DATA PROTECTION POLICY

1. Introduction

This Policy sets out the obligations of ATC regarding data protection and the rights of all data subjects, that is, Committee members, office holders, Coaches and members in respect of their personal data under the EU General Data Protection Regulation ("GDPR").

Personal Data is defined as any information relating to an identified or identifiable natural person (a data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

2. Data Protection

ATC shall ensure that all its Committee members, office holders, Coaches and members, agents, contractors, or other parties working on its behalf comply with the following when working with personal data:

2.1.1 Where any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of. Hardcopies should be shredded, and electronic copies should be deleted securely.

2.1.2 Personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances.

2.1.3 Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email itself should be deleted. All temporary files associated therewith should also be deleted.

2.1.4 Where Personal data is to be sent by facsimile transmission the recipient should be informed in advance of the transmission and should be waiting by the fax machine to receive the data.

2.1.5 Where Personal data is to be transferred in hardcopy form it should be passed directly to the recipient.

2.1.6 No personal data may be shared informally and if a Committee member, office holder, Coach, agent, sub-contractor, or other party working on behalf of ATC requires access to any personal data that they do not already have access to, such access should be formally requested from ATC's Data Protection Officer or a Committee member of ATC.

2.1.7 All hardcopies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet or similar.

2.1.8 No personal data may be transferred to any individuals, agents, contractors, or other parties, whether such parties are working on behalf of ATC or not, without the authorisation of ATC's Data Protection Officer or a Committee member of ATC.

2.1.9 Personal data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, agents, sub-contractors or other parties at any time.

2.1.10 If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it.

2.1.11 All personal data stored electronically should be backed up regularly.

2.1.12 All electronic copies of personal data should be stored securely using passwords approved by ATC's Data Protection Officer or a Committee member of ATC.

2.1.13 All passwords used to protect personal data should be changed regularly and should not use words or phrases that can be easily guessed or otherwise compromised. All passwords must contain a combination of uppercase and lowercase letters, numbers, and symbols. All software used by ATC is designed to require such passwords.

2.1.14 Under no circumstances should any passwords be written down or shared between any individual, agent, contractor, or other parties working on behalf of ATC. If a password is forgotten, it must be reset using the applicable method.

3. The Data Protection Principles

This Policy aims to ensure compliance with the GDPR. The GDPR sets out the following principles with which any party handling personal data must comply. All personal data must be:

3.1.1 Processed lawfully, fairly, and in a transparent manner in relation to the data subject.

3.1.2 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.

3.1.3 Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

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

3.1.5 Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is 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 organisational measures required by the GDPR in order to safeguard the rights and freedoms of the data subject.

3.1.6 Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

4. Lawful, Fair, and Transparent Data Processing

The GDPR seeks to ensure that personal data is processed lawfully, fairly, and

transparently, without adversely affecting the rights of the data subject. The GDPR states that processing of personal data shall be lawful if at least one of the following applies:

4.1.1 The data subject has given consent to the processing of his or her personal data for one or more specific purposes.

4.1.2 Processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract.

4.1.3 Processing is necessary for compliance with a legal obligation to which the controller is subject.

4.1.4 Processing is necessary to protect the vital interests of the data subject or of another natural person.

4.1.5 Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

4.1.6 Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

5. Processed for Specified, Explicit and Legitimate Purposes

5.1 ATC collects and processes the personal data set out in Part 12 of this Policy. This may include personal data received directly from data subjects (for example, contact details used when a data subject communicates with us) and data received from third parties (for example, dietician/nutrition experts marketing their services).

5.2 ATC only processes personal data for the specific purposes set out in this Policy (or for other purposes expressly permitted by the GDPR). The purposes for which we process personal data will be informed to data subjects at the time that their personal data is collected, where it is collected directly from them, or as soon as possible (not more than one calendar month) after collection where it is obtained from a third party.

6. Adequate, Relevant and Limited Data Processing

ATC will only collect and process personal data for and to the extent necessary for the specific purpose(s) informed to data subjects as set out in this Policy.

7. Accuracy of Data and Keeping Data Up To Date

ATC shall ensure that all personal data collected and processed is kept accurate and up-to-date. The accuracy of data shall be checked when it is collected and at regular intervals thereafter. Where any inaccurate or out-of-date data is found, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

8. Timely Processing

ATC shall not keep personal data for any longer than is necessary in light of the purposes for which that data was originally collected and processed. When the data

is no longer required, all reasonable steps will be taken to erase it without delay.

9. **Secure Processing**

ATC shall ensure that all personal data collected and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction or damage.

