LEIGH & LOWTON SAILING CLUB
Green Lane,
Lowton,
Warrington.
WA3 1BQ

Leigh & Lowton Sailing Club Data Privacy Policy

About this Policy

This policy explains when and why we collect personal information about our members and employees, how we use it and how we keep it secure and your rights in relation to it.

Anyone attending an Open Meeting at the Club is automatically enrolled as a Club Member for the duration of the Event.

Attendees at events arranged by Third Parties which take place on Club premises, such as Open Water Swimming Events or Art Club meetings, are subject to the Data Privacy Policy of the organising organisation.

We may collect, use and store your personal data, as described in this Data Processing Policy and as described when we collect data from you.

We reserve the right to amend this Data Processing Policy from time to time without prior notice. You are advised to check our website (www.llsc.org.uk) or our Club noticeboard regularly for any amendments. Amendments will not be made retrospectively.

We will always comply with the General Data Protection Regulation (GDPR) when dealing with your personal data. Further details on the GDPR can be found at the website for the Information Commissioner (www.ico.gov.uk). For the purposes of the GDPR, we will be the "controller" of all personal data we hold about you.

Who we are.

We are Leigh & Lowton Sailing Club. Our telephone number is 01942 673169, although it's normally best to contact us by email membership@llsc.org.uk or if your query is specific to Data Protection dpo@llsc.org.uk

What information we collect and why.

Type of information	Purposes	Legal basis of processing
Member's name, address, telephone numbers, email address(es).	Managing the Member's membership of the Club. Managing the duty roster. Managing incident reports	Performing the Club's contract with the Member. For the purposes of our legitimate interests in operating the Club. Managing incident reports with respect to legal reporting and insurance claims.
The names and ages of the Member's dependants	Managing the Member's and their dependants' membership of the Club Managing incident reports	Performing the Club's contract with the Member. Managing incident reports with respect to legal reporting and insurance claims

Emergency contact details	Contacting next of kin in the event of emergency	Protecting the Member's vital interests and those of their dependants
Bank account details of the member or other person making payment to the Club	Managing the Member's and their dependants' membership of the Club, the provision of services and events.	Performing the Club's contract with the Member.
Date of birth / age related information	Managing membership categories which are age related Managing incident reports	Performing the Club's contract with the Member. Managing incident reports with respect to legal reporting and insurance claims

Type of information	**Purposes**	**Legal basis of processing**
Gender	Provision of adequate facilities for members.	For the purposes of our legitimate interests in making sure that we can provide sufficient and suitable facilities (including changing rooms and toilets) for each gender.
	Reporting information to the RYA.	For the purposes of the legitimate interests of the RYA to maintain diversity data required by Sports Councils. Managing incident reports with respect to legal reporting and insurance claims.
	Managing incident reports.	
The Member's name, boat class and sail number	Managing race entries and race results. Sharing race results with other clubs, class associations, and the RYA, and providing race results to local and national media. Allocating berths within the boat yard. Managing incident reports	For the purposes of our legitimate interests in holding races for the benefit of members of the Club. For the purposes of our legitimate interests in promoting the Club. For the purposes of our legitimate interests in operating the Club Managing incident reports with respect to legal reporting and insurance claims

Type of information	Purposes	Legal basis of processing
Photos and videos of members and their boats.	Putting on the Club's website and social media pages and using in press releases.	Consent. We will seek the Member's consent on their membership application form and each membership renewal form. The Member may withdraw their consent at any time by contacting us by e-mail or letter.
The Member's name and e-mail address	Creating and managing the Club's Yearbook. This is used as a contact list for coordinating members' obligations to act as Race Officer and/or Safety Boat crews etc.	Performing the Club's contract with the Member. For the purposes of our legitimate interests in operating the Club.
Member's name and e- mail address	Passing to the RYA for the RYA to conduct surveys of members of the Club (and members of other clubs affiliated to the RYA). The surveys are for the benefit of the Clubs (and other clubs) and / or the benefit of the RYA.	For the purposes of our legitimate interests in operating the Club and / or the legitimate interests of the RYA in its capacity as the national body for all forms of boating
Employees' name, address, email addresses, phone numbers, NI numbers and relevant qualifications and/or experience.	Managing employment at the club.	For the purposes of our legitimate interests in managing employment, ensuring that we can contact employees and to meet our legal obligations as employers with HMRC.
CCTV images	Managing security in non-public areas of the club's premises by detecting crime.	For the purposes of our legitimate interests in managing security in non-public areas of the club's premises by detecting crime.
Instructor's name, address, email addresses, phone numbers and relevant qualifications and/or experience.	Managing instruction at the club.	For the purposes of our legitimate interests in ensuring that we can contact those offering instruction and provide details of instructors to members.

