



The Wokingham Society
Registered as a Charity (No. 274988)

Data Protection Policy and Practice

Policy

The only reason The Society collects personal data (as defined in UK Data Protection Law) is to enable it to achieve its aims.

The Society's Executive Committee elects an individual to act as Data Protection Officer (DPO). The DPO is responsible for advising the Committee on changes in legislation which might affect this policy and for monitoring the Society's adherence to the policy. The DPO will be responsible to the Trustees (ie the Executive Committee without the President).

Practice

The only data the Society holds for members of the Society is as follows:

- Title, initials and surname
- Address
- Email address if made available
- Telephone number
- Membership due date
- Type of membership - honorary, concession, life, couple, corporate
- Usual payment and whether standing order
- Comments eg name on standing order

There is no data held that is not relevant.

The data is used to manage the membership and to enable the following information to be provided:

- Annual and Special General Meetings [as per our Constitution]
- Events organised by the Society
- Events organised by other organisations in or concerned with the town of Wokingham which in the opinion of the Officers will enable further understanding of the town
- Volunteering opportunities for helping The Society or the Executive Committee
- For those on email, copies of any of the above, together with occasional eNewsletters.

If someone ceases to be a member the only information held about them is that required by law (e.g. 7 year financial records).

If someone continues to donate to the Society (e.g. through a non-cancelled Standing Order) we will deem them to be a donor rather than a member.

We keep contact and bank reference details alongside details of donations for as long as required by law (e.g. 7 year financial records). It may be necessary to contact a donor about a received donation, but we do not otherwise contact non-member donors.

The data is maintained by the Membership Secretary and the governance of the data rests with the Data Protection Officer. These are the only members of the Executive Committee that have access to the data.

The data is held on systems in compliance with UK data protection laws.

For membership organisations like the Society, where members have provided the data and subscribe annually, their consent is assumed. However, the Society will send all existing and any new members a Statement on the Society's Data Protection and Practices.

The distribution of the Statement to all members in its initial form, and of any subsequently revised version, will be recorded in the Minutes of the subsequent Executive Committee Meet

Any members who wish to know the details of the information the Society holds for them, they should contact the DPO whose contact details will be on the Statement sent to them.

Members should contact the Membership Secretary if they wish their data to be amended or to stop email, telephone calls, or addressed post directed to them personally. As an alternative to this, members can enter details on the Fundraising Preference Services website, or by calling the helpline on 0300 3033517.

Any data breach should be reported to the DPO who will contact any individuals impacted where there exists a high risk to their rights and freedoms, e.g. identity theft.

Privacy Impact Assessment

A Privacy Impact Assessment is a process which assists organizations in identifying and managing the privacy risks arising from new projects, initiatives, systems, processes, strategies, policies, business relationships etc. Where judged necessary by the Society's DPO, any proposed new project or activity will be subject to a Privacy Impact Assessment.

Essentially it is to check against the six data protection principles of the General Data Protection Regulations (GDPR). The form in Appendix A should be used as a checklist.

Appendix A - Privacy Impact Assessment Form

1. Lawfulness, fairness and transparency

Transparency: Tell the subject what data processing will be done. What is processed must match up with how it has been described. Personal data can only be processed in line with this document.

Check []

2. Purpose limitations

Personal data can only be obtained for “specified, explicit and legitimate purposes”. Data can only be used for a specific processing purpose that the subject has been made aware of and no other, without further consent.

Check []

3. Data minimisation

Data collected on a subject should be “adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed”. In other words, no more than the minimum amount of data should be kept for specific processing. Information that is not relevant for the purpose must not be collected simply because it might be useful.

Check []

4. Accuracy

Data must be “accurate and where necessary kept up to date”.

Take care when inputting information to ensure accuracy. Avoid creating duplicate records as these can get out of alignment when being updated.

Check []

5. Storage limitations

Regulator expects personal data is “kept in a form which permits identification of data subjects for no longer than necessary”, In summary, data no longer required should be removed.

Personal data cannot be kept in case it might be useful one day.

Check []

6. Integrity and confidentiality

Requires processors to handle data “in a manner [ensuring] appropriate security of the personal data including protection against unlawful processing or accidental loss, destruction or damage”.

Check []

Completed By The Society's Data Protection Officer	Date