STANDARD OPERATING PROCEDURE
DOCUMENT CONTROL

SOP Number GDPR001 – Data Protection Policy

Version Number 2.0

	NAME	TITLE	SIGNATURE	DATE
Author	Gary More	Finance, Data & IT Manager		
Reviewer	Alastair Floyd	CEO		
Authoriser	TSYT Board	TSYT Board		

Issue Date:	
Effective Date:	
Review Due:	

Version History

Previous version	Significant changes from previous version	Author	Date

Data Protection Policy

Introduction

In order to operate, Tall Ships Youth Trust (TSYT) needs to gather and use certain data about individuals. This includes customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact (members, service users, trustees, volunteers, job applicants, supporters, donors, funders, partners). TSYT has a responsibility to ensure all data gathered and stored is necessary and secure. This policy describes how we gather and process personal data whilst ensuring compliance with General Data Protection Regulations.

GDPR replaces the 1998 Data Protection Act, and requires additional compliance in the following areas:

- Where permitted by law, including under the Data (Use and Access) Act 2025 and the Privacy and Electronic Communications Regulations (PECR), Tall Ships Youth Trust may contact individuals by electronic means in connection with their prior engagement with our charitable activities. We will always provide a clear and simple opportunity to opt out of such communications at the point of data collection and in every subsequent communication.
- Personal data is processed only where TSYT has a valid lawful basis under UK GDPR. Depending on the purpose, this may include consent, contractual necessity, legal obligation, or TSYT's legitimate interests, balanced against the rights and expectations of the individual.
- We provide clear information at the point of data collection about how personal data will be used, including any profiling or research activities.
- Individuals have enhanced rights to access, correct, restrict, or erase their personal data, and to object at any time to direct marketing.
- We maintain appropriate records of processing activities to demonstrate compliance with data protection law.
- Personal data breaches are reported in accordance with statutory timeframes.
- We apply strict controls to data processors and third parties.

• Special Category data is subject to additional safeguards, particularly where it relates to young people.

Definitions

UK GDPR is the retained UK legal framework governing the collection and processing of personal data.

TSYT Entity - A TSYT establishment, including subsidiaries and joint ventures over which TSYT exercise management control.

Personal Information – Information about living individuals that enables them to be identified – e.g. names, addresses, telephone numbers and email addresses, sensitive data. It does not apply to information about organisations, companies and agencies but applies to named persons, such as individual volunteers of the Trust.

Data Subject/Service User – The individual whose personal information is being held or processed by TSYT (for example: a service user or a supporter).

Explicit Consent – any freely given, specific and informed indication of their wishes by which the data subject signifies their agreement to personal data relating to them being processed.

Data Controller – the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data.

Data Processor - a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.

Data Protection Officer (DPO) – A person formally appointed under UK GDPR to monitor compliance with data protection law. Tall Ships Youth Trust has not appointed a statutory Data Protection Officer. Overall accountability for data protection compliance rests with the Chief Executive Officer, who reports to the Trustees. The Compliance Officer provides operational oversight and acts as the primary point of contact for data protection matters.

Compliance Officer - The person appointed by TSYT as a coordinator of GDPR compliance, and a point of contact for enquiries. The Compliance Officer is Gary More.

Data Processing – any operation or set of operations performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

Special Category/Sensitive Data - includes the following:

- racial or ethnic origin of the data subject
- political opinions
- religious beliefs or other beliefs of a similar nature
- trade union membership
- physical or mental health/condition
- sexual orientation
- criminal record
- proceedings for any offence committed or alleged to have been committed

Children: for processing personal data, only children aged 13 or over are able provide their own consent. For children under this age, we need to get consent from whoever holds parental responsibility for the child. Should any TSYT entity foresee a business need for obtaining parental consent for information needed to deliver services offered directly to a child, guidance and approval must be obtained from the Compliance Officer before any processing of a child's personal Data may commence.

It should be noted that where processing is lawful under other grounds, consent need not be obtained from the child or the holder of parental responsibility.

