RYTON AND DISTRICT ANGLING CLUB:

FAIR PROCESSING NOTICE

(MEMBER'S DATA)

Contents

1. ABOUT THIS DOCUMENT

1.1 During the course of our activities we, Ryton and District Angling Club, will process personal data (which may be held on paper, electronically, or otherwise) we recognise the need to treat it in an appropriate and lawful manner, in accordance with the Data Protection Act 2018 (DPA)/GDPR. The purpose of this notice is to make you aware of how we will handle your personal data.

2. DATA PROTECTION PRINCIPLES

2.1 We will comply with the six data protection principles, in Article 5 of the GDPR requires that personal data must be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organizational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures."

2.2 "Personal data" means recorded information we hold about you from which you can be identified. It may include: Your name, Your Address Telephone & e-mail addresses, other personal information.

2.3 "Processing" means doing anything with the data, such as accessing, disclosing, destroying or using the data in any way.

3. FAIR AND LAWFUL PROCESSING

We will usually only process your personal data where you have given your consent to Ryton and District Angling Club directly, to comply with our legal obligations.

4. HOW WE ARE LIKELY TO USE YOUR PERSONAL DATA

We will process your data solely for the purpose of payment and delivery of Membership Cards ordered directly. We will not use your data for any marketing purposes or sell any of your data to any third parties. We will keep your name and address and details for Annual Renewal of membership purposes only.

5. PROCESSING FOR LIMITED PURPOSES

We will only process your personal data for the specific purpose or purposes notified to you or for any other purposes specifically permitted by the DPA/GDPR.

6. ADEQUATE, RELEVANT AND NON-EXCESSIVE PROCESSING

Your personal data will only be processed to the extent that it is necessary for the specific purposes notified to you.

7. ACCURATE DATA

We will keep the personal data we store about you accurate and up to date. Data that is inaccurate or out of date will be destroyed. Please notify us if your personal details change or if you become aware of any inaccuracies in the personal data we hold about you.

8. DATA RETENTION

We will not keep your personal data for longer than is necessary for the purpose. This means that data will 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: Mr. Derick Dodds, by Email: derickdodds1966@hotmail.com

PROCESSING IN LINE WITH YOUR RIGHTS

You have the right to:

(a) Request access to any personal data we hold about you.

(b) Prevent the processing of your data for direct-marketing purposes.

(c) Ask to have inaccurate data held about you amended.

(d) Prevent processing that is likely to cause unwarranted substantial damage or distress to you or anyone else.

(e) Object to any decision that significantly affects you being taken solely by a computer or other automated process.

10. DATA SECURITY

10.1 We will ensure that appropriate measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

10.2 We have in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. We will only transfer personal data to a third party if they agree to comply with those procedures and policies, or if they put in place adequate measures themselves.

10.3 Maintaining data security means guaranteeing the confidentiality, integrity and availability (for authorised purposes) of the personal data.

11. PROVIDING INFORMATION TO THIRD PARTIES

We use third parties to carry out certain activities on our behalf. Examples include sending postal mail packages, processing Cheque payments, These third parties have access to personal information needed to perform their functions, but may not use it for other purposes.

12. SUBJECT ACCESS REQUESTS

If you wish to know what personal data we hold about you, you must make the request in writing. All such written requests should be forwarded to: Mr Derick Dodds, Data Protection Representative, Ryton and District Angling Club. On the attached form and the address indicated.

Pre Audit Questionnaire

Ryton and District Angling Club - Pre-Audit Questionnaire

To be completed by a person responsible for Ryton and District Angling Club.

Please focus on your area of the business.

Question	Comment
"Personal data" is any information which relates to a living individual (the "data subject") who can be identified from it (including where such identification is only possible with further information also in/likely to come into the possession of [*xx*]. "Sensitive personal data" is a type of personal data regarding a data subject's racial/ethnic origin, political opinions, religious beliefs, trade union membership, medical health, sexual life or committed/alleged offences.	
Does your department hold personal data? (e.g. HR records, customer or member records etc.)	
Describe all the methods by which the department collects personal data? (e.g. directly or indirectly from a client/employee, via website/email/telephone/letter or bought in databases)	
What types of personal information does the department collect? (e.g. name, address, telephone number)	
Does the department collect special category/criminal personal data? What types of special category/criminal personal data does it collect?	
If applicable, describe all the methods by which the department collects sensitive personal data? (e.g. directly or indirectly from a customer/employee, via website/email/telephone/letter or bought in databases)	

Have you ever received a subject access request (this where an individual asks for a copy of his or her personal data)? If yes, what did you do?	
Do you store personal data within your department? Is it stored electronically, in paper form or otherwise?	
If you use paper files please describe the storage system	
Who has access to personal data within your department? Do all individuals have the same rights of access? If not, how are access rights decided/monitored?	
How does the department use the personal data it holds? (i.e. describe the ways you process or use personal data?)	
How does the department use any special category/criminal personal data it holds?	
Who authorises your use of personal data?	
How long does the department typically keep different types of personal data and how is the data destroyed or deleted? Do you have a data retention policy?	

