	POLICY	Document Number: DPPo01 Version number: 5 Updated: Jun-2023 Next Review Date: Jun-2025
YOUTH SPORT TRUST	**DATA PROTECTION**	

v.	Latest Amendment Details	Authorised by
5	2-year regular review undertaken – more specific detail on parental consent for the processing of children's data added.	YST Board (via NGR Committee)

WHO WE ARE

References to **we**, **our** or **us** in this policy are to the group of organisations below ("the Group"):

- **Youth Sport Trust (YST)** incorporated and registered in England and Wales with company number 4180163 and charity number 1086915, whose office is at SportPark, 3 Oakwood Drive, Loughborough, Leicestershire LE11 3QF. YST is registered with the Information Commissioner's Office as a Data Controller – registration number **Z7022336**.
- **Youth Sport Trust Enterprises Limited (YSTe)** (wholly owned trading subsidiary of Youth Sport Trust) incorporated and registered in England and Wales with company number 3289889, whose office is at SportPark, 3 Oakwood Drive, Loughborough, Leicestershire LE11 3QF. YSD is registered with the Information Commissioner's Office as a Data Controller – registration number **Z9369568**.
- **Youth Sport Trust International (YSTi),** registered in England and Wales as The Youth Sport UK Charitable Trust, with charity number 1040320, whose office is at SportPark, 3 Oakwood Drive, Loughborough, Leicestershire LE11 3QF. YSTi is registered with the Information Commissioner's Office as a Data Controller – registration number **Z9402507.**

'Data Protection Legislation' includes the Data Protection Act 2018 ("**DPA**"), the "UK GDPR" as defined in the DPA ("**GDPR**"), any subsequent amendments and all relevant UK data protection legislation.

INTRODUCTION

This policy sets out our commitment to ensuring that any personal data, including special category personal data, which we process, is carried out in compliance with Data Protection Legislation. We ensure that good data protection practice is embedded in the culture of our staff and our organisation.

Our other data protection and IT security related policies and procedures are:

- Privacy Notices (website, external, internal)
- DPP1 Personal Data Breach Incident procedure
- DPP2 Individual Rights Request procedure
- DPPo02 Retention & Disposal Policy
- DPPo03 Image Use Policy
- ITPo01 Information Security Policy

SCOPE

This policy applies to all personal data processed by us and is part of our approach to compliance with data protection legislation. All staff are expected to comply with this policy and failure to comply may lead to disciplinary action for misconduct, including dismissal. Obtaining (including accessing) or disclosing personal data in breach of this policy may also be a criminal offence.

OUR COMMITMENT

We will:

- ensure that the legal basis for processing personal data is identified in advance and that all processing complies with current data protection legislation;

- not do anything with personal data that data subjects would not expect given the content of this policy and our relevant privacy notice(s);
- ensure that appropriate privacy notices are in place advising staff and others how and why their data is being processed, and, in particular, advising data subjects of their rights;
- only collect and process the personal data that we need for purposes we have identified in advance;
- where we have identified a materially new or different use for the personal data, endeavour to update the privacy notice applicable to the data subjects who have been affected by the change;
- ensure that, as far as possible, the personal data we hold is accurate, or a system is in place for ensuring that it is kept up to date as far as possible;
- ensure that, in the case of sharing personal data, we will only disclose the data necessary to fulfil the purpose for which the sharing is required;
- only hold onto personal data for as long as it is needed, after which time we will securely erase or delete the personal data, as set out in our privacy notices and in accordance with our DPPo02 Retention & Disposal Policy;
- implement technical and organisational measures that ensure that personal data can only be accessed by those who need to access it and that it is held and transferred securely; and
- ensure that all staff who handle personal data on our behalf are aware of their responsibilities under this policy and other relevant data protection and information security policies, and that they are adequately trained and supervised.

DATA PROTECTION PRINCIPLES

We will comply with the six Data Protection Principles defined in Article 5 of the GDPR and set out below. When processing personal data, we will ensure that it shall be:

- processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
- 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, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
- accurate and, where necessary, kept up to date and that reasonable steps will be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are 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 in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures… in order to safeguard the rights and freedoms of the data subject ('storage limitation'); and
- 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 ('integrity and confidentiality').