10. **Accountability**

10.1 ATC's data protection officer is Peter Holt, BTF Level 2 Coach and ATC Committee member.

10.2 Where applicable, ATC shall keep written internal records of all personal data collection, holding, and processing, which shall incorporate the following information:

10.2.1 The name and details of ATC, its data protection officer, and any applicable third party data controllers.

10.2.2 The purposes for which ATC processes personal data.

10.2.3 Details of the categories of personal data collected, held, and processed by ATC; and the categories of data subject to which that personal data relates.

10.2.4 Details (and categories) of any third parties that will receive personal data from ATC.

10.2.5 Details of any transfers of personal data to non-EEA countries including all mechanisms and security safeguards.

10.2.6 Details of how long personal data will be retained by ATC.

10.2.7 Detailed descriptions of all technical and organisational measures taken by ATC to ensure the security of personal data.

11. **The Rights of Data Subjects**

A. Keeping Data Subjects Informed

11.1 Where applicable or necessary, ATC shall ensure that the following information is provided to every data subject when personal data is collected:

11.1.1 Details of ATC including, but not limited to, the identity of (or any replacement), its Data Protection Officer.

11.1.2 The purpose(s) for which the personal data is being collected and will be processed (as detailed in Part 12 of this Policy) and the legal basis justifying that collection and processing.

11.1.3 The legitimate interests upon which ATC is justifying its collection and processing of the personal data.

11.1.4 Where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed.

11.1.5 Where the personal data is to be transferred to one or more third parties, details of those parties.

11.1.6 Where the personal data is to be transferred to a third party that is located outside of the European Economic Area (the "EEA"), details of that transfer, including but not limited to the safeguards in place.

11.1.7 Details of the length of time the personal data will be held by ATC (or, where there is no pre-determined period, details of how that length of time will be determined).

11.1.8 Details of the data subject's rights under the GDPR.

11.1.9 Details of the data subject's right to withdraw their consent to ATC's processing of their personal data at any time.

11.1.10 Details of the data subject's right to complain to the Information Commissioner's Office (the 'supervisory authority' under the GDPR).

11.1.11 Details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data and details of any consequences of failing to provide it.

11.1.12 Details of any automated decision-making that will take place using the personal data (including but not limited to profiling), including information on how decisions will be made, the significance of those decisions and any consequences.

11.2 The information set out above shall, where appropriate, be provided to the data subject at the following applicable time:

11.2.1 Where the personal data is obtained from the data subject directly, at the time of collection.

11.2.2 Where the personal data is not obtained from the data subject directly (i.e. from another party):

11.2.2.1 If the personal data is used to communicate with the data subject, at the time of the first communication.

11.2.2.2 If the personal data is to be disclosed to another party, before the personal data is disclosed.

11.2.2.3 In any event, not more than one month after the time at which ATC obtains the personal data.

B. Data Subject Access

11.3 A data subject may make a subject access request ("SAR") at any time to find out more about the personal data which ATC holds about them. ATC is normally required to respond to SARs within one month of receipt (this can be extended by up to two months in the case of complex and/or numerous requests, and in such cases the data subject shall be informed of the need for the extension).

11.4 All subject access requests received must be forwarded to ATC's Data Protection Officer.

11.5 ATC does not charge a fee for the handling of normal SARs. ATC reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

C. Rectification of Personal Data

11.6 If a data subject informs ATC that personal data held by ATC is inaccurate or incomplete, requesting that it be rectified, the personal data in question shall be rectified, and the data subject informed of that rectification, within one month of receipt the data subject's notice (this can be extended by up to two months in the case of complex requests, and in such cases the data subject shall be informed of the need for the extension).

11.7 In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification of that personal data.

D. Erasure of Personal Data

11.8 Data subjects may request that ATC erases the personal data it holds about them in the following circumstances:

11.8.1 It is no longer necessary for ATC to hold that personal data with respect to the purpose for which it was originally collected or processed.

11.8.2 The data subject wishes to withdraw their consent to ATC holding and processing their personal data.

11.8.3 The data subject objects to ATC holding and processing their personal data (and there is no overriding legitimate interest to allow ATC to continue doing so).

11.8.4 The personal data has been processed unlawfully.

11.8.5 The personal data needs to be erased in order for ATC to comply with a particular legal obligation.

11.9 Unless ATC has reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the data subject informed of the erasure, within one month of receipt of the data subject's request (this can be extended by up to two months in the case of complex requests, and in such cases the data subject shall be informed of the need for the extension).

11.10 In the event that any personal data that is to be erased in response to a data subject request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

E. Restriction of Personal Data Processing

11.11 Data subjects may request that ATC ceases processing the personal data it holds about them. If a data subject makes such a request, ATC shall retain only the amount of personal data pertaining to that data subject that is necessary to ensure that no further processing of their personal data takes place.

