Charity No 2150180

GENERAL DATA PROTECTION REGULATIONS: POLICY SUMMARY

The Mothers' Union Diocese of Bath & Wells has a lawful basis for processing the personal data of its members and contacting them as it is a registered charity whose members expect to be kept up to date with news of its work. The charity has a Data Protection Licence. The Diocesan Secretary is the charity's Data Controller.

The basis of the Regulations is that personal data must be retained securely, disposed of securely when not needed and not passed to anyone outside the charity. In other words, treated as each of us would wish our own data to be treated. The charity's General Data Policy, of which this is a summary, can be viewed on our website: mubathandwells.org. Our Privacy Policy in respect of the use of our website can also be viewed there.

All personal data must be:

- adequate, relevant and processed only for the purposes intended;
- accurate, kept up to date where necessary and deleted when no longer needed: paper copies must be shredded; electronic files are to be deleted and then deleted from the Recycle Bin;
- personal data must not be transferred to anyone outside the charity;
- consent is required for photos, videos etc to be used where they might be used for external marketing purposes, eg Springs newsletter;
- financial records should be retained for no longer than seven years;
- paper copies of personal data (eg Diocesan Handbook) must be kept in a locked drawer, cabinet or similar;
- electronic documents containing personal data should be password protected: this is done by having the document on screen and following these procedures:

  In Word: from menu bar at the top of the screen, select File > Protect Document (Permissions) > Encrypt with Password > follow instructions on screen (you will be asked to enter a password and to confirm it > follow the prompt to save the document. You will need to enter the password to open the document.

  In Excel: from menu bar at the top of the screen, select File > Info > Protect Workbook > Encrypt with Password > follow instructions on screen (you will be asked to enter a password and to confirm it > follow the prompt to save the document. You will need to enter the password to open the document.

  Passwords must be changed often and must be 'strong' ie contain a combination of uppercase and lowercase letters, numbers and symbols rather than words or phrases which could be easily guessed. Passwords must not be shared.

- personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely and the email itself should be deleted and then deleted from the Deleted (or Trash) folder;
- paper copies of personal data needing to be transferred to another person should be passed directly to the recipient or sent using Royal Mail;
- no personal data may be transferred to anyone within or outside the charity without the authorisation of the Data Controller (Diocesan Secretary);
- personal data must be handled with care at all times and should not be left unattended or on view to unauthorised persons; computers and screens must be locked if they are to be left unattended when documents are on screen;
- personal data must not be stored on any mobile device.

Updated 6th March 2025
To be reviewed June 2026