How we protect your personal data

We will not transfer your personal data to jurisdictions not compliant with the GDPR, following current Information Commissioner's Office guidance.

We have implemented generally accepted standards of technology and operational security in order to protect personal data from loss, misuse, or unauthorised alteration or destruction. We will notify you promptly in the event of any breach of your personal data which might expose you to serious risk.

For any payments which we take from you online we will use a recognised online secure payment system. Please note however that where you are transmitting information to us over the internet this can never be guaranteed to be 100% secure.

We will notify you promptly in the event of any breach of your personal data which might expose you to serious risk.

Who else has access to the information you provide us?

We will never sell your personal data. We will not share your personal data with any third parties without your prior consent (which you are free to withhold) except where required to do so by law or as set out in the table above or paragraph 5.2 below.

We may pass your personal data to third parties who are service providers, agents and subcontractors to us for the purposes of completing tasks and providing services to you on our behalf (e.g. to print newsletters and send you mailings). However, we disclose only the personal data that is necessary for the third party to deliver the service and we have a contract in place that requires them to keep your information secure and not to use it for their own purposes.

How long do we keep your information?

We will hold your personal data on our systems for as long as you are a member of the Club and for as long afterwards as is necessary to comply with our legal obligations. We will review your personal data every year to establish whether we are still entitled to process it.

If we decide that we are not entitled to do so, we will stop processing your personal data except that we will retain your personal data in an archived form in order to be able to comply with future legal obligations e.g. compliance with tax requirements and exemptions, the tracing of ownership of property left on club premises by former members and the establishment exercise or defence of legal claims.

By default, all data will be deleted within three years of a person ceasing to be a member with the exception of historic race results and associated reports already in the public domain.

We securely destroy all financial information once we have used it and no longer need it.

Unless used as part of a legitimate investigation, CCTV images recorded in non-public areas for detecting crime are regularly and automatically deleted and over-written in accordance with the ICO CCTV Code of Practice.

Your rights

You have rights under the GDPR:

- to access your personal data
- to be provided with information about how your personal data is processed
- to have your personal data corrected
- to have your personal data erased in certain circumstances
- to object to or restrict how your personal data is processed
- to have your personal data transferred to yourself or to another business in certain circumstances.

You have the right to take any complaints about how we process your personal data to the Information Commissioner:
https://ico.org.uk/concerns/
0303 123 1113.
Information Commissioner's Office Wycliffe House
Water Lane
Wilmslow
Cheshire SK9 5AF
For more details, please address any questions, comments and requests regarding our data processing practices to our Commodore or Data Protection Officer via email dpo@llsc.org.uk

17.5.18

Appendix A – Subject Access Requests

SUBJECT ACCESS REQUEST FORM

You should complete this form if you want us to supply you with a copy of any personal data we hold about you. You are entitled to receive this information under the EU General Data Protection Regulation (GDPR), which comes into effect on 25 May 2018. We will also provide you with information about any processing of your personal data that is being carried out, the retention periods which apply to your personal data, and any rights to rectification, erasure, or restriction of processing that may exist.

We will endeavour to respond promptly and in any event within one month of the latest of the following:

- Our receipt of your written request; or
- Our receipt of any further information we may ask you to provide to enable us to comply with your request.

The information you supply in this form will only be used for the purposes of identifying the personal data you are requesting and responding to your request. You are not obliged to complete this form to make a request, but doing so will make it easier for us to process your request quickly.

SECTION 1: Details of the person requesting information

Full name:	
Address:	
Contact telephone number:	
Email address:	

A17965695

SECTION 2: Are you the data subject?

