle Diocese Mothers' Union (CDMU) regarding data protection and the rights of donors, members, beneficiaries and suppliers ("data subjects") in respect of their personal data under the General Data Protection Regulation (GDPR). GDPR alters how individuals and organisations can handle the personal information of the public. GDPR also boosts the rights of individuals and gives them more control over their information

1.2 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, volunteers, agents, contractors, or other parties working on behalf of the charity.

1.3 Definitions

- **Personal Data:** any information relating to an identified or identifiable person
- **Data Subject:** Individual member whose personal data is being stored
- **Identifiable Person:** Someone who can be identified, directly or indirectly
- **Responsible person:** Takes responsibility for Carlisle Diocese Mothers' Union ongoing compliance with this policy
- **Data Manager:** Manages the data on behalf of CDMU and MSH.

1.4 The CDMU 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 GDPR. GDPR sets out the following principles with which any party handling personal data must comply. All personal data must be:

Principle 1: Personal data shall be processed lawfully, fairly, and in a transparent manner in relation to the data subject.

Principle 2: Personal data shall be 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.

Principle 3: Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

Principle 4: Personal data shall be 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.

Principle 5: Personal data shall be 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.

Principles 6&7: Personal data shall be 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 'Data Owner' (for each activity is logged as responsible for the handling of personal data) to approve all subcontractors used by CDMU 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 *(See Appendix 1 for CDMU consent forms)*

- 4.1 Consent is not required for members data to be held by the CDMU, or for the CDMU, to communicate with members – this is 'legitimate interest'. The CDMU, 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. 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, CDMU requires additional consent from the person who has parental responsibility over the child and CDMU must be able to demonstrate that this additional consent has been provided, as per Parental Consent Form (see Appendix 1b) 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 branch is carried out according to the requirements of the GDPR. Including Permission to Share Details. (Appendix 5) |
| Treasurer | 1: To ensure that all financial records, including accounting and tax records are retained for no longer than 7 years. 2: To ensure that all relevant statutory and regulatory records are retained for statutory limitation periods. (with the exception of the aforementioned records listed above). 3: To ensure donor’s data, if lapsed, should not be kept beyond the 7 years tax audit. |
| 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). |
| Communications Coordinator: Diocesan Secretary | 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

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, Carlisle Diocese Mothers’ Union shall promptly assess the risk to people’s rights and freedoms and if appropriate report

this breach to the Information Commissioner's Office (ICO). CDMU 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.
- 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

CDMU is responsible for ensuring that all of its employees 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 CDMU's procedures. This will be achieved by 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.

(See Appendix 2 for the PIA form and an example completed PIA)

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.
- (see Appendix 4 for Subject access request form and procedure)

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:

10.1 Details of CDMU

- The purpose(s) for which the personal data is being collected and will be processed and the legal basis justifying that collection and processing.
- Details of the length of time the personal data will be held by CDMU (or, where there is no predetermined period, details of how that length of time will be determined);
- Details of the data subject's rights under GDPR.
- Details of the data subject's right to withdraw their consent to the CDMU's processing of their personal data at any time.

10.2 The information set out above shall be provided to the data subject at the following applicable times:

- Where the personal data is obtained from the data subject directly, at the time of collection.
- Where the personal data is not obtained from the data subject directly (i.e. from another party):
 - at the time of the first communication OR
 - before the personal data is disclosed OR
 - in any event, not more than three months after the time at which the MU obtains the personal data.

11. Data Protection Measures

- 11.1 Carlisle Diocese Mothers' Union shall ensure that personal data is stored securely using modern software that is kept-up to-date. Any paper records should be kept locked away. *(see Appendix 6 for data protection measures)*
- 11.2. Access to personal data shall be limited to personnel who need access and appropriate security should be in place to avoid unauthorised sharing of information.
- 11.3. When personal data is deleted this should be done safely such that the data is irrecoverable.
- 11.4. Appropriate back-up and disaster recovery solutions shall be in place.
- 11.5 A summary of these measures are provided by the CDMU's "GDPR at a glance for Deanery and Branch leaders". (See Appendix 6)

