Poole Yacht Club Cruising Section Data Protection Policy 2019

Poole Yacht Club Cruising Section (PYCCS)

Data Protection Policy

Context and overview

Key details

- Policy prepared by: Class Captain and Administrator,
- Policy became operational on: 1st December 2022
- Next review date: December 2024

Introduction

Poole Yacht Club Cruising Section (hereinafter referred to as PYCCS) needs to gather and use certain information about individuals.

These can include PYC berth holders, business contacts, committee members and other people the organisation has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the association's data protection standards - and to comply with the law.

Why this policy exists

This data protection policy ensures PYCCS:-

- Complies with data protection law and follows good practice
- Protects the rights of committee members, berth holders and partners
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

Data Protection Law

In 2018 the Data Protection Act 1998 was replaced by the General Data Protection Regulation (GDPR).

The GDPR sets out how businesses - including PYCCS - must collect, handle and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The GDPR is underpinned by eight important principles. These say that personal data must:

1. 1. Be processed fairly and lawfully
2. Be obtained only for specific, lawful purposes
3. Be adequate, relevant and not excessive
4. Be accurate and kept up to date
5. Not be held for any longer than necessary
6. Processed in accordance with the rights of data subjects
7. Be protected in appropriate ways
8. Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection

People, risks and responsibilities

Policy scope

This policy applies to:

- The Committee Members of PYCCS
- All activities of PYCCS
- All officers and members of PYCCS
- All contractors, suppliers and other people in association with business on behalf of PYCCS

It applies to all data that the business holds relating to identifiable individuals, even if that information technically falls outside of the GDPR.

This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- plus any other information relating to individuals

Data protection risks

This policy helps to protect PYCCS from some very real data security risks, including:

- **Breaches of confidentiality.** For instance, information being given out inappropriately.
- **Failing to offer choice**. For instance, all individuals should be free to choose how PYCCS uses data relating to them.
- **Reputational damage**. For instance, PYCCS could suffer if hackers successfully gained access to sensitive data.

Responsibilities

Everyone who is involved with PYCCS has some responsibility for ensuring data is collected stored and handled appropriately.

Each individual or team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

The **Class Captain** is ultimately responsible for ensuring that PYCCS meets its legal obligations.

The **Data Protection Officer** (Administrator) is responsible for:

- Keeping the Committee Members updated about data protection responsibilities, risks and issues.
- Reviewing all data protection procedures and related policies, in line with an agreed schedule.
- Arranging data protection training and advice for the people covered by this policy.
- Handling data protection questions from anyone covered by this policy.
- Dealing with requests from individuals to see the data PYCCS holds about them (also called 'subject access requests').
- Checking and approving any contracts or agreements with third parties that man handle the business's sensitive data.

The **Data Protection Officer** (Administrator)**,** is also responsible for:

- Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
- Performing regular checks and scans to ensure security hardware and software is functioning properly.
- Evaluating and third-party services the business is considering using to store or process data. For instance, cloud computing services.

The **Class Captain** is responsible for:

- Approving any data protection statements attached to communications such as emails and letters.
- Addressing any data protection queries from journalists or media outlets like newspapers.
- Where necessary, PYCCS business with other people to ensure marketing initiatives abide by data protection principles.

General guidelines

- The only people able to access data covered by this policy should be those who **need it for their PYCCS business**.
- Data **should not be shared informally**. When access to confidential information is required, people can request it from the Class Captain or Secretary.
- **PYCCS will provide training** to people as necessary to help them understand their responsibilities when handling data.
- People should keep all data secure, by taking sensible precautions and following the guidelines below.
    - ◊ In particular, **strong passwords must be used** and they should never be shared.
    - ◊ Personal data **should not be disclosed** to unauthorised people, either within the association or externally.
    - ◊ Data should be **regularly reviewed and updated** if it is found to be out of date. If no longer required, it should be deleted and disposed of.
    - ◊ People should **request help from** the Class Captain, Secretary or the data protection officer (Administrator) if they are unsure about any aspect of data protection.

Data storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the Administrator. When data is **stored on paper,** it should be kept in a secure place where unauthorised people cannot see it. These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept **in a locked drawer or filing cabinet.**
- People should make sure paper and printouts are **not left where unauthorised people could see them**, like on a printer.
- **Data printouts should be shredded** and disposed of securely when no longer required.