Does the department use third parties to process data for it (e.g. outsourcing)? If so, who does it use and how long has that contractor been used? Where does the third party process and store the data?	
Does the department share data with third parties (such as group companies, partner organisations, sponsors)? If so, who and why?	
Is there an agreement in place governing the data processing/sharing activities? If so, please provide copies	
In what circumstances (if any) does the department notify or collect consent from individuals when processing their data?	
What marketing activities does the department get involved in which involve the use of personal data?	
What steps are taken to keep the personal data accurate? How often are these steps taken?	
Describe security procedures within your department/team/office to keep data secure. This should include physical and technical security.	

How is personal data transferred between group companies and third parties (i.e e-mails, hard copy paper databases, access to central database, CD Rom etc)?	
What security measures are used in transferring the files (e.g. limited access rights, encryption, password protection or other measures)?	
Does the department send personal data outside of the EEA? If so, detail what data is sent, where it is sent and for what purpose?	
Does the department record conversations with its clients/customers and/or candidates? Is CCTV used by your department? If yes, describe.	
How long do you keep information in your department before it is destroyed or archived?	
Describe the destruction process including whether a third party is used to destroy information and any process they follow.	
Describe the archive process for old files.	
Do you know who to refer data protection questions to?	

Have you ever received any data protection training (either at [ ] or elsewhere)? Has a log been kept of that training?	
Do you expect there to be any changes in the way your department processes personal data in the next 12 months? Please describe	

Legitimate Interest Questionnaire

Legitimate Interest Questionnaire

A) IDENTIFYING A LEGITIMATE INTEREST

	Question	Answer	Guidance
1	What is the purpose of the processing operation		The first stage is to identify to a Legitimate Interest – what is the purpose for processing the personal data?
2	Is the processing necessary to meet one or more specific organisational objectives?		If the processing operation is required to achieve a lawful business objective, then it is likely to be legitimate for the purposes of this assessment.
3	Is the processing necessary to meet one or more specific objectives of any Third Party?		While you may only need to identify one Legitimate Interest for the purposes of an LIA – the interest that you are seeking to rely on - it may be useful to list all apparent interests in the processing, those of you as the Controller, as well as those of any Third Party who are likely to have a Legitimate Interest.
4	Does the GDPR, ePrivacy Regulation or other national legislation specifically identify the processing activity as being a legitimate activity, subject to the completion of a balancing test and positive outcome?		For example: Legitimate Interests might be relied onwhere an individual's (including client or employee) information is processed by a group of companies for the purposes of administration (Recital 48). If the Controller isprocessing sensitive Personal Data in the employee context, then they may be able to rely on Article 9(2) (b).

B) THE NECESSITY TEST

	Question	Answer	Guidance
1	Why is the processing activity important to the Controller?		A Legitimate Interest may be elective or business critical;however, even if the Controller's interest in processingpersonal data for a specific purpose is obvious andlegitimate, based on the objectives of the Controller, itmust be a clearly articulated and communicated to the individual.
2	Why is the processing activity important to other parties the data may be disclosed to, if applicable?		A Legitimate Interest could be trivial or business critical, however, the organisation needs to be able to clearly explain what it is. Some purposes will be compelling and lend greater weight to the positive side of the balance, while others may be ancillary and may have less weight in a balancing test. Consider whether your interests relate to a fundamental right, a public interest or another type of interest. Just because the processing is central to what the organisation does, does not make it legitimate. It is the reason for the processing balanced against the potential impact on an individual's rights that is key. It is important to consider whose Legitimate Interests are being relied on. Understanding this will help inform the context of the processing. In combination with the reason the Personal Data is being processed, this information will determine the weight of the Legitimate Interest that needs to be balanced.
3	Is there another way of achieving the objective?		• If there isn't, then clearly the processing is necessary;or• If there is another way but it would requiredisproportionate effort, then the processing is stillnecessary; or• If there are muitiple ways of achieving the objective,then a Privacy Impact Assessment should haveidentified the least intrusive means of processing thedata which would be necessary; or• If the processing is not necessary (It is unlikely thatthere will be many scenarios where a processingoperation is not necessary where it has been identifiedas being a means to achieve a stated businessobjective), then Legitimate Interests cannot be reliedon as a lawful basis for that processing activity

