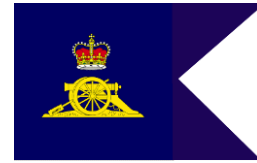




**Col N A Wilson**  
**Commodore**  
Royal Artillery Yacht Club  
Telephone:  
Mobile: 07795122009  
Email: [commodore@rayc.org.uk](mailto:commodore@rayc.org.uk)  
Website: [www.rayc.org.uk](http://www.rayc.org.uk)



---

## RAYC DATA PRIVACY POLICY

1. **Introduction.** Data Protection law in the UK will undergo some significant changes with the introduction of the General Data Protection Regulations (GDPR). The GDPR will replace the current Data Protection Act from 25<sup>th</sup> May 2018. (The Government has confirmed that "Brexit" will not affect GDPR from coming into effect).

### 2. **About this Policy**

- a. This policy explains when and why we collect personal information about our members, how we use it and how we keep it secure and your rights in relation to it.
- b. We may collect, use and store your personal data (see [Annex A](#) for definitions), as described in this Data Privacy Policy and as described when we collect data from you.
- c. We reserve the right to amend this Data Privacy Policy from time to time without prior notice. You are advised to check our website [[www.rayc.org.uk](http://www.rayc.org.uk)] regularly for any amendments (but amendments will not be made retrospectively).
- d. We will always comply with the 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](http://www.ico.gov.uk)). For the purposes of the GDPR, we will be the "controller" of all personal data we hold about you.

3. **Who are we?** We are the Royal Artillery Yacht Club (RAYC) Company Limited by Guarantee (CLG). We can be contacted via the:

RAYC Honorary Secretary  
5 Far Meadow Way, Emsworth, Hampshire, PO10 7PA  
Email: [sgray62@live.co.uk](mailto:sgray62@live.co.uk)  
Tel: 01243373211

4. **What information we collect and why.** A review of personal data (What we hold; whether we need it; where it came from and the basis on which it was collected; what we do and are planning to do with it; where and how we store it and how long we store it (Details are at [Annex B](#))) will be conducted and documented. Further guidance is at [Annex C](#).

Type of information	Purposes	Legal basis of processing
Member's name, address, telephone numbers, e-mail address(es) and relevant qualifications and/or experience.	<p>Managing the Member's membership of the Club.</p> <p>Creating and managing the Club's online Membership Directory.</p>	<p>Performing the Club's contract with the Member.</p> <p>For the purposes of our legitimate interests in operating the Club.</p> <p>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 to tell us that they no longer wish their details to appear in the Membership Directory.</p>
Emergency contact details	Contacting next of kin in the event of emergency	Protecting the Member's vital interests and those of their dependents
Date of birth / age related information (TBC)	Managing membership categories which are age related	Performing the Club's contract with the Member.
The Member's name, boat name and sail number	<p>Managing race entries and race results.</p> <p>Managing the RAYC Blue Ensign ownership</p> <p>Sharing race results with other clubs, class associations, and the RYA, and providing race results to local and national media.</p> <p>Allocating moorings spaces.</p>	<p>For the purposes of our legitimate interests in holding races for the benefit of members of the Club.</p> <p>For the purposes of our legitimate interests in promoting the Club.</p> <p>For the purposes of our legitimate interests in operating the Club</p>
Photos/ Images and videos of Members and their boats	Putting on the Club's website and social media pages and using in press releases. Further guidance is at <a href="#">Annex D</a> .	Consent. We will seek the Member's consent on their membership application form and each membership renewal form and the Member may withdraw their consent at any time by contacting us by e-mail or letter.
Radio call signs	Collected for an Offshore Regatta and shared between those participating in the regatta.	For the purposes of our legitimate interests in ensuring that boats on a regatta can maintain contact with each other
Bank account details of the member or other person making payment to the Club	Managing the Member's and their dependents' membership of the Club, the provision of services and events.	Performing the Club's contract with the Member.

## 5. How we protect your personal data

- a. We will not transfer your personal data outside the EU without your consent.

b. 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.

c. Please note however that where you are transmitting information to us over the internet this can never be guaranteed to be 100% secure.

d. For any payments, which we take from you online we will use a recognised online secure payment system (e.g. PayPal).

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

## 6. **Who else has access to the information you provide us?**

a. 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 below.

b. 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 the RAYC Yearbook 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?

c. 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 it is in the Clubs' legitimate interest to do so or for as long 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, and the establishment exercise or defence of legal claims.

