Angling Trust/Fish Legal

PD17 – Data Protection Policy

DOCUMENT CONTROL	
Version Number	1.4
Document Author	Alistair Middleton
Lead Director	Simon Bourne
Review Frequency	Biennial
Next Review Date	Nov 2023
Purpose	The purpose of this policy is to ensure that our acquisition, retention andstorage of personal data is appropriate, secure and compliant with all relevant legislation, and to set out the requirements, procedures and protections for dealing with all personal and sensitive data.

REVISION HISTORY			
Version	**Date**	**Summary of Changes**	**Author**
1.1	Aug 2011		James Baldwin
1.2	July 2014		Bob Dyer
1.3	Sept 2018	Updated Act details and incl GDPR	Alistair Middleton
1.4	Sept 2019	Front sheet updated, font changed	Alistair Middleton
1.4	Nov 21	Reviewed – contact details and ICO website URL updated.	Alistair Middleton

Approvals		
Approved by: ATB/FLC/CEO/COO/GOV COMM	**Date**	**Version**
AT Board	Aug 2012	1.1
AT Board	July 2014	1.2
AT Board	July 2016	1.2
At Board	Nov 2018	1.3

Distribution				
Audience	**Method**	**By whom**	**Date of issue**	**Version**
Staff, Directors Volunteers	Email		Nov 2021	1.4

Table of Contents

1. POLICY STATEMENT

1.1 Everyone has rights with regard to how their personal information is handled. During the course of our activities we will collect, store and process personal information about our staff, Volunteers, current and past members, partners, stakeholders, suppliers and we recognise the need to treat it in an appropriate and lawful manner. Under Article 5 of GDPR we must use data fairly, lawfully and transparently.

1.2 The types of information that we may be required to handle include details of current, past and prospective employees, suppliers, members (including juniors), angling coaches and others that we communicate with. The information, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the Data Protection Act. Note: - the original 1998 act has now been superseded by the Data Protection Act 2018 (DPA 2018) on the 23rd of May 2018. The DPA 2018 supplements the EU General Data Protection Regulation (GDPR), which came into effect on 25 May 2018. The GDPR regulates the collection, storage, and use of personal data significantly in a stricter manner.

1.3 This policy does not form part of any employee's contract of employment, board members' service agreement or volunteer's agreement and may be amended at any time. Any breach of this policy will be taken seriously and may result in disciplinary action.

1.4 Training will be provided to all staff, board members and key volunteers. For those individuals who have access to the membership database, the training will cover the storage, retention and deletion of data.

2. STATUS OF THE POLICY

2.1 This policy has been approved by the Board. It sets out our rules on data protection and the legal conditions that must be satisfied in relation to the obtaining, handling, processing, storage, transportation and destruction of personal information.

2.2 Our board of directors (the board) have overall responsibility for the effective operation of this policy. A designated Board Member is identified to have oversight responsibility for the Policy on behalf of the board. The board has delegated day-to-day responsibility for operating the policy and ensuring its maintenance and review to the Chief Executive. That post is held by Jamie Cook 07572 231329 jamie.cook@anglingtrust.net Any questions or concerns about the operation of this policy should be referred in the first instance to the Chief Executive.

2.3 If you consider that the policy has not been followed in respect of personal data about yourself or others you should raise the matter with your line manager or the Chief Executive.

3. DEFINITION OF DATA PROTECTION TERMS

3.1 **Data** is information which is stored electronically, on a computer, or in certain paper-based filing systems.

3.2 **Data subjects** for the purpose of this policy include all living individuals about whom we hold personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal data.

3.3 **Personal data** means data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual (such as a name, address or date of birth) or it can be an opinion (such as a performance appraisal).

3.4 **Data controllers** are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They have a responsibility to establish practices and policies in line with the Act. We are the data controller of all personal data used in our business.

3.5 **Data users** include employees whose work involves using personal data. Data users have a duty to protect the information they handle by following our data protection and security policies at all times.

3.6 **Data processors** include any person who processes personal data on behalf of a data controller. Employees of data controllers are excluded from this definition but it could include suppliers which handle personal data on our behalf.

3.7 **Processing** is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

3.8 **Sensitive personal data** includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Sensitive personal data can only be processed under strict conditions and will usually require the express consent of the person concerned.

3.9 **Privacy notice** is the way in which we tell our customers (other data subjects) about how we use their data. This could be an online privacy policy or notice on a website, a paragraph about how your information is used in your pension documents, or even giving our customers/members information over the phone about calls being recorded. GDPR specifically states that under its articles *13 and 14* customers have the right to be informed about how their data is used.

4. DATA PROTECTION PRINCIPLES

Anyone processing personal data must comply with the eight enforceable principles of good practice. These provide that personal data must be:

(a) Processed fairly and lawfully.
(b) Processed for limited purposes and in an appropriate way.
(c) Adequate, relevant and not excessive for the purpose.
(d) Accurate.
(e) Not kept longer than necessary for the purpose.
(f) Processed in line with data subjects' rights.
(g) Secure.
(h) Not transferred to people or organisations situated in countries without adequate protection.

5. Fair And Lawful Processing

5.1 The Act is intended not to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject. The data subject must be told who the data controller is the purpose for which the data is to be processed by us, and the identities of anyone to whom the data may be disclosed or transferred.

