The Wainwright Society

P1 Data Protection Policy

Date agreed by the Management Committee: August 2021 (Minute 86.7.5)

Minimum Review Frequency: 3 years

Next Review Date: December 2023

The Wainwright Society acknowledges that it holds personal data on trust and that harm may arise if that data is misused.

THEREFORE:

We will employ good practice in all matters concerned with the use of personal data.
We will take reasonable precautions to ensure that personal data is kept secure and is used only for properly authorised purposes.
We will ensure that the rights of data subjects are respected.
We will at all times actively seek to comply with the requirements of the General Data Protection Regulation GPDR.

The Wainwright Society holds personal data in order to perform its functions for the benefit of its members and such charitable and other causes as it may support. The Application Form for membership of the Society makes clear to all applicants the uses that will and will not be made of their personal data. The Society does not hold any sensitive personal data.

The General Data Protection Regulation 2018 sets out seven data protection principles. These are set out below, together with the Society's approach to them.

Data Protection Principle	Implications for The Wainwright Society
A: LAWFULNESS, FAIRNESS AND TRANSPARENCY Personal data shall be processed lawfully, fairly and in a transparent manner in relation to individuals.	To conform with GDPR, we obtain explicit consent for email communication, whilst other data processing has been assessed as necessary for the Society's legitimate interests.
B: PURPOSE LIMITATION 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.	We only use the data for purposes connected to their membership, and never share it with other persons or organisations, except as necessary, e.g. Reeds Printers for sending out "Footsteps" and CMS for sending calendars. We have obtained a guarantee from CMS and from Reeds on their use of personal data they obtain from us. Data about one member will be given to other member(s) only with permission.
C: DATA MINIMISATION Personal data shall be adequate,	The personal data kept by the Society is adequate and relevant for the purpose.

relevant and limited to what is necessary in relation to the purposes for which they are processed.	The only information held has been given by members, directly or through financial transactions.
D: ACCURACY Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.	We keep data on current members up to date (as and when they inform us of any changes). We do not keep data on lapsed members up to date; this is held for historic record purposes only.
E: STORAGE LIMITATION 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 are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.	The Society has a clear "if you don't need it, don't keep it" message to all who handle personal data on its behalf. Keeping data on lapsed members is justifiable for statistical purposes, and in case they re-join.
F: INTEGRITY AND CONFIDENTIALITY (SECURITY) 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 ('integrity and confidentiality').	Within the Society, personal data about Society members can only be accessed by Committee members who need it: such as for administering membership (Secretary, Membership Secretary), for research regarding potential development of the Society (Development Officer), or for specific activities or projects (eg Completers and merchandise) by the Committee member responsible for that service/project. Guarantees have been obtained from external organisations to whom the Society provides personal data, covering use and retention of the data, (The Society understands that obtaining these guarantees does not mitigate any risk and that risk cannot be transferred to another party. Liability remains with The Society). When sending emails to Members, the "blind copy" option is used to avoid

	divulging email addresses. The Membership database, and financial information relating to members, will be encrypted before transmission, and the passwords changed every 6 months.
G: ACCOUNTABILITY The accountability principle requires you to take responsibility for what you do with personal data and how you comply with the other principles. You must have appropriate measures and records in place to be able to demonstrate your compliance.	The Society is proactive about data protection and can evidence the steps it takes to meet its obligations and protect people's rights. The Society is responsible for, and can demonstrate, compliance with the other six GDPR principles. There are two key elements to accountability. First, the accountability principle makes it clear that we are responsible for complying with the GDPR. Second, we must be able to demonstrate our compliance. Ultimate responsibility for, and to be able to demonstrate compliance with, 'accountability' rests with the Committee.
RIGHTS. With the introduction of GDPR this is no longer a Principle but is covered by a separate provision in chapter 3 of Guide to the General Data Protection Regulation (GDPR), published by the Information Commissioner's Office. The GDPR provides the following rights for individuals: 1. The right to be informed 2. The right of access 3. The right to rectification 4. The right to erasure 5. The right to restrict processing 6. The right to data portability 7. The right to object 8. Rights in relation to automated decision making and profiling.	The Society respects and will honour the right of any Society member to be provided with a copy of the personal data held about them. The Society also recognises the other 7 GDPR rights for individuals and will acquiesce to any request made by any Society member in connection with these.

INTERNATIONAL TRANSFERS With the introduction of GDPR this is no longer a Principle but is covered by a separate provision in chapter 5 of Guide to the General Data Protection Regulation (GDPR), published by the Information Commissioner's Office. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.	We do not transfer personal data outside the UK, except as necessary for communicating with Society Members who live overseas.

The Society has carried out an assessment as to what data processing is carried out for the Society's own legitimate interests, balancing these against the interests of data subjects. Use of personal data to communicate with members by post or by phone is necessary in practice to maintain Society membership (which data subjects have chosen to have). Email communication will only take place where the member concerned has consented to this. The assessment has included consulting with some other similar organisations as to their intentions in this regard.

In the event of any complaint or expression of concern about the Society's collection or use of personal data, this will be investigated by a member of the Committee (to be selected by the Society Secretary) who was not involved in the matter which is the subject of concern. Any breach of this policy which is detected internally (including where a Committee member or volunteer realises that they have committed a breach) shall be reported to the Society Secretary and Membership Secretary, who shall consider and agree steps to prevent a repetition.

Responsibility for advice and monitoring of data protection issues within the Society shall rest with the Membership Secretary, who will conduct an audit of current practice at least every three years, with the results reported to the Committee. The last such audit was conducted in March 2021.