GDPR Data Protection Policy

1. Background

Farnham Angling Society adheres to the General Data Protection Regulation (GDPR), with respect to all information held about Members and Officers. The Society is a Data Controller and is registered with the Information Commissioner's Office - Registration Number A8395852.

The Data Protection Officer is Ian Gray and can be contacted via email at GDPR-DPO@farnhamanglingsociety.com

1.1. Definitions:

Automated Processing: any form of automated processing of Personal Data to evaluate certain personal aspects relating to an individual. E.g. Profiling is an example of Automated Processing. The Society does not process data in this way.

Consent: agreement which is freely given, specific, informed and unambiguous indication of the Data Subject's agreement to the processing of Personal Data relating to them.

Data Controller: the person or organisation that determines when, why and how to process Personal Data. It is responsible for establishing practices and policies in line with the GDPR. The Society is the Data Controller of all Personal Data relating to its Members and Officers.

Data Subject: a living, identified or identifiable individual about whom we hold Personal Data.

Data Processor: any person at the Society or a third-party nominated to act on behalf of the Society that is engaged in any activity that involves the use of Personal Data, for example collecting, storing, organising, amending, retrieving, disclosing, erasing or destroying it, or carrying out any operation on the data. Processing also includes transmitting or transferring Personal Data to third parties.

Data Privacy Impact Assessment (DPIA): tools and assessments used to identify and reduce risks of a data processing activity. DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or business change programs involving the Processing of Personal Data.

Data Protection Officer (DPO): the person with responsibility for data protection compliance.

EEA: the 28 countries in the EU, and Iceland, Liechtenstein and Norway.

Personal Data: any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Data includes Sensitive Personal Data and Pseudonymised Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Personal Data Breach: any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.

Privacy Notices: separate notices setting out information that may be provided to Data Subjects when the Society collects information about them.

Pseudonymisation: replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure. For example, Permit Number.

Sensitive Personal Data: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and Personal Data relating to breaches of Farnham Angling Society's byelaws or constitution.

2. Introduction

Farnham Angling Society needs to collect and process personal data about Members, Officers and sometimes their parents/guardians for various reasons including:

a) The recruitment and payment of contractors or volunteers
b) Member application and admission
c) The administration of newsletters, matches, teach-ins and exhibitions
d) Recording Members occupation of swims during bailiff rounds and conduct
e) Collecting fees
f) Keeping in touch with Members and Officers: Post, email and phone.
g) Complying with legal obligations to funding bodies and government including local government.

This Privacy Standard sets out how the Society handles the personal data of Members, Officers and other third parties. The Society recognises that the correct and lawful treatment of personal data and protecting the confidentiality and integrity of personal data is a critical responsibility that must be taken seriously at all times.

This Data Protection Policy applies to all personal data processed regardless of the media on which that data is stored or whether it relates to past or present Members, Officers, contacts, website users or any other Data Subject.

This Data Protection Policy sets out what is expected from Officers in order for the Society to comply with GDPR. Officers must read, understand and comply with this Data Protection Policy and complete training on its requirements. Compliance with this policy is mandatory and any breach may result in disciplinary action. All Senior Officers are responsible for ensuring Officers comply with this policy and need to implement appropriate practices, processes, controls and training to ensure such compliance.

This Data Protection Policy (together with related policies and guidance) is an internal document and cannot be shared outside the Society without prior authorisation from the Data Protection Officer (DPO).

The DPO is responsible for overseeing this Data Protection Policy and, as applicable, developing related policies and guidelines. Any questions about the operation of this policy or any concerns that this policy is not being followed should be forwarded to the DPO.

3. Personal Data Protection Principles

The Society adheres to the principles relating to processing of personal data set out in the GDPR which require personal data to be

a) Processed lawfully, fairly and in a transparent manner

b) Collected only for specified, explicit and legitimate purposes
c) Adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed
d) Accurate and where necessary kept up to date
e) Not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed
f) Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage
g) Not transferred to another country without appropriate safeguards being in place
h) Made available to Data Subjects and Data Subjects allowed to exercise certain rights in relation to their personal data

All Officers including Executive Committee members (responsible for Members and Officers data) are responsible for and must be able to demonstrate compliance with the data protection principles listed above.

3.1. Lawfulness, Fairness, Transparency

Personal data must be processed lawfully, fairly and in a transparent manner in relation to the Data Subject. Personal Data can only be collected, processed and shared lawfully and for specified purposes. The GDPR restricts actions regarding Personal Data to specified lawful purposes to ensure that processing of personal data is done fairly and without adversely affecting the Data Subject.

The GDPR allows processing for specific purposes:
a) the Data Subject has given his or her consent (not for 2018/19, but can address for 2019/20)
b) the processing is necessary for the performance of a contract with the Data Subject
c) to meet our legal compliance obligations
d) to protect the Data Subject's vital interests
e) to pursue our legitimate interests for purposes. The purposes for which the Society processes personal data for legitimate interests will be set out in applicable Privacy Notices.

