DATA PROTECTION POLICY

Introduction

This policy sets out how the Society seeks to protect personal data and ensure that the Executive Committee understand the rules governing their use of personal data to which they have access as a result of their position. In particular, this policy requires members of the Executive Committee to ensure that the Data Protection Officer (DPO) be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

Definitions

The expression “Society” means the Friends of North Cardiff Reservoirs.

The expression “Executive Committee” means the Executive Committee for the time being of the Society as defined in the current edition of the Society’s Constitution.

The expression “Member” means any individual person complying with the obligations of membership as set in the current edition of the Society’s Constitution.

The expression “Membership Purposes” means the purposes for which personal data may be used by us: Personnel, administrative, financial, regulatory, and Society development purposes.

Membership purposes include the following:

- *Compliance with our legal, regulatory and Club governance obligations and good practice*
- *Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests*
- *Ensuring Society policies are adhered to (such as policies covering email and internet use)*
- *Investigating complaints*
- *Monitoring members’ conduct, disciplinary matters*
- *Marketing the Society*
- *Improving services*

The expression “Personal Data” means information relating to identifiable individuals.

Personal data we gather may include: individuals' contact details, age, gender, areas of interest etc.

The expression “Sensitive Personal Data” means data about an individual's age, gender, race, ethnic background, political opinions, religious beliefs, health, sex life or orientation, etc

Scope

This policy applies to all members. You must be familiar with this policy and comply with its terms.

The Society may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be circulated to members before being adopted.

Who is responsible for this policy?

The Society's Data Protection Officer (DPO), for the time being, has overall responsibility for the day-to-day implementation of this policy.

Procedures

Fair and lawful processing

The Society will process personal data fairly and lawfully in accordance with individuals' rights. This generally means that personal data should not be processed unless the individual whose details are being processed has consented to this happening.

The DPO's responsibilities:

- Keeping the Executive updated about data protection responsibilities, risks and issues
- Reviewing all data protection procedures and policies on a regular basis
- Arranging data protection training and advice for all staff members and those included in this policy
- Answering questions on data protection from members and other stakeholders
- Responding to members who wish to know which data is being held on them by the Society
- Checking and approving with third parties that handle the company's data any contracts or agreement regarding data processing
- Ensuring all systems, services, software and equipment meet acceptable security standards
- Checking and scanning security hardware and software regularly to ensure it is functioning properly
- Researching third-party services, such as cloud services the Society may be considering using to store or process data
- Approving any data protection statements attached to emails and other marketing copy
- Addressing data protection queries from clients, target audiences or media outlets

- Ensuring all marketing initiatives adhere to data protection laws and the Society's Data Protection Policy

The processing of all data must be:

- Necessary to for the running of the Society
- In the legitimate interests of the Society and not unduly prejudice the individual's privacy
- In most cases this provision will apply to routine data processing activities.

Our Membership Application/Renewal Form contains a Privacy Notice to members on data protection.

The notice:

- Sets out the purposes for which the Society holds personal data on members
- Provides that members have a right of access to the personal data that the Society holds about them

Sensitive personal data

In most cases where the Society processes sensitive personal data it will require the data subject's explicit consent to do this unless exceptional circumstances apply or the Society is required to do this by law (e.g. to comply with legal obligations to ensure health and safety). Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

Accuracy and relevance

The Society will ensure that any personal data we process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. The Society will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

Individuals may ask the Society to correct inaccurate personal data relating to them. If any member believes that information is inaccurate they should record the fact that the accuracy of the information is disputed and inform the DPO.

Your personal data

Members must take reasonable steps to ensure that personal data held by the Society about them is accurate and updated as required. For example, if personal circumstances change, members should inform the DPO so that the Society can update your records.

Data security

The Society will keep personal data secure against loss or misuse.

Storing data securely

- In cases when data is stored on printed paper, it should be kept in a secure place where unauthorised personnel cannot access it
- Printed data should be shredded when it is no longer needed
- Data stored on a computer should be protected by strong passwords that are changed regularly.
- Data stored on CDs or memory sticks must be locked away securely when they are not being used
- The DPO must approve any cloud used to store data
- Data should be regularly backed up and the back up stored in accordance with this policy
- Data should never be saved directly to mobile devices such as laptops, tablets or smartphones

Data retention

The Society will retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained, but should be determined in a manner consistent with our data retention guidelines.

