South Yorkshire Boat Club GDPR

In accordance with the EU General Data Protection Regulation (GDPR)

25th May 2018

Context and overview

Key details

- Policy prepared by: Andrew Manson
- Approved by SYBC Committee: 01/05/18
- Policy became operational on: 25/05/18
- Next review date: 25/11/18

Introduction

South Yorkshire Boat Club (SYBC) needs to gather and use certain information about individuals.
These can include members, employees, suppliers, associated organisations and other people the club has a relationship with or may need to contact.
This policy describes how this personal data must be collected, handled and stored to meet SYBC GDPR protection standards — and to comply with the law.

Why this policy exists

This data privacy and protection policy ensures SYBC:
• Complies with data privacy and protection law and follows good practice
• Protects the rights of Club members, Club employees and associated organisations
• 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 must protect individuals data, this Act is being replaced by GDPR which will become law, organisations including SYBC must collect, handle and store personal information following the GDPR regulations.

These regulations 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 be disclosed unlawfully.

The Data Protection Act is underpinned by eight important principles.
These say that personal data must:
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:
• South Yorkshire Boat Club members
• All committee members acting as representatives of SYBC
• All staff employed by SYBC
• All contractors, suppliers and other people working on behalf of SYBC
It applies to all data that the SYBC 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 SYBC from some very real data security risks, including:
• **Breaches of confidentiality.** For example, information been given out inappropriately.
• **Failing to offer choice.** For instance, all individuals should be free to choose how SYBC uses data relating to them.
• **Reputational damage.** For instance, SYBC could suffer if hackers successfully gained access to sensitive data.

Responsibilities
Everyone who acts for or represents SYBC has some responsibility for ensuring data is collected, stored and handled appropriately.
Each individual 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 SYBC meets its legal obligations.
• **The Data Protection Officer (DPO) is responsible for**:
o Keeping the Committee updated about data protection responsibilities, risks and issues.
o Reviewing all data protection procedures and related policies, in line with an agreed schedule.
o Arranging data protection training and advice for the people covered by this policy.
o Handling data protection questions from members, employees and anyone else covered by this policy.
o Dealing with requests from individuals to see the data SYBC holds about them (also called ‘subject access requests’).
o Checking and approving any contracts or agreements with third parties that may handle the clubs sensitive data.

• **The IT Co-ordinator is responsible for:**

o Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
o Performing regular checks and scans to ensure security hardware and software is functioning properly.
o Evaluating any third-party services SYBC is considering using to store or process data. For instance, cloud computing services.
o Approving any data protection statements attached to communications such as emails and letters.
o Addressing any data protection queries from members or associate members.
o Where necessary, working with other committee members to ensure all Club correspondence abides by data protection principles.

General Committee guidelines

• The only people able to access data covered by this policy should be those who need it for their role on the Committee
• Data should not be shared informally. When access to confidential information is required, committee members can request it from the Club Secretary.
• SYBC will provide training to all committee members to help them understand their responsibilities when handling data.
• Committee members should keep all data secure, by taking sensible precautions and following the guidelines below.
• In particular, encryption and 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, downloading data should always be kept to a minimum and if printed must be shredded prior to disposal.
• Committee members should request help from the Club Secretary or the DPO if they are unsure about any aspect of the GDPR Law.

Data storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the Club Secretary or DPO.

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. (Committee Office)
• Committee Members 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 members
• If data is stored on removable media (like an encrypted USB drive), this should be kept locked away securely when not being used.
• Data should only be stored on designated encrypted & engraved USB drives and PCs.
• PCs containing personal data should be sited in a secure location, away from generally trafficked space.
• Data should be backed up frequently. Those backups should be tested regularly, in line with SYBC's standard backup procedures (Carried out ¼ ly by the IT Co-ordinator).
• Data should never be saved directly to laptops or other mobile devices like tablets or smart phones.
• All approved servers and computers containing data should be protected by approved security software and a firewall.

