Nottinghamshire County Sailing Club DATA PROTECTION POLICY

Introduction

In order to run effectively as a club, Nottinghamshire County Sailing Club (NCSC) needs to obtain and store relevant personal data regarding members, contractors and learners as part of its operation.

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

Why this policy exists

This data protection policy ensures NCSC:

- Complies with data protection law and follows good practice
- Protects the rights of members and customers
- Is open about how it stores and processes individual's data
- Protects itself from risk of data breaches

Data protection law

The General Data Protection Regulation (GDPR) to be fully introduced in May 2018 describes how organisations such as NCSC must collect, handle and store personal information.

These rules apply regardless of whether data are stored electronically or on paper.

To comply with the GDPR, 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:

- Be processed fairly and lawfully
- Be obtained only for specific, lawful purposes
- Be adequate, relevant and not excessive
- Be accurate and up to date
- Not kept for longer than necessary
- Be processed in accordance with the rights of data subjects
- Be kept and held securely
- Not be transferred to third parties or other countries without consent

In addition, NCSC must maintain data contracts with third parties in accordance with the GDPR

Policy Scope

This policy relates to:

- All members of NCSC
- The executive committee
- The sailing committee
- The training section

Personal Data

Personal data covers both facts and opinions about an individual where that data identifies an individual. These data include amongst other items

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- Age
- RYA Qualifications
- Duty roster abilities

Data protection risks

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

- Breaches of confidentiality
- Failure to offer choice in how data are used/stored
- Reputational damage in the event of a data loss or leak

Responsibilities

All members of NCSC particularly those with positions of responsibility have a responsibility to ensure data are collected, stored and handled appropriately. These people have particular responsibility.

- The flag officers
- The membership secretary
- The training secretary
- Publicity secretary

NCSC has no formal Data Protection Officer (DPO) but the function of ensuring that we maintain data protection standards in accordance with the requirements of the General Data Protection Regulation (GDPR) is vested in the office of the Commodore and supported by the Executive Committee.

General guidance

- The only people able to access data are those authorised by the executive committee who need such access for their function in the club
- Data should not be shared informally
- Passwords for electronic information databases should be strong and not shared
- Data should be regularly reviewed and updated and if no longer required should be deleted and appropriately disposed of
- Members should request guidance if they are unsure about any aspect of data protection from the executive via the club secretary

Data storage

When data are stored on paper:

- This should be in a secure place where unauthorised personas can not see or access it.
- When not required the paper or files should be kept in a locked drawer or filing cabinet.
- Data printouts should be shredded when no longer required

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

- It should be protected by strong passwords that are not shared between members
- Removable media should be kept locked away when not in use
- Data should be backed up frequently
- All computers containing data should be protected by approved security software, passwords and firewalls

Data Use

- Personal data should not be shared informally
- Personal data should be encrypted before being transferred electronically
- Personal data should never be transferred outside of the European Economic Area
- Members should not save copies of personal data to their own computers unless these are password and firewall protected and approved.

NCSC will not forward personal data for direct marketing and fund-raising purposes.

Sensitive Personal Data

NCSC will not collect or store sensitive personal data. This includes data relating to information regarding religion, race, sexual orientation, and criminal records and proceedings. The training section will obtain relevant medical data for the duration of a training course and only whilst it is relevant to the safe running of the course. Other club activities may obtain medical data regarding participants as well as emergency contact details only for the period required for the safe running of the course/activity

Rights of Access to Information

Members have the right of access to information held by NCSC. Any member wishing to access their personal data should put their request in writing to the Commodore via the Club Secretary. NCSC will respond to any such written requests as soon as is reasonably practicable and in any event, within the requirements of the GDPR.

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 rare circumstances NCSC will disclose requested data after ensuring that the request is legitimate.

Enforcement

If an individual believes that NCSC has not complied with this Policy or acted otherwise than in accordance with the Data Protection Act, the member should utilise the NCSC grievance procedure and should also notify the DPC.

CCTV

NCSC owns and operates a CCTV network for the purposes of crime prevention and detection, and Safeguarding.

Where a data subject can be identified, images must be processed as personal data.

Providing information

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

- How their data are being used
- How to exercise their rights

Author: Adrian Jones
Date: April 2018
Review: December 2019