The Toby Henderson Trust
The Doorway to Early Action in Autism

# Data Protection Policy

**SAFETY policies number 001**

**Renewal date: 02/06/2026**

## Contents



## Appendix

## Foreword

The UK General Data Protection Regulation ("the GDPR") and the Data Protection Act 2018 (DPA) set out the requirements for handling personal information.

The GDPR sets standards and rules and places obligations on those who process personal information while giving rights to those who are the subject of the data.

Personal information covers both facts and opinions about individuals. The rules and procedures cover the collection and use of the data; the quality and security of the data; and the rights of individuals regarding data about themselves.

The Toby Henderson Trust (TTHT) is a "data controller" as it collects and uses information about people to carry out its functions. In some cases, TTHT is required by law to collect and use information to comply with central government requirements.

TTHT will process personal data relating to service users, current, past and prospective employees, clients and suppliers in accordance with the requirements of the GDPR, DPA, common law duty of confidentiality and other relevant legislation.

Failure to adhere to this policy may result in disciplinary action for individuals, and enforcement action, financial loss and/or reputational damage to The Toby Henderson Trust.

This policy applies to all personal data collected, created or held by TTHT, in whatever format (for example paper, electronic, email, video and audio and however it is stored e.g. computerised system/records, cloud storage, email, filing cabinet.

## Responsibilities

Everyone collecting, using, storing and disposing of personal data is responsible for following good data protection practice.

All employees with access to The Toby Henderson Trust information are responsible for: Complying with this policy guidance.

The Senior Information Risk Owner (SIRO) is Lesley Henderson, and she has overall responsibility for the charities compliance with data protection legislation and this policy.

## Data protection objectives

The Toby Henderson trusts data protection objectives are to:

• Protect the confidentiality and integrity of personal data

• Build and maintain the confidence of service users of TTHT through the correct and lawful treatment of personal data

• Fulfil its responsibilities as a data controller under the GDPR TTHT will meet these objectives through applying the data protection principles, complying with other requirements of data protection legislation, and having due regard to guidance from the Information Commissioner's Office (ICO) on best practice.

## Data protection principles

All processing of personal data will follow the data protection principles set out in the GDPR.

## Lawfulness, fairness and transparency

Personal data processing must be lawful and transparent, ensuring fairness towards the individuals whose personal data is being processed. Personal data should only be collected, stored and processed when the legal basis relied on under GDPR has been identified and documented. Data subjects must be provided with specific detailed information about the processing in the form of a privacy notice.

## Purpose limitation

Specific purposes must be identified for processing personal data and employees and service users must be told of these when we are collecting their data. Personal data cannot be used for other purposes that are incompatible with this original purpose.

Data must be adequate, relevant and limited to what is necessary. When no longer required for the specified purpose data should be deleted or anonymized in accordance with retention guidelines. Accuracy Personal data must be accurate, kept up-to-date, and corrected if it is found to be inaccurate for its intended purpose. Storage limitation Personal data must not be stored for longer than necessary for the purposes for which it was collected including for the purpose of legal, accounting or reporting requirements. Security, integrity and confidentiality Personal data must be secured appropriately. The Toby Henderson Trust employees must take responsibility for their use of personal data and compliance, and they must have appropriate measures and records in place to be able to demonstrate that compliance. TTHT will demonstrate compliance by maintaining documentation including policies, procedures, privacy notices, records of processing activity, logs of incidents and information requests, and sharing agreements.

## Consent

One of the lawful bases for processing personal data set out in the GDPR is consent. To be valid under GDPR, consent for processing data must be:

• Obtained by opt-in through an affirmative action

• Fully informed

• Not subject to conditions

• Specific – kept separate from any other matters

• Easily withdrawn at any time at which point further processing must cease. If you intend to process the personal data for a different purpose which was not disclosed when first consented, you will need to seek fresh consent.

## Privacy Notices

The law requires certain information to be given to individuals at the point their personal data is collected. The Toby Henderson Trust will publish all privacy notices on its website.

The notice provides transparency to individuals as to what data is collected, by whom, from what purpose, which third parties it may be shared with, how long the information will be held and what data subject rights are available.

## Information sharing with other organisations

The Toby Henderson Trust shares data with other organisations we have contracts with but will do so only when a lawful basis for this sharing exists.

TTHT will be transparent and as open as possible about how and with whom data is shared; and for what purpose; and with what protections and safeguards.

When information is regularly shared with other partners specific protocols will be agreed and an information sharing agreement put in place and signed by all parties.

Notification of personal data breaches

Personal data breaches will be recorded and will be reported to the Information Commissioner's Office (ICO) and affected individuals (if the relevant threshold for risk or harm is reached).

## Training and awareness

All TTHT employees will undertake annual mandatory data protection training.

## Breach of policy

Failure to adhere to the standards set out in this policy may result in TTHT breaching its obligations under the GDPR and the possibility of regulatory action from the ICO. Breaches of this policy must be reported to Lesley Henderson CEO and may be subject to disciplinary proceedings. This policy is designed to ensure effective data protection practice, failure to adhere to the practices in this policy increases the likelihood of a personal data breach occurring.

## ROPA and IAR

Types of Data held by The Toby Henderson trust are–

1. Personnel files
2. Service user information.

## Personnel Files

The data we hold is both digital and paper. The information held is transferred in and out of organisation. Data can be received direct from Employee and shared with Payroll agency, HMRC and DBS as appropriate.