Principles

GDPR applies regardless of whether data is stored electronically, on paper or on other materials. To comply with GDPR, an organisation needs to embed six privacy principles within its operations:

Lawfulness, Fairness and Transparency

- Lawful: Personal data can only be obtained for "specified, explicit and legitimate purposes". Data can only be used for a specific processing purpose that the individual has been made aware of and no other, without further consent.
- Fair: What is processed must match up with how it has been described to the individual.
- Transparent: The subject must be made aware of what data processing will be done.

Data Minimisation

Data collected on a subject should be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed"

Accuracy

Data must be "accurate and where necessary kept up to date"

Storage limitations

The regulations require that personal data is "kept in a form which permits identification of data subjects for no longer than necessary"

Integrity and confidentiality

Requires processors to handle data "in a manner [ensuring] appropriate security of the personal data including protection against unlawful processing or accidental loss, destruction or damage"

Responsibilities

General

Everyone who works for or with TSYT (including freelance staff and volunteers) has some responsibility for ensuring data is collected, stored and handled appropriately. All staff will be given copies of all relevant policies and procedures during their induction process, including the Data Protection Policy, Privacy Policy and the operational procedures for handling personal data. All staff will be expected to adhere to all these policies and procedures. Data Protection will be included in the induction training for all volunteers. Volunteers should be aware that they can be personally liable if they use service's user personal data inappropriately.

The Trustees are ultimately responsible for ensuring that TSYT meets its legal obligations, and personal data is handled and processed in line with this policy and GDPR principles.

The CEO is responsible for:

- Keeping the board updated on their data protection responsibilities, risks and issues.
- Reviewing all data protection procedures and related policies, in line with an agreed schedule.
- Arranging data protection training and advice for the people covered by this policy.
- Handling data protection questions from staff and anyone else covered by this policy.
- Dealing with requests from individuals to see the data TSYT holds about them (also called 'subject access requests').
- Checking and approving any contract or agreements with third parties that may handle the company's sensitive data.

The Finance, Data & IT Manager is responsible for:

- Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
- Performing regular checks and scans to ensure security hardware and software is functioning properly.
- Evaluating any third-party services the charity is considering using to store or process data (e.g. cloud computing services) and ensuring the contract mandates GDPR compliance.

Head of Fundraising and Marketing is responsible for:

- Approving any data protection statements attached to communications such as emails and letters.
- Addressing any data protection queries from journalists or media outlets.
- Where necessary, working with other staff to ensure marketing initiatives abide by GDPR principles.
- Evaluating any third-party services the charity is considering and actively using when personal data is involved (e.g. face-to face/door-to door/tele fundraising agencies),

and ensuring the contract mandates GDPR compliance (as in the Fundraising Regulator's guidance on third party contracts)

- Ensuring marketing databases are checked against industry suppression files every six months.

Data Collection

Personal data must be processed fairly and lawfully by staff and volunteers and, crucially, data subjects should therefore be made aware of the purposes for which their data will be used and should be advised whom to contact if they wish to discuss the processing of their data. This will only be processed where TSYT has an appropriate lawful basis under UK GDPR, which may include consent, contract, legal obligation or legitimate interest.

The following statements should be used on all forms used to gather data and information that is stored by TSYT:

'I hereby give my consent to the processing of my personal data for the purpose of this booking.'

'TSYT will stay in contact with voyage information, fundraising, marketing and general charity updates. We will never sell your data, and we promise to keep your details safe and secure. You can update your preferences at any time simply by contacting us on at compliance@tallships.org.'
If you have any queries about how the TSYT uses the data we hold, please contact: compliance@tallships.org.'

Data Processing

The following procedures should be followed at the earliest reasonable opportunity after personal data (that is not generally in the public domain) is obtained about the data subject.

It must be confirmed that the data processing is necessary for:

- The charity's operations – this condition can be broadly interpreted to cover much of the processing of employee, voyager and service user data required for contracts. It also covers the processing of supporter data that is required for the fulfilment of financial transactions associated with their support of TSYT.
- Compliance with legal obligations other than an obligation imposed by contract.
- For the charity's 'legitimate interest'. Legitimate Interest - processing where we consider it is in the legitimate interest of the Tall Ships Youth Trust to process your data. We will always balance any potential impact on you and your rights against the identified legitimate interests.