11.12 In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

F. Data Portability

11.13 ATC processes personal data using automated means, namely retaining some emails and electronic documents.

11.14 Where data subjects have given their consent to ATC to process their personal data in such a manner, data subjects have the legal right under the GDPR to receive a copy of their personal data and to use it for other purposes (namely transmitting it to other data controllers, e.g. other organisations).

11.15 To facilitate the right of data portability, ATC shall make available all applicable personal data to data subjects in the following format:

11.15.1 Soft-copy/email format.

11.15.2 Hard-copy printed format.

11.16 Where technically feasible, if requested by a data subject, personal data shall be sent directly to another data controller.

11.17 All requests for copies of personal data shall be complied with within one month of the data subject's request (this can be extended by up to two months in the case of complex requests in the case of complex or numerous requests, and in such cases the data subject shall be informed of the need for the extension).

G. Objections to Personal Data Processing

11.18 Data subjects have the right to object to ATC processing their personal data based on legitimate interests (including profiling), direct marketing (including profiling), and processing for scientific and/or historical research and statistics purposes.

11.19 Where a data subject objects to ATC processing their personal data based on its legitimate interests, ATC shall cease such processing forthwith, unless it can be demonstrated that ATC's legitimate grounds for such processing override the data subject's interests, rights and freedoms; or the processing is necessary for the conduct of legal claims.

11.20 Where a data subject objects to ATC processing their personal data for direct marketing purposes, ATC shall cease such processing forthwith.

11.21 Where a data subject objects to ATC processing their personal data for scientific and/or historical research and statistics purposes, the data subject must, under the GDPR, 'demonstrate grounds relating to his or her particular situation'. ATC is not required to comply if the research is necessary for the performance of a task carried out for reasons of public interest.

H. Automated Decision-Making

11.22 In the event that ATC uses personal data for the purposes of automated decision-making and those decisions have a legal (or similarly significant effect) on data subjects, data subjects have the right to challenge to such decisions under the GDPR, requesting human intervention, expressing their own point of view, and obtaining an explanation of the decision from ATC.

11.23 The right described in Part 11.22 does not apply in the following circumstances:

11.23.1 The decision is necessary for the entry into, or performance of, a contract between ATC and the data subject.

11.23.2 The decision is authorised by law.

11.23.3 The data subject has given their explicit consent.

I. Profiling

11.24 Where ATC uses personal data for profiling purposes, the following shall apply:

11.24.1 Clear information explaining the profiling will be provided, including its significance and the likely consequences.

11.24.2 Appropriate mathematical or statistical procedures will be used.

11.24.3 Technical and organisational measures necessary to minimise the risk of errors and to enable such errors to be easily corrected shall be implemented.

11.24.4 All personal data processed for profiling purposes shall be secured in order to prevent discriminatory effects arising out of profiling.

12. Personal Data

The following personal data may be collected, held, and processed by ATC:

12.1 Name, residential address, telephone or other contact numbers, email address(es), date of birth, gender.

12.2 Next of kin/personal emergency contact name(s), relationship details and contact information, including email address(es) and contact number(s).

12.3 Medical conditions and general health and wellbeing relevant to participation in triathlon or similar sporting/physical activities.

12.4 Other relevant personnel records relating to the data subjects' membership of ATC.

13. Measures To Be Taken To Ensure Data Protection

ATC shall ensure that all its Committee members, Coaches employees, agents, contractors, or other parties working on its behalf comply with the following when working with personal data:

13.1 All emails containing personal data must be securely stored.

13.2 Where any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of. Hardcopies should be shredded, and electronic copies should be deleted securely.

13.3 Personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances.

13.4 Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email itself should be deleted. All temporary files associated therewith should also be deleted.

13.5 Where Personal data is to be sent by facsimile transmission the recipient should be informed in advance of the transmission and should be waiting by the fax machine to receive the data.

13.6 Where Personal data is to be transferred in hardcopy form it should be passed directly to the recipient.

13.7 No personal data may be shared informally and if an individual, agent, sub-contractor, or other party working on behalf of ATC requires access to any personal data that they do not already have access to, such access should be formally requested from ATC's Data Protection Officer or a Committee member of ATC.

13.8 All hardcopies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet or similar.

13.9 No personal data may be transferred to any individuals, agents, contractors, or other parties, whether such parties are working on behalf of ATC or not, without the authorisation of ATC's Data Protection Officer or a Committee member of ATC.

13.10 Personal data must be handled with care at all times and should not be left unattended or on view to unauthorised individuals, agents, sub-contractors or other parties at any time.