Transferring data internationally

There are restrictions on international transfers of personal data. The Society will not transfer personal data anywhere outside the UK without first consulting the DPO.

Subject access requests

Under the Data Protection Act 1998, individuals are entitled, subject to certain exceptions, to request access to information held about them.

If the Society receives a subject access request, it will refer that request immediately to the DPO. The Society may ask the applicant to help it comply with those requests.

Members should contact the DPO if they would like to correct or request information that the Society holds about them. There are also restrictions on the information to which members are entitled under applicable law.

Processing data in accordance with the individual's rights

The Society will abide by any request from a member not to use their personal data for direct marketing purposes and notify the DPO about any such request.

The Society will not send direct marketing material to any person electronically (e.g. via email) unless the person has specifically agreed to receive such material.

GDPR provisions

Privacy Notice - transparency of data protection

Being transparent and providing accessible information to individuals about how their personal data will be used is important for the Society. The following are details on how the Society will collect data and what it will do with it:

What information is being collected?	Contact details, expertise or interests related to activities or governance of the Society
Who is collecting it?	The Society Executive Committee
How is it collected?	Membership Application/Renewal Form and ad-hoc requests
Why is it being collected?	To facilitate the efficient running of the Society
How will it be used?	To contact members
Who will it be shared with?	Members of the Executive Committee
Details of transfers to third country and safeguards	Not applicable
Retention period	2 years after membership ceases

Conditions for processing

The Society will ensure any use of personal data is justified using at least one of the conditions for processing and this will be specifically documented. Any member of the Executive Committee responsible for processing personal data will be aware of the conditions for processing. The conditions for processing will be available to data subjects in the form of a privacy notice.

Justification for personal data

The Society will process personal data in compliance with all six data protection principles.

- used fairly, lawfully and transparently
- used for specified, explicit purposes
- used in a way that is adequate, relevant and limited to only what is necessary
- accurate and, where necessary, kept up to date
- kept for no longer than is necessary
- handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

The Society will document the additional justification for the processing of sensitive data and will ensure any biometric and genetic data is considered sensitive.

Consent

The data that the Society collects is subject to active consent by the data subject. This consent can be revoked at any time.

Criminal record checks

The Society will ensure that any criminal record checks are justified by law. Criminal record checks will not be undertaken based solely on the consent of the subject.

Data portability

Upon request, a data subject has the right to receive a copy of their data in a structured format. These requests should be processed within one month, provided there is no undue burden and it does not compromise the privacy of other individuals.

Right to be forgotten

A data subject may request that any information held on them is deleted or removed, and any third parties who process or use that data must also comply with the request. An erasure request may result in the forfeiture of membership of the Society if the Executive Committee deems that it hinders the efficient running of Society.

Privacy by design and default

Privacy by design is an approach to projects that promote privacy and data protection compliance from the start.

When relevant, and when it does not have a negative impact on the data subject, the Society will set privacy settings to the most private by default.

International data transfers

No data may be transferred outside of the UK without the approval of the DPO. Specific consent must also be obtained from the data subject prior to transferring their data outside the UK.

Data audit and register

Regular data audits to manage and mitigate risks will inform the data register. The register contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant.

Reporting breaches

All members have an obligation to report actual or potential data protection compliance failures. This allows the Society to:

- Investigate the failure and take remedial steps if necessary
- Maintain a register compliance failures

Monitoring

All members must observe this policy. The DPO has overall responsibility for this policy and will monitor it regularly to make sure it is being adhered to.

Consequences of failing to comply

The Society takes compliance with this policy very seriously. Failure to comply puts both the members and the Society at risk.

The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under our procedures which may result in expulsion.

If you have any questions or concerns about anything in this policy, do not hesitate to contact the DPO

Monitoring and Reviewing

The Executive Committee shall review the effectiveness of this Policy on an annual basis and overall content at least every 3 years.

Approved by Executive Committee: [DATE]

Date of Next Review: