



GDPR Policy

Middle Nene Cruising Club

Dated June 2018

**This policy to be reviewed
on or Before April 2020**

Table of Contents

| | |
|---|---|
| Purpose | 2 |
| Definition of Terms Used..... | 3 |
| The Data Protection Act 1998 | 3 |
| Applying the Data Protection Act 1998 within MNCC | 3 |
| Correcting data..... | 4 |
| Responsibilities | 4 |
| Procedures for Handling Data & Data Security | 5 |
| Privacy Notice and Consent Policy | 5 |
| Operational Guidance..... | 5 |
| Phone calls..... | 5 |
| Laptops and Portable Devices..... | 6 |
| Data Security and Storage | 6 |
| Passwords..... | 6 |
| Data Subject Access Requests (SAR) | 7 |
| Risk Management..... | 7 |

Purpose

The purpose of this policy is to set out the MNCC's commitment and procedures for protecting personal data. The officers and committee regard the lawful and correct treatment of personal information as very important to our Club, and to maintaining the confidence of our members and with whom we deal. We recognise the risks to individuals of identity theft and financial loss if personal data is lost or stolen.

We are committed to a policy of protecting the rights and privacy of individuals. We need to collect and use certain types of data to carry out our work in managing the Middle Nene Cruising Club (MNCC). This personal information must be collected and handled securely.

The Data Protection Act 1998 (DPA) and General Data Protection Regulations 2018 (GDPR) govern the use of information about people (personal data). Personal data can be held on computers, laptops, and mobile devices, or in a manual file and includes e-mail, minutes of meetings and photographs.

The Officers and Committee of MNCC will remain the Data Controller for the information held. The Club officers and committee members are personally responsible for processing and using personal information in accordance with DPA and GDPR. Officers and members who have access to personal information will therefore be expected to read and comply with this policy.

Definition of Terms Used

Data Controller - The Officers and Committee who collectively decide what personal information MNCC will hold, how it will be held or used.

Act – means The Data Protection Act 1998 and General Data Protection Regulations 2018 - the legislation that requires responsible behaviour by those using personal information.

Data Subject – the individual whose personal information is being held or processed by MNCC.

Consent – is freely given specific agreement by a Data Subject to the processing of personal information about him/her.

Explicit consent is needed for processing “sensitive information”, which includes: -

- a) Racial or Ethnic origin of the Data Subject
- b) Political opinions
- c) Religious beliefs or other beliefs of a similar nature
- d) Trade union membership
- e) Physical or mental health or condition
- f) Sexual orientation
- g) Criminal record
- h) Proceedings for any offence committed or alleged to have been committed

MNCC do not deem that the Club will have any necessity to request or process any type of sensitive information from a Data Subject.

Processing – means collecting, amending, handling, storing or disclosing personal information.

The Data Protection Act 1998

This contains several principles for processing personal data with which we must comply.

1. Shall be processed fairly and lawfully and shall not be processed unless specific conditions are met.
2. Shall be obtained only for one or more purposes specified in the Act and shall not be processed in any manner incompatible with that purpose or those purposes.
3. Shall be adequate, relevant and not excessive in relation to those purposes.
4. Shall be accurate and, where necessary, be kept up to date.
5. Shall not be kept for longer than necessary.
6. Shall be processed in accordance with the rights of Data Subjects under the Act.
7. Shall be kept secure by the Data Controller who takes appropriate technical and other measures to prevent unauthorized or unlawful processing or accidental loss or destruction of, or damage to, personal information.
8. Shall not be transferred to a country or territory outside the European Economic Area.

Applying the Data Protection Act 1998 within MNCC

We will let people know why we are collecting their data, which is for managing the Club, its events, activities and finances.

It is our responsibility to ensure this data is only used for these purposes. Access to this information shall be limited to officers, committee members and trustees of MNCC.

Correcting data

Individuals have a right to make a Subject Access Request (SAR) to find out whether the MNCC holds their personal data, where, what it is used for and to have data corrected if it is wrong, to prevent use which is causing them damage or distress, or to stop marketing information being sent to them. Any SAR should normally be dealt with within 30 days. Steps must be first be taken to confirm the identity of the individual before providing information. This might require photo identification or confirmation of address e.g. by passport, utility bill etc.

Responsibilities

The MNCC Officers and Committee are the Data Controller under the Act and legally responsible for complying with the Act, which means that it determines what purposes personal information held will be used for.

The Officers and Committee will consider legal requirements and ensure that it is properly implemented, and will through appropriate management, strict application of criteria and controls:

- a. Collect and use information fairly.
- b. Specify the purposes for which information is used.
- c. Collect and process appropriate information, and only to the extent that it is needed to fulfill its operational needs or to comply with any legal requirements.
- d. Ensure the quality of information used.
- e. Ensure the rights of people about whom information is held can be exercised under the Act.

