Aquarius Sailing Club (AQSC) – GDPR policy (General Data Protection Regulations)

Definitions:

Terms used are drawn from and defined within the following regulations:

The GDPR - Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (GDPR)
(https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN)

The Data Protection Act 2018 (DPA18)
http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

RYA advice on General Data Protection Regulations updated 5 October 2017
(http://www.rya.org.uk/SiteCollectionDocuments/legal/Web%20Documents/Legal%20Leaflets/Clubs/Laws%20and%20Regulations/GENERAL%20DATA%20PROTECTION%20REGULATIONS.pdf)

Controller – the person who, or body which, determines the basis and means of processing personal data, in this instance the AQSC management committee

Data subject – the person referred to in personal data held by AQSC

Processor – a provider of data services such as Google, Yahoo, Facebook, Dropbox, and Dutyman

Supervisory authority – within the UK, the Information Commissioner

Objectives:

AQSC processes personal data and other data on a number of bases set out in DPA18 Section 86 and Schedule 9. These include that it is necessary (b) for the performance of a **contract** to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract, (d) in order to **protect** the vital interests of the data subject or of another natural person, (c) for compliance with a **legal obligation** to which the controller is subject, and (f) for the purposes of the **legitimate interests** pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. Where the above bases do not apply, processing may arise on the basis that (a) the data subject has given **consent** to the processing of his or her personal data for one or more specific purposes.

Services to members for which the data in question is used include:

Recording the membership of AQSC and visits by potential members and others
Communication with members
Enabling communication between members
Protecting members assets
Controlling financial transactions with members
Maintaining accounting records
Negotiating insurance cover and contracts with other service providers
Identifying and addressing health and safety issues
Calculating statistical returns to bodies such as RYA

Calculating, recording and reporting on race series and annual results
Performing administrative functions such as electing officials and reporting to members on finances and membership
Providing a management function through the management committee
Advertising the social and sporting activities offered by AQSC in order to maintain viable membership levels
Maintaining a history of AQSC, its members and its sailing and social activities

Processing of data by AQSC involves no automated decision making such as profiling.

See the accompanying table of data fields held, AQSC GDPR data fields.ods, for data fields, basis for holding, and category of personal or non-personal data (personal, personal financial, special personal, non-personal). Note that special personal data, such as ethnicity, religious beliefs or medical conditions, is currently not held. Requests for modification of this GDPR policy for a particular member, such as the withholding of certain data fields or the recording of special categories of personal data, should be sent to the Hon. Secretary for consideration by the management committee.

Distribution of personal data and other data to members of the management committee

Acting as data protection officer, the Vice Commodore (Administration) maintains the club's prime data record in a Dropbox based structure with folders assigned to the following functions:

Administration – secretarial and finance
Commodore and President
Health and Safety
Premises
Programmes
Publicity
Race Officer
Share draft documents
Webmaster

Primary responsibility for each function is assigned to a small number of members of the management committee, who have read/write access. Other members of the management committee have read only access. All management committee members have read/write access to the folder named 'Share draft documents', which is used should the drafting of a specific document warrant read/write access for all management committee members prior to it being moved to the relevant specific functional folder. The prime record of members' personal data described in the accompanying table of data fields is held in the administration folder. Manual financial records are maintained by the treasurer and an electronic accounting record is maintained by the auditor on a separate Dropbox structure. The sailing secretary maintains race results on a personal database. Equivalent data relating to race results is maintained by the auditor in an Excel application in the Race Officer folder and reconciled weekly to that of the sailing secretary.

Distribution within the club house of personal and other data to members other than the management committee

The names of applicants for membership are displayed on the notice board in the club house pending approval.

Photos, names, functions and telephone numbers of the management committee are displayed on

the notice board in the club house.

Minutes of the meetings of the management committee are available to members in hard copy in the clubhouse.

A berth list showing the names of boat owners is displayed on the notice board in the club house.

Race results, containing participants' names, personal handicaps, and times and rankings, are disclosed in hard copy on the notice board in the club house.

A handwritten visitors book is maintained to meet licensing requirements and for health and safety considerations.

Distribution of personal and other data to the general membership other than via the club website

Emails to the general membership of the club are sent using bcc. The messages may contain the name, telephone number , and email address of the member, generally a management committee member, who is organising an event publicised in the email, and the banking details of the auditor when payment for the event by bank transfer is offered.

Personal and other data disclosed on the club website (http://www.sailaquarius.org.uk/)

The names, photos, roles and functional email addresses of management committee members are disclosed on the club's website. The home telephone numbers of the club secretary and sailing secretary are also shown on the website.

The website contains a link to the Dutyman service, which is used to administer the allocation of duties to members. This displays event, date, name of the member assigned the duty, and the nature of the duty. The Dutyman service stores personal email addresses. Members are able to log in to Dutyman and send requests for duty exchanges to other members. However, the messaging involved in exchanges does not disclose the email address of a member other than to the owner of that email address. The administration of the Dutyman service is performed by a member of the management committee.