Please tick the appropriate box and read the instructions which follow it.

☐ **YES**: I am the data subject. I enclose proof of my identity (see below). **(please go to section 4)**

☐ **NO**: I am acting on behalf of the data subject. I have enclosed the data subject's written authority and proof of the data subject's identity and my own identity (see below).

(please go to section 3)

To ensure we are releasing data to the right person we require you to provide us with proof of your identity and of your address. Please supply us with a photocopy or scanned image (do not send the originals) of one of both of the following:

1) Proof of Identity

Passport, photo driving licence, national identity card, birth certificate.

2) Proof of Address

Utility bill, bank statement, credit card statement (no more than 3 months old); current driving licence; current TV licence; local authority tax bill, HMRC tax document (no more than 1 year old).

If we are not satisfied you are who you claim to be, we reserve the right to refuse to grant your request.

SECTION 3

Details of the data subject (if different from section 1)

Full name:	
Address:	
Contact telephone number:	
Email address:	

SECTION 4: What information are you seeking?

Please describe the information you are seeking. Please provide any relevant details you think will help us to identify the information you require.

Please note that if the information you request reveals details directly or indirectly about another person we will have to seek the consent of that person before we can let you see that information. In certain circumstances, where disclosure would adversely affect the rights and freedoms of others, we may not be able to disclose the information to you, in which case you will be informed promptly and given full reasons for that decision.

While in most cases we will be happy to provide you with copies of the information you request, we nevertheless reserve the right, in accordance with section 8(2) of the DPA, not to provide you with copies of information requested if to do so would take "disproportionate effort", or in accordance with Article 12 of the GDPR to charge a fee or refuse the request if it is considered to be "manifestly unfounded or excessive"**.** However we will make every effort to provide you with a satisfactory form of access or summary of information if suitable.

SECTION 5: Information about the collection and processing of data If you want information about any of the following, please tick the boxes:

- Why we are processing your personal data ☐
- To whom your personal data are disclosed ☐
- The source of your personal data ☐

Note – this information is provided at a high level in the Data Protection Policy above.

SECTION 6: Disclosure of CCTV images
If the information you seek is in the form of video images captured by our CCTV security cameras, would you be satisfied with viewing these images?

YES ☐ NO ☐

SECTION 7: Declaration
Please note that any attempt to mislead may result in prosecution.

I confirm that I have read and understood the terms of this subject access form and certify that the information given in this application to Leigh & Lowton Sailing Club is true. I understand that it is necessary for Leigh & Lowton Sailing Club to confirm my / the data subject's identity and it may be necessary to obtain more detailed information in order to locate the correct personal data.

Signed…… **Date** ……..

Documents which must accompany this application:

- **Evidence of your identity (see section 2)**
- **Evidence of the data subject's identity (if different from above)**
- **Authorisation from the data subject to act on their behalf (if applicable)**

Please return the completed form to:

Data Protection Officer
Leigh & Lowton Sailing Club
Green Lane, Lowton
Nr Warrington, WA3 2BQ
Email: dpo@llsc.org.uk

Correcting Information

If after you have received the information you have requested you believe that:

- the information is inaccurate or out of date; or
- we should no longer be holding that information; or
- we are using your information for a purpose of which you were unaware;
- we may have passed inaccurate information about you to someone else;

then you should notify our Commodore or Data Protection Officer at once. dpo@llsc.org.uk

17 May 2018

Appendix B – Data Breach Reporting Process

Data Breach Reporting Process

Introduction

The GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority. You must do this within 72 hours of becoming aware of the breach, where feasible.

If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, you must also inform those individuals without undue delay.

Organisations should ensure they have robust breach detection, investigation and internal reporting procedures in place. This will facilitate decision-making about whether or not you need to notify the relevant supervisory authority and the affected individuals.

Organisations must also keep a record of any personal data breaches, regardless of whether we are required to notify.

This document describes the steps to be taken by Leigh & Lowton Sailing Club (LLSC) should such a breach be discovered or reported.

Guidance from the Information Commissioner's Office (ICO)

What is a personal data breach?