5.2 For personal data to be processed lawfully, certain conditions have to be met. These may include, among other things, requirements that the data subject has consented to the processing, or that the processing is necessary for the legitimate interest of the data controller or the party to whom the data is disclosed. When sensitive personal data is being processed, more than one condition must be met. In most cases the data subject's explicit consent to the processing of such data will be required.

6. Processing For Limited Purposes

Personal data may be processed for the specific purposes notified to the data subject when the data was first collected or for any other purposes specifically permitted by the Act. This means that personal data must not be collected for one purpose and then used for another. If it becomes necessary to change the purpose for which the data is processed, the data subject must be informed of the new purpose before any processing occurs.

7. Adequate, Relevant And Non-Excessive Processing

Personal data should only be collected to the extent that it is required for the specific purpose notified to the data subject. Any data which is not necessary for that purpose should not be collected in the first place.

8. Accurate Data

Personal data must be accurate and kept up to date. Information which is incorrect or misleading is not accurate and steps should therefore be taken to check the accuracy of any personal data at the point of collection and at regular intervals afterwards. Inaccurate or out-of-date data should be destroyed.

9. Timely Processing

Personal data should not be kept longer than is necessary for the purpose. This means that data should be destroyed or erased from our systems when it is no longer required. For guidance on how long certain data is likely to be kept before being destroyed, contact the Chief Executive.

10. Processing In Line With Data Subject's Rights

Data must be processed in line with data subjects' rights. Data subjects have a right to:

(a) Request access to any data held about them by a data controller.
(b) Prevent the processing of their data for direct-marketing purposes.
(c) Ask to have inaccurate data amended.
(d) Prevent processing that is likely to cause damage or distress to themselves or anyone else.

11. DATA SECURITY

11.1 We must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. Data subjects may apply to the courts for compensation if they have suffered damage from such a loss.

11.2 The Act requires us to put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data may only be transferred to a third-party data processor if he agrees to comply with those procedures and policies, or if he puts in place adequate measures himself.

11.3 Maintaining data security means guaranteeing the confidentiality, integrity and availability of the personal data, defined as follows:

(a) **Confidentiality** means that only people who are authorised to use the data can access it.
(b) **Integrity** means that personal data should be accurate and suitable for the purpose for which it is processed.
(c) **Availability** means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on our central computer system instead of individual PCs.

11.4 Security procedures include:

(a) **Entry controls.** Any stranger seen in entry-controlled areas should be reported.
(b) **Secure lockable desks and cupboards.** Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)
(c) **Methods of disposal.** Paper documents should be shredded. Storage media and CD-ROMs should be physically destroyed when they are no longer required.
(d) **Equipment.** Data users should ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC/ mobile device when it is left unattended.

12. DEALING WITH SUBJECT ACCESS REQUESTS

A formal request from a data subject for information that we hold about them must be made in writing. A fee is payable by the data subject for provision of this information. Any member of staff who receives a written request should forward it to their line manager OR the Chief Executive immediately.

13. PROVIDING INFORMATION OVER THE TELEPHONE

Any member of staff dealing with telephone enquiries should be careful about disclosing any personal information held by us. In particular they should:

(a) Check the caller's identity to make sure that information is only given to a person who is entitled to it.

(b) Suggest that the caller put their request in writing if they are not sure about the caller's identity and where their identity cannot be checked.

(c) Refer to their line manager or the Chief Executive for assistance in difficult situations. No-one should be bullied into disclosing personal information.

14. GDPR

GDPR (General Data Protection Regulation) is applicable from the 22nd of May 2018. It applies to both Data Controllers and Data processors, although applies to them in different ways. This has brought in a number of changes (the last time a major change to EU data privacy law since 1995). GDPR puts stringent rules on the increasingly sophisticated data processing that organisations carry out across the globe. Penalties (Article 83) would be 2% of global annual turnover for an organisation such as AT.

In relation to data protection AT will be compliant with the regulation. In particular the following Articles: -

(a) Article 3 – who does it apply to? and where does it apply?
(b) Article 4 – Data processors
(c) Articles 12-23 - Data rights
(d) Article 33 - Breach Notification
(e) Article 37 – Data protection officers
(f) Article 22 - Automated decision making
(h) Article 35 – Risk Assessments
(i) Article 5 – Records
(j) Article 4 – Pseudonymisation and Anonymization

15. MONITORING AND REVIEW OF THE POLICY

15.1 This policy is reviewed annually by our board of directors and the Business and IT manager

15.2 We will continue to review regularly the effectiveness of this policy to ensure it is achieving its stated objectives.

Data Protection Statement

Angling Trust is registered to collect data in accordance with the principles of the Data Protection Act 2018.

Data Controller Name: **Angling Trust**
Registration Number: Z1580725

Data Protection Principles
There are eight principles put in place by the Data Protection Act 2018 to make sure that information is handled properly.

These state that data must be:

1. fairly and lawfully processed
2. processed for limited purposes
3. adequate, relevant and not excessive
4. accurate
5. not kept for longer than is necessary
6. processed in line with your rights
7. secure
8. not transferred to countries without adequate protection.

By law data controllers have to keep to these principles.

If you require further information visit the Information Commissioner's Office Website: https://ico.org.uk/