Data Protection policy

This policy provides information about the data protection legislation, including the General Data Protection Regulation ("GDPR") with which Touch Trust ("we", "our", "us") must comply.

This policy applies to all members of staff, trustees, volunteers and others who do work for us.

This policy provides a general overview of the legal requirements. It sets out what we expect from you in general terms when handling personal information, regardless of the format in which it is stored. This includes information about:

- Current or former employees and workers and applicants
- Current or former volunteers and applicants
- Current or former trustees and applicants
- Beneficiaries/clients/users of our services
- Users of our online and digital media channels
- Current, former or potential supporters, donors and funders including individuals and representatives of organisations
- People with whom we engage in relation to our campaigning activity
- Representatives of organisations with whom we have partnerships or we are collaborating
- Representatives of our suppliers

You must read, understand and comply with this policy when handling personal information on our behalf and attend any compulsory training on its requirements. The policy may be supplemented by specific guidance relevant to your role.

Your compliance with this policy is mandatory. Any breach of this policy may result in disciplinary action.

1. DEFINITIONS

The following definitions are used in this policy:

Controller	means the person or organisation that determines when, why and how to process Personal Data. We are the Data Controller of all Personal Data used in our organisation for our own purposes
Data Subject	means a living, identified or identifiable individual about whom we hold Personal Data

Data Privacy Impact Assessment (DPIA)	means a tools and assessment used to identify and reduce risks of a data processing activity. A DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or business change programs involving the processing of Personal Data
Data Processors	means any third parties who we use to Process Personal Data on our behalf
Data Protection Officer (DPO)	means the person with responsibility for data protection compliance within our organisation. The current person is Beverly Garside, CEO. Bev.Garside@touchtrust.co.uk
Personal Data	means any information identifying a Data Subject or information relating to a Data Subject form which we can identify (directly or indirectly) a Data Subject whether from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Data includes Special category Personal Data and Pseudonymised Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour
Personal Data Breach	means any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach
Privacy by Design	means implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the data protection legislation
Privacy Notice	means a notice setting out information that should be provided to Data Subjects when we collect information about them
Processing or Process	means any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. processing also includes transmitting or transferring Personal Data to third parties
Pseudonymisation or Pseudonymised	means replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure

Special Category Personal Data	means information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and relating to criminal offences and convictions

2. DATA PROTECTION PRINCIPLES

The law requires that Personal Data must be:

- Processed lawfully, fairly and in a transparent manner;
- collected only for specified, explicit and legitimate purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;
- accurate and where necessary kept up to date;
- not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is processed;
- processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.

Personal Data must also not be transferred to outside the UK and the EEA country without appropriate safeguards being in place.

We are required to enable Data Subjects to exercise certain rights in relation to their Personal Data.

We must also comply with particular legal requirements when suppliers that carry out services for us have access to Personal Data and when we are working with organisations and need to share Personal Data.

We are responsible for and must be able to demonstrate compliance with the requirements under the law (accountability).

3. LAWFULNESS AND FAIRNESS

Personal data must be processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

You may only collect, Process and share Personal Data fairly and lawfully and for specified purposes. The law restricts our actions regarding Personal Data to specified lawful purposes. These restrictions are not intended to prevent processing, but ensure that we Process Personal Data fairly and without adversely affecting the Data Subject.

The lawful bases available when processing non-special category personal data are:

- the Data Subject has given consent to the processing of his or her personal data for one or more specific purposes
- the processing is necessary for the performance of a contract between us and the Data Subject or in order to take steps at the request of the Data Subject prior to entering into a contract

- the processing is necessary for compliance with a legal obligation to which we are subject
- the processing is necessary in order to protect the vital interests of the Data Subject or of another natural person
- the processing is necessary for the performance of a task carried out in the public interest
- the processing is necessary for the purposes of legitimate interests we are pursuing or which a third party is pursuing, except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject which require protection of personal data, in particular where the Data Subject is a child.

A range of additional legal requirements apply when processing special category personal data. One of the lawful basis identified above is required as well as a separate lawful basis from the following list:

- processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by law;
- processing is necessary to protect the vital interests of the data subject or of another natural person or guardians where the data subject is **physically or legally incapable and vulnerable** to make informed decisions in accordance with the definition of Mental Capacity Act (2005);
- processing of personal data is required from parents and/or guardians where the data subject is under 16, but it is best practise to do make the consent explained in an accessible manner and obtained where appropriate from the data subject as the UK has determined the relevant age at which a child can give their own consent is 13;
- processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;
- processing relates to personal data which are manifestly made public by the data subject;
- processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity
- processing **is necessary for reasons of substantial public interest**, on the basis of the aim pursued and/or the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject
- processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services
- processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical

devices, for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy

4. TRANSPARENCY

The law requires us to provide detailed, specific information about our use of Personal Data to Data Subjects. Such information must be provided through appropriate Privacy Notices which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a Data Subject can easily understand them.

Whenever we collect Personal Data directly from Data Subjects, we must provide the Data Subject with information including who we are and how and why we will Process, disclose, protect and retain their Personal Data. This is done through a Privacy Notice which must be presented when the Data Subject first provides the Personal Data.