Sensitive personal data must only be processed if one of the conditions listed in the section above has been met and one of the following conditions:

- The data subject has given their explicit consent to the processing – this means that, wherever possible, when sensitive personal data is obtained the data subject's verbal or written agreement to the processing of this data must be obtained and a record made of this consent.
- The processing is necessary for the purposes of exercising statutory functions – this covers processing related, for example, to the administration of maternity pay.
- The processing is performed under a legal obligation in connection with employment.

Data Use

Under the terms of the GDPR, personal data should be processed only in a manner compatible with one or more specified and lawful purposes. The purposes for which personal data held by TSYT may be used are listed below. No member of staff or volunteer should process personal data for any other purpose. In addition, no member of staff or volunteer should process personal data in any way listed below if this would violate a data subject's rights in relation to data processing, or is likely to cause substantial, unwarranted distress to themselves, or for direct marketing.

Members and Service Users data may be used for the following purposes:

- To contact by post, telephone, e-mail or text message, as appropriate, with information about The TSYT's services and activities. (Telephone marketing will only be carried out where permitted under PECR and relevant suppression lists)
- To register attendance at services and activities.
- To monitor and evaluate services and activities both internal and external purposes to enable us to review, develop and improve our activities.
- To contact next of kin in the event of emergencies.

Employees (current and past) **Trustees/Directors, Job Applicants and Volunteers** data may be used and stored for various purposes, for full details please see 'Staff Privacy Policy'

Partners, Donors and Supporters data may be used for the following purposes:

- For contacting the supporter by post, telephone, fax, e-mail or text message, as appropriate, with information about The TSYT's activities and campaigns.
- To help administer the ways they support TSYT.
- For research to enable us to review, develop and improve our activities and the service we offer supporters.
- To enable us to meet our legal obligations relating to recording contributions and administering Gift Aid Declarations and Deeds of Covenant.

Members, Service Users, Partners, Donors and Supporters

Our transformational youth work is only made possible thanks to the generosity of our supporters – so it is vital that our fundraising efforts are as effective as they can be. By developing a better understanding of our supporters through researching them using publicly available sources we can tailor and target our fundraising events and communications to those most likely to be interested in them.

By providing information which helps us to continually review and improve our fundraising and services. Profiling, segmentation and wealth screening allow Tall Ships Youth Trust to manage resources efficiently and proportionately, including through the use of trusted third-party prospect research providers

To create a profile, we (and a trusted third party) may combine information you provide to us with publicly available data.

Using this information, we may segment our supporter database, putting supporters into groups with similar characteristics. We may use this information to help us determine if you might be interested in getting involved in other fundraising or volunteering activities or to send information that we feel may be of interest.

We believe we have a legitimate interest in undertaking this work which allows us to understand our supporters further so we can:

- ensure communications are relevant and timely
- ensure we send information that we believe is of interest to you
- understand how you may be able to help us in the future
- raise funds in the most cost-effective ways

Data Retention

Retention periods are informed by statutory, regulatory, safeguarding, and accounting requirements. The following guidelines are established for the retention of personal data in TSYT

Donors:
Information may be retained for **6 years**.

Members:
Information will be kept for as long as the individual is a member. Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of. After 6 years we will keep historical records containing only names.

Service Users and Volunteers:
Application forms will be kept for **6 years**. After 6 years we will keep historical records containing only names.

Employees, subcontractors/freelance, Trustees and Vice-Patrons:
A summary of record of service e.g. name, position, and dates of employment will be kept for **10 years** from the end of the contract/tenure.

Data Security

This policy helps to protect TSYT from some very real data security risks, including:

- Breaches of confidentiality. For instance, information being given out inappropriately.
- Failing to offer choice. For instance, all individuals should be free to choose how the Trust uses data relating to them.
- Reputational damage. For instance, the Trust could suffer if hackers successfully gained access to sensitive data.

Each TSYT entity must adopt physical, technical, and organisational measures to ensure the security of personal data. This includes the prevention of loss or damage, unauthorised alteration, access or processing, and other risks to which it may be exposed by virtue of human act or the physical, cyber or natural environments.