When data is **stored electronically**, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data should be **protected by strong passwords** that are changed regularly and never shared between people.
- If data is **stored on removable media** (like a CD or DVD), these should be kept locked away securely when not being used.
- Data should only be **stored on designated drives and servers**, and should only be uploaded to an **approved cloud computing services**.
- Servers containing personal data should be **sited in a secure location**, away from general office space.
- Data should be **backed up frequently**. Those backups should be tested regularly, in line with the association's standard backup procedures.
- Data should **never be saved directly** to laptops or other mobile devices like tablets or smart phones.
- All servers and computers containing data should be protected by **approved security software and a firewall.**

Data use

Personal data is of no value to PYCCS unless the Section can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When using personal data, people should ensure **the screens of their computers are always locked** when left unattended.
- Personal data **should not be shared informally**. In particular, it should never be sent by email, as this form of communication is not secure.
- Data must be **encrypted before being transferred electronically**. The IT support person can explain how to send data to authorised external contacts.
- People **should not save copies of personal data to their own computers**.
- People should **always access and update the central copy** of any data.

Data accuracy

The law requires PYCCS to take reasonable steps to ensure data is kept accurate and up to date. The more important it is that the personal data is accurate, the greater the effort PYCCS should put into ensuring its accuracy.
It is the responsibility of all people who do business with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in as **few places as necessary**. People should not create any unnecessary additional data sets.
- People should **take every opportunity to ensure data is updated**. For instance, by confirming a person's details when they contact the business.
- PYCCS will make it **easy for data subjects to update the information** PYCCS holds about them. For instance, via the PYCCS website.
- Data should be **updated as inaccuracies are discovered**. For instance, if a person can no longer be reached on their stored telephone number, it should be removed from the database.

Subject access requests

All individuals who are the subject of personal data held by PYCCS are entitled to:

- Ask **what information** the section holds about them and why.
- Ask **how to gain access** to it.
- Be informed **how to keep it up to date**.
- Be informed how the association is **meeting its data protection obligations**.

If an individual contacts the PYCCS requesting this information, this is called a subject access request. Subject access requests from individuals should be made by email, addressed to the data controller at geraldldavies36@icloud.com The data controller can supply a standard request form, although individuals do not have to use this.

Individuals will not be charged for the first subject request, but will be charged £10 per subsequent subject access request or request for a further copy. The data controller will aim to provide the relevant data within 14 days.

The data controller will always verify the identity of anyone making a subject access request before handing over any information.

Disclosing data for other reasons

In certain circumstances, the GDPR allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, PYCCS will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the committee and from the section's legal advisers where necessary.

Providing information

PYCCS aims to ensure that individuals are aware that their data is being processed, and that they understand:-

- How the data is being used
- How to exercise their rights

To these ends, the section has a privacy statement (below), setting out how data relating to individuals is used by the association.

[This is available on request. A version of this statement is also available on the PYCCS's website.]

Poole Yacht Club Cruising Section

Data Protection Privacy Notice

Your Personal Data:

What we need

Poole Yacht Club Cruising Section (hereinafter called the PYCCS) will be what's known as the 'Controller' of the personal data you provide to us. We only collect basic personal data about you which does not include any special types of information or location based information. This does however include name, address, email etc.

Why we need it

We need to know your basic personal data in order to provide you with information and support in events and activities as part of the PYCCS. We will not collect any personal data from you we do not need in order to provide and oversee this service to you.

What we do with it

All the personal data we process is processed by us in the UK for the purposes of the PYCCS and this information is located on servers within the European Union. No 3rd parties have access to your personal data unless the law allows them to do so.

We have a Data Protection regime in place to oversee the effective and secure processing of your personal data. More information on this can be found on our website.

How long we keep it

We keep your basic personal data (name, address, contact details etc.) for the time you are a member with us. Should you remove your business from PYCCS your data will be deleted from our Data Base and Records. Your information will not be used for marketing purposes and will be kept with us until you notify us that you no longer wish to receive information about PYCCS and associated matters.

What are your rights?

If at any point you believe the information we process on you is incorrect you can request to see this information and even have it corrected or deleted. If you wish to raise a complaint on how we have handled your personal data, you can contact our Data Protection Officer (Administrator) at geraldldavies36@icloud.com who will investigate the matter. If you are not satisfied with our response or believe we are processing your personal data not in accordance with the law you can complain to the Information Commissioner's Office (ICO).