Data Protection & Privacy Policy (2019)

Ryston Runners AC is committed to complying with data protection law and to respecting the privacy rights of individuals. The policy applies to all of our volunteers and members.

This Data Protection Policy sets out our approach to data protection law and the principles that we will apply to our processing of personal data. The aim of this Policy is to ensure that we process personal data in accordance with the law and with the utmost care and respect.

WHO IS RESPONSIBLE FOR DATA PROTECTION?

All our members and volunteers are responsible for data protection, and each person has their role to play to make sure that we are compliant with data protection laws.

The membership secretary is our designated Data Protection Officer (DPO), who oversees our compliance with data protection laws.].

WHY DO WE HAVE A DATA PROTECTION POLICY?

We recognise that processing of individuals' personal data in a careful and respectful manner cultivates trusting relationships with those individuals and trust in our brand/club. We believe that such relationships will enable our organisation to work more effectively with and to provide a better service to those individuals.

STATUS OF THIS POLICY AND THE IMPLICATIONS OF BREACH.

Any breaches of this Policy will be viewed very seriously. Breaching this Policy is a disciplinary offence and will be dealt with under our Disciplinary Procedure.

If you are aware of or believe that the club are not complying with Data Protection Laws and/or this Policy you should report it in confidence to the DPO.

DATA PROTECTION LAWS

This Policy is written in line with General Data Protection Regulation (GDPR), which came into force in on 25th May 2018.

The Data Protection Laws require that personal data is processed in accordance with the Data Protection Principles (on which see below) and gives individuals rights to access, correct and control how we use their personal data (on which see below).

KEY WORDS IN RELATION TO DATA PROTECTION

Personal data is data that relates to a living individual who can be identified from that data (or from that data and other information in or likely to come into our possession).

Identifiable means that the individual can be distinguished from a group of individuals (although the name of that individual need not be ascertainable). The data might identify an individual on its own (e.g. if a name or video footage) or might do if taken together with other information available to or obtainable us (e.g. a job title and company name).

Data subject is the living individual to whom the relevant personal data relates.

Processing is widely defined under data protection law and generally any action taken by us in respect of personal data will fall under the definition, including for example collection, modification, transfer, viewing, deleting, holding, backing up, archiving, retention, disclosure or destruction of personal data, including CCTV images.

DRAFT

Data controller is the person who decides how personal data is used, for example we will always be a data controller in respect of personal data relating to our employees.

Data processor is a person who processes personal data on behalf of a data controller and only processes that personal data in accordance with instructions from the data controller, for example an outsourced payroll provider will be a data processor.

Personal data

Data will relate to an individual and therefore be their personal data if it:

- identifies the individual. For instance, names, addresses, telephone numbers and email addresses;
- its content is about the individual personally. For instance, medical records, credit history, a recording of their actions, or contact details;
- relates to property of the individual, for example their home, their car or other possessions;
- it could be processed to learn, record or decide something about the individual (or this is a consequence of processing). For instance, if you are able to link the data to the individual to tell you something about them, this will relate to the individual (e.g. salary details for a post where there is only one named individual in that post, or a telephone bill for the occupier of a property where there is only one occupant);
- is biographical in a significant sense, that is it does more than record the individual's connection with or involvement in a matter or event which has no personal connotations for them. For instance, if an individual's name appears on a list of attendees of an organisation meeting this may not relate to the individual and may be more likely to relate to the company they represent;
- has the individual as its focus, that is the information relates to the individual personally rather than to some other person or a transaction or event he was involved in. For instance, if a work meeting is to discuss the individual's performance this is likely to relate to the individual;
- affects the individual's privacy, whether in their personal, family, organisation or professional capacity, for instance, email address or location and work email addresses can also be personal data;
- is an expression of opinion about the individual; or
- is an indication of our (or any other person's) intentions towards the individual (e.g. how a complaint by that individual will be dealt with).

Examples of information likely to constitute personal data:

- Unique names;
- Names together with email addresses or other contact details;
- Job title and employer (if there is only one person in the position);
- Video - and photographic images;
- Information about individuals obtained as a result of Safeguarding checks;
- Medical and disability information;
- CCTV images;
- Member profile information (e.g. marketing preferences); and
- Financial information and accounts (e.g. information about expenses and benefits entitlements, income and expenditure).

LAWFUL BASIS FOR PROCESSING

DRAFT

For personal data to be processed lawfully, we must be processing it on one of the legal grounds set out in the Data Protection Laws.

For the processing of ordinary personal data in our organisation these may include, among other things:

- the data subject has given their consent to the processing (perhaps on their membership application form or when they registered on the club's website)
- the processing is necessary for the performance of a contract with the data subject (for example, for processing membership subscriptions);
- the processing is necessary for the legitimate interest reasons of the data controller or a third party (for example, keeping in touch with members, athletes, coaches, volunteers and officials about competition dates, upcoming fixtures or access to club facilities).

SPECIAL CATEGORY DATA

Special category data under the Data Protection Laws is personal data relating to an individual's race, political opinions, health, religious or other beliefs, trade union records, sex life, biometric data and genetic data.

Under Data Protection Laws this type of information is known as special category data and criminal records history becomes its own special category which is treated for some parts the same as special category data. Previously these types of personal data were referred to as sensitive personal data and some people may continue to use this term.