LAWFUL PROCESSING

- We will ensure that the legal basis for processing personal data is identified in advance and that all processing complies with the law.
- All processing of personal data must meet one of the six lawful bases defined in Article 6(1) of the GDPR:
    - Where we have the **consent** of the data subject;
    - Where it is in our **legitimate interests** and this is not overridden by the rights and freedoms of the data subject;
    - Where necessary to meet a **legal obligation;**
    - Where necessary to fulfil a **contract**, or pre-contractual obligations;
    - Where we are protecting someone's **vital interests;** or
    - Where we are fulfilling a **public task** or acting under official authority.
- Furthermore, and in addition to the above duty, any special category data (sensitive types of personal data as defined in Article 9(1) of the GDPR) must be processed only in line with one of the conditions specified in Article 9(2).
- The most appropriate lawful basis, depending on the purpose, must be set out in the relevant privacy notice.
- Where processing is based on consent, the data subject must have the option to easily withdraw their consent.
- We will ensure that any electronic direct marketing communications are sent in accordance with the Privacy and Electronic Communications (EC Directive) Regulations 2003, which usually require us to obtain consent by a means other than email prior to adding a person to our marketing lists. Where electronic direct marketing communications are being sent, the recipient should have the option to opt-out in each communication sent, and this choice should be recognised and adhered to by us.
- We will keep a register of all those who have withdrawn their consent or chosen not to consent to marketing or data processing which will be kept up to date.
- Where the processing is based on legitimate interests, and no other legal basis applies, we will make a legitimate interest's assessment to ensure the processing of the personal data is necessary and balance this against the business' legitimate interest.

ACCOUNTABILITY

- The 'Data Protection Lead' (DPL) has the specific responsibility of overseeing data protection and ensuring that we comply with the data protection principles and relevant legislation.
- Individual members of staff have a duty to comply with our data protection policies and procedures.
- Where there is likely to be a high risk to individuals rights and freedoms due to a processing activity, we will first undertake a Data Protection Impact Assessment (DPIA) and consult with the ICO prior to processing, if necessary.

USE OF PROCESSORS

- We will only appoint processors who can provide sufficient guarantees around compliance with the GDPR and that the rights of data subjects will be protected.

- Where a processor can demonstrate that they adhere to approved codes of conduct or certification schemes, this should be taken into consideration for choice of supplier.
- Where we use a processor, a written contract with compulsory terms as set out in Article 28 of the GDPR must be in place (see our contractual 'Data Protection Schedules'). Processors can only act on our instructions.

DATA TRANSFERS TO OTHER CONTROLLERS

- We may enter into contracts with organisations that will become a data controller of the personal data we transfer to it. Where this is the case, we will ensure contractual obligations are in place to ensure the safe transfer of personal data.
- In rare cases, this may mean transferring the personal data outside of the UK. Where this is the case, we will ensure that at least one of the conditions in Article 44 to 50 of the GDPR apply to the transfer.

ROLE OF THE DATA PROTECTION LEAD

The responsibilities of the DPL are to:

- assist us to:
  - monitor our internal compliance;
  - inform and advise on our data protection obligations;
  - provide advice regarding Data Protection Impact Assessments; and
  - act as a contact point for data subjects and the Information Commissioner's Office;
- advise us and report to Senior Management on data protection matters;
- be easily accessible as a point of contact for staff for data protection issues and be identified as the point of contact in our privacy notice and other external material;
- identify, organise and deliver training for staff and meet with new staff during their induction to discuss data protection matters, including this policy;
- keep records of data protection matters including recording all data protection breaches in a detailed log;
- have appropriate knowledge of data protection law and best practice and be provided with adequate resources to help them carry out their role. This might include appropriate training and accreditation where identified;
- be nominally responsible for carrying out responses to requests made by data subjects, reporting breaches and drawing up policies and procedures;
- take steps to undertake due diligence on organisations which we may share personal data with, data controllers and processors alike; and
- to function as an independent point of view on commercial matters that may affect the personal data we control.

The above does not preclude another responsible member of staff from carrying out these duties.