Data use

Personal data is of no value to SYBC 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, committee members should ensure the device used is approved for compliance with GDPR, the screen of the computer is always locked when left unattended.
• Personal data should not be shared informally. In particular, it should never be sent by personal email, as this form of communication is not secure.
• Data must be encrypted before being transferred electronically. The Club Secretary or DPO will be the only authorised Club representatives who can share any information with authorised external contacts in the unlikely event of legal obligation.
• Personal data should never be transferred outside of the European Economic Area.
• Committee members should not save copies of personal data to their own personal home computers. Each committee member allocated a SYBC approved encrypted and engraved USB Drive will be expected to keep that drive safe and up to date, with information relevant to the specific committee role (the IT Coordinator will assist with excel files etc, as necessary).

Data accuracy

The law requires SYBC 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 SYBC should put into ensuring its accuracy.
It is the responsibility of each committee member who has access to a Club USB Drive to take reasonable steps to ensure it is kept as accurate and up to date as possible, with data only relevant to their role on the committee.
• Data will be held in as few places as necessary. Committee members should not create any unnecessary additional data sets.

• Committee members should take every opportunity to ensure data is updated. For instance, by confirming new member details when they apply for membership providing this information to the Club Secretary to upload and record on the official central data device.
• SYBC will make it easy for data subjects to update the information SYBC holds about them. For instance, via the Clubs official website, ***www.sybc.org.uk***
• Data should be updated as inaccuracies are discovered. For instance, if a member can no longer be reached on their stored telephone number, it should be removed from the database by the Club Secretary.
• It is the Club Secretary's responsibility to ensure all communication databases are checked against suppression files every month and kept up-to date.

Subject access requests

All individuals who are the subject of personal data held by SYBC are entitled to:
• Ask what information the Club 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 an 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 DPO at ***gdpr@sybc.org.uk***

The DPO can supply a standard request form, although individuals do not have to use this.
The DPO will aim to provide the relevant data stored on the consent form within 14 days in paper format.
The DPO 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, GDPR Law allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.
Under these circumstances, SYBC will disclose requested data. However, the DPO will ensure the request is legitimate, seeking assistance from the Committee and from the Clubs legal advisers where necessary.

Providing information
SYBC 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 Club has a privacy statement, setting out how data relating to individuals is used by the company.
[This is available on request. A version of this statement is also available on the Clubs website.] ***www.sybc.org.uk***

Version 1 (25/5/2018)

SYBC Authorised Storage & Access Devices:

Master Copy Data: Club Secretarys Authorised Secure Device (Committee Office).

E-Mail Addresses: Communications Officer Secure Online Cloud

Club Approved IT Devices:

Secretary's Personal Home GDPR Compliant PC

Treasurer's Personal GDPR Compliant Laptop

SYBC Committee Room GDPR Compliant PC's x 2 (Labelled SYBC 1 & SYBC 2)

Club Approved USB Drives & Data Required by Authorised Committee Members:

Number 1 = Secretary (All Data) Name, Address, Email, Tel 1, Tel 2, in case of emergency contact details, boat name, spouse/partner details.

Number 2 = Treasurer (All Data) Name, Address, Email, Tel 1, Tel 2, in case of emergency contact details, boat name, spouse/partner details.

Number 3 = Mooring Officer: (Name, Boat Name, Tel, licence expiry date)

Number 4 = New Member Liaison (Name, Boat Name, Tel)

Number 5 = Insurance Officer (Name, Boat Name, Tel, insurance expiry date)

Number 6 = Duty Officer (Name, Boat Name, Tel, mooring number)

Number 7 = Slipway officer (Name, Boat Name, Tel)

Number 8 = Electricity meters (Name, Boat Name, mooring number)

Number 9 = Spare (Blank)

Number 10= Spare (Blank)

The process for reporting breaches in data protection:

All Committee members and club members have an obligation to report data protection breaches or contact the DPO if they have concerns of such a breach. This will allow the IT Co-ordinator or DPO to investigate further and take the appropriate steps to fix the issue in a timely manner.

Personal information is collected on a voluntary basis, when joining SYBC or each year thereafter with membership subscription. A completed signed personal data sheet is required from all members who wish to subscribe to club communications.