C) THE BALANCING TEST

	Question	Answer	Guidance
1	Would the individual expect the processing activity to take place?		If individuals would expect the processing to take place then the impact on the individual is likely to have already considered by them and accepted. If they have no expectation, then the impact is greater and is given more weight in the balancing test.
2	Does the processing add value to a product or service that the individual uses?		
3	Is the processing likely to negatively impact the individual's rights?		
4	Is the processing likely to result in unwarranted harm or distress to the individual?		
5	Would there be a prejudice to Data Controller if processing does not happen?		
6	Would there be a prejudice to the Third Party if processing does not happen?		
7	Is the processing in the interests of the individual whose personal data it relates to?		
8	Are the legitimate interests of the individual aligned with the party looking to rely on their legitimate interests forthe processing?		What are the benefits to the individual or society? If the processing is to the benefit of the individual, then itis more likely that Legitimate Interests can be relied on, as the individual's interests will be aligned with those of the Controller. Where the processing is more closely aligned with the interests of the Controller or a Third Party, than with those of the individual, it is less likely that the interests will be balanced and greater emphasis needs to be placed on the context of the processing and relationship with the individual.
9	What is the connection between theindividual and the organisation?		• Existing customer • Lapsed/cancelled customer • Employee or contractor • Business client • Prospect (never purchasedgoods or services) •Supplier • None of above
10	What is the nature of the data to beprocessed? Does data of this nature have any special protections under GDPR?		Data relating to a child etc. If processing Special Categories of Personal Data, an Article 9 condition must be identified as the lawful basis of processing.
11	Is there a two-way relationship in place between the organisation and the individual whose personal information is going to be processed? If so how close is that relationship?	• Ongoing• Periodic• One-offNo relationship, or relationship has effectively ceased	Where there is an on going relationship, or indeed a more formal relationship, there may well be a greater expectation on the part of the individual that their information will be processed by the organisation. The opposite is also possible but it does depend on the purpose of processing.
12	Would the processing limit or undermine the rights of individuals?		If processing would undermine or frustrate the ability to exercise those rights in future that might well affect the balance.
13	Has the personal information been obtained directly from the individual, or obtained indirectly?	• Directly• Indirectly• A mix of both	If the information was obtained directly from the individual then you should take due consideration of the notice offair processing (e.g. your Privacy Notice), the relationship with the individual and their expectations of use. If the data was collected directly and these factors are positive, then it may help to tip the balance in favour of the processing operation. Where Personal Data is not collected directly,there may need to be a more compelling Legitimate Interest to overcome this. It will also depend on the context of the processing and if the organisation has a two-way relationship with the individual.
14	Is there any imbalance in who holds the power between the organisation and the individual?		Does the individual have a choice regarding the processing of their personal information? If the organisation has a dominant position, this will tip the balance slightly against the use of Legitimate Interests. That said, the rights and freedoms of individuals laid down in the GDPR go someway to redressing this issue. The Controller will need to consider how it addresses any imbalance of power to ensure individuals' rights are not impacted.

	Question	Answer	Guidance
15	Is it likely that the individual may expect their information to be used for this purpose?	• Yes• No• Not sure	Given the relationship between the parties, services/products being provided, including the information notices available, would the individual reasonably expect or anticipate that their information would be used for those or connected purposes? The stronger the expectation, the greater the chances that Legitimate Interests can be relied on.
16	Could the processing be considered intrusive or inappropriate? In particular,could it be perceived as such by the individual or in the context of the relationship?		Processing should not be unwarranted - intrusion into the private life of an individual may be justified based onthe nature of the relationship or special circumstances. However, the greater the intrusion, perceived or otherwise, the more overwhelming the Legitimate Interest should be and the more the rights of the individual must be considered within the balance. Consider here the way the data is processed (e.g. large scale, data mining, profiling, disclosure to a large number of people or publication).
17	Is a fair processing notice provided to the individual, if so, how? Are they sufficiently clear and up front regarding the purposes of the processing?		Remember that the more unusual, unexpected or intrusive the processing, the greater the importance of making the individual aware of the processing. Particularly where Legitimate Interests are to be relied on.
18	Can the individual, whose data is being processed, control the processing activity or object to it easily?	• Yes (cover how you do this in thenext section on "Mitigation andCompensating Controls") • No • Partly Explain!	Giving the individual increased control or elements of control may help a Controller rely on Legitimate Interests where otherwise they could not. If individual control is not possible or not appropriate, explain why.
19	Can the scope of the processing be modified to reduce/mitigate any underlying privacy risks or harms?	• Yes (cover how you intend to do this in the next section"Mitigation and CompensatingControls")	This is a similar concept to a Data Protection Impact Assessment. Where a DPIA might identify potential privacy harms it also allows the organisation to mitigate the risk of non-compliance by adapting or altering the scope of the activity. The same is true for an LIA. If you conclude that the processing presents a privacy risk to the individual, the processing can be limited or adapted to reduce the potential impact.