13.11 If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it.

13.12 No personal data should be stored on any mobile device (including, but not limited to, laptops, tablets and smartphones), whether such device belongs to ATC or otherwise without the approval of ATC's Data Protection Officer or a Committee member of ATC and, in the event of such approval, strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary.

13.13 No personal data should be transferred to any device personally belonging to an individual and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of ATC where the party in question has agreed to comply fully with the letter and spirit of this Policy and of the GDPR (which may include demonstrating to ATC that all suitable technical and organisational measures have been taken).

13.14 All personal data stored electronically should be backed up regularly.

13.15 All electronic copies of personal data should be stored securely using passwords data encryption approved by ATC's Data Protection Officer or a Committee member of ATC.

13.16 All passwords used to protect personal data should be changed regularly and should not use words or phrases that can be easily guessed or otherwise compromised. All passwords must contain a combination of uppercase and lowercase letters, numbers, and symbols.

13.17 Under no circumstances should any passwords be written down or shared between any individuals, agents, contractors, or other parties working on behalf of ATC, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method.

13.18 All individuals, agents, contractors, or other parties working on behalf of ATC shall be made fully aware of both their individual responsibilities and ATC's

responsibilities under the GDPR and under this Policy, and shall be provided with a copy of this Policy.

13.19 Only individuals, agents, sub-contractors, or other parties working on behalf of ATC that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data held by ATC.

13.20 All individuals, agents, contractors, or other parties working on behalf of ATC handling personal data will be appropriately trained to do so.

13.21 All individuals, agents, contractors, or other parties working on behalf of ATC handling personal data will be appropriately supervised.

13.22 Methods of collecting, holding and processing personal data shall be regularly evaluated and reviewed by ATC's Committee.

13.23 The performance of those individuals, agents, contractors, or other parties working on behalf of ATC handling personal data shall be regularly evaluated and reviewed by ATC's Committee.

13.24 All individuals, agents, contractors, or other parties working on behalf of ATC handling personal data will be bound to do so in accordance with the principles of the GDPR and this Policy by contract.

13.25 All agents, contractors, or other parties working on behalf of ATC handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant individuals of ATC arising out of this Policy and the GDPR.

13.26 Where any agent, contractor or other party working on behalf of ATC handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless ATC against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

14. Transferring Personal Data Outside the EEA

14.1 ATC may from time to time, albeit in limited circumstances, transfer ('transfer' includes making available remotely) personal data to countries outside of the EEA.

14.2 The transfer of personal data to a country outside of the EEA shall take place only if applies:

14.2.1 The transfer is to a country, territory, or one or more specific sectors in that country (or an international organisation), that the European Commission has determined ensures an adequate level of protection for personal data.

14.2.2 The transfer is to a country (or international organisation) which provides appropriate safeguards in the form of a legally binding agreement between public authorities or bodies; binding corporate rules; standard data protection clauses adopted by the European Commission; compliance with an approved code of conduct approved by a supervisory authority (e.g. the Information Commissioner's Office); certification under an approved certification mechanism (as provided for in the GDPR); contractual clauses agreed and authorised by the competent supervisory authority; or provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority.

14.2.3 The transfer is made with the informed consent of the relevant data

subject(s).

14.2.4 The transfer is necessary for the performance of a contract between the data subject and ATC (or for pre-contractual steps taken at the request of the data subject).

14.2.5 The transfer is necessary for important public interest reasons.

14.2.6 The transfer is necessary for the conduct of legal claims.

14.2.7 The transfer is necessary to protect the vital interests of the data subject or other individuals where the data subject is physically or legally unable to give their consent.

14.2.8 The transfer is made from a register that, under UK or EU law, is intended to provide information to the public and which is open for access by the public in general or otherwise to those who are able to show a legitimate interest in accessing the register.

15. Procedure for Notifying a Data Breach

15.1 In the circumstances of an actual, perceived or suspected breach of data security, the following procedure must be adhered to by all staff:

15.1.1 Immediately report the actual or suspected breach to ATC's Data Protection Officer or a Committee member of ATC.

15.1.2 If there is a risk to the rights of data subjects, the Data Protection Officer must ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.

15.1.3 If there is a high risk to the rights of data subjects, the Data Protection Officer must ensure that all affected data subjects are informed of the breach directly and without delay.

15.2 Notices regarding an actual or suspected data breach shall include the following:

15.2.1 The categories and approximate number of data subjects concerned.

15.2.2 The categories and approximate number of personal data records concerned.

15.2.3 The name and contact details of ATC's data protection officer (or other contact point where more information can be obtained).

15.2.4 The likely consequences of the breach.

15.2.5 Details of the measures taken, or proposed to be taken, by ATC to address the breach including, where appropriate, measures to mitigate its possible adverse effects.