

## **Mothers' Union Diocese of Peterborough GDPR Reference Sheet**

### **Introduction**

The Mothers' Union Diocese of Peterborough is committed to protecting and respecting members' privacy. We are governed by our General Data Protection Policy which ensures data is collected, retained and destroyed in line with the General Data Protection Regulation.

This sheet is a reference giving an outline and is designed to be an aid to coordinators, officers, deanery and branch leaders and others who may legitimately hold data. Specific policies should be consulted for full details and the Data Controller is available to answer questions.

We all hold information about members, volunteers, donors, supporters and beneficiaries for several reasons including:

- To know details about our members, volunteers and people who benefit from our projects;
- To keep our members, donors and supporters informed about what Mothers' Union is doing;
- To ensure that all subscriptions are received and to administer Gift Aid; and
- To inform members about any changes.

All personal information, such as names and contact details, whether held on a computer or in a relevant filing system, needs to be held in accordance with the General Data Protection Regulation (GDPR) which came into effect in the UK on 25th May 2018. This is the new legal framework in the EU for data protection and the UK government has confirmed that the decision to leave the EU will not affect the implementation of the GDPR.

All the information we hold in the Mothers' Union Diocese of Peterborough is purely for Mothers' Union use and is not divulged to any third parties, so we do not need to register with the Information Commissioner's Office. Despite this we still need to comply with the Regulation. Please remember that whilst it is acceptable to share information with other members of the Mothers' Union, they must have a legitimate need for it and treat it in accordance with our Policies. Another acceptable way to collect data on members is when members give specific consent.

An illustration of legitimate need might be for the Diocesan Members coordinator to share contact details of an individual Diocesan member with the branch leader local to them so that the Diocesan member can be invited to a meeting.

We are aware that in many cases members may also be personal friends. It is therefore very important that all those responsible for personal data maintain separate Mothers' Union specific records and these are not muddled with personal records such as an address book.

We recommend that all Mothers' Union records are marked as such and kept, in accordance with our policy, in a separate place.

There are 8 Principles of Good Practice and these are:

### **1. Data must be fairly and lawfully processed**

Make sure you are dealing with the right person. Only the owner of the information can give you permission as to what you can and cannot do with the information. With data protection, vulnerable adults and children also have rights. Depending on the data that is being collected, consent may be needed from the parent/guardian and also the vulnerable adult or child. It is good practice to ensure that children are aware of what their parents are consenting to as a safeguard and to give children a voice to decide what personal data can be accessed by whom.

We don't expect to keep data on children but some of our Indoor members may be considered vulnerable adults. If permission is required, please do so with the guardian, prime carer or Power of Attorney holder, and remember that you can also get support from the Data Controller.

### **2. Data must be collected for specific lawful purposes only**

Use data only for the purpose for which you collected it. The individual has a right to know what that purpose is. Data collected to update a membership database can only be used for membership related purposes. Disclosing the information to the local WI is incompatible as it is not the purpose for which it was collected. However using it to send Mothers' Union meeting minutes to members is a related purpose. Please note that a member has a right to decline information or permission for some types of data use, for example, permission is needed to use photographs of members at events and meetings. These discretionary options are listed on the diocesan membership form.

### **3. Only collect the data you need – adequate and relevant**

There is no need to collect personal information, unless it is necessary for your use. So be clear about what data you need and why you need it. A good example is bank details – there is no need to collect this unless you have a financial relationship with the individual and need to administer transactions such as Direct Debit, payroll or BACS. The membership form outlines what the Board of Trustees feel is required; if you think you need something additional, please contact the Data Controller for support.

Please note that it is permissible, as we are a charity, to put names on minutes in an attendance list. However it is good practice to note what was said and not who said it. In the same way, it should be noted that a motion was proposed, seconded and carried (or not) but not who proposed and seconded the motion.

#### **4. Data must be accurate and where necessary up to date**

Always keep data up to date. Changes of address and relaying of deaths of members are critical. The Mothers' Union Diocese of Peterborough requires that changes of information be updated within the Branch and with the Data Controller within 28 days.

#### **5. Never keep data longer than necessary**

For example:

- Details about Gift Aid need to be kept for a minimum of six years after the end of the gift aid donation. Please note that you will need to keep the information as long as the donor is actively gift aiding his/her donations.
- Criminal data and data associated with security will need to be kept longer – but only keep the data relevant for the purpose.
- Bank details for Direct Debit purposes should not be kept after the member has stopped the mandate.

Data can be kept for statistical purposes without information of a personal nature, including names and addresses. You can keep membership profiles from the past but always ask whether you need to keep data in the format you are keeping it. For example, keep an individual's initials and date of joining as a 'membership number', then date of birth, positions held, etc, but not bank details or their name and address as once the member has left, you do not need this information. If you do not use statistics to analyse your membership, please destroy all data once a member leaves or becomes deceased.

