How does the South Devon Mountaineering Club (SDMC) comply with Data Protection Legislation?

The data the South Devon Mountaineering Club (SDMC) hold is:

- Name;
- Address;
- Email address;
- Telephone number;
- Date of birth;
- Next of Kin (NOK) details.

It is held in a secure data store within a secure account online. Only the Chair, Secretary and Webmaster have access to this data and access credentials are updated when the holders of these posts change.

This information is provided by SDMC members when they fill out the on-line membership form. Members notify the Secretary of any changes and all information is replaced annually when members renew their membership.

The data is kept for that membership year and one previous year only.

We also send the data to the BMC via their secure online membership database, as required by the BMC.

Member contact details are shared with all club members.

In the event of an incident only the Secretary or Chair may provide just the NOK details to the Emergency Services.

When members join or renew they provide explicit consent for this use of their data.

In addition, the SDMC have an up to date data protection policy that is adhered to by all officers of the club.

DATA PROTECTION POLICY For South Devon Mountaineering Club

Our data protection policy sets out our commitment to protecting personal data and how we implement that commitment with regards to the collection and use of personal data.

We are committed to:

- Ensuring that we comply with the eight data protection principles, as listed below
- Meeting our legal obligations as laid down by the Data Protection Act 1998
- Ensuring that data is collected and used fairly and lawfully
- Processing personal data only in order to meet our operational needs or fulfil legal requirements
- Taking steps to ensure that personal data is up to date and accurate
- Establishing appropriate retention periods for personal data
- Ensuring that data subjects' rights can be appropriately exercised
- Providing adequate security measures to protect personal data
- Ensuring that a nominated club officer is responsible for data protection compliance and provides a point of contact for all data protection issues
- Ensuring that all club officers are made aware of good practice in data protection
- Providing adequate training for all staff responsible for personal data
- Ensuring that everyone handling personal data knows where to find further guidance
- Ensuring that queries about data protection, internal and external to the club, are dealt with effectively and promptly
- Regularly reviewing data protection procedures and guidelines within the club

Data protection principles

1. Personal data shall be processed fairly and lawfully
2. Personal data shall be obtained for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed
4. Personal data shall be accurate and, where necessary, kept up to date
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes
6. Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act 1998
7. Appropriate technical and organisational measures shall be taken against unauthorised and unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data
8. 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

Adopted on 27 November 2017

FULL EXPLANATION OF THE EIGHT DATA PROTECTION PRINCIPLES

First Principle [Processed fairly and lawfully]
Personal Data shall be processed fairly and lawfully and in particular, shall not be processed unless

- At least one of the conditions of Schedule 2 is met, and
- In the case of sensitive Personal Data, at least one of the conditions of schedule 3 is also met.

Schedule 2

- The Data Subject has given consent
- The processing is required to meet a legal obligation
- It is required for the performance of a contract
- It is necessary to protect the vital interests of the individual; carry out public functions
- It is necessary to pursue the legitimate interests of the Data Controller or third parties.

Schedule 3

- Explicit consent of the Data Subject
- To comply with the employers legal duty
- To protect the vital interests of the Data Subject or another person
- Carried out by certain not for profit bodies
- In legal proceedings
- To exercise legal rights
- To carry out public functions
- For medical purposes
- For equal opportunities monitoring
- As specified by order.

Second Principle [Processed for specified, lawful and compatible purposes]
Personal Data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with purpose or those purposes.

Third Principle [Adequate, relevant and not excessive]
Personal Data shall be adequate, relevant and not excessive in relationship to the purpose for which they are processed.

Fourth Principle [Accurate and up to date]
Personal Data shall be accurate and, where necessary, kept up to date.

Fifth Principle [Not kept longer than necessary]
Personal Data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

Sixth Principle [Processed in accordance with the rights of the individual] Personal Data shall be processed in accordance with the rights of Data Subjects under the DPA.

Data Subject Rights:

- To subject access
- To prevent processing
- To prevent processing for direct marketing
- In relation to automated decision-making
- To rectification, blocking, reassure and destruction
- To ask the Information Commissioner to assess whether the DPA has been contravened
- To compensation

The three most important and relevant ones to clubs:

To subject access

An individual who makes a written request and pays a fee is entitled to be:

- Told whether any Personal Data is being processed;
- Given a description of the Personal Data, the reasons it is being processed, and whether it will be given to any other organisations or people;
- Given a copy of the information comprising the data; and
- Given details of the source of the data (where this is available).

To prevent processing

- An individual has a right to object to processing only if it causes unwarranted and substantial damage or distress. If it does, they have the right to require an organisation to stop (or not to begin) the processing in question.
- So, in certain limited circumstances, you must comply with such a requirement. In other circumstances, you must only explain to the individual why you do not have to do so.

To prevent processing for direct marketing

• An absolute right - individuals have the right to prevent their Personal Data being processed for direct marketing. An individual can, at any time, give you written notice to stop (or not begin) using their Personal Data for direct marketing. Any individual can exercise this right, and if you receive a notice you must comply within a reasonable period.

Seventh Principle [Processed with appropriate security]
Appropriate technical and organisation measures shall be taken against unauthorised or unlawful processing of Personal Data and against accidental loss or destruction of, or damage to, Personal Data.

Eighth Principle [Not transferred abroad without an adequate level of protection] Personal Data shall not be transferred to a country or territory outside the EEA 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.