It is a pre requisite requirement of the club that all members with an allocated mooring, provide as a minimum: Name, Home Address, Emergency Contact Telephone Number, current copy of insurance certificate.

It is the responsibility of each Club member to advise of any changes to their personal data this should be submitted by completing and signing the ***PERSONNAL DATA RECORD & CONSENT FORM*** *available to print off on the clubs website* ***www.sybc.org.uk*** , and *posting in the Committee Office post box addressed to the Club Secretary.*

Version 1 (25/5/2018)

SYBC PRIVACY NOTICE
&
DATA RETENTION STATEMENT

SYBC PRIVACY NOTICE

SYBC uses members personal data/information for the following reasons: in an emergency, to distribute club matters arising, social events and general club communications.

SYBC uses employees personal data/information for the following reasons: to process employee payment data, for normal employment management purposes, in general club communications and for in an emergency.+

SYBC will, under NO CIRCUMSTANCE, unless under legal obligation, offer or share ANY personal data for general distribution to any organisation or individual. The information provided is expressly reserved for use by the duly elected SYBC Committee.

Should Members require any further information regarding anything contained within this GDPR Policy, these can be obtained by contacting the Data Protection Officer via the following email: ***gdpr@sybc.org.uk***

DATA RETENTION STATEMENT

Any Personal information collected by SYBC will be disposed of after a period of 7 years, should membership of the club cease. All communications from the Club will cease immediately after membership ends. All paper copies of data will be stored in the clubs Archive Room for 7 years after which they will be shredded before disposal.

SYBC uses Members personal data/information for the following reasons: In an emergency, to distribute club matters arising, Social events and general club communications.

SYBC, Will, Under NO CIRCUMSTANCE unless under legal obligation, offer or share ANY Personal data for general distribution to any organisation or Individual. The information provided is expressly reserved for use by the duly elected SYBC Committee.

Should Members require any further information regarding anything contained within this GDPR Policy, these can be obtained by contacting the Data Protection Officer via the following email: ***gdpr@sybc.org.uk***

SYBC COMMITTEE GOOD PRACTICE AND S.O.P

SYBC AS A CLUB HAVE A MANDATORY OBLIGATION TO PROTECT MEMBERS DATA.

SYBC must adopt and ensure all paper copies of data is kept in a locked cupboard within the clubs Committee office.

SYBC's elected means of storing personal information electronically is via the CLUBS approved PC's and approved encrypted and engraved USB drives.

It is a breach of GDPR to download or copy any information stored on these PCs or USB drives to unauthorised devices.

The only individuals allowed to access and distribute any communication from data stored on the USB drives are those members of the Committee who are responsible for the USB drives.

Any correspondence for distribution electronically must be forwarded by committee members, to the Communications Officer using the specific Communications Officer official club email address (**root@sybc.org.uk**). The Communications Officer can use any device which is GDPR compliant (i.e. encrypted) to open and distribute any communications from SYBC to the membership. The use of a GDPR compliant device is the only method which can be used by any committee member to access members electronic distribution lists. It is the expressed responsibility of the Communications Officer to ensure that any Club communication requested for distribution does not contain viruses prior to distribution.

It is the IT Co-ordinators responsibility to ensure that the club approved PC is kept up to date with the latest virus protection and the firewall is always active and up to date.

All communications must contain the Clubs disclaimer regarding viruses at the bottom and advise to check all attachments with virus protection prior to opening. This is the responsibility of any committee member forwarding communications electronically.

SYBC keeps a paper copy of members original data & signed Personal Data Consent Form in the locked cupboard in the Committee Office. This file cannot be removed from Club premises under any circumstances. All obsolete or archived data must be shredded after 7 years before disposal.

Version 1 (25/5/2018)

In the event of a data breach or if a data breach is suspected, the DPO must be informed within 24 hours **(gdpr@sybc.org.uk)** , the Communications Officer must subsequently when deemed necessary advise the members without delay of the breach or suspected breach.

