Data Protection and Personal Information Management Policy

1. Purpose of this policy

This policy sets out how Tom's Trust complies with the UK data protection legislations, including the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA18), the Privacy and Electronic Communications Regulations 2003 (PECR), and the Data (Use and Access) Act 2025 (DUAA).

It sets out how we collect, use, store, share and protect personal data lawfully, fairly and transparently. It should be read alongside our Privacy Policy which explains to individuals how and why we use their personal information.

2. Scope

This policy applies to all personal data held or processed by Tom's Trust, including data relating to:

- Donors and supporters and prospective supporters
- Beneficiaries and their families
- Staff, volunteers and job applicants
- Event participants and attendees
- Website and digital service users

It applies to personal data held electronically in our approved systems and platforms as well as information held in paper records.

3. Data we collect and process

We collect and process personal information where it is relevant and proportionate to our work.

This may include:

- identity and contact information, such as name, address, email address and telephone number

- donation, fundraising, event and engagement history
- interests, relationships and communication preferences
- information relevant to supporter stewardship, prospect research and fundraising, including information obtained from reputable publicly available sources or trusted service providers
- limited health and other special category information where necessary for our work with beneficiaries, families, staff or volunteers and where appropriate safeguards are in place
- website and digital usage information, including relevant analytics and cookie identifiers.

We will only collect and retain personal information that is necessary and proportionate for the purpose for which it is being used.

4. Lawful bases for processing

We only process personal data where we have a lawful basis to do so under UK data protection law. Depending on the purpose, we may rely on:

- Consent – where an individual has given us clear consent to use their information for a specific purpose, including certain electronic marketing where consent is required.
- Contract – where processing is necessary to enter into or fulfil a contract with an individual, for example in relation to employment or certain services.
- Legal obligation – where processing is necessary to meet a legal requirement, for example Gift Aid, financial reporting or other regulatory obligations.
- Legitimate interests – where processing is necessary for Tom's Trust's legitimate interests, or those of a third party, and these interests are not overridden by the individual's rights and interests. This may include managing supporter relationships, fundraising and stewardship, maintaining accurate records and proportionate supporter research and profiling. We will document our assessment where appropriate and provide individuals with clear information about the processing and their right to object.
- Vital interests – where processing is necessary to protect someone's life.

- Recognised legitimate interests – where processing is necessary for one of the specific purposes recognised in UK data protection legislation. This is distinct from the ordinary legitimate interests basis above and will not normally apply to fundraising, marketing or supporter profiling.

Special category data

Some personal information requires additional protection under data protection law, including information about health, ethnicity, religion and sexual orientation. Where Tom's Trust processes special category data, we will identify both an appropriate lawful basis for processing and an additional condition for processing that information under UK data protection law. We will only collect and use this information where necessary and will apply appropriate safeguards.

5. Data storage and security

Tom's Trust takes appropriate technical and organisational measures to protect personal data against unauthorised or unlawful access, use, disclosure, alteration, loss or destruction.

- Personal data is stored only in approved systems, platforms and locations with appropriate security and access controls.
- Access to personal data is limited to staff, volunteers and others who need it for their role and have received appropriate training.
- Personal data must only be accessed, stored, transferred or shared using approved methods and systems.
- Paper records containing personal data must be stored securely and disposed of securely when no longer required.
- Access permissions and security arrangements are reviewed as appropriate.

6. Data sharing

Tom's Trust does not sell or rent personal data.

We may share personal data where necessary with:

- trusted service providers who process information on our behalf, such as mailing, payment processing, IT and data services
- professional advisers, such as auditors, accountants, insurers and legal advisers
- regulatory, statutory or public authorities where required or permitted by law

- other organisations where there is a lawful basis for doing so and appropriate safeguards are in place.

We only share the personal data necessary for the relevant purpose and require organisations processing personal data on our behalf to handle it appropriately and securely.

Where personal data is transferred outside the UK, we will ensure that appropriate safeguards are in place as required by UK data protection law.

7. Retention of data

Tom's Trust will only retain personal data for as long as it is needed for the purpose for which it was collected, or where we are required to retain it for legal, regulatory, financial, safeguarding or other legitimate purposes.

Retention periods will take account of the type of information, the reason it is held and any relevant legal or regulatory requirements. Where information is no longer required, it will be securely deleted, destroyed or anonymised.

Some records, including financial, donation, legacy and safeguarding information, may need to be retained for longer periods. We will keep only the information necessary for those purposes and review it appropriately.

Our detailed retention periods are set out in our data retention schedule.

8. Individual rights and subject access

Individuals have rights over their personal data under UK data protection law. Depending on the circumstances, these include the right to:

- access their personal data
- have inaccurate information corrected
- request erasure or restriction of their personal data
- receive or transfer their personal data where the right to data portability applies
- withdraw consent where we rely on consent
- object to direct marketing at any time
- object to processing based on legitimate interests

Requests should be sent to info@tomstrust.org.uk and will be handled in accordance with applicable data protection law.

Subject Access Requests (SARs): We will respond to Subject Access Requests without undue delay and normally within one month. We will carry out searches that are reasonable and proportionate in the circumstances.

Where we reasonably require further information to identify the individual or clarify the information being requested, the response period may be paused until that information is received, where permitted by law.