3.2. Consent

A Data Subject consents to processing of their personal data if they indicate agreement clearly either by a statement or positive action to the processing. Consent must be freely given and requires affirmative action. Data Subjects are able to withdraw consent to processing at any time and withdrawal must be

actioned promptly. Consent may need to be refreshed if data is to be used for a different purpose which was not disclosed when the Data Subject first consented.

Explicit Consent is required for processing Sensitive Personal Data and the Privacy Notice identifying the Sensitive Personal Data and the purpose for collection must be issued to the Data Subject: the only thing I can think of is disability information including mental wellbeing.

Consent would also be required for Automated Decision-Making and for cross border data transfers, but these activities are not part of the Society's normal business and must not take place.

Any forms used to gather personal data must include a statement referring the individual to the Privacy Notice explaining the reasons for collecting the data. Evidence of consent must be recorded so that the Society can demonstrate compliance with consent requirements.

3.3. Transparency

The Society must provide detailed, specific information to Data Subjects on the information collected directly or from elsewhere. This information is provided in the Privacy Notices. The Privacy Notices must be presented to the Data Subject when he/she first provides the Personal Data. Therefore, it must be made available in the most relevant format e.g. web site, hyperlink or paper copy.

When Personal Data is collected indirectly from a third party, the Society must also check that the personal data was collected by the third party in accordance with the GDPR.

3.4. Specific Purpose

Personal data must be collected only for specified, explicit and legitimate purposes as stated in the Privacy Notices. It must not be further processed for new or different purposes from that indicated when it was first obtained unless the Data Subject is informed of the new purposes and they have consented where necessary.

3.5. Adequate

Personal data collected must be adequate and relevant for the intended purposes. Personal data must only be processed as part of the duties for which you are employed. You cannot process personal data for any reason unrelated to

those duties. Only the personal data that is required to fulfil these duties must be collected: do not collect excessive data. When personal data is no longer needed for the specified purposes, it must be deleted or anonymised in accordance with the Society's data retention guidelines.

3.6. Accuracy

Individuals who provide their personal data are responsible for ensuring that it is accurate and up-to-date. Any changes should be notified to the Society, and the Society will amend the records or correct any errors without delay.

3.7. Data Retention

Personal data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data was collected. The Society will maintain retention policies and procedures to ensure personal data is deleted after a reasonable time for the purposes for which it was being held, unless a law requires the data to be kept for a minimum time.
All reasonable steps must be taken to destroy or erase all personal data that is no longer required in accordance with all the Society's data retention guidelines. This includes requiring third parties to delete such data where applicable.
Data Subjects are informed of the period for which data is stored in the Privacy Notices.

3.8. Protecting Personal Data

Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful processing, and against accidental loss, destruction or damage. The Society implements and maintains appropriate safeguards to ensure security of personal data. These include:

a) keeping all physical records of personal data and minutes and papers distributed at those and associated meetings in a lockable office/house with key-controlled access
b) personal data held electronically is accessed by authorised staff only via a password protected account
c) placing any PCs or terminals, CCTV that show personal data so that they are not visible except to authorised staff.
d) ensuring that computers which left unattended are locked with a password.
e) data no longer required is disposed of / deleted / destroyed so that it is no longer readable or accessible.

All officers are responsible for protecting the personal data held by the Society. Officers must implement reasonable and appropriate security measures against unlawful or unauthorised access to or processing of personal data and against the accidental loss of, or damage to, personal data. Officers must exercise particular care in protecting Sensitive Personal Data from loss and unauthorised access, use or disclosure.

Officers must follow all procedures and technologies put in place by the Society to maintain the security of all personal data from the point of collection to the point of destruction. Officers must only transfer Personal Data to third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

Officers must maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

a) Confidentiality means that only people who have a need to know and are authorised to use the personal data can access it.
b) Integrity means that personal data is accurate and suitable for the purpose for which it is processed.
c) Availability means that only authorised users are able to access the personal data when they need it for authorised purposes.

Officers must comply with all applicable aspects of the IT Security and Acceptable Use Policy and comply with and not attempt to circumvent the administrative, physical and technical safeguards put in place to protect personal data. This includes working off-site.

3.9. Reporting A Personal Data Breach

The GDPR requires Data Controllers to notify a Personal Data Breach to the Information Commissioner's Office and, in certain instances, the Data Subject. The Society has put in place procedures to deal with any suspected Personal Data Breach and will notify Data Subjects or any applicable regulator where it is legally required to do so.

If you know or suspect that a Personal Data Breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the DPO. You should preserve all evidence relating to the potential Personal Data Breach.

3.10. Transfer Limitation

The GDPR restricts data transfers to countries outside the EEA in order to ensure that the level of data protection afforded to individuals by the GDPR is not undermined. The Society does not require any such transfers to be made in the course of its business, therefore, no member of Officers must transfer any data to countries outside of the EEA. Any requests to do so must be made to the DPO. Only transfers where the Data Subject has provided Explicit Consent to the proposed transfer will be considered.

