Data Protection Policy

1. Introduction

In the course of its activities, Triathlon Scotland will collect, store and process personal information. Triathlon Scotland recognises that the correct and lawful handling of this information will maintain confidence in Triathlon Scotland as an organisation and is conducive to Triathlon Scotland's successful operations.

The types of personal information that Triathlon Scotland may handle includes information about:

- members (of both Triathlon Scotland, affiliated clubs and approved centres) and, where applicable, their guardians;
- current, past and prospective employees, officers, board and committee members, volunteers, Triathlon Scotland representatives, advisers, consultants, contractors and agents;
- registered athletes, being individuals who are members of National Programmes who compete and represent Scotland at a national level and their training partners;
- those individuals who have undertaken training or qualifications through Triathlon Scotland or partner organisations;
- coaches and course providers registered with Triathlon Scotland;
- suppliers and sponsors; and
- others with whom it communicates.

The personal information, which may be held within highly structured paper filing systems, on a computer or other media, is subject to certain legal safeguards specified in the Data Protection Act 2018 (the Act), the General Data Protection Regulation (GDPR) and other regulations. The Act and the GDPR impose restrictions on how Triathlon Scotland may process personal information, and a breach could give rise to criminal and civil sanctions as well as bad publicity and damage to Triathlon Scotland's reputation.

2. Status of the Policy

This policy sets out Triathlon Scotland's rules on data protection and sets out how Triathlon Scotland will comply with the seven data protection principles set out in the GDPR. These principles specify the legal conditions that must be satisfied in relation to the obtaining, handling, processing, transportation and storage of personal information.

This policy is a condition of employment and therefore any employees, in addition to all others who obtain, handle, process, transport and store personal information, including board and committee members, volunteers, Triathlon Scotland representatives, advisers, consultants, contractors and

agents, will adhere to the rules of the policy. Any breach of the policy will be taken seriously and may result in disciplinary action. Negligent or deliberate breaches could also result in personal criminal liability for the individual(s) involved.

Any employee, board or committee member, volunteer, Triathlon Scotland representative, adviser, consultant, contractor or agent who considers that the policy has not been followed in respect of personal information about themselves or others should raise the matter with the Triathlon Scotland Chief Executive Officer in the first instance.

3. The Meaning of Data Protection Terms

The Act is a complex law and uses technical terminology. It is important that these terms are understood. They are explained below and used throughout this policy.

Data is recorded information whether stored electronically, on a computer, or in certain highly structured paper-based filing systems.

Data subjects include all living individuals about whom Triathlon Scotland holds personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information.

Data controllers are the people or organisations who 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. Triathlon Scotland is the data controller of all personal data used in its activities and undertakings. There can be more than one data controller in respect of the same information. For example, in addition to Triathlon Scotland, a member club may also be a data controller jointly with Triathlon Scotland.

Data users form part of the data controller and include employees whose work involves using personal information. Data users have a duty to protect the information they handle by following Triathlon Scotland's 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 board and committee members, volunteers, Triathlon Scotland representatives, advisers, consultants, contractors and agents who handle personal data on Triathlon Scotland's behalf, for example where Triathlon Scotland has a volunteer inputting a new member's details onto its system.

Personal data means data relating to a living individual who can be identified from that data (or from that data and other information in the possession of Triathlon Scotland). 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). It can even include a simple e-mail address. However, it is important that the information has the data subject as its focus and affects the data subject's privacy in some way. Mere mention of a data subject's name in a document does not constitute personal data, but personal details such as contact details, participation details or details of any medical condition would still fall within the scope of the Act.

Processing is any activity that involves use of the data, including simply viewing 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 (even partner organisations), which may be based overseas.

Sensitive personal data comprises information about a data subject'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, including the explicit consent of the data subject.