The diocese has a Record Retention policy which gives the period for which certain data should be kept. [See General Data Protection Policy]

#### **6. Personal data will be kept and used in accordance with the General Data Protection Regulation**

The General Data Protection Regulation gives rights to individuals about whom information is held. These include the right to:

- Ask to see the information held about them.
- Object to an organisation holding or processing information about them if it causes unwarranted damage or distress.

- Prevent their data being used without their consent for marketing purposes. Specific permission must be obtained for marketing purposes.

## 7. Always safeguard data against unauthorised or unlawful processing, accidental loss or damage

Data kept on a personal home computer which can be accessed by others is not a safe way of storing data. If the computer is accessible to others then you must password protect the sections that hold information relating to members, using strong passwords. Make sure all portable devices – such as memory sticks and laptops – used to store personal information are encrypted.

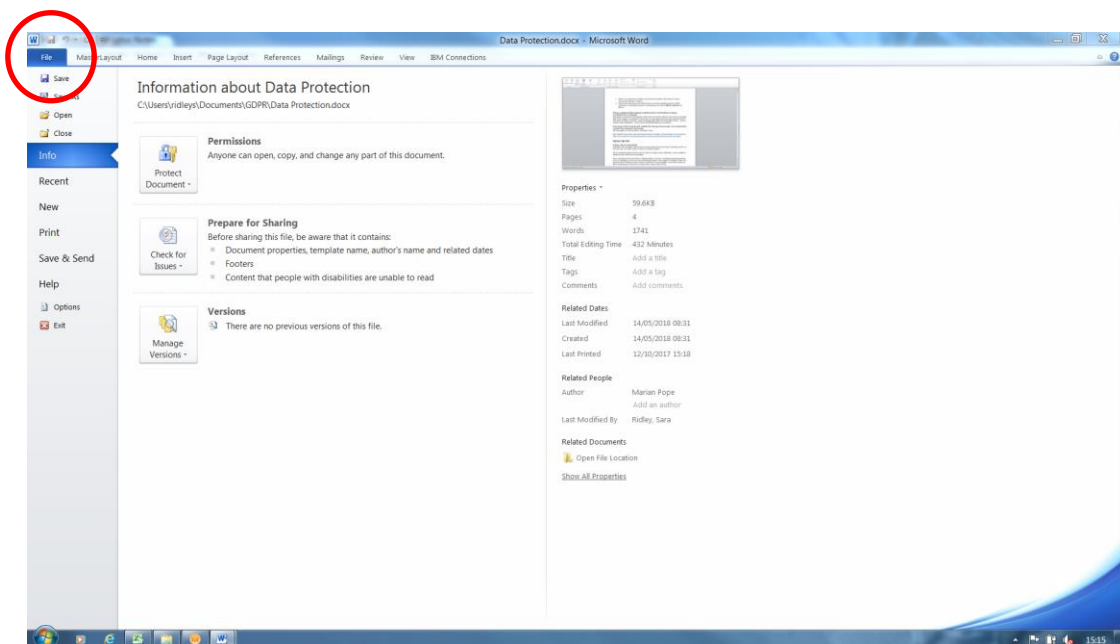
A strong password should be at least 8 characters long and include capital and lower case letters, numbers and symbols, e.g. P4ssw#rd1/

Always use a different password for each set of data.

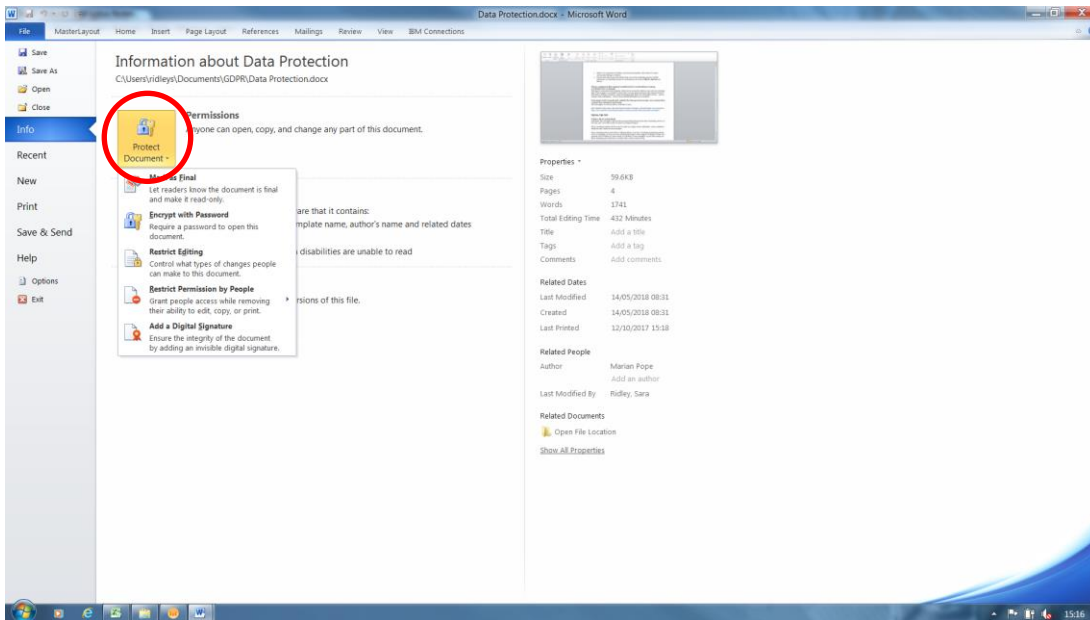
It can be useful to think of a phrase and change letters for symbols or numbers, e.g. Tell out my soul becomes: T3lloutmys#ul