Data Protection complaints

Individuals have the right to complain to Tom's Trust about how their personal data has been handled. We will acknowledge data protection complaints within 30 days and take appropriate steps to investigate and respond without undue delay.

Data protection complaints will be recorded and monitored by the Data Protection Lead, with significant or repeated issues escalated to the CEO and Trustees where appropriate.

Individuals also have the right to raise concerns with the Information Commissioner's Office (ICO).

9. Direct marketing and supporter communications

Tom's Trust communicates with supporters about our work, fundraising, events and ways to support our charitable purposes. We will comply with UK data protection law and the Privacy and Electronic Communications Regulations (PECR) when carrying out direct marketing.

Post

We may contact supporters by post where we have a legitimate interest in doing so, taking account of the individual's relationship with Tom's Trust, their reasonable expectations and their right to object.

Electronic communications

We may send fundraising and other direct marketing by email, text message or other electronic messaging where:

- the individual has given valid consent; or
- the charitable purposes soft opt-in applies.

Where we rely on the charitable purposes soft opt-in, Tom's Trust must have obtained the individual's contact details directly from them on or after 5 February 2026 when they expressed an interest in, offered or provided support for our charitable purposes. They must have been given a clear

opportunity to opt out when their details were collected and must be given a simple opportunity to opt out in every subsequent marketing communication.
We will maintain appropriate records of the basis on which we send direct marketing communications and respect individuals' communication preferences and objections.
Individuals can opt out of direct marketing at any time.

10. Data breach procedure

Any actual or suspected personal data breach must be reported immediately to the Data Protection Lead or CEO.

Tom's Trust will investigate the breach promptly, take appropriate steps to contain it and assess the potential risk to individuals.

Where a personal data breach is likely to result in a risk to individuals' rights and freedoms, Tom's Trust will notify the Information Commissioner's Office without undue delay and, where required, within 72 hours of becoming aware of the breach.

Where a breach is likely to result in a high risk to individuals, we will also inform affected individuals without undue delay where required by law.

All personal data breaches will be recorded, including the circumstances of the breach, its effects, action taken and the reasons for any decision about whether notification was required. Appropriate corrective action will be taken to reduce the risk of recurrence.

11. Staff and volunteer responsibilities

Everyone who handles personal data on behalf of Tom's Trust has a responsibility to protect it and follow this policy and our related procedures.
Staff and volunteers must:

- complete appropriate data protection training on induction and refresher training as required
- only access and use personal data necessary for their role
- use approved systems and follow secure working practices when accessing, storing, transferring or sharing personal data
- take reasonable steps to keep personal data accurate and up to date
- only retain personal data for as long as it is required and store it in the appropriate location

- not disclose or share personal data unless authorised to do so and there is an appropriate basis for sharing it
- report any actual or suspected data breach or other data protection concern immediately to the Data Protection Lead or CEO.

Failure to follow this policy may be dealt with under Tom's Trust's relevant disciplinary or volunteer procedures.

12. Cookies, similar technologies and PECR/DUAA

Tom's Trust uses cookies and similar technologies on its website and digital services. We will comply with applicable data protection legislation and the Privacy and Electronic Communications Regulations (PECR) when using these technologies.

Cookies and similar technologies that require consent will not be used unless the user has given valid consent. Where consent is not required by law, we will provide appropriate information about their use and any available options to object or opt out.

Users will be provided with clear information about the cookies and similar technologies we use, their purposes and how they can manage their preferences through our Cookie Notice and website controls.

We will review the cookies and similar technologies used on our website periodically and when significant changes are made to the website or the services we use.

13. Governance and accountability

The Board of Trustees has overall responsibility for ensuring that Tom's Trust meets its data protection obligations.

The CEO is accountable to the Board for data protection and the designated Data Protection Lead oversees day-to-day compliance, provides advice and supports staff in applying this policy.

Tom's Trust will maintain appropriate records to demonstrate compliance with data protection law. These will include, where relevant:

- records of processing activities
- data processing and data sharing agreements
- Data Protection Impact Assessments (DPIAs)
- Legitimate Interests Assessments (LIAs)

- records relating to data breaches, complaints and individual rights requests
- records of consent and communication preferences where appropriate.

Data protection risks and compliance will be reviewed periodically, with significant issues reported to the CEO and Trustees as appropriate.

14. Monitoring and review

This policy will be reviewed annually, or sooner where there are significant changes to legislation, regulatory guidance or the way Tom's Trust collects or uses personal data.

The Data Protection Lead is responsible for coordinating the review and the policy will be approved by the Board of Trustees.

15. Contact

Questions or complaints about this policy:
info@tomstrust.org.uk
Tom’s Trust, PO Box 276, Saffron Walden, Essex CB10 9GE

Chief Executive Officer (CEO)
Rebecca Wood
Email: rebecca.wood@tomstrust.org.uk

Designated Data Protection Lead
Kirsty Keegan, Head of Fundraising & Communications
Email: kirsty.keegan@tomstrust.org.uk

This is the Tom’s Trust GDPR & Data Protection Policy

Next review: August 2027 (or sooner if ICO/Government guidance changes)

Andrew Woosey

Chair

September 2026