4. Data Protection Principles

Data controllers must comply with the seven data protection principles set out in the GDPR. These provide that personal data must be:

1. Lawfulness, fairness and transparency
2. Purpose limitation
3. Data minimisation
4. Accuracy
5. Storage limitation
6. Integrity and confidentiality (security)
7. Accountability

There is stronger legal protection for more sensitive information, such as:

- race
- ethnic background
- political opinions
- religious beliefs
- trade union membership
- genetics
- biometrics (where used for identification)
- health
- sex life or orientation

Principle 1 - Lawfulness, Fairness and Transparency

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, in a privacy notice, who the data controller is, the purpose for which their data is to be processed by Triathlon Scotland, and the identities of anyone to whom the data may be disclosed or transferred. In addition, the data protection notice must be given to the data subject at the time the data is obtained and where the personal data is obtained from a third-party source e.g. an affiliated club or centre, the data protection notice must be provided at the point that that data is first processed by Triathlon Scotland. If a member club has already told the data subject that their personal data will be passed to Triathlon Scotland and has informed the data subject of the purposes for which Triathlon Scotland will process that data subject's personal data then Triathlon Scotland need not tell the individual again. Data protection notices must be prominent and legible and included at every point of collection of personal data.

Additional specific conditions have to be met to comply with this principle. These include, among other things, requirements that the data subject has consented to the processing, or that the processing is necessary for the legitimate interests of the data controller or the party to whom the data is disclosed. When sensitive personal data is being processed, further conditions must be met. For example, information concerning a data subject's health, sex life, political opinions, race, ethnicity or religious beliefs can only be processed where the individual has given explicit consent for this or in certain other limited circumstances, for example where Triathlon Scotland is required by employment law to process such sensitive information to monitor equality of opportunity, for example. In most cases, the data subject's explicit consent to the processing of such data should be obtained.

Principle 2 - Purpose Limitation

Personal data may only be processed for the specific purposes notified to the data subject within the privacy notice. 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 via an updated privacy notice before any processing for that new purpose occurs.

Principle 3 - Data Minimisation

Personal data should only be processed to the extent that it is required for the specific purpose notified to the data subject at the time at which the data was initially collected. Any data which is not necessary for that purpose should not be collected in the first place.

Principle 4 - Accuracy

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 by, for example, writing to data subjects regularly and asking them to check the personal data that Triathlon Scotland holds on them.

Principle 5 - Storage Limitation

Personal data should not be kept longer than is necessary for the purpose. This means that personal data should be destroyed or erased from Triathlon Scotland's systems when it is no longer required. Personal data which is held for historical or statistical purposes (such as qualifications, results of competitions, etc.) can be held indefinitely. Although details of previous members should not be held indefinitely, anonymised information about members (i.e. information which does not identify specific individuals) is not regarded as personal data and can be held indefinitely).

Principle 6 - Integrity and Confidentiality

TS must ensure that appropriate security measures are put in place to protect 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 loss.

This means that Triathlon Scotland must 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 the data processor enters into a contract with TS in terms of which the data processor undertakes to put such measures, policies and procedures in place.

Maintaining data security means guaranteeing the confidentiality, integrity and availability of the personal data, defined as follows:

- **Confidentiality** means that only people who are authorised to use the data can access it.
- **Integrity** means that personal data should be accurate and suitable for the purpose for which it is processed.
- **Availability** means that authorised users should be able to access the data if they need it for authorised purposes. High risk personal data to which limited access is necessary should therefore be stored on the Triathlon Scotland central computer system instead of individual PCs.

Security procedures include:

- **Log On System**. All IT systems have a log on system which allows only authorised personnel access to personal data. Passwords on all computers are changed frequently and must be alphanumeric and must not be disclosed to others.
- **Secure lockable desks and cupboards**. Desks and cupboards are kept locked if they hold confidential information of any kind and can only be accessed by certain individuals. (Personal and financial information and child protection data is always considered confidential and additional security measures are in place for such information.)
- **Methods of disposal**. Paper documents must be shredded. CD-ROMs and flash storage drives should be physically destroyed when they are no longer required.
- **Equipment**. Data users should ensure that individual monitors do not show confidential information to passers-by (using screen guards, where appropriate) and that they lock or log off from their PC when it is left unattended.

Principle 7 – Accountability

Triathlon Scotland responsible for complying with the Data Protection Act 2018 and can demonstrate this compliance. Triathlon Scotland has put in place technical and organisational measures to meet the requirements of accountability. These include:

- Implementing this data protection policy;
- Ensuring appropriate data protection measures in place throughout the entire lifecycle of our processing operations;
- Creating written contracts with organisations that process personal data on our behalf;
- Maintaining documentation of processing activities;
- Recording and reporting, where necessary, personal data breaches;
- Implementing security measures;
- Carrying out data protection impact assessments for uses of personal data that are likely to result in high risk to individuals' interests; and
- Adhering to codes of conduct.