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

## 7. **Your rights**

a. You have rights under the GDPR:

- (1) to access your personal data
- (2) to be provided with information about how your personal data is processed
- (3) to have your personal data corrected
- (4) to have your personal data erased in certain circumstances
- (5) to object to or restrict how your personal data is processed
- (6) to have your personal data transferred to yourself or to another business in certain circumstances.

b. You have the right to take any complaints about how we process your personal data to the Information Commissioner:

<b>Address</b>	<b>Tel</b>	<b>Email</b>
Information Commissioner's Office Wycliffe House, Water Lane Wilmslow, Cheshire SK9 5AF	03031231113	<a href="https://ico.org.uk/concerns/">https://ico.org.uk/concerns/</a>

For more details, please address any questions, comments and requests regarding our data processing practices to our Data Protection Manager, The Honorary Membership Secretary, [mailto: [membership@rayc.org.uk](mailto:membership@rayc.org.uk)].

N A Wilson  
Col  
Commodore RAYC

Annexes:

- A. [GDPR Definitions.](#)
- B. [General Data Time Periods.](#)
- C. [GDPR Guidelines.](#)
- D. [Guidance on Use of Images.](#)

## DEFINITIONS

The GDPR relates to **personal data** and **special categories of personal data**.

### Personal data

Any information relating to an identified or identifiable natural person (referred to as the **Data Subject**). A person is identifiable if they “*can be identified, directly or indirectly, by reference to an identifier such as name, an identification number, location data, an online identifier or to one or more factors, specifically the physical, physiological, genetic, mental, economic, cultural or social identity of that actual person*”.

Examples are:

- Name
- Address
- Phone Numbers(s)
- Email

### Special categories of personal data (Sensitive personal data)

Personal data “*revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation*”. The special categories of personal data do not include personal data relating to criminal convictions and offences but there are similar extra safeguards in relation to those types of data.

- Health Data – JSATFA – DDH Certificate
- Financial Information - PayPal
- Passport Details – JSATFA – App 1

### Processing

“*Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, determination or otherwise making available, alignment or combination, restriction, erasure or destruction*”.

### Data Controller

“*The natural or legal person, public authority, agency or other body which, alone or jointly, with others determines the purposes and means of the processing of personal data*”.

**GENERAL DATA TIME PERIODS**

<b>Issue</b>	<b>Period<sup>1</sup></b>	<b>Trigger/ from</b>
<b>Claims in contract</b>	6 years (Limitation)	Date of breach
<b>Tort<sup>2</sup></b> (Excluding Personal Injury)	6 years (Limitation)	The date the damage is suffered
<b>Personal injury</b>	3 years (Limitation)	The date the damage occurred or the <b>date of knowledge of the injured person</b>
<b>Negligence</b>	(in respect of latent damage): three years or six years, subject to a maximum period 15 years from the negligent act or omission. (Limitation)	Negligence (in respect of latent damage): the later of six years from three years from the date on which the claimant had the requisite such an action.
<b>Defamation</b>	One year (Limitation)	From date of publication
<b>Company records – General books &amp; accounts</b>	3 years (Retention)	From date record made
<b>Board minutes</b>	10 years (Retention)	Date of meeting
<b>Tax</b> (for businesses)	Latest of the 5 <sup>th</sup> anniversary of the 31 January next following the year of assessment or 6 <sup>th</sup> anniversary of the end of the period where the return is for a period not in a tax year (Retention)	
<b>VAT</b>	All VAT records- Minimum 6 years (Retention)	The date on which records were made

---

<sup>1</sup> In some cases, statute provides the minimum or maximum time documents must be held, these are marked “Retention” in this guide. “Limitation” refers to the maximum period within which legal proceedings must be brought, and would therefore suggest a sensible period for which to keep documents, should an action be brought concerning them.

<sup>2</sup> a wrongful act or an infringement of a right (other than under contract) leading to legal liability.