In the event of electronic breach,

The IT Co-ordinator must be advised and undertake ***Steps 1 & 2*** below.

(The IT Co-ordinator must advise the DPO should any breach of the security be suspected.)

The DPO will undertake ***Step 3*** "unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons".

The Communications Officer will undertake ***Step 4***, as advised by the DPO.

Step (1) Identifying and resolving the point of failure or attack source;
Step (2) Gathering information relating to the factual, technical and legal background to the data breach;
Step (3) Reporting to the data protection regulator (ICO) and to other sector-specific regulators (such as the Financial Conduct Authority and Prudential Regulation Authority) as necessary; and,
Step (4) Reporting to data subjects. (i.e. membership when deemed necessary by the DPO or Committee)

Each of these points, independently and in combination, represents a potential area that could mean the downfall of an organisation. The GDPR is focused on empowering data subjects and shaping behaviours through its enforcement regime.

SYBC Committee Guide To GDPR responsibility.

The European Data Protection Directive (95/46/EC) (**the Directive**) contains no obligations whatsoever with respect to notifying parties of a personal data breach. Nevertheless, the various European Member States have sporadic pockets of implied obligations of breach disclosure through regulatory guidance.

The General Data Protection Regulation (**GDPR**) introduces a much more onerous and far-reaching regime with respect to Personal Data breach notification.

Regulatory notification under the GDPR

The DPO must notify the supervisory authority without undue delay (and certainly within 72 hours of becoming aware of a breach), *"unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons".*

Notifying the data subjects

The GDPR compels SYBC to inform a data subject when a breach is likely to affect the protection of the personal data or privacy of that data subject all such communications will be communicated via the clubs elected Communications Officer. That notification must occur without undue delay.

Consequences of non-compliance

Under the GDPR law, data protection regulators are armed with a whole new arsenal, for which the heavy artillery is represented by the new civil monetary penalty regime of up to of £20M or 4% of total annual turnover of the preceding financial year (whichever is higher). Furthermore, the GDPR law includes an explicit statutory ability for affected data subjects to claim compensation and join class action (even for distress alone).
The mandatory disclosing element will mean that breaches will be publicised not frequently and sooner in the process and will likely cause significant immediate reputational damage.

Natural selection through breach notification

The breach notification requirements of the GDPR law represent a major change and SYBC must comply and devote significant resource as it approaches GDPR “day zero” in May 2018.
Once SYBC is aware of a personal data breach, it is going to have to act quickly. The first 24 to 48 hours following any breach is the period of least activety. SYBC simply cannot afford for that to be the case under the GDPR.
In the event that SYBC identifies a breach, it will have to be prepared to take action in a very short period of time, which includes:
(1) Identifying and resolving the point of failure or attack;
(2) Gathering information relating to the factual, technical and background to the data breach;
(3) Reporting to the data protection regulator as necessary (ICO),
(4) Reporting to data subjects (Members).

Each of these points, independently and in combination represent a potential area that could mean the downfall of SYBC.

Version 1 (25/5/2018)

GDPR is focused on empowering data subjects and shaping behaviours through its enforcement regime. SYBC will need to evolve in order to Comply with this new challenge.

ICO CONTACT DETAILS
FOR GUIDANCE ON
REPORTING DATA BREACHES

0303 123 1113

Version 1 (25/5/18)

SYBC MEMBERS GDPR FAQ's

Q: What information does SYBC hold about me?

A: SYBC store name, address, telephone, email address, insurance details and in case of emergency contact details.

Q: How can I check my information is up to date.

A: This is called "Subject Access Request" and should be by email to the GDPR Officer via the relevant official club email address.

Q: Who can see my information.

A: See Clubs Privacy Statement on the notice board and on the website**.**

Q: Can I refuse to give my information to SYBC

A: Members can refuse to give their personal data, however, the Club cannot accept responsibility for any oversight as a direct result.

A: Members with an allocated mooring must as a minimum provide their full name, home address, emergency contact and insurance details.

Q: What happens to my information if I no longer want to be a member of SYBC.

