Teesdale Athletics Club

GDPR Policy

Contents

1. Aims

Teesdale Athletics Club (TAC) aims to ensure that all personal data collected about members and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) (EU) 2016/679 and the Data Protection Act 2018 (DPA 2018).

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Legislation and guidance

This policy meets the requirements of the GDPR and the provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR.

In addition, this policy complies with TACs constitution.

3. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, living individual. This may include the individual's: • Name (including initials) • England Athletics identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural, or social identity.

Special categories of personal data	Personal data, which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Genetics • Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing, or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than a member of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. The data controller

TAC processes personal data relating to members and others and therefore is a data controller.

5. Roles and responsibilities

This policy applies to **all members** of TAC and to external organisations or individuals working on our behalf. Members who do not comply with this policy may face disciplinary action.

5.2 The Committee

TAC committee has overall responsibility for ensuring that all members comply with all relevant data protection obligations.

5.3 The GDPR committee member

The GDPR committee member is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

The GDPR committee member will provide an annual report of their activities directly to the clubs AGM and, where relevant, report any incidents of data protection and the actions taken.

The GDPR committee member is also the first point of contact for individuals whose data TAC processes, and for the Information Commissioner's Office (ICO).

Our GDPR committee member is listed on the clubs website and is contactable via the clubs secretary.

5.4 All members

TAC committee members are responsible for:

- Collecting, storing, and processing any personal data in accordance with this policy
- Informing the club of any changes to their personal data, such as a change of address
- Contacting the GDPR committee member in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - If they have any concerns that this policy is not being followed ○
    - If they are unsure whether they have a lawful basis to use personal data in a particular way
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area

- If there has been a data breach ○ Whenever they are engaging in a new activity that may affect the privacy rights of individuals
- If they need help with any contracts or sharing personal data with third parties

6. Data protection principles

The GDPR is based on data protection principles that TAC must comply with.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner.
- Collected for specified, explicit and legitimate purposes.
- Adequate, relevant, and limited to what is necessary to fulfil the purposes for which it is processed.
- Accurate and, where necessary, kept up to date.
- Kept for no longer than is necessary for the purposes for which it is processed.
- Processed in a way that ensures it is appropriately secure.

This policy sets out how the Club aims to comply with these principles.

7. Collecting personal data

7.1 Lawfulness, fairness, and transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

The data needs to be processed so that the Club can **fulfil a contract** with the individual, or the individual has asked the Club to take specific steps before entering into a contract.

- The data needs to be processed so that TAC can **comply with a legal obligation**.
- The data needs to be processed to ensure the **vital interests** of the individual or another person e.g. to protect someone's life.
- The data needs to be processed for the **legitimate interests** of the Club or a third party, provided the individual's rights and freedoms are not overridden.
- The individual has freely given clear **consent.**

For **special categories** of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018:

- The individual has given **explicit consent**.
- The data needs to be processed in the vital interests of the individual or another person, where the individual is physically or legally incapable of giving consent.
- The data has already been made **manifestly public** by the individual.
- The data needs to be processed for the establishment, exercise or defence of **legal claims**.
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation.
- The data needs to be processed for **health or social care purposes**, and the processing is done by, or under the direction of, health or social care purposes, or by any other person obliged by confidentiality under law.
- The data needs to be processed for **public health reasons,** and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law.
- The data needs to be processed for **archiving purposes**, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest.

For criminal offence data, we will meet both a lawful basis and a condition set out under data protection law. Conditions include:

- The individual has given **consent**.
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent.
- The data has already been made **manifestly public** by the individual.
- The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of **legal rights**.
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation.

Whenever we first collect data directly from individuals, we will provide them with the relevant information required by data protection law.

We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect or use personal data in ways which have unjustified adverse effects on them.

7.2 Limitation, minimisation, and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so and seek consent where necessary.

Committee members must only process personal data where it is necessary to do their roles.

We will keep data accurate and, where necessary, up to date. Inaccurate data will be rectified or erased when appropriate.

In addition, when committee members no longer need the personal data they hold, they must ensure it is deleted or anonymised.

8. Sharing personal data

We will not normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. These include, but are not limited to, situations where:

- There is an issue with a member that puts the safety of our other members at risk.
- We need to liaise with other agencies – we will seek consent as necessary before doing this.
- England Athletics and other agencies need data to enable them provide services to our members. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law.
    - Establish a contract with the agency a to ensure the fair and lawful processing of any personal data we share.
    - Only share data that the agency needs to carry out their service.

We will also share personal data with law enforcement and government bodies where we are legally required to do so.

We may also share personal data with emergency services and local authorities to help them to respond to an emergency that affects any of our members.