We must:

- Prevent unauthorised persons from gaining access to data processing systems in which Personal Data are processed.
- Prevent persons entitled to use a data processing system from accessing personal data beyond their needs and authorisations.
- Ensure that personal data in the course of electronic transmission during transport cannot be read, copied, modified or removed without authorisation.
- Ensure that access logs are in place to establish whether, and by whom, the personal data was entered into, modified on or removed from a data processing system.
- Ensure that in the case where processing is carried out by a Data Processor, the data can be processed only in accordance with the instructions of the Data Controller.
- Ensure that personal data is protected against undesired destruction or loss.
- Ensure that personal data collected for different purposes can and is processed separately.

- Ensure that personal data is not kept for longer than necessary (see above).
- All personal data is stored securely and only accessed by authorised individuals

It is important to note that these rules apply to both controllers and processors -- meaning 'clouds' will not be exempt from GDPR enforcement.

Data Accuracy

The law requires TSYT to take reasonable steps to ensure data is kept accurate and as up to date as possible. To ensure data accuracy we must ensure:

- Any inaccuracy in personal data that is brought to the attention of a member of staff or volunteer (either by the data subject or as a result of the combination or alignment of two or more sources of data) should be corrected as soon as possible by an appropriate member of staff or volunteer.
- Data subjects should be given the opportunity to view the data held about them by TSYT. In particular, subject access requests must be responded to appropriately. All such requests should be directed to the Compliance Officer.
- Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets.
- Staff should take every opportunity to ensure data is updated. For instance, by confirming a customer's details when they call.
- TSYT will make it easy for data subjects to update the information held on them.
- Data should be updated as inaccuracies are discovered. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.

Data Subject Access Requests

GDPR requires TSYT to have documented processes for handling Subject Access requests. The Compliance Officer will establish a system to facilitate the exercise of Data Subjects' rights relating to:

- Information access.

- Objection to Processing.
- Objection to automated decision-making and profiling.
- Restriction of Processing.
- Data portability.
- Data rectification.
- Data erasure.

If an individual makes a request relating to any of the rights listed above, TSYT will consider each such request in accordance with all applicable Data Protection Regulations. No administration fee will be charged for considering and/or complying with such a request unless the request is deemed to be unnecessary or excessive in nature.

Data Subjects are entitled to obtain, based upon a request made in writing to the Compliance Officer and upon successful verification of their identity, the following information about their own personal data:

- The purposes of the collection, processing, use and storage of their Personal Data.
- The source(s) of the Personal Data, if it was not obtained from the Data Subject;
- The categories of Personal Data stored for the Data Subject.
- The recipients or categories of recipients to whom the Personal Data has been or may be transmitted, along with the location of those recipients.
- The envisaged period of storage for the Personal Data or the rationale for determining the storage period.
- The use of any automated decision-making, including Profiling.
- The right of the Data subject to: object to Processing of their Personal Data; lodge a complaint with the Data Protection Authority; request rectification or erasure of their Personal Data; request a restriction on processing of their Personal Data.

All requests received for access to or rectification of Personal Data must be directed to the Compliance Officer, who will log each request as it is received. A response to each request will be provided within **30 days** of the receipt of the written request from the Data Subject. Appropriate verification must confirm that the requestor is the Data Subject or their

authorised legal representative. Data Subjects shall have the right to require TSYT to correct or supplement erroneous, misleading, outdated, or incomplete Personal Data.

If TSYT cannot respond fully to the request within **30 days**, the Compliance Officer shall nevertheless provide the following information to the Data Subject or their authorised legal representative within the specified time:

- An acknowledgement of receipt of the request.
- Any information located to date.
- Details of any requested information or modifications which will not be provided to the Data Subject, the reason(s) for the refusal, and any procedures available for appealing the decision.
- An estimated date by which any remaining responses will be provided.
- An estimate of any costs to be paid by the Data Subject (e.g. where the request is excessive in nature).
- The name and contact information of the TSYT individual who the Data Subject should contact for follow up.

Situations may arise where providing the information requested by a Data Subject would disclose Personal Data about another individual. In such cases, information must be redacted or withheld as may be necessary or appropriate to protect that person's rights.