Files can be password protected by:

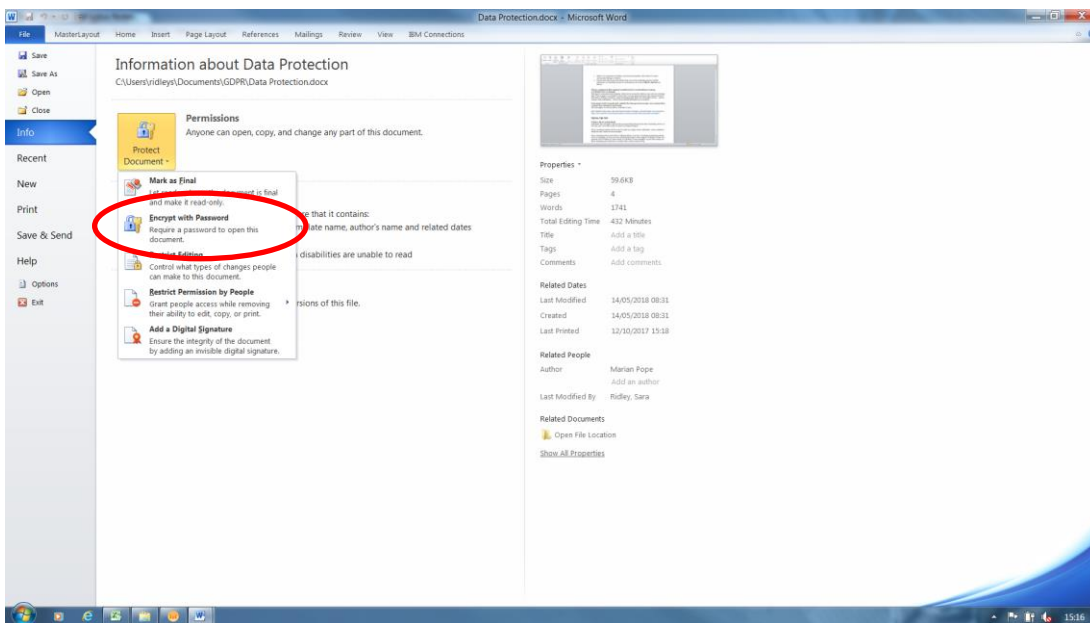
Click on the File tab:



Click on Protect Document:



Click on “Encrypt with a Password”:



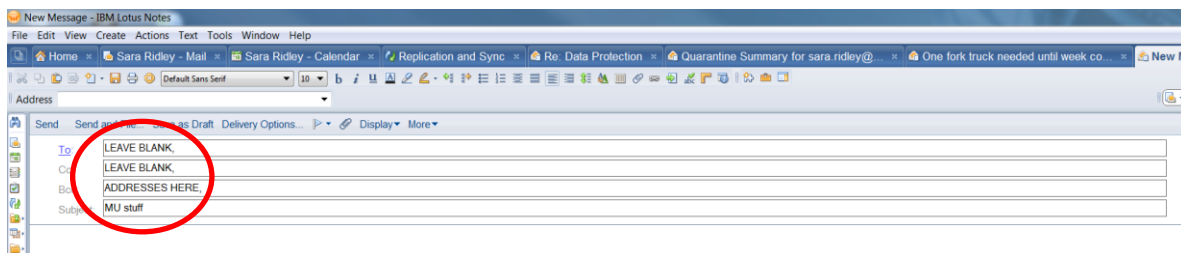
Make sure you know what your password will be and type VERY carefully.

It is possible to encrypt in other ways but this is the simplest way. Data on memory sticks can be encrypted in exactly the same way.