<b>Payroll</b>	Records for purposes of tax returns <ul style="list-style-type: none"> <li>• 6 years minimum (Retention)</li> <li>• Payroll and wage records- Unincorporated associations – 5 years minimum retention Company- 6 years minimum</li> </ul>	<ul style="list-style-type: none"> <li>• Tax- from the end of the assessment period</li> <li>• (Association) After 31 Jan following the year of assessment</li> <li>• (Company) The financial year in which records were made.</li> </ul>
<b>Employment</b>	Contract- 6 years after employment ceases (Retention) Reports, references, reviews- 6 years after employment ceases. ID documents for foreign nationals- 2 years minimum Pension documents- 6 years minimum	<ul style="list-style-type: none"> <li>• End of employment</li> </ul>
<b>Community Amateur Sports Clubs</b>	6 years from the end of the accounting period in which they relate.	<ul style="list-style-type: none"> <li>• 6 years after the year the records relate to (Therefore 7 years is a possibility).</li> </ul>

**GDPR GUIDANCE**

<b>THE PRACTICALITIES</b>	<b>THE LAW</b>
<p><b>Membership Information</b></p> <ul style="list-style-type: none"> <li>● Only collect the information which you need and be clear on the application form (whether paper or online) what you will use the information for. (See “<b>Collecting and Keeping Data</b>”).</li> <li>● Store application forms securely. Consider: <ul style="list-style-type: none"> <li>○ who needs to see them;</li> <li>○ how long they need to be kept;</li> <li>○ the relevance of the application form once the applicant has been accepted or rejected.</li> </ul> </li> <li>● If your application form asks the applicant to provide bank details (e.g. for direct debit purposes) separate the financial information from the rest of the application.</li> <li>● Store financial information separately from the application form.</li> <li>● If the application is rejected, destroy the financial information – you no longer need it</li> <li>● If your application form is online and you take payment electronically use a recognised online secure payment system.</li> </ul> <p>Make sure that you keep all membership information up to date. If you renew memberships annually, ask members to check their information at renewal and provide an easy method for them to give you up to date information.</p>	<p><b>Types of data</b></p> <p>You are likely to collect all or some of the following data:</p> <ul style="list-style-type: none"> <li>● Name, address, e-mail address, phone numbers and other contact details of members.</li> <li>● Grade of membership.</li> <li>● Name and details of the boats owned by members.</li> <li>● Date of joining the Club.</li> <li>● Name, address, e-mail address, phone numbers and other contact details of suppliers, staff, volunteers, coaches and trainers.</li> <li>● Name, address, date of birth, e-mail address, phone numbers and other contact details of participants in events and regattas, plus details of the boats they own.</li> <li>● Race results (which includes names and possibly other details of members).</li> </ul> <p>Health information of members and others (which may be necessary for risk assessments).</p>
<p><b>Former members</b></p> <ul style="list-style-type: none"> <li>● Store separately the information you hold about former members from the information you hold about current members (whether on paper or electronically).</li> </ul> <p>Securely destroy all financial information you have about them.</p> <ul style="list-style-type: none"> <li>● Consider the purposes for which you need to retain information about former members and record the reasons and the time period. (See <b>Storing Data</b>).</li> <li>● Destroy all information about former members in line with your</li> </ul>	<p><b>Collecting and Keeping Data</b></p> <p>Data can only be processed lawfully, fairly and transparently.</p> <p>You can only process (and therefore collect) personal data in certain circumstances:</p> <ul style="list-style-type: none"> <li>● Consent of the Data Subject.</li> <li>● The legitimate interests of the data controller.</li> <li>● Necessary for the performance of the contract with the data subject.</li> </ul>

Retention Policy.

- Compliance with a legal obligation to which you are subject.
- Necessary to protect the vital interests of the data subject or of another natural person.
- Necessary for performance of a task carried out in the public interest.

We recommend that, as far as possible, you only collect data which is necessary for the performance of the membership contract with the member. You can rely on that basis where, for example, you use information on an application form in a way which is necessary for the purposes of the membership of the applicant. So you can use contact details to notify members of, for example, club events and mooring issues, without needing consent each time, but you are not able to include a member's details in a club directory without their consent. You should not assume that you can rely on your "legitimate interests" as data controller for all processing. Although that reason may be available to you it should not be regarded as a "catch all" and it is highly unlikely that it will be a valid basis for compiling a membership directory which is made available to members.

You must record the basis on which you collect and use data.

You must only collect the data you need for the purposes you have specified.

When you collect data you must provide the data subject with certain information:

- Your identity and contact details.

How you intend to use their data.

Your lawful basis for processing their data.

Details of anyone who may receive the data.

Your data retention policy.

