POOLBEG
YACHT & BOAT CLUB

Data protection policy

Key details

- Policy prepared by: GDPR Sub Committee
- Approved by Committee on: 1st May2018
- Policy became operational on: 25th May 2018
- Next review date: 1st May 2019

Introduction

Poolbeg Yacht & Boat Club needs to gather and use certain information about individuals.

These can include members, customers, suppliers, business contacts, employees 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 company's data protection standards — and to comply with the law.

Why this policy exists

This data protection policy ensures Poolbeg Yacht & Boat Club:

- Complies with data protection law and follow good practice
- Protects the rights of staff, customers and partners
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

Data protection law

The Data Protection Act 1998 describes how organisations — including Poolbeg Yacht & Boat Club— 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 Data Protection Act is underpinned by eight important principles. These say that personal data must:

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

Policy scope

This policy applies to:

- The head office of Poolbeg Yacht & Boat Club
- All branches of Poolbeg Yacht & Boat Club
- All staff and volunteers of Poolbeg Yacht & Boat Club
- All contractors, suppliers and other people working on behalf of Poolbeg Yacht & Boat Club

- The Committee and Trustees of Poolbeg Yacht & Boat Club

It applies to all data that the club holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 1998. 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 Poolbeg Yacht & Boat Club 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 the club uses data relating to them.
- **Reputational damage.** For instance, the company could suffer if hackers successfully gained access to sensitive data.

Responsibilities

Everyone who serves, works or volunteers for or with Poolbeg Yacht & Boat Club has some responsibility for ensuring data is collected, stored and handled appropriately.

Each 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 **Committee** is ultimately responsible for ensuring that Poolbeg Yacht & Boat Club meets its legal obligations.
- The, Data **Protector,** is responsible for:
- Keeping the Committee 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 staff and anyone else covered by this policy.
- Dealing with requests from individuals to see the data Poolbeg Yacht & Boat Club holds about them (also called 'subject access requests').
- Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.
- The, Data **Protector,** is 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 any third-party services, the Club is considering using to store or process data. For instance, cloud computing services.
- The, **Data Protector,** 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, working with other staff to ensure marketing initiatives abide by data protection principles.
- In the event of an actual or potential data breach e.g. loss of any device (including personal devices). This must be reported to the Office of the Data Commissioner immediately.

General Staff Guidelines

- The only people able to access data covered by this policy should be those who **need it for their work**.
- Data **should not be shared informally**. When access to confidential information is required, employees and volunteer can request it from their line managers.
- **will provide training** to all employees and volunteers to help them understand their responsibilities when handling data.
- Each new person appointed to committee, assigned a task where data is handled or employed shall attend an induction where they will be advised of the GDPR policy and procedure of the club.
- Employees and volunteers 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 club 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.
- Employees and volunteers **should request help** from their line manager or the data protection champion if they are unsure about any aspect of data protection.
- No paper records shall be removed from the club without the Data Protector being aware and granting permission to do so. There must be adequate reason for this temporary removal.
- Contact with Junior members should not be made directly but through their parents/ guardians contact details unless their parent / guardian has given permission in writing.
- Loss of any data or any device on which data is stored must be reported to the Data Protector immediately.

Data Storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the Data Protector.

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**.
- Employees and volunteers 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 employees and volunteers.
- 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 company'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 Poolbeg Yacht & Boat Club unless the club 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 working with personal data, employees and volunteers 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 manager can explain how to send data to authorised external contacts.
- Personal data should **never be transferred outside of the European Economic Area**.
- Employees and volunteers **should not save copies of personal data to their own computers.** Always access and update the central copy of any data.
- On completion of a person's term of office, resignation or termination of employment that person shall remove all club data from their personal devices and return all data held in paper form or any other form to the data protector. They must advise the data protector that they have complied with this requirement.

Data Accuracy

The law requires Poolbeg Yacht & Boat Club 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 Poolbeg Yacht & Boat Club should put into ensuring its accuracy.

It is the responsibility of all employees and volunteers who work 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**. Staff and volunteers should not create any unnecessary additional data sets.
- Staff and volunteers should **take every opportunity to ensure data is updated.** For instance, by confirming a customer's details when they call.
- The Data Protection Champion will make it **easy for data subjects to update the information Poolbeg Yacht & Boat Club** holds about them. For instance, via the company website.
- Data should be **updated as inaccuracies are discovered**. For instance, if a customer or member can no longer be reached on their stored telephone number, it should be removed from the database.
- It is the I.T manager's responsibility to ensure **marketing databases are checked against industry suppression files** every six months.

Subject Access requests

All individuals who are the subject of personal data held by Poolbeg Yacht & Boat Club are entitled to:

- Ask **what information** the company 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 Club is **meeting its data protection obligations**.

If some individual contacts the club 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 [email address to be implemented] or in writing.

The data controller will aim to provide the relevant data within 14 days.

If a person requests the amendment or removal of their personal data their request shall be dealt with as soon as is practicable.

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 Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, Poolbeg Yacht & Boat Club will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers where necessary.

Providing Information

Poolbeg Yacht & Boat Club 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 right

How we provide data to the ISA

In becoming a member of renewing your membership of Poolbeg yacht and boat club you automatically become a member of Irish Sailing, the national governing body.

We will share certain information about you with them including your name and email address, so they can include you on updates of operational activity, their monthly news letter and invitations to certain events such as the Irish sailing awards, conferences, agm etc.