PENGWERN BOAT CLUB CIC

DATA PROTECTION POLICY

Our Policy

Pengwern Boat Club is committed to complying with data protection law and to respecting the privacy rights of individuals. The policy applies to all of our volunteers and Committee Members.

This Data Protection Policy ("**Policy**") sets out our approach to data protection law and the principles that we will apply to our processing of personal data. The aim of this Policy is to ensure that we process personal data in accordance with the law and with the utmost care and respect.

We recognise that you have an important role to play in achieving these aims. It is your responsibility, therefore, to familiarise yourself with this Policy and to apply and implement its requirements when processing any personal data. ***Please pay special attention to sections 3,*** *Error! Reference source not found.* ***and 4 as these set out the practical day to day actions that you must adhere to when working or volunteering for the club.***

Data protection law is a complex area. This Policy has been designed to ensure that you are aware of the legal requirements imposed on you and on us and to give you practical guidance on how to comply with them. However, this Policy is not an exhaustive statement of data protection law nor of our or your responsibilities in relation to data protection.

If at any time you have any queries on this Policy, your responsibilities or any aspect of data protection law, seek advice. Contact the Club Secretary or the club's Data Protection Officer (DPO).

1. Who is responsible for data protection?

1.1 All our Committee Members are responsible for data protection, and each person has their role to play to make sure that we are compliant with data protection laws.

1.2 We are not required to appoint a Data Protection Officer (DPO), but we have chosen to do so.

2. Why do we have a data protection policy?

2.1 We recognise that processing of individuals' personal data in a careful and respectful manner cultivates trusting relationships with those individuals and trust in our brand. We believe that such relationships will enable our organisation to work more effectively with and to provide a better service to those individuals.

2.2 This Policy works in conjunction with other policies implemented by us from time to time.

3. Your main obligations

3.1 What this all means for you can be summarised as follows:

3.1.1 Treat all personal data with respect;

3.1.2 Treat all personal data how you would want your own personal data to be treated;

3.1.3 Immediately notify the Club Secretary or the DPO if any individual says or does anything which gives the appearance of them wanting to invoke any rights in relation to personal data relating to them;

3.1.4 Take care with all personal data and items containing personal data you handle or come across so that it stays secure and is only available to or accessed by authorised individuals; and

3.1.5 Immediately notify the DPO if you become aware of or suspect the loss of any personal data or any item containing personal data.

4. **Practical matters**

4.1 Whilst you should always apply a common-sense approach to how you use and safeguard personal data, and treat personal data with care and respect, set out below are some examples of dos and don'ts:

4.1.1 Do not take personal data out of the organisation's premises (unless absolutely necessary).

4.1.2 Only disclose your unique logins and passwords for any of our IT systems to authorised personnel (e.g. IT) and not to anyone else.

4.1.3 Never leave any items containing personal data unattended in a public place, e.g. on a train, in a café, etc and this would include paper files, mobile phone, laptops, tablets, memory sticks etc.

4.1.4 Never leave any items containing personal data in unsecure locations, e.g. in car on your drive overnight and this would include paper files, mobile phone, laptops, tablets, memory sticks etc.

4.1.5 If you are staying at a hotel then utilise the room safe or the hotel staff to store items containing personal data when you do not need to have them with you.

4.1.6 Do encrypt laptops, mobile devices and removable storage devices containing personal data.

4.1.7 Do lock laptops, files, mobile devices and removable storage devices containing personal data away and out of sight when not in use.

4.1.8 Do password protect documents and databases containing personal data.

4.1.9 Never use removable storage media to store personal data unless the personal data on the media is encrypted.

4.1.10 When picking up printing from any shared printer always check to make sure you only have the printed matter that you expect, and no third party's printing appears in the printing.

4.1.11 Use confidential waste disposal for any papers containing personal data, do not place these into the ordinary waste, place them in a bin or skip etc, and either use a confidential waste service or have them shredded before placing them in the ordinary waste disposal.

4.1.12 Do dispose of any materials containing personal data securely, whether the materials are paper based or electronic.

4.1.13 When in public place, e.g. a train or café, be careful as to who might be able to see the information on the screen of any device you are using

when you have personal information on display. If necessary move location or change to a different task.

4.1.14 Do ensure that your screen faces away from prying eyes if you are processing personal data, even if you are working in the office. Personal data should only be accessed and seen by those who need to see it.

4.1.15 Do challenge unexpected visitors or employees accessing personal data.

4.1.16 Do not leave personal data lying around, store it securely.

4.1.17 When speaking on the phone in a public place, take care not to use the full names of individuals or other identifying information, as you do not know who may overhear the conversation. Instead use initials or just first names to preserve confidentiality.

4.1.18 If taking down details or instructions from a customer in a public place when third parties may overhear, try to limit the information which may identify that person to others who may overhear in a similar way to if you were speaking on the telephone.

4.1.19 Never act on instructions from someone unless you are absolutely sure of their identity and if you are unsure then take steps to determine their identity. This is particularly so where the instructions relate to information which may be sensitive or damaging if it got into the hands of a third party or where the instructions involve money, valuable goods or items or cannot easily be reversed.

4.1.20 Do not transfer personal data to any third party without prior written consent of the Club Secretary or our DPO.

4.1.21 Do notify the Club Secretary or our DPO immediately of any suspected security breaches or loss of personal data.

4.1.22 If any personal data is lost, or any devices or materials containing any personal data are lost, report it immediately to our DPO.

4.2 However, you should always take a common-sense approach, and if you see any areas of risk that you think are not addressed then please bring it to the attention of our DPO.

5. Notification and response procedure for member enquiries

5.1 If a Committee Member has a request or believes they have received a request from a Member to exercise one of their data protection rights, they should:

5.1.1 pass the call to the Club Secretary. The Club Secretary should take and record all relevant details and explain the procedure. If possible, try to get the request confirmed in writing addressed to our DPO; and

5.1.2 inform our DPO of the request.

5.2 If a letter or fax exercising a Right is received:

5.2.1 pass the letter to the Club Secretary;

5.2.2 the Club Secretary must log the receipt of the letter with our DPO and send a copy of it to them; and

5.2.3 our DPO will then respond to the Member on our behalf.

5.3 If an email exercising a Rights is received:

5.3.1 pass the email to the Club Secretary;

5.3.2 the Club Secretary must log the receipt of the email with our DPO and send a copy of it to them; and

5.3.3 our DPO will then respond to the Member on our behalf.

5.4 Our DPO will co-ordinate our response [which may include written material provided by external legal advisors. The action taken will depend upon the nature of the request. The DPO will write to the individual and explain the legal situation and whether we will comply with the request. A standard letter/email from the DPO should suffice in most cases.

5.5 The DPO will inform the relevant Committee Member of any action that must be taken to legally comply.

5.6 The Committee Member who receives the request will be responsible for ensuring that the relevant response is made within the time period required.

5.7 The DPO's reply will be validated by the Club Secretary and the Club Chairperson. For more complex cases, the letter/email to be sent may be checked by legal advisors.

6. **Queries**

6.1 If you have any queries about this Policy please contact either the Club Secretary on secretary@pegwern-rowing.co.uk or the DPO on data.protection@pengwern-rowing.co.uk