The individual's right to complain to the ICO if they believe there is a problem with your handling of their data.

You must make sure the data remains accurate and therefore you must keep it up to date.

	<ul style="list-style-type: none"> <li>You must keep the data for no longer than is necessary for the purpose for which you obtained it. If you make sure that you dispose of data when you no longer need it you reduce the risk that it will become inaccurate, out of date or irrelevant and therefore reduce your security risk</li> </ul>
<p><b>Member Directories</b></p> <ul style="list-style-type: none"> <li>Consider the purposes of your Members' Directory. It must only contain the information necessary to fulfil those purposes (e.g. the usual purpose of a members' directory is to enable members to contact each other so name of member and telephone number and boat name is likely to be sufficient). It is unlikely that there is a need to include members' home addresses in the directory.</li> <li>You can only include a member's details in your Member Directory if they agree that you can do so.</li> <li>Your application form must contain a box for them to tick (or something similar) to show they have agreed. You cannot use a pre-ticked opt-in box nor an opt-out box.</li> </ul> <p>The form must therefore make clear the information to be included in the Members' Directory.</p> <ul style="list-style-type: none"> <li>They must be able to change their mind at any time and no longer be included in the Members' Directory.</li> <li>If your Members' Directory is online then updates should be made regularly.</li> <li>If your Members' Directory is in hard copy then you should update it and circulate it annually. In that case you should make clear, when you seek consent for a member's details to be included, that their details will be included for the whole year.</li> </ul> <p>You cannot make membership of the club or association conditional on a member agreeing to have their name in the Members' Directory.</p>	<p><b>Using data</b></p> <p>You may only use personal and sensitive personal data you have collected for the purposes you specified at the time you collected it.</p> <p>If you are relying on Consent as the basis for your use of the data, you need to be aware that the GDPR requirement for consent is more stringent than under the Data Protection Act:</p> <ul style="list-style-type: none"> <li>Consent must be given freely, be specific, be informed and be unambiguous.</li> <li>There must be a positive opt-in - you cannot infer consent either from inactivity, silence or pre-ticked boxes.</li> <li>Consent must be separated out from any other terms and conditions.</li> <li>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.</li> </ul> <p>The ICO has a 2-page checklist of things to consider and include when you are seeking consent. <a href="https://ico.org.uk/media/for-organisations/documents/1625126/privacy-notice-checklist.pdf">https://ico.org.uk/media/for-organisations/documents/1625126/privacy-notice-checklist.pdf</a></p> <p>Whilst you may have relied on obtaining the data subject's consent for information which you already hold you need to check that the consent you have complies with the GDPR requirements.</p> <p>You must keep evidence of the consent.</p>
<p><b>Entries for Regattas and Events</b></p> <ul style="list-style-type: none"> <li>Only collect the information which you need and be clear on the application form (whether paper or online) what you will use the information for.</li> <li>Store application forms securely. Consider:</li> </ul>	<p><b>Storing data</b></p> <p>You should have a data retention policy that takes into account the purposes for which the data is kept, for how long the data needs to be kept (and why) and how the data will be destroyed. You should not be tempted to keep all data indefinitely "just in case".</p>

