Bedale and Aiskew Runners

General Data Protection Regulation (GDPR) Policy Document

1. Policy Statement

(a) Bedale and Aiskew Runners (BAR) complies with all applicable laws in connection with processing data, including the General Data Protection Regulation (GDPR) and Data Protection Act 2018. Our data protection standards are underpinned by this policy as well as our Code of Conduct. Data users are obliged to comply with this policy when processing personal data.

2. Data Protection Definitions

(a) Data is information which is held electronically, or in structured paper-based filing systems.

(b) Data Subjects for the purpose of this policy include all living individuals about whom we hold personal data.

(c) Personal Data means data relating to a living individual who can be identified from that data (or in combination with other information in our possession). Personal data can be factual (such as a name, employee number or date of birth) or it can be an opinion about that person, their actions and behaviour.

(d) Data Controllers (specific BAR Committee members: Chairman, Club Secretary & Membership Secretary) are the decision makers over the processing of personal data. They exercise control over the purposes and means of any processing.

(e) Data Processors processes personal data on the instruction of a data controller.

(f) Data Users are those BAR members whose work involves processing personal data on behalf of BAR.

(g) Processing is any activity that involves use of the data. It includes collecting, recording or holding the data, or carrying out any operation on the data including organising, amending, retrieving, using, disclosing, erasing, or destroying it. Processing also includes transferring personal data to other parties.

(h) Special Category Personal Data includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, genetic data or biometric data, physical or mental health or condition or sexual life or sexual orientation (and such other categories as may be added from time to time). Special category personal data can only be processed under certain conditions.

(i) DP Legislation refers to any current or future laws or directives that are or will be applicable in the UK with respect to data processing. This includes the Data Protection Act 2018 and the General Data Protection Regulation.

3. Data protection principles

(a) Anyone processing Personal Data must comply with the six principles for processing Personal Data as are contained within DP Legislation. These provide that Personal Data must be:

i) Processed fairly, lawfully and transparently;

(b) Personal Data must be processed in a way that is not unduly detrimental, unexpected or misleading. Personal Data may only be processed if there is a legal ground for that processing. One of the following conditions must be met:

i) Performance of a contract

ii) Legal obligation (where Processing is required to comply with a common law or statutory obligation)
iii) Legitimate interest (applicable where BAR or the wider society has a benefit in processing Personal Data and where such processing is balanced against the rights and freedoms of individuals)
iv) Consent (where the Data Subjects have given their permission to process their Personal Data: annual membership renewal; media articles)

(c) Personal Data must be processed in an open and honest manner. Individuals must be informed as to how their data is processed.

(d) When Special Category Personal Data is required to be processed, additional conditions to those set out above must also be met.

(e) Processed for the specified purpose

i) The purpose(s) of the Processing must be clear from the start and must be recorded.

(f) Minimised;

i) The data collected must be adequate, relevant and limited to what is necessary to fulfil the stated purpose(s) of the Processing.

(g) Accurate

i) Steps must be taken to maintain the accuracy of data, including correcting information that is incorrect or misleading. BAR members are responsible for checking and updating their Personal Data held on the England Athletics portal and should update with changes to their personal circumstances.

(h) Not kept longer than necessary for the purpose; and

(i) Processed securely;

i) All Personal Data is classified as 'Confidential' (information that must not be disclosed unless appropriate). This principle means that Personal Data must be kept secure by maintaining the confidentiality, integrity and access to the data. Data Users must employ reasonable security measures including, where appropriate and/or relevant

4. Data sharing

(a) Personal Data may be shared with members of the BAR Committee only on a "need to know" basis and where the appropriate and/or relevant approval has been sought.

(b) Personal Data may only be disclosed externally if there is a legitimate basis to do so:
i) England Athletics for purpose of registering as a member of England Athletics.
ii) Bedale Sports Club (BSC) for registration purposes
iii) Other relevant third parties where appropriate/relevant.

(c) Before sharing Personal Data, there are likely to be a number of factors that the Data User must consider before sharing it. Some or all of the following factors will likely need to be considered before sharing Personal Data:
i) The objective – this will help to provide clarity on what data needs to be shared, if any, and to whom.
ii) Data required – the data that is shared must be minimised to the data that is required
iii) Recipients of data – data should only be shared on a 'need to know' basis

iv) Frequency of data sharing – Personal Data should not be shared more frequently than necessary. Data users must consider whether it is appropriate to share data on an exceptional basis, on-going or routinely
v) Mode of sharing – data must be shared in a secure manner
vi) Risk of sharing Personal Data – data users should consider risks to the Data Subjects
vii) Anonymising data – data users should consider if the objective can still be achieved by anonymising data

5. Data transmission

(a) Data transmission is the transfer of data from one location to another. It comprises the transmission of physical data and electronic data.

(b) Physical transfer of data carries with it greater Personal Data risk due to the inherent lack control in the event of a potential data breach. Accordingly, physical data transfers should only be carried out where there is no electronic alternative available or if it would not be practical to transfer the data in another manner.

(c) Where electronic transfer is appropriate, it is required to be transferred securely.

6. Data Retention

(a) We will not keep personal data longer than is necessary for the purpose or purposes for which they were collected. We will take all reasonable steps to destroy or erase from our systems, all data which is no longer required.

7. Data Subject's rights under DP Legislation

(a) We will process all Personal Data in accordance with Data Subjects' rights where it is applicable, and in particular their right to:

i) request to have inaccurate data amended

ii) request access to any data held about them by a data controller

iii) be informed about how their Personal Data is processed

iv) prevent the processing of their data for direct-marketing purposes

v) object to the processing of their Personal Data in certain instances

vi) restrict the processing of their Personal Data in certain instances

vii) withdraw their consent in the case where consent had previously been granted (h) request erasure in certain instances

(b) In most cases, we are required to comply with any Data Subject request within 1 month of the request being submitted. In the case of (a) data users should proceed with the request to have information requested without consulting with Group Compliance.

8. Data breaches and complaints

(a) A potential data breach is an incident in which sensitive, confidential or otherwise Personal Data has been accessed, disclosed or handled in a manner inconsistent with the intended treatment of that information.

(b) A data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data. This includes breaches that are the result of both accidental and deliberate causes.

(c) A non-comprehensive list of potential data breach examples includes:

i) Unauthorised deletion of data
ii) Sending data to an unintended recipient
iii) Access to data by an unauthorised individual
iv) Sending BAR confidential data to a personal email address for non-club related use
v) Loss or theft of a laptop
vi) Alteration of data without permission
vii) Misplacing data
viii) Cyber attack

(d) Data breaches may also include cases where Data Subjects' rights are not managed appropriately.

(e) It is important that we are able to deal with any data incident as soon as possible to effectively manage the incident.

(f) As such, all BAR members must notify the Secretary immediately after becoming aware of any data incident. In no circumstances should you communicate details of the incident outside of those managing the data security incident without first contacting the Secretary. A committee member will be assigned to consider the potential data breach facts and the Secretary will determine the course of action to take according to the findings.

9. Consequences of breaching this policy

(a) Non-compliance with this policy by members may result in disciplinary action as stated in the constitution.

10. Speaking up

(a) If you have a concern or suspect a violation of this policy, we want you to speak up immediately. Speaking up can be a difficult thing to do, so be reassured that all information received will be treated seriously and investigated appropriately.

BAR contact information:

infor@bedaleandaiskewrunners.org.uk

secretary@bedaleandaiskewrunners.org.uk