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

Example

Personal data breaches can include:

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission; and
- loss of availability of personal data.

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

Recital 87 of the GDPR makes clear that when a security incident takes place, you should quickly establish whether a personal data breach has occurred and, if so, promptly take steps to address it, including telling the ICO if required.

What breaches do we need to notify the ICO about?

When a personal data breach has occurred, you need to establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it's likely that there will be a risk then you must notify the ICO; if it's unlikely then you don't have to report it. However, if you decide you don't need to report the breach, you need to be able to justify this decision, so you should document it.

In assessing risk to rights and freedoms, it's important to focus on the potential negative consequences for individuals. Recital 85 of the GDPR explains that:

"A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their

personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned."

This means that a breach can have a range of adverse effects on individuals, which include emotional distress, and physical and material damage. Some personal data breaches will not lead to risks beyond possible inconvenience to those who need the data to do their job. Other breaches can significantly affect individuals whose personal data has been compromised. You need to assess this case by case, looking at all relevant factors.

Example

The theft of a customer database, the data of which may be used to commit identity fraud, would need to be notified, given the impact this is likely to have on those individuals who could suffer financial loss or other consequences. On the other hand, you would not normally need to notify the ICO, for example, about the loss or inappropriate alteration of a staff telephone list.

So, on becoming aware of a breach, you should try to contain it and assess the potential adverse consequences for individuals, based on how serious or substantial these are, and how likely they are to happen.

How much time do we have to report a breach?

You must report a notifiable breach to the ICO without undue delay, but not later than 72 hours after becoming aware of it. If you take longer than this, you must give reasons for the delay.

Section II of the Article 29 Working Party Guidelines on personal data breach notification gives more details of when a controller can be considered to have "become aware" of a breach.

What information must a breach notification to the supervisory authority contain?

When reporting a breach, the GDPR says you must provide:

- a description of the nature of the personal data breach including, where possible:
- the categories and approximate number of individuals concerned; and
- the categories and approximate number of personal data records concerned;
- the name and contact details of the data protection officer (if your organisation has one) or other contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

What if we don't have all the required information available yet?

The GDPR recognises that it will not always be possible to investigate a breach fully within 72 hours to understand exactly what has happened and what needs to be done to mitigate it. So Article 34(4) allows you to provide the required information in phases, as long as this is done without undue further delay.

However, we expect controllers to prioritise the investigation, give it adequate resources, and expedite it urgently. You must still notify us of the breach when you become aware of it, and submit further information as soon as possible. If you know you won't be able to provide full details within 72 hours, it is a good idea to explain the delay to us and tell us when you expect to submit more information.

Example

You detect an intrusion into your network and become aware that files containing personal data have been accessed, but you don't know how the attacker gained entry, to what extent that data was accessed, or whether the attacker also copied the data from your system.

You notify the ICO within 72 hours of becoming aware of the breach, explaining that you don't yet have all the relevant details, but that you expect to have the results of your investigation within a few days. Once your investigation uncovers details about the incident, you give the ICO more information about the breach without delay.

Process

Any Officer or Member of the Club should report it immediately to the Club's Data Protection Officer (DPO).

The DPO will notify the Commodore and/or President that such a breach has occurred.

Using the ICO Guidance outlined above, the DPO will assess the severity of the breach and advise the Commodore whether or not a report to the ICO is appropriate. If appropriate, such a breach shall be reported to the ICO within 72 hours of its discovery by or notification to LLSC by a third party.

Regardless of whether or not a report to the ICO is appropriate, the DPO shall record the same information as is contained in an ICO report, arrange for any mitigations to be put in place without delay and arrange for the report to be discussed by the Executive Committee either at the next scheduled meeting or at an Emergency Meeting convened by the Commodore and/or President.

The DPO's Data Breach report shall contain, as a minimum, the following information:

- a description of the nature of the personal data breach including, where possible:
- the categories* and approximate number of individuals concerned; and
- the categories* and approximate number of personal data records concerned;
- the name and contact details of the data protection officer (if your organisation has one) or other contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

* as currently defined by the ICO on their website www.ico.org.uk