DATA PROTECTION POLICY

Policy number	2008-01	Version	7
Drafted by	Trustee, Ann Fox	Approved by Board on	Sept 2021
Responsible person	Trustee	Scheduled review date	Sept 2023

POLICY STATEMENT

This policy provides a framework for ensuring that NWR meets its obligations under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 18). It applies to all the processing of personal data carried out by NWR.

The GDPR sets out seven key principles:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

As a not for profit organisation NWR is not obliged to register with the Information Commissioner, however, it is committed to upholding the principles of the GDPR and the DPA. This extends to all data whether held electronically or in structured files.
NWR will not share any information with a third party unless legally obliged to do so.
Any member may request to receive a copy of information held about them.
Only those individuals who are officers, employees or under contract to the organisation have access to the NWR Membership database or to copies of it.

The National Organiser is NWR's Data Protection Officer.

PROCEDURE
NWR exists to put like-minded women in touch with each other. To be effective, NWR operates with a database and holds the following personal data (data which enables a person to be identified) about every member where the member has given the information.

- Name
- Home address
- Group name, if a group member
- Telephone number
- Email address
- Date of membership renewal

- Gift Aid eligibility
- Age Range

Personal data about lapsed members is archived to make it easier for a lapsed member to rejoin without extra administrative procedures and for the organisation to contact ex-members regarding possible events of interest. Personal details will be deleted after 2 years.
Personal data about members who have attended NWR's annual National Conference, workshop and events is held for 12 months after the end of the event for audit purposes and communications regarding future conferences.

Financial records that may contain some members' bank details will be held only as long as required to meet audit and statutory obligations.

THE NWR OFFICE, STAFF AND TRUSTEES

- Use membership data solely for the purposes connected with the business and running of NWR.
- Never knowingly pass personal data onto individuals or organisations without the express permission of those concerned.
- Only give the names and phone numbers/email addresses of enquirers to group LOs (or designated contact person) and vice versa who have agreed to be a contact.
- Ensure that personal details are never displayed on the website.
- Keep all personal data secure by ensuring it is locked away.
- Data is password protected
- Take weekly backups
- Ensure that computers containing membership records or NWR accounts are protected by a firewall.
- Conduct regular and up-to-date virus scans on all computers.
- Ensure that structured paper-based files only contain information necessary for audit, legal and good practice purposes.
- Delete, destroy or remove any unnecessary or out-of-date personal data and, where paper-based, destroy it via shredding or dispose of it as confidential waste.

Organisers of NWR's Special Groups, Events Organisers, Area Organisers, Local Organisers and Treasurers all possess personal data about other members of NWR and NWR officials. They are required to:

- Keep the data in a designated and secure place and not leave it laying around when they are not working on it.
- Keep NWR data separate from their own personal data.
- Protect NWR data on their computers with a password.
- Have an up-to-date virus package and a firewall on their computers.
- Ensure all NWR data is treated as confidential.
- Make sure that data is not visible to others and that it does not fall into the wrong hands if they are working with it in a public place or whilst travelling. Make sure sensitive conversations are not overheard.
- Give an enquirer the name and phone number only of a member and then only with that member's permission. In preference, pass the enquirer's name to the member and ask the member to make the call.
- Advise a member if she is to expect a call from a stranger.

- Remove details of members' addresses and phone numbers from group programmes handed out to enquirers.

REQUESTS FOR COPIES OF PERSONAL DATA

Members wishing to apply for copies of the data held must make their request in email or in writing to our Head Office. This information will be made available within 40 working days.