WSC – GDPR Compliance Procedures V1.0

1.0 Procedures in event of a member/staff seeking to see personal data held (i.e. Subject Access Request)

1.1 Preliminary Action

On the receipt of a request from a Club member or Club staff to see their personal data held by WSC, the Administrator, as the WSC Data Controller, is to:

1. Note that the whole process is to take no more than one month, assign following tasks accordingly.
2. Confirm that the requestee is a bone-fide current or previous Club member or Club employee.
3. Ask the requesting person to complete a Part 1 of a Subject Access Request Form (SARF) (attached), highlighting which forms said member has previously completed and the dates concerned.
4. On receipt of the completed Subject Access Request Form, check with the DPO, that the request is reasonable and not excessive. If the request is **manifestly unfounded or excessive** then agree with the Hon Treasurer a reasonable fee for the cost of the administrative effort to carry out the requested work.
5. Agree with the requestee that the search is to proceed at stated cost.

1.2 Data research

The Administrator is to:

1. having first checked receipt of any fees due, complete a Data Holding Report Request.
2. Forward Data Holding Report Request (part 2 of SARF) to accounts staff, Club officers and volunteer co-ordinators who process (including holding) the relevant Club forms and hold other soft copy personal data of the requestee, stating timescale for return.
3. Personally, list all data on requesting data subject held on ESP, or otherwise on forms held in the WSC Admin Office.
4. Assemble a data request file containing all the requested information from own (i.e. Admin Office) research and the completed Data Holding Reports from accounts, offices and co-ordinators provided on SAR Part 2).
5. Make copy of completed personal data file for Club records.
6. Forward one copy of the completed Personal Data File to the requestee, under cover of a letter signed by Hon Sec.

2.0 Procedures in the Event of Member /Staff seeking to change personal data records

On receipt of a request to update/correct personal data, the Administrator is to:

1. Note that the request for correction must be provided in writing.
2. Confirm that the requestee is a bone-fide current or previous Club member or Club employee and that the requested change is reasonable.
3. Identify the holder (Admin, accounts, official or co-ordinator) who holds the hard/soft copy of the personal data to be changed.
4. Request the data holder to make the change and report when completed.
5. Report back to requestee that the change has been made, keeping a copy of the original request and the change conformation for the record.

3.0 Procedures in Event of a Data Breach

3.1 General

A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means that a breach is more than just losing personal data.

We have to notify the relevant supervisory authority (i.e. the ICO) within 72 hours of a breach where it is likely to result in a risk to the rights and freedoms of individuals or if unaddressed is likely to have a significant detrimental effect on individuals – for example, result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage. It is permissible to provide information in phases.

The need to report is to be assessed on a case by case basis. For example, we will need to notify the relevant supervisory authority about a loss of member details where the breach leaves individuals open to identity theft. On the other hand, the loss or inappropriate alteration of the Who's Who, for example, would not meet this threshold. In WSC, the DPO will decide if the ICO is to be informed in consultation with the WSC Data Controller (i.e. Administrator) and the WSC Data processor (i.e. Chairman of the IT Committee).

Where a breach is likely to result in a high risk to the rights and freedoms of individuals, we must directly notify those members or staff concerned. A 'high risk' means the threshold for notifying individuals is higher than for notifying the relevant supervisory authority.

If the breach is sufficiently serious to warrant notification to the public, The DPO will discuss this with the Commodore, who makes press announcements on the behalf of WSC.

3.2 Actions

Every data breach will be dealt with depending on its circumstances. However, the WSC DPO will:

1. Ask the WSC Data Processor to take action to remedy any on-line leak;
2. Ask the WSC Data Processor to report the detail of all soft copy personal Data illegally accessed/lost and provide a list of effected data subject. Note that the WSC Data Privacy Policy requires that all soft copy personal data held on portable devices (e.g. laptops, tablets, mobile phones, back up discs) is to be encrypted;
3. Ask the WSC Data Controller to report the detail of all hard copy personal data illegally accessed/lost and provide a list of effected data subjects. The WSC Data Controller will ask the holders of such information (e.g. club officials) to report the necessary details;
4. Assemble the necessary reports for the ICO, the initial report being sent within 72 hours.
5. Assemble to necessary reports for effected data Subjects, if they are placed at high risk of e.g. identity theft;
6. Prepare press statements for the Commodore, if a press release is appropriate.

Note: if the Club has taken out Cyber Insurance, then this will include assistance from the insurer in the event of a data breech, provided all data held on portable devices is encrypted. In this case the above functions will be carried out by the insurer's provided expert assistance.

Reports to the ICO must contain as a minimum:

1. the nature of the personal data breach including, where possible, the categories and approximate number of both the individuals and personal data records concerned;
2. the name and contact details of the data protection officer (i.e. Hon Sec) as contact point where more information can be obtained;
3. a description of the likely consequences of the personal data breach;
4. a description of the measures, either proposed or taken, to deal with the personal data breach; and, where appropriate, of the measures taken to mitigate any possible adverse effects.