When Personal Data is collected indirectly (for example, from a third party or publicly available source), we must provide the Data Subject with the Privacy Notice information as soon as possible but no later than one month after collecting/receiving the data. We must also check that the Personal Data was collected by the third party in accordance with law and on a lawful basis which contemplates our proposed Processing of that Personal Data.

Informed consent must be sought from all parties for collection of any Personal Data, including video and audio recordings. Consent should be collected in writing on a form that is understandable and makes clear any use of the Data. Children under 16 and Vulnerable Adults who may have not capacity to make decisions under Mental Capacity Act (2006) are not automatically presumed to be legally competent to make decisions about their preferences. However, it is vital that we seek consent from them as some are deemed competent if presented in a way the subject understands what is proposed as well as from their trusted guardians and agencies to act in the best interest for the Data Subject.

5. PURPOSE LIMITATION

Personal Data must be collected only for specified, explicit and legitimate purposes. It must not be further processed in any manner incompatible with those purposes.

You cannot use Personal Data for new, different or incompatible purposes from that disclosed when it was first obtained unless you have informed the Data Subject of the new purposes and there is a lawful basis for doing so.

6. DATA MINIMISATION

Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

You may only collect Personal Data that you require for your duties: you should not collect excessive data. You should ensure any Personal Data collected is adequate and relevant for the intended purposes.

7. ACCURACY

Personal Data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.

You should ensure that the Personal Data we use and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it. You should check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. You must take all reasonable steps to amend inaccurate or out-of-date Personal Data.

8. RETENTION

Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed. We will maintain retention policies and procedures to ensure Personal Data is deleted in accordance with this requirement.

9. SECURITY

Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

You are responsible for protecting the Personal Data we hold.

You may only Process Personal Data when required to do so as part of your role. You cannot Process Personal Data for any reason unrelated to your role.

You must ensure that you follow all guidelines issued to you that are designed to protect against unlawful or unauthorised processing of Personal Data and against the accidental loss of, or damage to, Personal Data. You must exercise particular care to protecting Special Category Personal Data from loss and unauthorised access, use or disclosure.

10. REPORTING A DATA BREACH

The law requires Data Controllers to notify any Personal Data Breach to the Information Commissioner's Office (ICO) and, in certain instances, the Data Subject.

If you know or suspect that a Personal Data Breach has occurred, do not attempt to investigate the matter yourself. You should follow the Personal Data Breach reporting policy. You should **immediately** contact the DPO or in his/her absence, their line manager. You should preserve all evidence relating to the potential Personal Data Breach. This include accidental data breaches such as leaving your unprotected computer / data in a café or theft of an unprotected device.

11. TRANSFER LIMITATION

The law restricts data transfers to countries outside the UK and European Economic Area (EEA) where they do not have adequate data protection laws. If you need to send Personal Data outside, you should contact the DPO for advice.

12. DATA SUBJECT RIGHTS

Data Subjects have rights when it comes to how we handle their Personal Data. These include rights to:

- where processing is based on the lawful basis of consent, to withdraw consent to processing at any time;
- receive certain information about our processing activities;
- request access to their Personal Data that we hold;
- prevent our use of their Personal Data for direct marketing purposes;
- ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or processed or to rectify inaccurate data or to complete incomplete data;
- restrict processing in specific circumstances;
- challenge processing which has been justified on the basis of our legitimate interests or in the public interest;
- be notified of a Personal Data breach which is likely to result in high risk to their rights and freedoms; and
- in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine readable format.

You must immediately forward any Data Subject request you receive to the DPO.

13. SHARING DATA

You may only transfer Personal Data to third-party service providers who agree to comply with our policies and procedures and who agree to put adequate security measures in place, as requested. We must have a written data processing agreement in place with any such service providers we are using.

In addition, although it is not a legal requirement, it is good practice to have a data sharing agreement with any partners with which we are working that deals with sharing Personal Data. It is essential that you have a clear lawful basis for sharing Personal Data with such partners and that you transmit the Personal Data securely.

14. DEMONSTRATING COMPLIANCE

The law requires us to keep full and accurate records of all our processing activities. You should ensure that any processing of Personal Data that you undertake is included in the records by checking with the DPO.

We are required to ensure all people who work for us have undergone adequate training to enable them to comply with data privacy laws.

We are required to implement Privacy by Design measures when processing Personal Data by implementing appropriate technical and organisational measures (like Pseudonymisation) in an effective manner, to ensure compliance with data privacy principles. Emails and files which may contain any Personal Data should be password protected (through office logins and emails) and if sending/receiving outside the organisational emails, they must be password protected or pseudonymised.

Data controllers must also conduct DPIAs in respect to high risk processing. If you believe processing that you are carrying out is high risk, please speak to the DPO.

We must also regularly test our systems and processes to assess compliance. You must regularly review all the systems and processes under your control to ensure they comply with this policy and check that adequate governance controls and resources are in place to ensure proper use and protection of Personal Data.

This policy will be reviewed every three years or whenever new legislation makes it necessary (Last updated May 2022)