D) SAFEGUARDS AND COMPENSATING CONTROLS

Safeguards and Compensating Controls Safeguards include a range of compensating controls or measures which may be put in place to protect the individual, or to reduce any risks or potentially negative impacts of processing. These are likely to have been identified via a Privacy Impact Assessment conducted in relation to the proposed activity. For example: dataminimisation, de-identification, technical and organisational measures, privacy by design, adding extra transparency, additional layers of encryption, multi-factor authentication, retention, restricted access, opt-outoptions. , hashing, salting, and other technical security methods used to protect data.

E) REACHING A DECISION AND DOCUMENTING THE OUTCOME

Using the responses above now document if you believe you are able to rely on Legitimate Interests for the processing operation. Please explain, perhaps using bullet points, why you are, or are not, able to rely on this legalbasis. You should draw on the answers you have provided in this LIA.

Outcome of Assessment:

Signed by:	Role:
Dated:	
Review date:	

Ryton and District Angling Club:

Personal Data and Record Retention Policy:

1. Principles:

Ryton and District Angling Club recognises the importance of effective file keeping records and data management. This requires a data and record retention policy. To comply with the principles of the Data Protection Act, records containing personal data must be:

- Stored appropriately having regard to the sensitivity and confidentiality of the material recorded
- Retained for only as long as necessary
- Disposed of securely to prevent them falling into the hands of any unauthorised person.

This guidance is in accordance with Ryton and District Angling Club's Data Protection Policy.

2. Scope:

The policy applies to all Ryton and District Angling Club's information, irrespective of the data location or the type of device it resides on or paper copy. It should be used by all committee members who interact with information held by Ryton and District Angling Club.

Any information/documents we have should be held for the appropriate time period of that document then disposed of securely via a secure shredding device.

Any Legal or contractual stipulations over Information held by Ryton and District Angling Club take precedence over this Standard. IE: If the data is required for a court case then that data needs to be kept longer than the recommended guidance.

3. Assumptions:

Committee members of Ryton and District Angling Club are expected to follow and conform to the guidance contained in this document. The legal definitions laid out in the Data Protection Act continue to be relevant and require the currently understood levels of protection.

4 Responsibilities: Storage of Data & Records Statement:

All committee members are responsible for any documents that they generate regardless of the classification. All data and records should be stored as securely as possible in order to avoid potential misuse or loss. All data and records will be stored in the most convenient and appropriate location having regard to the period of retention required and the frequency with which access will be made to the record.

- Data and records which are active should be stored in the most appropriate place for their purpose.
- Data and records which are no longer active, due to their age or subject, should be stored in the most appropriate place for their purpose.
- The degree of security required for file storage will reflect the sensitivity and confidential nature of any material recorded.
- Any data file or record which contains personal data of any form can be considered as confidential in nature.

5 Retention Statement:

Data and records should not be kept for longer than is necessary. This principle finds statutory form in the Data Protection Act 1998 and introduction of GDPR in 2018, which requires that personal data processed for any purpose "shall not be kept for longer than is necessary for that purpose".

No data file or record should be retained for more than five years after it is closed unless a good reason for longer retention can be demonstrated. It is to be emphasised that the period of five years is a maximum period. It may well be appropriate having regard to the nature of the record to opt for a shorter period. Reasons for longer retention will include the following: The record contains information relevant to legal action which has been started or is in contemplation

Whenever there is a possibility of litigation, the records and information that are likely to be affected should not be amended or disposed of until the threat of litigation has been removed

6 Destruction and Disposal Statement:

All information of a confidential or sensitive nature on paper or electronic media must be securely destroyed when it is no longer required. This ensures compliance with the Data Protection Act 1998 and GDPR 2018 and the duty of confidentiality we owe to our members.

7 Destruction and Disposal Procedures:

All information, in any format, destroyed from any location must have due regard to confidentiality of our members. When records or data files are identified for disposal in the Policy are destroyed, a register of such records needs to be kept. The procedure for the destruction of Confidential or Sensitive Waste on paper, card as follows:

All office quality white or coloured paper should be mechanically shredded or a contracted shredding service must be used.

The procedure for the destruction of Confidential or Sensitive Waste on electronic media such as tape, disk, cassette/cartridge, hard drives, CD-Rom, DVD and ZIP drive is as follows:

Media that are being destroyed because they are showing signs of damage or are obsolete should be physically destroyed by being cut into pieces or other ways prior to disposal

i. Review

This policy will be reviewed periodically to take into account of any changes in law and guidance issued by the government.

9 Disciplinary Consequences of this policy

Unlawful obtaining or disclosure of personal data (including the transfer of personal data outside the EEA in contravention of the above) or any other breach of the Data Protection Act 1998 (Revised 2013) and GDPR 2018 or any failure to report a breach of the Act. Will be treated seriously by Bemodern Ltd and may result in disciplinary action.

Signed .....

Mr. Derick Dodds
Data Protection representative
Reviewed: 08/01/2018
Updated: 26/09/2018