To lawfully process special categories of personal data we must also ensure that either the individual has given their explicit consent to the processing or that another of the following conditions has been met:

- the processing is necessary for the performance of our obligations under employment law;
- the processing is necessary to protect the vital interests of the data subject. The ICO has previously indicated that this condition is unlikely to be met other than in a life or death or other extreme situation;
- the processing relates to information manifestly made public by the data subject;
- the processing is necessary for the purpose of establishing, exercising or defending legal claims; or
- the processing is necessary for the purpose of preventative or occupational medicine or for the assessment of the working capacity of the employee.
- To lawfully process personal data relating to criminal records and history there are even more limited reasons, and we must either:
- ensure that either the individual has given their explicit consent to the processing; or
- ensure that our processing of those criminal records history is necessary under a legal requirement imposed upon us.

When do we process personal data?

Virtually anything we do with personal data is processing including collection, modification, transfer, viewing, deleting, holding, backing up, archiving, retention, disclosure or destruction. So even just storage of personal data is a form of processing. We might process personal data using computers or manually by keeping paper records.

Examples of processing personal data might include:

DRAFT

- Using personal data to correspond with members;
- Holding personal data in our databases or documents; and
- Recording personal data in personnel or member files.

Outline

The main themes of the Data Protection Laws are:

- good practices for handling personal data;
- rights for individuals in respect of personal data that data controllers hold on them; and
- being able to demonstrate compliance with these laws.

In summary, data protection law requires each data controller to:

- only process personal data for certain purposes;
- process personal data in accordance with the 6 principles of 'good information handling' (including keeping personal data secure and processing it fairly and in a transparent manner);
- provide certain information to those individuals about whom we process personal data which is usually provided in a privacy notice,
- respect the rights of those individuals about whom we process personal data (including providing them with access to the personal data we hold on them); and
- keep adequate records of how data is processed and, where necessary, notify the ICO and possibly data subjects where there has been a data breach.

Every member that comes into contact with personal data has an important role to play in achieving these aims. It is your responsibility, therefore, to familiarise yourself with this Policy.

Data protection law in the UK is enforced by the Information Commissioner's Office ("**ICO**"). The ICO has extensive powers.

DATA PROTECTION PRINCIPLES

The Data Protection Laws set out 6 principles for maintaining and protecting personal data, which form the basis of the legislation. All personal data must be:

- processed lawfully, fairly and in a transparent manner and only if certain specified conditions are met;
- collected for specific, explicit and legitimate purposes, and not processed in any way incompatible with those purposes ("purpose limitation");
- adequate and relevant, and limited to what is necessary to the purposes for which it is processed ("data minimisation");
- accurate and where necessary kept up to date;
- kept for no longer than is necessary for the purpose ("storage limitation");
- processed in a manner that ensures appropriate security of the personal data using appropriate technical and organisational measures ("integrity and security").

Data subject rights

Under Data Protection Laws individuals have certain rights (**Rights**) in relation to their own personal data. In summary these are:

- The rights to access their personal data, usually referred to as a subject access request
- The right to have their personal data rectified;
- The right to have their personal data erased, usually referred to as the right to be forgotten;

DRAFT

- The right to restrict processing of their personal data;
- The right to object to receiving direct marketing materials;
- The right to portability of their personal data;
- The right to object to processing of their personal data; and
- The right to not be subject to a decision made solely by automated data processing.

The exercise of these Rights may be made in writing, including email, and also verbally and should be responded to in writing by us (if we are the relevant data controller) without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. We must inform the individual of any such extension within one month of receipt of the request, together with the reasons for the delay.

Where the data subject makes the request by electronic form means, any information is to be provided by electronic means where possible, unless otherwise requested by the individual.

If we receive the request from a third party (e.g. a legal advisor), we must take steps to verify that the request was, in fact, instigated by the individual and that the third party is properly authorised to make the request. This will usually mean contacting the relevant individual directly to verify that the third party is properly authorised to make the request.

There are very specific exemptions or partial exemptions for some of these Rights and not all of them are absolute rights. However the right to not receive marketing material is an absolute right, so this should be complied with immediately.

Where an individual considers that we have not complied with their request e.g. exceeded the time period, they can seek a court order and compensation. If the court agrees with the individual, it will issue a Court Order, to make us comply. The Court can also award compensation. They can also complain to the regulator for privacy legislation, which in our case will usually be the ICO.

In addition to the rights discussed in this document, any person may ask the ICO to assess whether it is likely that any processing of personal data has or is being carried out in compliance with the privacy legislation. The ICO must investigate and may serve an "Information Notice" on us (if we are the relevant data controller). The result of the investigation may lead to an "Enforcement Notice" being issued by the ICO. Any such assessments, information notices or enforcement notices should be sent directly to our DPO from the ICO.

In the event of a member receiving such a notice, they must immediately pass the communication to our DPO.

NOTIFICATION AND RESPONSE PROCEDURE

If a member has a request or believes they have a request for the exercise of a Right, they should inform the DPO of the request.

The DPO will co-ordinate the response. The action taken will depend upon the nature of the request. The DPO will write to the individual and explain the legal situation and whether we will comply with the request. A standard letter/email from the DPO should suffice in most cases.

The DPO will inform the committee of any additional action that must be taken to legally comply.

DRAFT