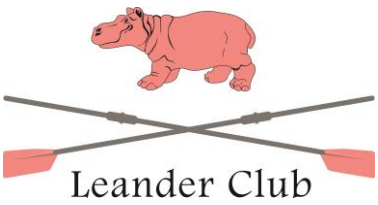

Leander Club Data Protection Policy

Leander Club takes its responsibilities with regard to the management of the requirements of data protection laws, including the General Data Protection Regulation ("GDPR") very seriously. This document provides the policy framework through which effective management of Data Protection matters can be achieved.

1. Scope of the Policy

The purpose of this policy is to ensure that Leander Club through its staff and volunteers ("Staff") comply with the provisions of all relevant data protection legislation, including GDPR, when processing personal data. Any infringement of this policy may be considered a disciplinary matter at the Club's discretion. This policy applies regardless of where Leander Club data is held, including if it is held on personally-owned equipment or outside Leander Club property.

There are eight statutory principles of data protection. Those principles are that personal data shall be:

1. Processed fairly and lawfully
2. Processed for specified purposes only
3. Adequate, relevant and not excessive
4. Accurate and up to date
5. Not kept longer than necessary
6. Processed in accordance with data subjects' rights
7. Processed and held securely
8. Not transferred outside the countries of the European Economic Area without adequate protection.

GDPR places further regulation on these principles regarding consent and protection to which Leander Club must adhere.

2. Responsibilities

a. Leander Club responsibilities

As a data controller and data processor, Leander Club is responsible for establishing policies and procedures in order to comply with statutory data protection requirements.

b. Committee Responsibilities

The Committee holds responsibility for:

- drawing up guidance, giving advice and promoting compliance with this policy in such a way as to ensure the easy, appropriate and timely retrieval of information;
- the appropriate compliance with subject access rights and ensuring that data is released in accordance with subject access legislation;

- ensuring that any data protection breaches are resolved, catalogued and reported appropriately in a swift manner and in line with guidance from the Information Commissioner's Office;
- investigating and responding to complaints regarding data protection including requests to cease processing personal data, removal of personal data, and lack of consent.

c. Staff responsibilities

Staff who process personal data about staff, members, volunteers and/or athletes must ensure that:

- all personal data are kept securely;
- no personal data are disclosed either orally or in writing, accidentally or otherwise, to any unauthorised third party;
- personal data are kept in accordance with Leander Club's retention schedule;
- any queries regarding data protection, including subject access requests and complaints, are promptly directed to the Chairman and the General Manager;
- any data protection breaches are swiftly brought to the attention of both the Chairman and the General Manager and that they provide support in resolving breaches;
- where there is uncertainty around a data protection matter advice is sought from appropriate sources, which may be other members of the Committee, legal counsel or other reasonable outside agents.

When Staff are responsible for supervising athletes or any activity which deals with the processing of personal data of athletes, they must ensure that those athletes are aware of the Data Protection Principles, in particular, the requirement to obtain the data subject's informed, positive, consent where appropriate. Staff must obtain those consents, which should be kept securely on file in the Club Office, prior to any activity which requires the processing of that personal data. Junior athletes, or any athlete who cannot legally provide consent for any reason should have the written, informed, positive consent of at least one parent or legal guardian.

If Staff are unsure about who are the authorised third parties to whom they can legitimately disclose personal data they should seek advice from the Chairman or General Manager.

d. Third-Party Data Processors

Where external companies are used to process personal data on behalf of Leander Club, responsibility for the security and appropriate use of that data remains with Leander Club. Where a third-party data processor is used:

- a data processor must be chosen which provides sufficient guarantees about its security measures to protect the processing of personal data;
- reasonable steps must be taken that such security measures are in place;
- a written contract establishing what personal data will be processed and for what purpose must be set out;
- a data processing agreement, which would usually be part of the initial contract, must be signed by both parties.

For further guidance about the use of third-party data processors please contact the Chairman and/or the General Manager.

e. Athletes' responsibilities

Athletes are responsible for:

- familiarising themselves with the Data Protection Agreement provided when they enrol in the Leander Club Academy training programme;
- ensuring that their personal data provided to Leander Club are accurate and up to date.

3. Subject Access Requests

If asked to do so via a subject access request, Leander Club is required to permit individuals to access their own personal data held by Leander Club. Any individual wishing to exercise this right should apply in writing to the Chairman. A reasonable charge may be made for this request.

Leander Club aims to comply with requests for access to personal information as quickly as possible, but will ensure that any requested data held is provided within the 40 calendar day limit set out in the Data Protection Act 1998.

Individuals will not be entitled to access information to which any of the exemptions in the Act applies. However, only those specific pieces of information to which the exemption applies will be withheld and determining the application of exemptions will be made by the Chairman and/or General Manager, taking advice if required.

Leander Club charges £10 to make a subject access request, plus £0.10 per page for any page required to be printed by person making the request. These charges may increase as reasonably required and permitted.

4. Data Protection breaches

Where a Data Protection breach occurs, or is suspected, it should reported immediately to both the Chairman and the General Manager. They will then decide the appropriate course of action.

End