This data is not transferred outside the EEA. It is transferred in and out of the organisation by secure encrypted transfer. Internally it is held in a secure folder within the organisation's online SharePoint and access to this data is limited to senior management only.

## Service User Information

The data we hold for families is both digital and paper. The information is transferred in and out of the organisation. Data can be received by hand directly from the NHS and returned once processed and discharged by hand.

Internally the paper copies of information are held in lockable filing cabinets within a first-floor locked office with no access to the public. The corresponding digital information is held in a secure folder within the organisation's online SharePoint and also external encrypted hard drive. Access to this data is limited.

We operate within the Government framework for information sharing. We have a secure online encrypted portal with password security.

Personnel data is held for 7 years. Service user Information data is held for 5 years.

Our Information Asset Owner (IAO) is Lynda Richardson.

## Appendix 1

### Your rights about your personal information

There are rules about how organisations keep people's personal information.

These rules are called the General Data Protection Regulations or GDPR.

The rules give people rights about how organisations keep their personal information.

### What is personal information?

Personal information is information that can be used to identify you. This includes:

• Your name

• Your address

• Your telephone number

• Your email address

• Links to your social media accounts like Facebook, Twitter or Instagram

### Your rights

You have the right to be told if anyone is collecting or using your personal information. You have the right to know:

• Why they have collected your personal information

• How long they will keep it for

• Who they will share it with

### How Toby Henderson Trust store and use your records

- The Toby Henderson trust keeps records in-line with laws on data protection and confidentiality.
- We share information with those who are involved in providing you with care and treatment. – with your permission
- In some circumstances we will also share anonymised information for research.
- We share information when the law requires us to do so.

- You have the right to be given a copy of your records.
- You have a right and say on the sharing of your personal information.

**Appendix 2**

Service users - privacy notice

## What data do we have?

So that we can provide a safe and professional service, we need to keep certain records about you. We may process the following types of data:

- Your basic details and contact information e.g. your name, address, date of birth and next of kin.
- Your financial details (if applicable) e.g. details of how you may donate to us.

We also record the following data which is classified as “special category”:

- Health and social care data about you, which might include both your physical and mental health data.
- We may also record data about your race, ethnic origin, sexual orientation or religion.

## Why do we have this data?

We need this data so that we can provide high-quality care and support. By law, we need to have a lawful basis for processing your personal data.

We may also process your data with your consent. If we need to ask for your permission, we will offer you a clear choice and ask that you confirm to us that you consent. We will also explain clearly to you what we need the data for and how you can withdraw your consent at any time.

Where do we process your data?

So that we can provide you with high quality care and support we need specific data. This is collected from or shared with:

1. You or your legal representative(s).
2. Third parties.

We do this face to face, via phone, via email and via post.

Third parties are organisations we might lawfully share your data with. These include:

- Other parts of the health and care system such as the GP, social workers, clinical commissioning groups, and other health and care professionals.

- The Local Authority.
- Your family or friends – with your permission.
- Organisations we have a legal obligation to share information with i.e. for safeguarding.
- The police or other law enforcement agencies if we have to by law or court order.

## Appendix 3

Employees of The Toby Henderson trust privacy notice

**What data do we have?**

So that we can provide a safe and professional service, we need to keep certain records about you. We may record the following types of data:

- Your basic details and contact information e.g. your name, address, date of birth, National Insurance number and next of kin.
- Your financial details e.g. details so that we can pay you, insurance, pension and tax details.
- Your training records.

We also record the following data which is classified as “special category”:

- Health and social care data about you, which might include both your physical and mental health data – we will only collect this if it is necessary for us to know as your employer, e.g. fit notes or in order for you to claim statutory maternity/paternity pay.
- We may also, with your permission, record data about your race, ethnic origin, sexual orientation or religion.

As part of your application, you are required to undergo a Disclosure and Barring Service (DBS) check (Criminal Record Check). We do not keep this data once we’ve seen it.

We require this data so that we can contact you, pay you and make sure you receive the training and support you need to perform your job. By law, we need to have a lawful basis for processing your personal data.

We process your data because

- We have a legal obligation under UK employment law.
- We are required to do so in our performance of a public task.

We process your special category data because

- It is necessary for us to process requests for sick pay or maternity pay.

If we request your criminal records data, it is because we have a legal obligation to do this due to the type of work you do. This is set out in the Data Protection Act 2018 and the Rehabilitation of Offenders Act 1974 (Exceptions) Order 1975. We do not

keep a record of your criminal records information (if any). We do record that we have checked this.

We may also process your data with your consent. If we need to ask for your permission, we will offer you a clear choice and ask that you confirm to us that you consent. We will also explain clearly to you what we need the data for and how you can withdraw your consent.

**Where do we process your data?**

As your employer we need specific data. This is collected from or shared with:

1. You or your legal representative(s).
2. Third parties.

We do this face to face, via phone, via email, via post and via application forms.

Third parties are organisations we have a legal reason to share your data with. These include:

- Her Majesty's Revenue and Customs (HMRC).
- Our pension
- Our external payroll provider
- Organisations we have a legal obligation to share information with i.e. for safeguarding.
- The police or other law enforcement agencies if we have to by law or court order.

The DBS Service used by TTHT is Aarons Department, 43 Church Lane, Pudsey, Leeds, West Yorkshire LS28 7RR.


the Toby Henderson
Trust