**Data Protection policy for LMC**

**Club statement**

To operate effectively and fulfil its legal obligations, the LMC (Lomond Mountaineering Club) needs to collect, maintain and use certain personal information about current, past and prospective employees, its members and other individuals with whom it has dealings. All such personal information, whether held on computer, paper or other media, will be obtained, handled, processed, transported and stored lawfully and correctly, in accordance with the safeguards contained in the Data Protection Act 1998 (DPA).

**Membership statement**

The LMC (Lomond Mountaineering Club) will use your personal data for the purposes of your

involvement in club activities. I understand that by submitting this form I am

consenting to receiving information about the club by post, email/MMS, online or

phone. Your data will not be shared with any third party and the principles of the

Data Protection Act 1988 will be adhered to.

Data will be shared with the MCofS to meet membership requirements. The MCofS will use personal data only for your involvement in mountaineering activities. I understand that by submitting this form, I am consenting to receiving information from the LMC about mountaineering, including my MCofS membership details, by post, email, or phone unless stated otherwise.

**DATA PROTECTION POLICY**

**For LMC (Lomond 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 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 – data will be deleted after one year if the member does not renew their membership

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 – All data will be help on a password protected USB stick and maintained by the membership secretary

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 18th April 2018

**FULL EXPLANATION OF THE EIGHT DATA PROTECTION PRINCIPLES**

**First Principle** [Processed fairly and lawfully]

* Personal Data shall be processed fairly and lawfully and, 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 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.

* For member details to be made available to other club members (in any format) the specific consent from each member will be needed
* Clubs must allow members to opt-in to what details are circulated and must allow members the option of not having any details circulated. It must not be a condition of membership of the club that details have to be shared.
* Clubs will need to re-ascertain consent on a regular basis, ideally at least once a year · Clubs need to be mindful that even though consent may have been given at one point it can be withdrawn at any future point, including the day after a club has posted out a club list to every member. If an individual withdraws their consent the club needs a clear way to action the withdrawal of that data. This could potentially result in a recall of all the club lists that have been posted out or the club may not be allowing the individual their lawful right of withdrawing consent. Because of this risk, clubs may decide that if they wish to use a club list then a secure area on the club website is easier to manage.
* Clubs need to ensure that data is accurate. If a member changes their contact details after the list has been produced clubs need to consider how the club will ensure that the club lists are updated, and that inaccurate data is not available to other members.
* Clubs should consider what data needs to be circulated for communications between members, i.e. is a full postal address really needed in the 21st century, or is a phone number and/or email address more appropriate? · Clubs need to tell the recipients (members) what they can/can’t do with the data in the lists, i.e. they can’t pass or sell the data on to anyone else, and members can only use the data for club related communication.
* Clubs need to ensure that data is not held for longer than is needed. A system would be needed by the club to ensure that club lists are deleted by members once superseded / not needed.

DATA PROTECTION AGREEMENT

The Lomond Mountaineering Club will use your personal data for the purposes of your involvement in club activities.

|  |  |
| --- | --- |
| First Name |  |
| Surname |  |
| Main contact number |  |
| Address 1 |  |
| Address 2 |  |
| Address 3 |  |
| Post Code |  |
| In case of emergency name |  |
| In case of emergency Main contact number |  |

I understand that by submitting this form I am consenting to receiving information about the club by post, email/MMS, online or phone. Your data will not be shared with any third party and the principles of the Data Protection Act 1988 will be adhered to. Data will be shared with the LMC to meet membership requirements. The LMC will use personal data only for the purpose of your involvement in mountaineering activities.

I understand that by submitting this form, I am consenting to receiving information from the LMC about mountaineering, including my LMC membership details, by post, email, or phone unless stated otherwise.

Signature

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_