Torry Development Trust is a Company Registered as SC480641 (Scotland) and a Charity Registered as SC047191

Data Protection Policy
Version 1.0

Date:
April 2024

CONTENTS

The Trust will be responsible for reviewing this policy from time to time and updating the Website in relation to its data protection responsibilities.

Data Protection Policy

1 Overview

1.1 Torry Development Trust (TDT) takes the security and privacy of personal information seriously. As part of its activities, the Trust needs to gather and use personal information about a variety of people including members, former members, employees, officeholders and generally people who are in contact with us. The Data Protection Act 2018 (the "2018 Act") and General Data Protection Regulation ("GDPR") regulate the way in which personal information about living individuals is collected, processed, stored, or transferred.

1.2 This policy explains what the Trust will do when any personal data belonging to or provided by data subjects, is collected, processed, stored, or transferred on its behalf by others. TDT expects anyone processing personal data on its behalf (see paragraph 5 for a definition of "processing") to comply with this policy in all respects.

1.3 The Trust has a separate Privacy Notice which outlines the way in which we use personal information provided to us.

1.4 All personal data will be held in accordance with our Data Retention Policy, which is an appendix to this Policy. Data will only be held for as long as necessary for the purposes for which it is collected.

1.5 This policy does not form part of any contract of employment (or contract for services if relevant) and can be amended by the Trust at any time. It is intended that this policy is fully compliant with the 2018 Act and GDPR. If any conflict arises between those laws and this policy, the Trust intends to comply with the 2018 Act and GDPR.

1.6 Any deliberate or negligent breach of this policy by an employee or office-bearer of the Trust may result in disciplinary action being taken in accordance with our disciplinary procedure. It is a criminal offence to conceal or destroy personal data which is part of a subject access request (see Paragraph 12) and such conduct by an employee would amount to gross misconduct which could result in dismissal.

2 Data Protection Principles

2.1 Personal data will be processed in accordance with the six '**Data Protection Principles**.' It must:

- be processed fairly, lawfully, and transparently.
- be collected and processed only for specified, explicit and legitimate purposes.
- be adequate, relevant, and limited to what is necessary for the purposes for which it is processed.

- be accurate and kept up to date. Any inaccurate data must be deleted or rectified without delay.
- not be kept for longer than is necessary for the purposes for which it is processed.
- be processed securely.

We are accountable for these principles and must be able to demonstrate compliance.

3 Definition of personal data

3.1 **"Personal data"** means information which relates to a living person (a "data subject") who can be identified from that data on its own, or when taken together with other information which is likely to come into the possession of the data controller. It includes any expression of opinion about the person and an indication of the intentions of the data controller or others, in respect of that person. It does not include anonymised data.

3.2 This policy applies to all personal data whether it is stored electronically, on paper or on other materials.

3.3 '**Special categories of personal data**' are types of personal data consisting of information revealing:

racial or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; genetic or biometric data; health; sex and sexual orientation; and any criminal convictions and offences.

4 Definition of processing and how personal data should be processed.

4.1 **'Processing'** means any operation which is performed on personal data, such as collection, recording, organisation, structuring or storage; adaption or alteration; retrieval, consultation or use; disclosure by transmission, dissemination or otherwise making available; and restriction, destruction or erasure.

4.2 Everyone who processes data on behalf of the Trust is responsible for ensuring that the data collected and stored is handled appropriately, in line with this policy, our Data Retention policy and our Privacy Notice.

4.3 Personal data should only be accessed by those who need it for their activities on behalf of the Trust. Data should be used only for the specified lawful purpose for which it was obtained.

4.4 The legal bases for processing personal data (other than special category data, which is referred to in Paragraph 8) are that the processing is necessary for the purposes of the Trust's legitimate interests; or that (so far as relating to any staff whom we employ) it is necessary to exercise the rights and obligations of the Trust under employment law.

4.5 Personal data held in all ordered manual files and databases should be kept up to date. It should be shredded or disposed of securely when it is no longer needed. Unnecessary copies of personal data should not be made.

5. Privacy Notice

5.1 If someone would not reasonably expect the way in which we use their personal data, we will issue information about this using a Privacy Notice which will be given to them at the point when the data is provided.

5.2 If our use of personal data is what someone would reasonably expect, we will provide information about this using a Privacy Notice which will be available on the Trust's website and will be printed from time to time in Trust communications.

6. Keeping personal data secure

6.1 Personal data should not be shared with those who are not authorised to receive it. Care should be taken when dealing with any request for personal information over the telephone or otherwise. Identity checks should be carried out if giving out information to ensure that the person requesting the information is either the individual concerned, or someone properly authorised to act on their behalf.

6.2 Hard copy personal information should be stored securely (in lockable storage, where appropriate) and not visible when not in use. Filing cabinets and drawers and/or office doors should be locked when not in use. Keys should not be left in the lock of the filing cabinets/lockable storage.

6.3 Passwords should be kept secure, should be strong, changed regularly and not written down or shared with others.

6.4 Emails containing personal information should not be sent to or received at a work email address as this might be accessed by third parties.

6.5 The 'bcc' rather than the 'cc' or 'to' fields should be used when emailing a large number of people, unless everyone has agreed for their details to be shared amongst the group.

6.6 Personal data should be encrypted or password-protected before being transferred electronically.

7. Sharing personal data

7.1 TDT will only share someone's personal data where there is a legal basis to do so, including for any legitimate interests within the operations of the Trust. This may require information relating to criminal proceedings or offences or allegations of offences to be processed for the protection of children or adults who may be at risk.

7.2 We will not send any personal data outside the United Kingdom. If this changes, all individuals affected will be notified and the protections put in place to secure the personal data, in line with the requirements of the GDPR.

8. How to deal with data security breaches

8.1 Should a data security breach occur likely to result in risk to the rights and freedoms of any individuals, then the Information Commissioner's Office (ICO) must be notified within 72 hours.

8.2 Breaches will be handled by the ICO under data security breach management procedure.

9. Subject access requests

9.1 Data subjects can make a subject access request to find out what information is held about them to Torry Development Trust Ltd, c/o Grant Smith Solicitors and estate Agents, Amicable House, 252 Union Street, Aberdeen AB10 1TN and a response should be expected within the necessary time limit (30 days).

9.2 It is a criminal offence to conceal or destroy personal data which is part of a subject access request.

10. Data subject rights

10.1 Data subjects have the right to request that TDT corrects any inaccuracies in their personal data and erase their personal data where we are not entitled by law to process it or it is no longer necessary to process it for the purpose for which it was collected. Data should be erased when an individual revokes their consent (and consent is the basis for processing); when the purpose for which the data was collected is complete; or when compelled by law.