Race results, containing participants' names, personal handicaps, and times and rankings, are disclosed on the website.

The website shows the sailing and social programs and contains reports on sailing and social events. These may contain photos and the names of members participating in those events.

The website contains an archive which contains equivalent data from previous years.

Personal and other data disclosed on the club Facebook website
(https://www.facebook.com/aquariussailingclub)

The club Facebook website contains posts on forthcoming events, reports on past events, and photos.

Both the club website and the Facebook website are subject to exemptions from DPA18 which are permitted by Article 85 (2) of DPA18 and defined in more detail in Schedule 2, Parts 5 and 6. The two websites also benefit from the application of Article 11 of the GDPR and the definition of 'personal data' in DPA18 Article 3.

Data protection and safeguards when personal data is transferred to a third country

Data to which members of the management committee have access is stored on computers subject to password access control. The data is synchronised by and backed up on the Dropbox service. The servers used are located in the USA. Dropbox meets the ISO 27018 standard for protecting personally identifiable information in the cloud and will be compliant with GDPR when it takes effect on 25th May 2018. The USA is also included in the list of countries judged by the EU Commission to offer an adequate level of protection. See - https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en#dataprotectionincountriesoutsidetheeu

Note: The issue of the location of processing requires more work by industry service providers, as the breadth of the definition of 'processing' in Article 4 (2) of the GPDR, the distributed architecture of the internet, and the poor coverage of the EU Commission's judgements on the quality of protection in specific countries, make it advisable to rely on certification, such as the ISO 27018 mentioned above, and the oversight of the processor's home country regulator (see Article 46, 2. (f) of the GDPR). AQSC should record service provider, home country regulator, international standards met, statement of GDPR readiness, link to terms and conditions for the service used.

Data accuracy

The register of current members, boats owned by current members, berths and lockers constitutes the prime data record used by the membership secretary. Its accuracy is maintained by a physical inspection of the site by the auditor in preparation for the annual subscription process, together with the reporting back to the member of personal data subject to change, such as address, telephone numbers and email addresses.

Data retention

Personal data on prior members is segregated from data on current members in a separate archive. . Manual records of financial transactions are maintained at least for the period set by the Limitation Act 1980. Differing retention standards may be offered by service providers such as Dropbox, Dutyman and the website host. Retention of data in the club's historical archives is controlled by the management committee, who receive an annual inventory of archived data which they compare with the bases of processing and uses of the data.

Procedures for data processed on the basis of consent.

Should AQSC find that it needs to process personal data on the basis of consent, the following requirements apply:

Consent must be given freely, be specific, be informed and be unambiguous. Re 'specific', the individual must be informed of the use for which consent is being obtained.

There must be a positive opt-in – you cannot infer consent either from inactivity, silence or pre-ticked boxes.

Consent must be separated out from any other terms and conditions.

Individuals must be given the right to withdraw their consent at any time and this must be as easy to do as it was to give consent in the first place.

You must keep evidence of consent.

Rights of the individual data subject

These are defined in Chapter 3 of DPA18 and include to have access to the following information:

the identity of the controller
the basis and purpose of processing
the details of the legitimate interest, if this basis is applied
the recipients of the personal data
the safeguards applied when data it transferred to a third country
the period of storage or criteria applied for such decisions
the right to request from the controller access to the data processed, rectification, erasure and the restriction of processing
the right to withdraw consent when that is the basis of processing
the right to be informed prior to personal data being used for a purpose not previously reported
the right to complain to the supervisory authority
details of any automated decision making within the processing, such as profiling.

As permitted by DPA18 Article 93 (2) this is achieved by making this policy generally available on the AQSC website.

Outstanding matters

Confirming the identity of the data controller – done, the AQSC management committee, as a ‘body’ can perform this function.

Address the question of the Data Protection Officer – done, VC admin

Initial inventory of data types held on the website, period held, to be added as a separate document to support the annual decision to retain data - done.

Initial inventory of processors used, protection standards – further work required

Presentation to the management committee, decision on adequacy of this policy and minuting, decision on data retained in archives on the website -

Build a report of personal data held within the membership records – done, see tab “Personal data report”

Advise members of the new policy, send data

Review the application form and procedure – done, needs updating to point to website

Add statement – no sensitive data held - done

Add statement – no automated decision making, such as profiling – done

Add statement that requests for modification of the GDPR policy for a particular member, such as the withholding of certain data fields or the recording of special categories of personal data, should be sent to the Hon. Secretary for consideration by the management committee. - done

Add GDPR folder to Dropbox with policy, data fields, review of archived data, regulations etc – done

Switch from .odt to .doc and from .ods to .xls

Add GDPR subfolders by year to store details of reviews etc.

Move from provision of GDPR information to advice in application forms that rights to information may be exercised by viewing website or by request to the membership secretary.