<ul style="list-style-type: none"> <li>○ who needs to see them;</li> <li>○ how long they need to be kept;</li> <li>○ the relevance of the application form once the applicant has been accepted or rejected or the event completed.</li> </ul> <ul style="list-style-type: none"> <li>● If your application form asks the applicant to provide bank details for payment purposes, separate the financial information from the rest of the application.</li> <li>● Store financial information separately from the application form</li> <li>● If the application is rejected, destroy the financial information – you no longer need it</li> </ul> <p>If your application form is online and you take payment electronically use a recognised online secure payment system.</p> <ul style="list-style-type: none"> <li>● If a sponsor of the event or regatta wants the details of those taking part you can only provide that data to the sponsor if the individual entrants agree. The application form for the regatta or event needs to make clear that you wish to pass their data to the sponsor and must give them a box to tick if they agree. <ul style="list-style-type: none"> <li>○ Consent requires a positive opt-in under the GDPR (you cannot use pre-ticked opt-in boxes or opt out boxes).</li> <li>○ Entrants must be able to change their mind at any time and you must provide an easy way for them to do so.</li> <li>○ You cannot make entry to the event conditional on a participant agreeing to allow their name to be made available to the sponsor.</li> </ul> </li> </ul> <p>There is guidance from the ICO about consent <i>[to be inserted when final guidance published]</i>.</p>	<p>General correspondence between your organisation and a member may only need to be kept for a short period. Correspondence relating to a potential claim or disciplinary matter may need to be kept for a number of years.</p> <p>Personal and sensitive personal data must be kept securely. You should consider the risks and decide on your levels of security accordingly. You must take appropriate measures to prevent unauthorised or unlawful processing of the data and against accidental loss or destruction of, or damage to, the data.</p> <p>There is useful guidance on IT Security from the ICO: <a href="https://ico.org.uk/media/for-organisations/documents/1575/it_security_practical_guide.pdf">https://ico.org.uk/media/for-organisations/documents/1575/it_security_practical_guide.pdf</a></p> <p>Personal data cannot be transferred to a country or territory outside the EEA unless that country or territory provides a suitable level of protection for data.</p>
<p><b>Giving Data to others</b></p> <ul style="list-style-type: none"> <li>● The basic rule is that you cannot pass any data you have about individuals to anyone else (e.g. sponsors of events, other clubs) without the agreement of the individual (See sections <b>Entries for Regattas and Events, and Expulsion of Members</b> for further information).</li> <li>● If you are being asked to provide data about a member to anyone other than that member, you should seek legal advice.</li> </ul> <p>If another organisation (e.g. an insurance company) wants you to send out information about their services to your members, you are not able to do that unless you have the agreement of each person to whom you are going to send the information.</p>	<p><b>Access to data you hold/Subject Access Request</b></p> <ul style="list-style-type: none"> <li>● An individual can ask to see the data you hold about them. This is known as making a Subject Access Request.</li> <li>● The GDPR allows one month from the receipt of the request to respond.</li> <li>● The GDPR does not allow you to charge a fee for responding to a Subject Access Request unless it is manifestly unfounded, excessive or repetitive.</li> <li>● The ICO has useful guidance on subject access requests. <a href="https://ico.org.uk/for-organisations/guide-to-data-protection/principle-6-rights/subject-access-request/">https://ico.org.uk/for-organisations/guide-to-data-protection/principle-6-rights/subject-access-request/</a></li> </ul> <p>We have produced a separate Guidance Note on <a href="#">Subject Access Requests</a>.</p>

<p><b>Expelling / Disciplining Members</b></p> <p>If you decide to discipline a member:</p> <ul style="list-style-type: none"> <li>• Opinions about a member are personal data and so the member could require to see that data through a subject access request.</li> <li>• The member is entitled to make a subject access request and ask for the data you hold about their discipline / expulsion and any other personal data you hold about them.</li> <li>• Data about the member's expulsion are data relating to that member so other members do not have the right to see that data.</li> <li>• If others object to a member's discipline you cannot disclose the data to them – they must obtain it from the member (if the member is willing to provide it to them).</li> <li>• There are issues of confidentiality as well as data protection.</li> </ul> <p>See Section Access to Data you hold / subject Access Request</p>	<p><b>Individuals' Rights</b></p> <p>Under the GDPR individuals have various rights, such as:</p> <ul style="list-style-type: none"> <li>• The right to be informed.</li> <li>• The right of access.</li> <li>• The right to rectification.</li> <li>• The right to erasure.</li> <li>• The right to restrict processing.</li> <li>• The right to data portability.</li> <li>• The right to object.</li> </ul> <p>The right not to be subject to automated decision-making including profiling.</p>
<p><b>Looking after Data / Security</b></p> <ul style="list-style-type: none"> <li>• You have a responsibility to look after data which you hold.</li> <li>• You must take particular care of financial information as there is a serious risk to the owners of that information if it falls into the wrong hands.</li> <li>• Your security obligations must be taken equally seriously whether you hold data in hard copy or electronically.</li> <li>• See the section Storing Data for a link to advice from the Information Commissioner.</li> </ul> <p>Data in hard copy form should be kept in a locked cabinet to which access is restricted. It is preferable for appropriate steps to be taken to provide secure storage at your club premises if that is practical and is likely to be safe. If that is not practical or if you don't have club premises and you have hard copy data then it must still be kept securely. Therefore if the data is kept at an officer's home it should still be in a locked cabinet to which access is restricted.</p> <ul style="list-style-type: none"> <li>• If you store data electronically be very careful if it is stored in "the Cloud".</li> <li>• Cloud computing means access to computing resources on demand i.e. access to hardware and/or software.</li> <li>• Cloud computing carries data protection risks which are not always obvious. Generally you, as the cloud customer, will be the data controller</li> </ul>	<p><b>Data Breaches</b></p> <p>You must have documented procedures to detect, report and investigate data breaches.</p> <p>A data breach is a breach of security which leads to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. A breach is therefore more than just losing personal data.</p> <p>If the breach is likely to result in a risk to the rights and freedoms of anyone, you have to notify the ICO. This has to be considered on a case by case basis. You need to consider the potential detrimental effect on the individual (for example discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage).</p> <p>If a breach is likely to result in high risk to the rights and freedoms of anyone then you have to notify the individuals concerned.</p>