4.0 Procedures for Data Controller processing records

The WSC Data Controller (i.e. Administrator) is required to maintain internal records of processing activities related to personal data carried out within WSC to demonstrate accountability. Records are to include:

1. Name and details of WSC officials or third parties carrying out the processing of personal data (e.g. officials dealing with hard copy forms, creating lists and spreadsheets on their laptops and Data Processors (e.g. accounts personnel, Data Processors (i.e. IT committee members) running queries and reports on ESP.
2. Purposes of the processing.
3. Description of the categories of individuals and categories of personal data.
4. Recipients of the processing undertaken, including third parties.
5. Details of transfers of data to third countries including documentation of the transfer mechanism safeguards in place.
6. Details of the retention of such processed data.
7. Description of technical and organisational security measures implemented to secure the processed data.

WSC may be required to make these records available to the relevant supervisory authority for purposes of an investigation.

5.0 Procedures for Data Processor processing records

The WSC data processor (i.e. Chairman of the IT committee) is to maintain the necessary records of all personal data related processing activities undertaken by or for WSC to demonstrate WSC accountability for data processing.

1. The name and contact details of the processor or processors and, where applicable, of the processor's representative and data protection officer;
2. A description of processing carried out;
3. A record of all personal data provided to 3rd parties (e.g. data processors, RYA, commercial companies and sponsors) including legal basis and/or permissions;
4. where applicable, a record of personal data to a third country or an international organisation, including the identification of that third country or international organisation and the documentation of suitable safeguards;
5. where possible, a general description of the technical and organisational security measures implemented.

Published by Hon Sec WSC

Version 1.0, dated 5 Feb 2018

Appendix A, WSC Subject Access Request

DATE:

PART 1

Data Subject' Name				
Address				
Telephone				
email				
Summary of Personal Data Requested				
Indicate Organisers spreadsheets etc to be searched	Bar Duty Roster	Yes / No	Dates From:	TO:
	Duty man Racing	Yes / No	Dates From:	TO:
	Dutyman Security	Yes / No	Dates From:	TO:
	Dinghy registration	Yes / No	Dates From:	TO:
	Dinghy racing results	Yes / No	Dates From:	TO:
	Cruising racing Results	Yes / No	Dates From:	TO:
	Mooring Holder Lists	Yes / No	Dates From:	TO:
	Spring Series Registration	Yes / No	Dates From:	TO:
	Spring Series Results	Yes / No	Dates From:	TO:
	Youth Sailing Registrations	Yes / No	Dates From:	TO:
Indicate Hard Copy Lists to be searched	Who's Who	Yes / No	Dates From:	TO:
		Yes / No	Dates From:	TO:
		Yes / No	Dates From:	TO:
		Yes / No	Dates From:	TO:
		Yes / No	Dates From:	TO:
		Yes / No	Dates From:	TO:
		Yes / No	Dates From:	TO:
Indicate Forms previously submitted to WSC to be searched	Membership	Yes / No	Dates From:	TO:
	Dinghy Reg	Yes / No	Dates From:	TO:
	Pursuit Reg	Yes / No	Dates From:	TO:
	Training Reg	Yes / No	Dates From:	TO:
	Youth Sailing Registration	Yes / No	Dates From:	TO:
	Spring Series Registration	Yes / No	Dates From:	TO:
	Bar Volunteer	Yes / No	Dates From:	TO:
	Mooring Application	Yes / No	Dates From:	TO:
	SH Pound Application	Yes / No	Dates From:	TO:

	Lob Pound Application	Yes / No	Dates From:	TO:
	Skills Form	Yes / No	Dates From:	TO:
	Event Booking	Yes / No	Dates From:	TO:
	Temporary Membership	Yes / No	Dates From:	TO:
	Direct Debit	Yes / No	Dates From:	TO:
	Staff Details	Yes / No	Dates From:	TO:
Indicate Data Bases to be searched	ESP Membership Data BAse	Yes / No	Dates From:	TO:
		Yes / No	Dates From:	TO:
		Yes / No	Dates From:	TO:
		Yes / No	Dates From:	TO:
By Data Controller	Confirmed Member: Yes…./ No		Reasonable Request: Yes / No	
	If request "not reasonable" then obtain a search fee from Hon Treasurer:		£	
Data Subject Confirmation Signature				

PART 2

Actions by WSC	1. Copies of this form are to be provided to each Club officer/official/co-ordinator who is responsible for reporting personal Data held. 2. Reports are to be returned to the WSC Administrator by **DATE**:		
WSC Official lists here all personal data held on the data subject			
Official's name:		Official's Signature:	
Date Provided to Admin		Date received by Admin	
By Admin: extracted into overall report		Date	