Direct Marketing

Data Subjects have the right to stop or prevent the processing of their data for the purposes of direct marketing. TSYT will treat the following solicited direct communication with individuals as marketing:

- seeking donations and other financial support;
- promoting any TSYT services;
- promoting TSYT events;
- promoting sponsored events and other fundraising exercises;
- Marketing on behalf of any other external company or voluntary organisation.

Whenever data is first collected which might be used for any marketing purpose, this purpose will be made clear, and the Data Subject will be given a clear opt out. If it is not possible to give a range of options for no longer receiving communications, any opt-out which is exercised will apply to all TSYT marketing.

Data Disclosure

In certain circumstances, the Data Protection Regulation allows personal data to be disclosed to law enforcement agencies without the consent of the data subject. Under these circumstances, we will disclose the requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the board and from the charity's legal advisers where necessary.

The Police

If the police contact the trust for data, we will confirm with the police that the reason for the request is that they wish to contact a named individual about a named criminal investigation (regardless of whether that individual is a suspect or witness) and that failure to release the data would prejudice the investigation. Most police forces will have their own request form which should always include a statement confirming that the information requested is required for the purposes covered in the Data Protection Regulation, a brief outline of the nature of the investigation and the subject's role in that investigation, and the signature of the investigating officer. This document must be obtained prior to the release of any information. All requests from the Police should be sent to the Compliance Officer using compliance@tallships.org.

Other third parties

If TSYT is approached with a request for information about a data subject from any other third party the following approach should be taken. As a general rule TSYT only considers approaching a data subject if releasing information will be in the best interest of the data subject. The Trust needs to get written consent from the data subject allowing the information to be released. We need to let the data subject know as much information as we can about the request so that they can make an informed decision as to whether they

are willing to let the information be released. We will record who made the request, what information they want and why. There are instances where The Trust can proceed without consent and it will approach these requests on a case by case basis. This criterion includes parents who wish to see data. Even if a parent or guardian was present at the time the data was collected, we require consent from their child before releasing information to them. Please refer all disclosure matters to the Compliance Officer using compliance@tallships.org.

Court Order

We may receive a request for disclosure through Court Order. In these circumstances, you should contact the Compliance Officer using compliance@tallships.org.

Research

Occasionally a company or a funder will wish to use our data for research purposes. If this is the case all data will be anonymized.

Disclosure and Barring Service

If an individual is requested to supply TSYT with a copy of a recent Disclosure and Barring Service (DBS) Certificate in connection with their role at TSYT this will only be viewed by staff required to process it. DBS certificates obtained upon employment and periodically will be kept on file for 6 months and thereafter destroyed.

Transfers Between TSYT Entities

In order for TSYT to carry out its operations effectively across its various entities, there may be occasions when it is necessary to transfer Personal Data from one TSYT Entity to another, or to allow access to the personal data from an overseas location. Should this occur, the TSYT Entity sending the personal data remains responsible for ensuring protection for that personal data.

Complaints Handling

Data Subjects with a complaint about the processing of their personal data, should put forward the matter in writing to the Compliance Officer. An investigation of the complaint will

be carried out to the extent that is appropriate based on the merits of the specific case. The Compliance Officer will inform the Data Subject of the progress and the outcome of the complaint within a reasonable period. If the issue cannot be resolved through consultation between the Data Subject and the Compliance Officer, then the Data Subject may, at their option, seek redress through mediation, binding arbitration, litigation, or via complaint to the Data Protection Authority within the applicable jurisdiction.

Breach Reporting

The consequences of breaching Data Protection can cause harm or distress to service users. This policy is designed to minimise the risks and to ensure that the reputation of the charity is not damaged through inappropriate or unauthorised access and sharing.

Any individual who suspects that a Personal Data Breach has occurred due to the theft or exposure of personal data must immediately notify the Compliance Officer providing a description of what occurred. Notifications of the incident can me made via e-mail to compliance@tallships.org. The Compliance Officer will investigate all reported incidents to confirm whether or not a personal data breach has occurred. If a personal data breach is confirmed, the Compliance Officer will follow the relevant authorised procedure based on the criticality and quantity of the personal data involved. For severe personal data breaches, the CEO will initiate and chair an emergency response team to coordinate and manage the personal data breach response.

Penalties

Organisations can be fined for infringement regarding data protection.