and have overall responsibility for complying with data protection rules. Cloud computing is not a “one size fits all” and so the data protection issues which apply can vary. If you are using cloud computing you should ensure that you have a written agreement with the cloud services provider. You may need to seek legal advice on the agreement and the data protection provisions which it should contain.

- It is important you know in which country the cloud service provider stores your data. If it is outside the EU/EEA you have additional responsibilities.
- There is guidance from the ICO about cloud computing [https://ico.org.uk/media/1540/cloud\\_computing\\_guidance\\_for\\_or\\_ganisations.pdf](https://ico.org.uk/media/1540/cloud_computing_guidance_for_or_ganisations.pdf)
- Whether data is stored in hard copy or electronically you should consider who should be able to access which data e.g. the Treasurer may be the only officer who needs access to financial information. If so, the financial information should be stored in such a way that only the Treasurer can get access to it plus perhaps one other person in the event of an emergency if the Treasurer is ill or away.
- Data held electronically should be encrypted.
- If you have arrangements with suppliers who process personal data on your behalf (e.g. the printer of your members' directory) the GDPR requires you to have a written agreement with them containing certain provisions.

## **GUIDANCE ON THE USE OF IMAGES**

1. **Introduction.** Taking and using pictures of individuals raises two separate legal issues. As a rule of thumb, it is suggested that those taking or using pictures should firstly consider how they would expect or want their own image used and what they would expect to be told or asked. It may not be strictly necessary to obtain the consent of the subject to take or use images in certain circumstances but that doing so may be the most practical way to avoid disputes at a later date.
2. **Images as data - Is an image personal data?**
  - a. Guidance from the Information Commissioner suggests that in order for an image to amount to personal data, it must be possible to identify an individual from information within the image or text associated with the image e.g. names of prize winners. Being recognised by family or friends is not the same as being identified. As a result, crowd or distance shots are unlikely to amount to personal data. A portrait without anything to identify the individual may be argued not to amount to personal data but you should consider what the individual's reaction will be if they found themselves on a poster or similar or what your own reaction would be.
  - b. If it is possible to identify the individual, perhaps as a result of additional information contained in the image, the image will be considered personal data for the purposes of data protection legislation.
3. If an image is personal data, what do I need to do?
  - a. In common with all other personal data, it is necessary to have a legal basis or reason for processing that data. The basis are:
    - (1) Legitimate interests.
    - (2) Necessity for contract.
    - (3) Consent.
    - (4) Compliance with a legal obligation.
    - (5) Necessary to protect the vital interest of the subject.
    - (6) Necessary for a task carried out in the public interest.
  - b. It is likely that contract, legitimate interests or consent are likely to be the most relevant grounds for processing an image which amounts to personal data.
4. Each legal basis has its own specific considerations which will need to be taken into account when determining which is the most appropriate.
  - a. **Contract.** Personal data required to perform a contract can be collected and used for the purposes of the contract. As a result, personal data such as names and contact details can easily be brought within this ground. It may be possible to bring an image within this ground if it is required to perform a contract, however the image can only be used for the purposes of performing the contract.
  - b. **Legitimate interests.** Interests may be those of the organisation wanting to use the

image or a third party, however these interests must be balanced against the rights of the subject. This is assessed by carrying out a legitimate interest's assessment or LIA. It is important that records of such LIAs are retained, in order to demonstrate the reasoning for relying on this ground. Legitimate interest is a broad ground, and while it may be possible to justify using an image in a particular way, consideration should be given to the reaction of the data subject, who may not be expecting their image to be used or who may want payment for the use of their image.