These include:

- f. The right to be informed that processing is undertaken.
- g. The right of access to one's personal information.
- h. The right to prevent processing in certain circumstances, and the right to correct, rectify, block or erase information that is regarded as wrong information.
- i. Take appropriate technical and organisational security measures to safeguard personal information,
- j. Ensure that personal information is not transferred abroad.

All MNCC members are aware that a breach of the rules and procedures identified in this policy may lead to action taken against them.

The Data Controller

Will be responsible for ensuring that the policy is implemented and will have overall responsibility for:

- a) Everyone processing personal information understands that they are responsible for following good data protection practice
- b) Everyone processing personal information is appropriately instructed to do so

- c) Anybody wanting to make enquiries about handling personal information knows what to do.
- d) Dealing responsibly and courteously with any enquiries about handling personal information.
- e) Describe clearly how MNCC handles personal information.
- f) Will regularly review and audit ways it holds, manages and uses personal information.

This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments to The Data Protection Act 1998.

In case of any queries or questions in relation to this policy please contact the Club Secretary

Procedures for Handling Data & Data Security

MNCC has a duty to ensure that appropriate technical and organisational measures and instruction are undertaken to prevent:

- Unauthorised or unlawful processing of personal data
- Unauthorised disclosure of personal data
- Accidental loss of personal data

All officers, members and trustees must therefore ensure that personal data is dealt with properly no matter how it is collected, recorded or used. This applies whether or not the information is held on paper, in a computer or recorded by some other means e.g. tablet or mobile phone.

Personal data relates to data of living individuals who can be identified from that data and use of that data could cause an individual damage or distress. This does not mean that mentioning someone's name in a document comprises personal data; however various data elements such as a person's name or contact details would be classified as personal data and falls within the scope of the DPA. It is therefore important that every member of MNCC consider any information (which is not otherwise in the public domain) that can be used to identify an individual as personal data and observe the guidance given below.

Privacy Notice and Consent Policy

The privacy notice and consent policy are as follows:

Consent forms will be stored by the secretary in a securely held electronic or paper file.

Operational Guidance

Email

All members of MNCC should consider whether an email (both incoming and outgoing) would need to be kept as an official record. If the email needs to be retained it should be saved into the appropriate folder or printed and stored securely.

Remember, emails that contain personal information no longer required for operational use, should be deleted from the personal mailbox and any "deleted items" box.

Phone calls

Phone calls can lead to unauthorised use or disclosure of personal information and the following precautions should be taken:

- Personal information should not be given out over the telephone unless you have no doubts

as to the caller's identity and the information requested is innocuous.

- If you have any doubts, ask the caller to put their enquiry in writing.
- If you receive a phone call asking for personal information to be checked or confirmed be aware that the call may come from someone impersonating someone with a right of access.

Laptops and Portable Devices

All laptops and portable devices that hold data containing personal information **must** be protected with a suitable encryption program (Password).

Ensure your laptop is locked (Password protected) when left unattended even for short periods of time.

Never leave laptops or portable devices unattended in restaurants or bars, or any other venue.

When travelling on public transport keep it with you at all time, do not leave it in luggage racks or even on the floor alongside you.

Data Security and Storage

Store as little personal data as possible on your computer or laptop; only keep those files that are essential. Personal data received on a disk or memory stick should be saved to the relevant file on the server or laptop. The disk or stick should then be securely returned (if applicable) safely stored or wiped and securely disposed of.

Always lock (password protect) your laptop or computer when left unattended.

Passwords

Do not use passwords that are easy to guess. All your passwords should contain both upper and lower-case letters and preferably contain some numbers. Ideally should be 6 characters or more in length. Protect your password; do not give it to others, write it on your device or in your device case.

Data Storage

Personal data will be stored securely and will be only accessible to authorised Club members.

Information will be stored only as long as it is needed or required by statute and will be disposed of appropriately. For financial records this will be up to 7 years. Archived material such as minutes and legal documents will be stored indefinitely. Other correspondence and emails will usually be disposed of when no longer needed or when members leave.

All personal data held for the MNCC must be non- recoverable from any computer that has been passed on/sold to a third party.

Data Subject Access Requests (SAR)

We may occasionally need to share information with other agencies in circumstances that are not in furtherance of the management of the MNCC. The circumstances where the law allows the Club to disclose data without the data subject's consent are:

- a) Carrying out a legal duty or as authorized by the Secretary of State protecting vital interests of a Data Subject or other person e.g. child protection.
- b) The data Subject has already made the information public.
- c) Conducting any legal proceeding, obtaining legal advice or defending any legal rights

We regard the lawful and correct treatment of personal information as very important to successful management of the Club and to maintaining the confidence of those with whom we deal.

We intend to ensure that personal information is treated lawfully and correctly.

Risk Management

The consequences of breaching Data Protection can cause harm or distress to members if their information is released to inappropriate people.

All members should be aware that they could be personally liable if they use the personal information obtained on behalf of the Club (not that of your own private contacts) inappropriately.

This policy is designed to minimize the risks and ensure that the reputation of MNCC is not damaged by inappropriate or unauthorised access and sharing.