4. Data Subject's Rights and Requests

Data Subjects have rights when it comes to how the Society handles their personal data. These include rights to:

a) withdraw consent to processing at any time; (How does this affect membership ? & monies received ?)
b) receive certain information about the Data Controller's Processing activities
c) request access to their personal data that the Society holds
d) prevent use of their personal data for direct marketing purposes
e) ask for their personal data to be erased if it is no longer necessary in relation to the purposes for which it was collected or processed or to rectify inaccurate data or to complete incomplete data
f) restrict processing in specific circumstances
g) challenge processing which has been justified on the basis of a legitimate interests or in the public interest
h) request a copy of an agreement under which personal data is transferred outside of the EEA
i) prevent processing that is likely to cause damage or distress to the Data Subject or anyone else
j) be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms
k) make a complaint to the ICO
l) ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format.

Officers must verify the identity of an individual requesting data under any of the rights listed. Officers must immediately forward any Data Subject request received to the DPO.

5. Accountability

The Society has implemented appropriate technical and organisational measures to ensure compliance with data protection principles and is required to demonstrate its compliance. Controls are in place to ensure and document GDPR compliance including:

a) appointment of a DPO and a Senior Officer accountable for data protection
b) integrating data protection into internal documents including this Data Protection Policy, Privacy Notices, Data Retention Guide
c) regular training for Officers on the GDPR, and data protection matters including, for example, Data Subject's rights, Consent, Legal basis, and Personal Data Breaches. The Society will maintain a record of training completed by Officers
d) regular testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort
e) implementing Privacy by Design when Processing Personal Data and completing Data Protection Impact Assessments where processing presents a high risk to rights and freedoms of Data Subjects.

5.1. Record Keeping

The GDPR requires the Society and all its officers to keep full and accurate records of all data Processing activities. Officers must keep and maintain accurate records reflecting the processing including records of Data Subjects' consents and procedures for obtaining consents.

6. Privacy by design and Data Protection Impact Assessment (DPIA)

The Society must consider Privacy by Design measures when processing personal data by implementing appropriate technical and organisational measures (like pseudonymisation) in an effective manner, to ensure compliance with data privacy principles. Officers should consider what Privacy by Design measures can be implemented to further improve effectiveness of data protection.

The Society must also conduct DPIAs in respect to high risk processing, for example when implementing a major system change program involving the processing of personal data including use of new technologies, use of Automated Processing or large-scale processing of sensitive data.

7. Automated Processing (Including Profiling) And Automated Decision-Making

Automated processing (including profiling) and automated decision making is not conducted at the Society as part of its usual business. A DPIA must be carried out before any Automated Processing (including profiling) or ADM activities are introduced.

8. Direct Marketing

The Society must abide by rules and privacy laws when marketing to customers. For example, a Data Subject's prior consent is required for electronic direct marketing (by email, text or automated calls). The right to object to direct marketing must be explicitly offered to the Data Subject in an intelligible manner so that it is clearly distinguishable from other information.

A Data Subject's objection to direct marketing must be promptly honoured. If a Data Subject opts out at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

9. Sharing Personal Data

The Society will only share Personal Data with specified third parties and will ensure that safeguards and contractual arrangements have been put in place.

Officers may only share the personal data we hold with another officer who needs to have access for Society business.

Officers may only share the personal data the Society holds with third parties, such as our service providers if:

a) they have a need to know the information for the purposes of providing the contracted services
b) sharing the Personal Data complies with the Privacy Notice provided to the Data Subject and, if required, the Data Subject's Consent has been obtained
c) the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place
d) the transfer complies with any applicable cross border transfer restrictions

e) a fully executed written contract that contains GDPR approved third party clauses has been obtained.

Officers must not disclose personal data with anyone unless it complies with the above.

The Society will not, under any circumstances, sell any of its databases to a third party.

10. Email

It is Society policy that senders and recipients of Society emails are made aware that the contents of emails may be disclosed in response to a request for information. Senders of Society emails are also made aware that under Regulation of Investigatory Powers Act 2000, Lawful Business Practice Regulations, any emails sent to or from the Society may be accessed by someone other than the recipient for system management and security purposes.

11. CCTV

CCTV operates within the Society (King's Pond) for the purposes of protecting fish stocks and property. The Society will only process personal data obtained by the CCTV system in accordance with Data Protection and Use of CCTV Policy.

12. Review of the Data Protection Policy and Further Information

This policy will be updated as necessary to reflect best practice or future amendments made to the General Data Protection Regulations.

Please follow this link to the Information Commissioner's Office website (www.ico.gov.uk) which provides further detailed guidance on a range of topics including individuals' rights, exemptions, dealing with subject access requests, how to handle requests from third parties for personal data to be disclosed etc. In particular, you may find it helpful to read the Guide to Data Protection which is available from the website.

Last Review: July 2018