12. Organisational Measures

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

- a) All employees, volunteers, agents, contractors, or other parties working on behalf of CDMU 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, volunteers, agents, sub-contractors, or other parties working on behalf of CDMU 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 CDMU;
- c) All employees, volunteers, agents, contractors, or other parties working on behalf of CDMU handling personal data will be appropriately trained to do so.
- d) All employees, volunteers, agents, contractors, or other parties working on behalf of CDMU handling personal data will be appropriately supervised.
- e) Methods of collecting, holding and processing personal data shall be regularly evaluated and reviewed.
- f) The performance of those employees, volunteers, agents, contractors, or other parties working on behalf of CDMU handling personal data shall be regularly evaluated and reviewed.
- g) All employees, volunteers, agents, contractors, or other parties working on behalf of CDMU handling personal data will be bound to do so in accordance with the principles of GDPR and this Policy by contract.
- h) All volunteers, agents, contractors, or other parties working on behalf of CDMU 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 CDMU arising out of this Policy and GDPR;
- i) Where any volunteers, agent, contractor or other party working on behalf of CDMU handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless CDMU 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 3rd June 2020. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

This GDPR Policy should be reviewed annually by CDMU at the October Diocesan Council Meeting.

This Policy has been approved and authorised by:

Signature:

Name:

Position:

Date:

Due for Review by:

APPENDICES

Appendix 1a: CDMU Data Consent Form

Appendix 1b: Parental Consent Form

Appendix 2a: PIA Form

Appendix 2b: An example of a completed PIA form

Appendix 3: Fair Processing Notice

Appendix 4: Subject access request form and procedure

Appendix 5: Permission to share information

Appendix 6: GDPR at a glance for Deanery and Branch Leaders



MSH Membership Communication Project –Information accessed by MSH and Carlisle Diocese MU only

Essential Information Name of Branch

Title_____ Forename(s) _____ Surname _____

Full Address _____ **Post Code** _____

Optional Information

Date of Birth ___/___/___ Tel.no. _____

E-Mail _____

Are you willing to have your photograph used in MU publicity? YES/NO

Date joined MU ___/___/___ Gift Aid Yes/No Families First Yes/No MU e letter Yes/No

Skills _____ Mothers' Union Role _____

Do you wish to receive Marketing or Fundraising communication from MSH? Yes/ No I understand that all personal data will be held in accordance with the Data Protection Act 1998, the General Data Protection Regulation and all relevant legislation and best practice guidance

Signed _____ Date _____



MSH Membership Communication Project –Information accessible by MSH and Carlisle Diocese MU only

Essential Information Name of Branch

Title_____ Forename(s) _____ Surname _____

Full Address _____ **Post Code** _____

Optional Information

Date of Birth ___/___/___ Tel.no. _____ E-Mail _____

Are you willing to have your photograph used in MU publicity? YES/NO

Date joined MU ___/___/___ Gift Aid Yes/No Families First Yes/No MU e letter Yes/No

Skills _____ Mothers' Union Role _____

Do you wish to receive Marketing or Fundraising communication from MSH? Yes/ No I understand that all personal data will be held in accordance with the Data Protection Act 1998, the General Data Protection Regulation and all relevant legislation and best practice guidance

Signed _____ Date _____



Registration and Consent Form - Mothers' Union Led Children's Groups and Trips

Name of MU Branch

Family contact details:-

Full name of parent and/or responsible accompanying Adult
.....

Child's Full NameDate of birth.....

Parent/ Guardian's mobile number. and

E.mail

Responsible accompanying adult's details if different from above:-
.....
.....

About your child:-

Does your child have any food allergies? Please specify
.....

Does your child have any special needs which we need to know about?
.....
.....

Is there anything you would like us to know about your child?
.....
.....

Emergency contact details for parents/guardians:-

Contact name for carer or an alternative adult in case of an emergency:
.....

Tel.no.....Relationship to you or your child

Declaration

I give permission for my child to attend and take part in the activities organised by Mothers' Union.

Signed (responsible adult/parent/guardian)

Dated.....

Taken from Parish Safeguarding Handbook, Church of England. Model registration form – Activities and Trips

FOR APPENDICES 2A PIA Forms and 2B - An example of completed PIA see separate attachments.

(To be used on the reverse of Appendix 1a and Appendix 5)* **Appendix 3*

Fair Processing Notice for Members

Personal Data of members is required for legitimate purposes with CDMU and will be retained for as long as they remain members.

The member has the right to:

1. Access personal information
2. Withdraw consent
3. Amend personal data.
4. Request that personal data be permanently deleted.
5. Strict processing ie. By following laid down procedures on member's behalf
6. Raise an official complaint with the relevant authority.