A: In the event that membership lapses or is terminated all stored information specific to the individual will be removed from SYBC records after 7 years, in accordance with the clubs data retention policy. No further communication of any type will be received from SYBC.

Q: What happens if there is a security breach at SYBC.

A: Any member who suspects a breach of security must inform the DPO on the relevant official club email, this will then be investigated. Any confirmed breaches will be advised to all members who have elected to submit data, these will include the type of breach. This will be done by the Communications Officer, in the form of an official Club correspondence.

Q: What if my personal details change.

A: If any information changes, members are obliged to complete a replacement Personal Data Form and submit it to the DPO or Club Secretary. This must be done in paper form and posted in the Committee office post box. Copies of this blank form are freely available upon request or can be downloaded from the website. **(www.sybc.org.uk).**

Version 1 (25/5/2018)

Q: Who is responsible for securing my data.

A: The Committee share joint responsibility for all individual's data. The IT Co-ordinator is responsible for all IT security, The Club Secretary is responsible for safe disposal of obsolete data. All paper records are shredded before safe disposal.

The clubs policy regarding data privacy and protection under the new GDPR regulations and relative blank Personal Data form can be found and downloaded in full on the website (www.sybc.org.uk)

Version 1 (25/5/2018)

Dear SYBC Member,

The law regarding data protection is changing.

SYBC will comply with the new regulations which are known as GDPR and has a written GDPR policy regarding your rights to access data and how the club will ensure it is protected.

Recently all members received the Annual Mooring Application and Insurance Details form, this now forms part of the new GDPR regulations to ensure we comply with the law. Please complete the form, if you haven't already, if you have an assigned mooring it is a mandatory requirement that the Club holds your personal data including a copy of your current boat insurance document.

It is also essential that you sign this letter giving consent to the Club to securely store your data and also consent to its use for general club matters arising.

I give consent for my data to be used by SYBC as described above.

*Full Name*_____ *Mooring No*_____ *Date* _____

Explicit consent is required for the following uses:

- *Displaying name & contact details on Member Notice Boards*

  *Signed:*_____

- *Communication via email*

  *Signed*_____

- *Use of name & photos of yourself and/or family members under 16 years of age in official club publications (Websites & Basin Gen)*
  Disclaimer: We cannot prevent club members or members of the public taking photographs/videos at Club events. Therefore, SYBC cannot be held responsible for photos/videos that others publish in the public domain

  *Signed*_____

This letter and all signed Annual Mooring Application and Insurance Details forms including insurance details should be returned to the Club before 01/05/2018.

For further information or if you have any questions please contact Andy Manson SYBC GDPR Data Protection Officer.

Thank you

Andy Manson
On Behalf of SYBC Elected Committee
GDPR Data Protection Officer

A summary of the Information Commissioner's Office's 12-point GDPR checklist

A summary of the Information Commissioner's Office's 12-point GDPR checklist

1. Ensure senior/key people (Committee Members) are aware of GDPR and appreciate its impact.
2. Document any personal data you hold, where it came from and who you share it with. Conduct an information audit if needed.
3. Review your privacy notices and plan for necessary changes before GDPR comes into force.
4. Check your procedures cover all individuals' rights under the legislation – for example, how you would delete personal data or provide data electronically in a commonly used format.
5. Plan how you will handle subject access requests within the new timescales and provide any additional information.
6. Identify and document your legal basis for the various types of personal data processing you do.
7. Review how you seek, obtain and record consent. Do you need to make any changes?
8. Put systems in place to verify individuals' ages and, if users are children (likely to be defined in the UK as those under 13), gather parental consent for data processing activity.
9. Make sure you have the right procedures in place to detect, report and investigate a personal data breach.
10. Adopt a "privacy by design" and "data minimisation" approach, as part of which you'll need to understand how and when to implement Privacy Impact Assessments.
11. Designate a Data Protection Officer or someone responsible for data protection compliance; assess where this role will sit within in your organisation's structure/governance arrangements.
12. If you operate internationally, determine which data protection supervisory authority you come under.

Version 1 (25/5/2018)