5. Individual Rights

The GDPR provides the following rights for individuals:

- The right to be informed
  Individuals have the right to be informed about the collection and use of their personal data and this information can be found in Triathlon Scotland's Privacy Notices.

- The right of access
  Individuals have the right to access their data and can do so by submitting an access request either verbally or in writing.

- The right to rectification
  Individuals have the right to have inaccurate personal data rectified, or completed if it is incomplete.

- The right to erasure
  Individuals have the 'right to be forgotten' and can request this either verbally or in writing. Triathlon Scotland may not erase data if processing is still necessary as laid out in the GDPR.

- The right to restrict processing

Individuals are allowed to request the restriction or suppressing of their personal data. If this request is granted Triathlon Scotland will continue to store the individual's personal data but will not process it as per the request from the individual.

- The right to data portability
  Individual can obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without affecting its usability.

- The right to object
  Individuals have the right to object to the processing of their personal data in certain circumstances and have the absolute right to stop their data being used for direct marketing. Information about individual's right to object is within Triathlon Scotland's Privacy Notices.

- Rights in relation to automated decision making and profiling.
  None of Triathlon Scotland's computer systems use automatic decision making or profiling.

Triathlon Scotland will respond to all data requests within 1 month and no fee will be charged. Refer to '8. Dealing with Subject Access Requests'

6. International Transfers

Personal data transferred outside of the European Economic Area (EEA) risks losing the protection of the GDPR. Personal data should not be transferred to a country outside the EEA unless the country to which the personal data is being transferred provides adequate data protection. In many cases this will necessitate the data subject consenting to the personal data being transferred. Where TS does transfer data outside of the EEA, Triathlon Scotland ensures that the organisation agrees to comply with data protection principles by signing up to the Privacy Shield. Triathlon Scotland's Privacy Notices detail out the organisations used to store personal information.

7. Practical Pointers

To maintain data security and compliance with the law, data users should:

- when sending emails to more than one data subject (whether by a distribution list or otherwise), consider 'blind copying' each data subject so that each data subject's contact details are not disclosed to the other data subjects.
- ensure that no information is published on the Triathlon Scotland website in respect of a data subject unless the information is already in the public domain or that data subject has been informed and has consented to such publication.
- exercise care when disclosing information about a data subject. Only do so if the data subject has consented or the Act permits disclosure without the consent of the data subject.

8. Dealing with Subject Access Requests

A formal request from a data subject for personal data that Triathlon Scotland holds about them must be made verbally or in writing. Employees, board or committee members, volunteers, TS representatives, advisers, consultants, contractors and agents who receive a written request should forward it to the Data Protection Compliance Officer appointed by Triathlon Scotland immediately. Triathlon Scotland must respond to the request within 1 month and will not charge a fee.

When receiving telephone enquiries, employees, volunteers, board or committee members, Triathlon Scotland representatives, advisers, consultants, contractors and agents should be careful about disclosing any personal data held on Triathlon Scotland systems. In particular they should:

- check the caller's identity to make sure that personal data is only given to a person who is entitled to it. A common sense approach should be taken when verifying the identity of the caller. For example, if you personally know the individual and are satisfied that they are calling this ought to be sufficient. If you do not know the caller, you could ask to return their call and ensure that the number given tallies with that on the membership database record for the person. Alternatively, if individuals have been issued with a password the information can be released if they correctly disclose their password;
- suggest that the caller put their request in writing where the employee, board or committee member, volunteer, Triathlon Scotland representative, adviser, consultant, contractor or agent is not sure about the caller's identity and where their identity cannot be checked. Alternatively, the individual should be asked to attend in person (especially if the information is of a sensitive nature); or
- refer to the Data Protection Compliance Officer appointed by Triathlon Scotland for assistance in difficult situations (for example, where any request might involve disclosing someone else's personal data). Employees, board or committee members, volunteers, Triathlon Scotland representatives, consultants, advisers, contractors and agents should not be bullied into disclosing personal data.

9. General

This policy will be reviewed annually or more frequently should circumstances require in order to maintain its currency and relevance with periodic reports to the Triathlon Scotland Board on the implementation and operation of the policy.

Any questions or concerns about the interpretation or operation of this policy should be taken up in the first instance with the Triathlon Scotland Chief Executive Officer.

10. Review

The policy will be reviewed on a yearly basis.

11. Endorsement

This policy was approved by the Triathlon Scotland Executive Board in December 2020.