**Remember, if in doubt contact the Data Controller.**

There are further things to consider when using email:

When you send an email to multiple recipients, you cannot show their addresses to others. To prevent this happening you must put the addresses in the Bcc (blind carbon copy) box:



You can do this with lists you have created. People can still click to reply to all and no addresses will be shown.

## **8. Data must not be transferred outside the European Economic Area unless that country has adequate protection**

This also applies to overseas offices of Mothers' Union. Please do not share outside of the Diocese of Peterborough without the permission and guidance of the Board of Trustees.

### **Direct Marketing:**

Individuals have the right to prevent their personal data being used for direct marketing and can, at any time, give you written notice to stop (or not begin) doing so.

Direct marketing includes all the means by which you might contact individuals, such as mailshots, telephone calls, emails and text messages [see the guide at the end of this document].

Direct marketing doesn't just relate to selling products or services: it includes promoting particular views or campaigns. So even if you are using personal data to elicit support for Mothers' Union (or a particular area of Mothers' Union activity or a Mothers' Union campaign) you are still carrying out direct marketing and would have to comply with a written notice to stop.

If you receive a notice to stop, you must comply within a reasonable period which the Mothers' Union Diocese of Peterborough has defined as 28 days.

We do not anticipate that anyone within the Mothers' Union Diocese of Peterborough will engage in direct marketing, however to remain safe please undertake the following:

1. Do not mix messages for fundraising or marketing from other organisations you belong to with those for MU. For instance, whilst you may seek assistance for MU members to run a stall at the Parish fete, do not advertise the W.I. meeting next month.
2. If there is a Worldwide MU initiative, such as the "Big Summer Appeal" that you want to share with members, check their membership form to see if they have agreed to accept appeals literature. Members have the right to say no.  
If members do not want information about appeals, this must be ticked on their membership form.

With some organisations, it is possible to ask members to actively “Opt Out” – in other words you will share information unless they tell you not to – however, the Diocese of Peterborough Board of Trustees requires that consent is actively obtained by the express giving or withholding of consent. Please ensure that the tick boxes on the membership form is filled in correctly.

### **Recording of consent**

You should keep clear records of what a person has consented to, and when and how you got this consent, so that you can demonstrate compliance in the event of a complaint.

### **What happens if I do something wrong?**

Everyone makes mistakes but there are some things that **MUST** happen if do.

This is called an involuntary breach and might be caused by:

- Emails are sent with recipients addresses on view; or
- Contact details are shared with a church member who is not a member of Diocese of Peterborough Mothers’ Union.

Other things might also be involuntary breaches, for instance if a laptop containing member information is stolen.

If anything like this happens, or you think it may have, contact the Data Controller immediately who will advise you of what is necessary and help you. Information accidentally shared within the Mothers’ Union is serious but less so than anything externally shared and this latter must be properly reported.

Voluntary Breaches are likely to be rare but occur when a person in possession of the data knowingly or maliciously shares the data. This is very serious and may be an offence in law. If this has happened or you suspect it might, please contact the Data Controller immediately as this must be reported through the appropriate channels.

### **Data Controller for Mothers’ Union Diocese of Peterborough:**

Mrs. Jean Rose

Phone 01933 663778

Email [jeanerose@btinternet.co](mailto:jeanerose@btinternet.co)

## **General Rules for Communicating**

### **Email & Text Messages**

#### **Do**

Seek consent from members and beneficiaries to communicate with them in this fashion for the following specified reasons. Emails are free to send, convenient and a perfectly acceptable way to communicate in most circumstances. It is therefore desirable for us to continue to be able to communicate in this fashion.

#### **Don't**

Send emails or text messages without active consent – remember legitimate interest cannot be used as a lawful justification for communicating in this way when it comes to appeals, campaigns, selling MU products etc.

#### **Post**

##### **Do**

Feel free to communicate to members on a legitimate interest basis concerning: their membership; the activities of the branch, diocese or worldwide movement; and policy campaigns of the movement at any level.

Communicate with current beneficiaries on a legitimate interest basis concerning programmes or activities.

Communicate with recent former members and beneficiaries on a legitimate interest basis where you have good reason to believe that a forthcoming programme or activity may be of benefit to them.

Communicate with branch speakers on a legitimate interest basis.

Communicate with local clergy on a legitimate interest basis concerning MU activities that will have an impact on the parish.

##### **Don't**

Stray outside the bounds of legitimate interest when sending letters if relying solely on that basis. If in doubt perform a legitimate interest assessment or seek guidance from your diocese.

### **Telephone**

##### **Do**

Feel free to communicate with members by phone on a legitimate interest basis concerning their membership or the activities of the local MU.

Feel free to communicate with current beneficiaries concerning the project and activity they are actively engaging with.

##### **Don't**

Communicate by phone for any other purpose without the active consent of the individual being dialled.