Fair Processing Notice for Members

Personal Data of members is required for legitimate purposes with CDMU and will be retained for as long as they remain members.

The member has the right to:

1. access personal information
2. withdraw consent
3. amend personal data.
4. Request that personal data be permanently deleted.
5. Strict processing ie. By following laid down procedure on member's behalf
6. Raise an official complaint with the relevant authority.

**Mothers' Union Diocese of Carlisle (CDMU)
Subject Access Request Form (by a third party)**

1. DATA SUBJECT DETAILS

Title Surname
First Name(s)
Current Address
.....

Telephone Numbers:
Home.....
Work
Mobile.....

E Mail Address
Date of Birth __ / __ / ____
Means of identification provided to confirm name of data subject:
.....
.....

Details of data requested:
.....
.....

2. DETAILS OF PERSON REQUESTING THE INFORMATION

Are you acting on behalf of the data subject with their written (or other) legal authority? Yes
No

If 'Yes' please state your relationship with the data subject (e.g. parent, legal guardian or solicitor)
.....

Please enclose proof that you are legally authorised to obtain this information

Title Surname.....
First Name(s)
Current Address (incl Post Code).....
.....

Telephone Numbers:

Home
Work
Mobile

Email Address

I have included valid proof of identification (copies of valid passports or driving licences are acceptable)

DECLARATION

I,, the signatory and person identified above as the data subject, hereby request that CDMU provide me with the personal data about me identified above.

Signature:

Date:

SAR form received by Responsible Officer: (This is the person within the CDMU responsible for the processing of the SAR.)

I,, the signatory and person identified at section 2 above, hereby request that CDMU provide me with the personal data identified above.

Signature:

Date:

SAR form received by [Responsible Officer]:

CDMU Subject Access Procedure

1. Scope

This procedure covers all personal data that is processed by CDMU with the exception of personal data that is routinely requested by Data subjects.

It is the right of all data subjects to ask CDMU the following:

1. What personal data is being processed about that person by CDMU;
2. To be provided with a description of the personal data processed by CDMU about that person;
3. The purpose or purposes for which the personal data is being processed
4. Confirmation of who will have access to the personal data; AND
5. To be provided with a copy of the personal data, as well was a confirmation of where CDMU acquired that personal data.

2. Responsibilities

The (Responsible Officer) shall be responsible for the application and functionality of the procedure and shall handle all Subject Access Requests ("SARs). They shall inform the Head of IT at Mary Sumner House an all matters relating to SARs.

3. Procedure

All SARs are made using form Subject Access Request Form.

The data subject is required to provide evidence of his or her identity by way of current passport or driving licence and his or her signature must be cross-referenced with the signature provided on the Subject Request Access Form.

The following information must be provided by the data subject on the Subject Access Request Form: the personal data that is being requested, whether specific data or all data held by CDMU where it is being held.

CDMU is required to record the date on which the Subject Request Access Form, with the accompanying identification evidence is submitted.

CDMU has one month from this date to provide to the data subject the personal data requested. Should CDMU fail to provide the requested information within the one month window, this shall be in direct breach of the GDPR. No extension shall be allowed under any circumstances.

It is vital that the Subject Access Form is sent to the Responsible Officer straight away, to ensure that the requested data is collected within the one month window.

The Responsible Officer will carry out data collection by one of the following steps:

1. Collecting the personal data requested; OR
2. Carrying out a search of all electronic and hard-copy databases including manual files, backup and archived files as well as email folders and archives.

They shall at all times have access to a data map which sets out the location of all CDMU's stored data.

At no time may personal data ever be altered or destroyed in order to avoid disclosure.

RESPONSIBILITIES

The Responsible Officer is responsible for the following:

1. Keeping a record of all SARs made, including the date on which the SAR was received.
2. Reviewing all the documents provided to a data subject pursuant to an SAR to check for the mention of any third parties and if a third party is mentioned, to prevent the disclosure of the identity of the third party to the data subject, or to seek written consent from the third party as to the disclosure to their identity.

Personal data exemption categories

The following data exemption categories apply, meaning that CDMU does not have to provide personal data covered below:

- The prevention and detection of crime.
- Negotiations with the data subject matter maker.
- Management forecasts.
- Confidential references provided by CDMU however not references provided to CDMU
- Data covered by legal professional privilege.
- Data used for research, statistical or historical reasons.

