# GDPR Advice for Mothers’ Union branches

## Introduction

The General Data Protection Regulation (GDPR) came into force in May 2018. All organisations in the UK must comply, including charities such as Mothers’ Union. The legislation has been brought in to protect the privacy of people throughout the EU, and was needed because some organisations persisted in misusing and selling personal information.

Full details about GDPR can be found on the Information Commissioner’s Office website <https://ico.org.uk/>, however the GDPR is written as principles which must be interpreted to suit each organisation. Mothers’ Union at Mary Sumner House is providing guidance on how Dioceses should comply with GDPR. This includes templates for a data protection policy, privacy impact assessments, website privacy statement, checklists and logs etc.

## Personal data

Personal data means any information relating to a living person – for MU purposes this is most likely to include members’ names and addresses, phone numbers, email addresses and in some cases dates of birth. In addition, details of Families First subscriptions and Gift Aid will be held in the Diocese, and some branches may hold personal data about baptism families and/or wedding couples in their parish.

## Consent

Members have chosen to join MU, so we do not need their consent to hold their personal data because this is deemed ‘legitimate interest’. However if we wanted to send a marketing appeal then consent would be needed first. Consent is also required for all photos used on the website, social media or publicity materials – not just for photos of children.

## Individual’s rights

A person has the right to ask what personal information is held on them and for what purpose, and the Diocese would have to reply within one month.

A person can request that they are removed from all systems including historic information, but this would not override any legal requirements eg to keep financial records for six years.

A person can also opt out of any mailing list.

## Practical guidelines for MU trustees and branches

## General

Make sure your members know why you have their data and what you are using it for.

Only keep personal data as long as you need it, and only use it for the purpose that it was obtained for.

## Emails

It is good practice to use blind copy (Bcc) when sending out an email to a group of people, particularly if the individuals do not need to see each other’s responses. You can put your name in the To box (this means that you know when the email has been sent successfully), and all others in the Bcc box.

When forwarding on an email, please look carefully down the whole email trail and if there are personal email addresses then delete those parts of the email trail before forwarding on.

## Personal data on your laptop / tablet / smartphone

If you have any documents, spreadsheets or other files on your laptop / tablet which contain personal data about MU members or personal data about other people for MU purposes (eg baptism families, wedding couples), then please ensure that you protect the data in either of two ways:

1. Password protection on your device so that only you can login and access your files or email account
2. Protecting each file that contains personal data. In Word and Excel this can be done by selecting File, Info, Protect Document/Workbook, Encrypt with Password.

Passwords should be ‘strong’ – this means not easy to guess, and using a mixture of lower and upper case letters, numbers and ideally a symbol.

When you delete information held electronically, remember to empty the Recycle Bin or Trash Folder so that the items are truly deleted and not recoverable.

## Personal data on paper

If you have any personal data on paper (eg members list, Diocesan Directory), keep it in a locked drawer or locked filing cabinet. When you dispose of it, burn or shred it.