Where we transfer personal data internationally, we will do so in accordance with data protection law.

9. Subject access requests and other rights of individuals

9.1 Subject access requests

Individuals have a right to make a ‘subject access request’ to gain access to personal information that TAC holds about them. This includes:

- Confirmation that their personal data is being processed.

- Access to a copy of the data.
- The purposes of the data processing.
- The categories of personal data concerned.
- Who the data has been, or will be, shared with.
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period.
- Where relevant, the existence of the right to request rectification, erasure, or restriction, or to object to such processing.
- The right to lodge a complaint with the ICO or another supervisory authority.
- The source of the data, if not the individual.
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual.
- The safeguards provided if the data is being transferred internationally.

Subject access requests can be submitted in any form, but we may be able to respond to requests more quickly if they are made in writing to the Secretary or GDPR committee member and include:

Name of individual

- Correspondence address
- Contact number and email address
- Details of the information requested

If Secretary or any committee member receive a subject access request, they must immediately forward it to the GDPR committee member.

9.2 Children and subject access requests

Personal data about a child belongs to that child and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request or have given their consent.

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. This is not a rule and a child's ability to understand their rights will always be judged on a case-by-case basis.

Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers may not be granted without the

express permission of the child. This is not a rule and a child's ability to understand their rights will always be judged on a case-by-case basis.

9.3 Responding to subject access requests When responding to requests, we:

- May ask the individual to provide 2 forms of identification.
- May contact the individual via phone to confirm the request was made.
- Will respond without delay and within 1 month of receipt of the request (or receipt of the additional information needed to confirm identity, where relevant).
  • Will provide the information free of charge.
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month and explain why the extension is necessary.

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the member or another individual.
- Would include another person's personal data that we cannot reasonably anonymise, and we do not have the other person's consent and it would be unreasonable to proceed without it.
- Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege.

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which considers administrative costs. We will consider whether the request is repetitive in nature when making this decision.
When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO or they can seek to enforce their subject access rights through the courts.

9.4 Other data protection rights of the individual

In addition to the right to make a subject access request (see above) and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time.
- Ask us to rectify, erase or restrict processing of their personal data or object to the processing of it (in certain circumstances).
- Prevent use of their personal data for direct marketing.

- Challenge processing which has been justified based on public interest, official authority, or legitimate interests.
- Challenge decisions based solely on automated decision making or profiling (i.e. making decisions or evaluating certain things about an individual based on their personal data with no human involvement).
- Be notified of a data breach (in certain circumstances).
- Make a complaint to the ICO.
- Ask for their personal data to be transferred to a third party in a structured, commonly used, and machine-readable format (in certain circumstances).

Individuals should submit any request to exercise these rights to the GDPR committee member. If members receive such a request, they must immediately forward it to the GDPR committee member.

10. Photographs and videos

As part of our activities, we may take photographs and record images of individuals within our club.

In TAC we will obtain written consent from members for photographs and videos to be taken for communication, marketing, and promotional materials.

Uses may include:

- on notice boards and in brochures, newsletters, etc.
- Online on both the TAC websites or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

11. Data protection by design and default

We will put measures in place to show that we have integrated data protection into all our data processing activities, including:

- Appointing a member of the committee to oversee GDPR.
- Only processing personal data that is necessary for each specific purpose of processing and always in line with the data protection principles set out in relevant data protection law (see section 6).
- Integrating data protection into internal documents including this policy, any related policies and privacy notices.
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant.
- Appropriate safeguards being put in place if we transfer any data outside of the EEA, where different data protection laws apply.
- Maintaining records of our processing activities, including:

- For the benefit of data subjects, making available the name and contact details of our GDPR committee member and all information we are required to share about how we use and process their personal data (via our privacy notices).
- For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third party recipients, any transfers outside of the EEA and the safeguards for those retention periods and how we are keeping the data secure.

12. Data security and storage of records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing, or disclosure, and against accidental or unlawful loss, destruction, or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Papers containing confidential personal data must not be pinned to notice/display boards or left anywhere else where there is general access
- Members who store personal information on their personal devices are expected to follow security procedures.
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

13. Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records and overwrite or delete electronic files.

14. Personal data breaches

TAC will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, when appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a club context may include, but are not limited to:

- A non-anonymised dataset being published on the club website which shows members personal information.
- Safeguarding information being made available to an unauthorised person.

- The theft of a members laptop containing non-encrypted personal data about other members.

15. Training

Data protection will form part of continuing development where changes to legislation, guidance or the club's processes make it necessary.

16. Monitoring arrangements

The GDPR committee member is responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated every 3 years and approved by members at the annual general meeting.