Personal data provided by CDMU to a data subject pursuant to a SAR shall be in electronic format, unless the SAR expressly requests or otherwise and all items shall be scheduled, displaying the subject's name and the date on which the data item was delivered.

4. Document owner

The Responsible officer is the owner of this policy and must ensure that it is periodically reviewed according to the requirements contained herein.

The latest version of this policy document dated 3rd June 2020 is available to all employees and volunteers of CDMU on the Diocesan website.

This policy document was approved by CDMU Board of Trustees and is issued by the Diocesan President on a version controlled basis.

Name of DP

Date

PERMISSION TO SHARE INFORMATION WITHIN CDMU

In order to Produce a paper list of officers within the Diocese we need a signed authority.

I.....give permission to CDMU to publish and share my contact information with other officers of the Mothers’ Union within Carlisle Diocese only. I also understand that my details will be deleted securely when my term of office ends.

The information will be shared with other Officers within CDMU only. The information required is for the purpose of contact with other Branches/Deaneries for sending out invitations, arranging joint functions, sharing information especially where Officers do not have access to the Membership Database.

Name:.....Telephone No.....

Branch/Deanery.....Email address:-.....

Officers details to be deleted when their term of office ends.

PERMISSION TO SHARE INFORMATION WITHIN CDMU

In order to Produce a paper list of officers within the Diocese we need a signed authority.

I.....give permission to CDMU to publish and share my contact information with other officers of the Mothers’ Union within Carlisle Diocese only. I also understand that my details will be deleted securely when my term of office ends.

The information will be shared with other Officers within CDMU only. The information required is for the purpose of contact with other Branches/Deaneries for sending out invitations, arranging joint functions, sharing information especially where Officers do not have access to the Membership Database.

Name:.....Telephone No.....

Branch/Deanery.....Email address:-.....

Officers details to be deleted when their term of office ends.

Appendix 6

The General Data Protection Regulation (GDPR) was introduced 25th May 2018 to update previous data protection laws in line with increasing use of digital records. Consent is not required for members data to be held by the charity to communicate with members – this is a legitimate interest. Permission must be sought from Members before contacting them solely with regard to marketing appeals or products.

Carlisle Diocese Mothers' Union is committed to processing data in accordance with its responsibilities under GDPR, according to the following principles:-

Principle 1. Personal data shall be processed lawfully, fairly and in a transparent manner in relation to all members.

Principle 2. Personal data shall be collected for specific, explicit and legitimate reasons and not shared with others.

Principle 3. Personal data shall be adequate, relevant and limited to what is necessary for the purpose.

Principle 4. Personal data shall be accurate and kept up to date.

Principle 5. Personal data shall be kept in a form which permits identification of persons no longer than is necessary for what is required.

Principle 6. Personal data shall be processed in a manner that ensures appropriate security. Protection against unauthorised or unlawful processing, against loss of records, destruction or damage

Action required for each of the principles.

1.& 2. Branches should keep Registers of attendance and records of members as appropriate for the requirements of the Branch for Mothers' Union purposes only and details are not to be shared with anyone else.

3. CDMU will produce a list of Branch, Deanery Leaders and Officers with their names, telephone numbers and e mail addresses only, with the individual's permission to do so. If addresses are required you must ring the person concerned for that information.

4. Branches should inform the Data Manager of changes to members' details and provision is being made on the Annual Branch Report Form to ensure accuracy of our records. New members will be required to complete a Membership Data Form and it would be advisable to report the death of a member as soon as appropriate.

5. Archiving of Branch records. Official records, branch accounts, minute books and personal records of members should be kept no longer than seven years and should then be sent to the local Archive office for secure storage. All paper documents not required to be saved should be shredded and disposed of responsibly.

Contact information for speakers etc. should only be kept for as long as necessary and to be kept securely and shredded when no longer required.

6. Every precaution should be used to make sure information on Mothers' Union members is not accessible to anyone else. Digital records must be password protected and computer screens not left on unattended. Members' personal information is not to be stored on mobile phones or memory sticks. E mails containing members' personal information should be sent Password Protected. Paper records should be stored securely.

Where MU holds personal data of children under the age of 16, permission must be obtained from the person who has parental responsibility for the child. (Parental Consent Form)

Any Breach of Data must be reported to Carlisle Diocese Mothers' Union.

A full copy of the Carlisle Diocese Mothers' Union GDPR Policy is held by the Diocesan President and will be reviewed annually at Diocesan Council.