

Winchester & District PROBUS Club - Data Protection Policy

The policy sets out the requirements that the Club has for gathering personal data about its members. The policy details how data will be gathered, stored and managed in line with the General Data Protection Regulation (GDPR). The policy is reviewed regularly to ensure that the Club is compliant. This policy should be read in tandem with the Club's Privacy Policy.

This data protection policy is to ensure that the Club

- Complies with data protection law and follows good practice.
- Protects the rights of members and their partners.
- Is open about how it stores and processes members' personal data.
- Protects itself and its members against the risks of a data breach.

General guidelines for the Club's Committee members:-

- Access to data covered by this policy will be limited to those who need to contact our members or provide a service to them.
- The Club will provide training to Committee members and future Committee members to help them understand their responsibilities when handling personal data.
- The Club will keep all personal data secure, by taking sensible precautions and following the guidelines below.
- Strong passwords will be used on personal data and they will be never be shared.
- Members' personal data will not be disclosed outside of the Club unless with prior consent and/or for specific and agreed reasons.
- The Club will request help from Information Commissioners Office if we are unsure about any aspect of data protection.

The General Data Protection Regulation identifies eight data protection principles.

Principle 1 - Personal data shall be processed lawfully, fairly and in a transparent manner

Principle 2 - Personal data can only be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

Principle 3 - The collection of personal data must be adequate, relevant and limited to what is necessary.

Principle 4 – Personal data held should be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data is correct and any inaccurate data is erased or rectified without delay.

Principle 5 – Personal data which is kept in a form which permits identification of individuals shall not be kept for longer than is necessary.

Principle 6 - Personal data must be processed in accordance with the individuals' rights.

Principle 7 - Personal data must be processed in a manner that ensures appropriate security of the personal data against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Principle 8 - Personal data cannot be transferred to a country unless that country ensures an adequate level of protection for the rights of individuals in relation to the processing of personal data.

The Club requires data from members so that it can contact them about their involvement with the Club. The form used to request data contains a privacy statement as to why information is being requested and what it will be used for. Members will be asked to provide consent for their data to be held and a record of this consent and their data will be securely held. Members can, at any time, remove their consent by contacting the Membership Secretary. If a member requests not to receive certain contact this will be acted upon promptly and reported to him.

Members will be told how the Club uses their personal data. Appropriate use of member data will include:

- Contacting members about the Club's events and activities
- Contacting members about specific issues that may have arisen during the course of their membership.

The Club will endeavour to ensure inappropriate contact is not made to our members such as marketing and/or promotional materials from external service providers.

The Club will ensure that use of members' data does not infringe their rights which include:

- The right to be informed.
- The right of access.
- The right to rectification.
- The right to erasure.
- The right to restrict processing.
- The right to data portability.
- The right to object.

Members will only be asked to provide data that is relevant for membership purposes.

Any further data will be obtained with the specific consent of the member who will be informed as to why this data is required. Where a member's data needs to be shared with a third party due to an accident or incident involving statutory authorities then consent does not have to be sought from the member.

The Club has a responsibility to ensure members' data is kept up to date. Members will be asked to let the Membership Secretary know if any of their data changes.

The Club will ensure that it is compliant with data protection requirements and can prove it. Members will be asked to provide consent which will be securely held as evidence of compliance. The Club will review data protection and what data is held and who has access to it on a regular basis.

The Club is contracted for services from the following third party data processors:

- a company that provides website services
- a printer to print membership lists

The Club has scrutinised the companies' Terms and Conditions and believes they are GDPR compliant.

Members can request access to the data the Club holds on them by contacting the Membership Secretary. A record will be kept of the date of the request and the date of the response.

Where a data breach has occurred action will be taken to minimise the harm. The Club will then seek to rectify the cause of the breach as soon as possible and will contact the Information Commissioners Office within 72 hours of the breach being reported to the Club.

The Club will contact the relevant members to inform them of the data breach and actions taken to resolve it.

If a member contacts the Club feeling that there has been a breach, he will be asked to produce written evidence detailing his concern. The Club will then investigate the breach. The member will also be informed that he can report his concerns to the Information Commissioners Office. Breach matters will be subject to a full investigation, records will be kept and all those involved notified of the outcome.

Policy review date: April 2019

issue 1.1 April 2018