c. **Consent.** Consent must be specific and informed. Opt out boxes are no longer permitted and it must be possible to withdraw consent as easily as it was given. As a result, consent is most appropriate when it is not possible to rely on any of the other legal basis for processing data. As consent must be specific, widely drafted consent clauses purporting to give consent for all possible use of personal data are unlikely to be effective and great care should be taken to ensure the consent provided does actually cover the intended use. Consideration should also be given to the practicalities of relying on consent, as managing an event where not everyone has provided consent, either intentionally or by not ticking the appropriate box, or where it may be not to be possible to match the relevant consent form to an individual in a photograph may be problematic.

d. It will be for the organisation to decide if an image amounts to personal data, and if so, which is the most appropriate ground for processing. Below are examples of common scenarios.

## 5. Examples

a. A picture of a crowd without any way to identify individuals: If they cannot be identified, then the picture is not personal data.

b. Pictures of prize or race winners: Subject to completing a LIA it may be decided that it is in the interests of the organiser or the club to take and use the image for publicity purposes. It is likely the subject would appreciate such a picture would be taken. It may be possible include a provision in the entry terms stating that a winner will participate in publicity, thereby opening the possibility of relying on the basis of necessity for the performance of a contract for use of personal images.

c. A staged picture of an individual e.g. at a try sailing event taken to use in marketing material: It may be more difficult to justify this as a legitimate interest, although it may be possible. It is likely that express consent would be most applicable and in this example should be included in the booking form.

d. A portrait taken for use on an event security pass: This would be necessary for the performance of a contract, as it would be necessary to gain access to the event.

e. Pictures or video of individuals sailing taken by a sailing coach who has been engaged by an individual, club or class association to coach sailors: This might fall within the performance of a contract if the coach has been engaged specifically to provide video coaching services, it may also be in the coach's legitimate interest for feedback to be provided in this way. However, it may not be in the data subject's interests for such an image to be used in a different context and therefore such images should only be used for coaching purposes unless specific consent is obtained to use the images for a different purpose.

## 6. **Other data considerations.**

a. Data subjects have a number of rights under data protection legislation. Some of these rights are linked to the basis under which data was collected, for instance the right to withdraw consent if given, however others are more general, such as the right to request that data be updated or deleted.

b. As a result, when an image is treated as personal data it is possible for the subject to exercise their rights as a data subject and a subject may request that their data be removed or deleted. If you receive a request to stop using an image, it may be preferable to stop using it than to seek a justification or enter a dispute with the subject. It may be simple to stop using an image online but more of a challenge for printed material and so your privacy notice and or consent wording should make it clear that it may not be possible for printed material to be taken out of circulation or altered until the next print run.

## 7. **Images as property**

a. There are some who view the use of their image as a way to make money, or may see such an opportunity once they see their image in use.

b. If you intend to publish an image, or suspect you might wish to publish the image in the future, it would be wise to ask the subject to confirm that they assign any rights in that image to the user and that there will be no charges (or alternatively agree and document the arrangement reached).

c. Practically, this means subjects should sign a waiver. This may be included in the terms and conditions of entering an event, or may take the form of a standalone document completed at the time the image was taken.

d. The desirability of signing a waiver from a commercial perspective may influence the legal basis for processing the image as data, as if necessary to obtain a written waiver, it may be relatively straightforward to obtain consent at the same time, assuming consent is the appropriate basis for processing the image.

## 8. **Children.** Additional issues must be considered when taking or using pictures of children:

a. If relying on consent as a ground for processing an image as personal data, consent should be obtained from the parent/guardian.

b. Consideration should be given to the appropriateness of the picture from a safeguarding perspective. More information can be found on the [Safeguarding](#) section of the website.

9. **Practically.** If an image is believed to be personal data, the use must be brought within one of the legal basis for processing. It will be for the organisation to determine which of the basis is applicable and it may be that consent is not necessary or appropriate in some circumstances.

10. From practical perspective, when faced with an individual complaining about the use of their image, the ability to point to an express consent to use that image will be invaluable, even if the individual later decides to withdraw such consent. Further, a written waiver of the rights in that

image will reduce the risk of disputes over the ownership or payment for use of that image.

11. For this reason the RAYC has included both consent wording and a waiver on its new RAYC Membership Application.

12. Can I use this image.

