Angling Trust/Fish Legal

PD17 – Data Protection Policy

DOCUMENT CONTROL	
Version Number	1.5
Document Owner	Karen Watkinson/Various
Lead Director or CEO	Jamie Cook
Review Frequency	Biennial
Next Review Date	Apr 25

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 2021	Reviewed – contact details and ICO website URL changed	Alistair Mddleton
1.5	Apr 2023	Subject Access Request detail added	Sue Woollard

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

Distribution				
Audience	Method	By whom	Date of issue	Version
Staff, Directors, Volunteers	SharePoint	Gov Assistant	Apr 23	1.3

Legislation Reference within Document
Data Protection Act 2018 (DPA 2018), EU General Data Protection Regulation (GDPR)

Contents

1. POLICY STATEMENT 4
2. STATUS OF THE POLICY 4
3. DEFINITION OF DATA PROTECTION TERMS 4
4. DATA PROTECTION PRINCIPLES 5
5. FAIR AND LAWFUL PROCESSING 6
6. PROCESSING FOR LIMITED PURPOSES 6
7. ADEQUATE, RELEVANT AND NON-EXCESSIVE PROCESSING 6
8. ACCURATE DATA 6
9. TIMELY PROCESSING 6
10. PROCESSING IN LINE WITH DATA SUBJECT'S RIGHTS 6
11. DATA SECURITY 7
12. DEALING WITH SUBJECT ACCESS REQUESTS 7
13. PROVIDING INFORMATION OVER THE TELEPHONE 8
14. GDPR 8
15. MONITORING AND REVIEW OF THE POLICY 8
DATA PROTECTION STATEMENT – ANGLING TRUST 9
DATA PROTECTION STATEMENT – FISH LEGAL 10
APPENDIX 1 11

1. POLICY STATEMENT

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.

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 Note: - the original 1998 act has now been superseded by the Data Protection Act 2018 (DPA 2018) on the 23rd of May 2018.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.

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.

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

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.

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.

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

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

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.

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).

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.

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.

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.

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.

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.

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

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.

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

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.

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.

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.

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 may be 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. The request must be dealt with within one month of the request date. Please see appendix 1 and visit the ICO website for further information on how to correctly deal with a Subject Access Request. https://ico.org.uk/

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
g) Article 35 – Risk Assessments
h) Article 5 – Records
i) Article 4 – Pseudonymisation and Anonymization

15. MONITORING AND REVIEW OF THE POLICY

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

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

DATA PROTECTION STATEMENT – ANGLING TRUST

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:

a) fairly and lawfully processed
b) processed for limited purposes
c) adequate, relevant and not excessive
d) accurate
e) not kept for longer than is necessary
f) processed in line with your rights
g) secure
h) 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/

DATA PROTECTION STATEMENT – FISH LEGAL

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

Data Controller Name: **Fish Legal**

Registration Number: Z6347283

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:

i) fairly and lawfully processed
j) processed for limited purposes
k) adequate, relevant and not excessive
l) accurate
m) not kept for longer than is necessary
n) processed in line with your rights
o) secure
p) 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/

APPENDIX 1

SARs QUICK GUIDE

ICO website: https://ico.org.uk/

Consult the ICO website for further information and more information on dealing with Subject Access Requests.

CONSIDER THE REQUEST

Make sure you check the ID of the requester. This should not be formal ID but maybe in the form of questions about membership or significant dates that only the requester would know. Do not ask for photo ID if you have never met the requester. The ID asked for should be relevant and proportional.

Check that the request is valid – does the subject have a right to the information. If they are requesting information on another person, do they have written authority to act on behalf of that person or a document showing power of attorney?

Children over 12 can make their own request. If you are asked by a parent you should get the child's consent if they are over 12.

REMINDERS

- You have 1 month from the date of the request. If you need to check validity first, you can start the clock from one month once you have ascertained validity.
- If you receive a request on a non working day, you still have one month from that date.
- If the due date falls on a weekend, you can move the due date to the next working day.
- You cannot add extra days when the month is shorter eg February.
- TIP – set a reminder for 28 days from the request date to be sure you will be on time!
- If it is a very complex request, you can take up to 2 months but you must inform the subject that there is a delay before the end of the first calendar month.

WHAT HAVE THEY ASKED TO SEE?

If you have the request in writing, check to make sure you understand what is being asked for. They may only want information on one event rather than everything you have.

SEARCH

Search for the information using all of the search tools available to you and in all areas that we hold information. Consider files, external hard drives, tablets, phones, portable memory sticks, call recordings, social media posts and CCTV. Anything that is possible should be checked until you are satisfied you have searched all areas.

REDACT

You MUST check all information and check that the requester is entitled to have that information. Anything relating to people other than the subject must be redacted. One way is to copy and paste relevant information only to a new document. Another way is to black out the information using redacting pens. Beware of ordinary markers as information can sometimes still be seen from the reverse of the document.

If you redact using software, make sure it is saved to a new copy and protected from editing to avoid anyone being able to remove your redacting.

There may be occasion on which the information may indirectly identify someone else. In this case, you would need to consider the impact of that and weigh up the right to information against the impact of them being able to identify someone else. See case study below:

For example, Samira is an employee who has made a SAR for her personnel file. In her file is a complaint a colleague, Tom, made about Samira. Although the information in the complaint is about Samira, if you release it to her, it might identify Tom. You need to weigh up Samira's right to her personal data, against giving out information about Tom without good reason.

There are three options here:

1. If Samira knows all about the complaint, what was said and who said it; you could give her the information as it is, without redacting Tom's details.
2. If Samira doesn't know about the complaint and wouldn't guess that it came from Tom, you could supply the details of the complaint, but redact Tom's name or any other identifying information.
3. If Samira doesn't know about the complaint but would guess that it came from Tom, whether his details were redacted or not; you may need to consider whether it's necessary to get Tom's consent.

It's a balancing act between making sure Samira is given the data she's entitled to, and not disclosing Tom's details if you don't have to.

If you think releasing the information to Samira may mean that there would be a negative impact on Tom, then you could consider withholding this piece of information altogether. If you do this, you should make a note of why you withheld it.

If in doubt – contact the ICO for advice.

REPLY

If you received a SAR by email, you can reply by email unless the requester said otherwise. Check what format they would like to receive the information and keep a record of what was sent and when. Keep a dated record and also keep a record of any responses.

FEE

In most circumstances, you CANNOT charge a fee. Only if the request is considered excessive or is a repeat request after a previous request then you can charge a fee that is reasonable and for admin costs (this is usually quite low).

If you decide to charge a fee, you must let the requester know asap and you can then wait until the fee is paid.

REFUSAL

You have to respond within one month even if that response is to refuse the request (for which you would need valid and solid reasons).

You are unlikely to be able to refuse a request but if you do, you will need to provide the reasons for refusal AND be able to justify those reasons. If you wish to refuse, seek advice and be sure you are correct in your decision to refuse.

You do not have to comply if someone is seeking information about someone who has died. Data Protection laws apply to living people. Likewise, if the person dies before you respond, you no longer have to complete the request. Information on dead people can be sought in certain circumstances but is more likely to be information such as medical records etc.