DATA SUBJECT RIGHTS

We will facilitate any request from a data subject who wishes to exercise their rights under data protection legislation as appropriate, always communicating in a concise, transparent, intelligible and easily accessible form and without undue delay (within one month of receipt as far as possible), in accordance with our 'Data Subject - Individual Rights Procedure' (DPP2). All staff have received training

and are aware of the rights of data subjects. Staff can identify such a request and know who to send it to. Our DPP2 procedure covers the following:

Subject access: the right to request information about how personal data is being processed, including whether personal data is being processed and the right to be allowed access to that data and to be provided with a copy of that data along with the right to obtain the following information:

- the purpose of the processing;
- the categories of personal data;
- the recipients to whom data has been disclosed or which will be disclosed;
- the retention period;
- the right to lodge a complaint with the Information Commissioner's Office;
- the source of the information if not collected direct from the subject; and
- the existence of any automated decision making.

Rectification: the right to allow a data subject to rectify inaccurate personal data concerning them.

Erasure: the right to have data erased and to have confirmation of erasure, but only where:

- the data is no longer necessary in relation to the purpose for which it was collected;
- where consent is withdrawn;
- where there is no legal basis for the processing; or
- there is a legal obligation to delete data.

Restriction of processing: the right to ask for certain processing to be restricted in the following circumstances:

- if the accuracy of the personal data is being contested;
- if our processing is unlawful but the data subject does not want it erased;
- if the data is no longer needed for the purpose of the processing but it is required by the data subject for the establishment, exercise or defence of legal claims; or
- if the data subject has objected to the processing, pending verification of that objection.

Data portability: the right to receive a copy of personal data which has been provided by the data subject and which is processed by automated means in a format which will allow the individual to transfer the data to another data controller. This would only apply if we are processing the data using consent or on the basis of a contract.

Object to processing: the right to object to the processing of personal data relying on the legitimate interests processing condition unless we can demonstrate compelling legitimate grounds for the processing which override the interests of the data subject or for the establishment, exercise or defence of legal claims.

DATA BREACHES

Data breaches will be dealt with in accordance with our Data Loss Procedure (DPP1), which covers the following:

- A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
- All members of staff should be vigilant and able to identify a suspected personal data breach. A breach could include:
    - loss or theft of devices or data, including information stored on USB drives or on paper;
    - hacking or other forms of unauthorised access to a device, email account, or the network;

- disclosing personal data to the wrong person, through wrongly addressed emails, or bulk emails that inappropriately reveal all recipients email addresses; or
- alteration or destruction of personal data without permission.

- Where a member of staff discovers or suspects a personal data breach, this should be reported to the DPL as soon as possible.
- Where there is a likely risk to individuals' rights and freedoms, the DPL will report the personal data breach to the ICO within 72 hours of the organisation being aware of the breach.
- Where there is also a likely high risk to individuals' rights and freedoms, we will inform those individuals without undue delay.
- The DPL will keep a record of all personal data breaches reported and follow up with appropriate measures and improvements to reduce the risk of reoccurrence.

PROCESSING CHILDREN'S DATA

- We recognise that when processing personal data that relates to children, we will need to afford them particular protection as children will be less aware of the risks involved.
- When consent of the data subject is required to process personal data about the data subject, any child who is under 13 (minimum) will be required to have consent from whoever has parental responsibility for the child. Where the data subject is a child aged 13 or over, the consequences of consenting to the data processing will be clearly explained and we will not rely on the child's consent alone unless we are satisfied that the child is in a position to give considered consent with an understanding of the decision.
- In addition, documented, parental consent will be obtained for the processing of voice recordings and recognisable images (e.g., photographs and videos) of any individuals under 18 years of age, as set out in our Image Use Policy (DPPo03). Such voice recordings and images will generally be retained for a maximum of 5 years.
- Generally, any third party sharing of personal data relating to children will be taken with caution and will only be done if there is a compelling reason to share the data. In cases where the sharing is necessary but may introduce risks to the security of the personal data, then the DPL may elect to undertake a data protection impact assessment.

DATA RETENTION

Retention and disposal of data is dealt with in accordance with our Retention & Disposal Policy (DPPo02).