Data protection policy - The Cotton Tree Trust

Aims

The Cotton Tree Trust ('the Trust') is committed to complying with the requirements of the Data Protection Act 1998 (DPA) and the General Data Protection Regulation (GDPR). In order to carry out its services, the Trust needs to obtain and hold certain personal data about individuals (trustees, employees, volunteers, and service users). The purpose of this policy is to ensure that this data is treated and held in the correct and lawful way, in order to protect the privacy of the individuals whose personal data is being obtained and held.

All employees, trustees, volunteers, and people working on behalf of the charity have a responsibility to be aware of and to follow these guidelines on the handling of personal data. The Trust is responsible for ensuring that everyone has access to and has read and understood this document.

Information Commissioner's Office

The Trust is registered as a data controller with the Information Commissioner's Office.

Definitions

Personal data is defined by the GDPR as any information relating to an identified or identifiable person. This may include (but is not limited to):

- Names and addresses of employees, trustees, volunteers
- Records on performance and training
- Job applications and CVs
- Payroll information
- Personal information and case notes about service users
- Personal information about donors
- Location data or online identifiers

Special categories of personal data are defined by the GDPR as data that pertain to:

- The racial or ethnic origin of the subject

- The subject's political opinions
- The subject's religious or philosophical beliefs
- Whether the subject is a member of a trade union
- Information on the subject's physical or mental health condition
- Information on the subject's sex life or sexual orientation
- Genetic or biometric data

Special categories of personal data can only be processed with the explicit consent of the data subject, or where it is in the substantial public interest, necessary to protect the vital interests of the data subject or another person, or required by law.

Data Controller: the Cotton Tree Trust acts as a Data Controller under the GDPR, meaning that it determines the purposes for which personal information will be used.

Data Processor: a third party that processes data on behalf of the Data Controller (such as an external supplier). The Trust is responsible for ensuring that any external suppliers who process data comply with data protection requirements.

General Data Protection Regulation - principles of data protection

The GDPR outlines six principles for obtaining, handling, processing, transporting and storing personal data. All employees, trustees, volunteers, and people working on behalf of the charity must adhere to these principles at all times:

1. **Lawfulness, fairness, and transparency.** Data subjects must be made aware of how their data will be processed. Data processing must meet one of the legal justifications for processing.
2. **Purpose limitation.** Personal data can only be obtained for 'specified, explicit, and legitimate purposes'. Data can only be used for the specific processing purpose of which the subject has been made aware and no other, without further consent or lawful basis.
3. **Data minimisation.** Data collected should be 'adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed'.
4. **Accuracy.** Data must be accurate and kept up to date.
5. **Storage limitation.** Data should be 'kept in a form which permits identification of data subjects for no longer than necessary', i.e., it should be deleted, destroyed, or anonymised when it is no longer required.
6. **Integrity and confidentiality.** Data has to be handled securely and be protected against unlawful processing or accidental loss, destruction, or damage.

Processing data

- If the Trust plans to carry out any data processing that poses a high level of risk to the data subject, it must first carry out a Data Protection Impact Assessment examining potential risks and how these can be mitigated. If the level of risk is still determined to be high, then the Trust should contact the ICO for further guidance.

- The Trust will hold a Data Inventory specifying what data the Trust holds, where it is stored, how it has been processed, and the legal justification for processing.
- The Trust will be responsible for testing and updating data systems on a regular basis.

Data collection

The Trust is responsible for ensuring that data is collected within the boundaries defined in this policy. When collecting data, the Trust will:

- Ensure that the subject understands why the information is needed and what it will be used for
- Obtain the subject's consent to the collection and processing of data
- Only collect information that it is needed to fulfil operational needs or legal requirements

Data storage

All data needs to be stored securely to avoid loss or damage, and to ensure that access to personal data is restricted to authorised persons. In order to ensure this, the following procedures will be followed:

- All hard copy files on personnel and service users will be kept in a locked cabinet and can only be accessed by trustees and authorised employees
- Any sensitive data can only be accessed with the appropriate level of authorisation, and only by employees/volunteers who specifically require this information to carry out their duties
- All data on laptops, smartphones, and other devices must be password protected and have anti-virus software installed
- Data will be appropriately saved and backed up to allow for the ability to restore access to data in case of loss or technical difficulties
- Passwords must be secure and must be changed on a regular basis
- Employees/volunteers are responsible for ensuring that any personal data that they hold is stored securely and that personal information is not disclosed either orally or in writing or otherwise to any unauthorised third party
- The Trust will take reasonable steps to ensure that data held is up to date by asking data subjects whether there have been any changes.

Disposing of data

All documents containing personal data, whether in paper or electronic format, will be disposed of securely when they are no longer needed.

- Paper documents containing personal data will be shredded
- Information stored on old employee electronic equipment will be erased before the equipment is disposed of
- Employees, volunteers and trustees are responsible for ensuring that any documents containing personal data which are brought home are disposed of with the same level of care
- Any employees, volunteers, or trustees who leave the Trust must responsibly dispose of any data at their home or kept on their electronic devices when their involvement comes to an end

Disclosure

The Cotton Tree Trust may from time to time share data with other agencies in order to offer its services. Where this is the case:

- Any data processors used by the trust will be required to provide sufficient guarantees for their data security measures and compliance
- The data subject will be made aware of how and with whom their information will be shared
- The data will not be shared without the consent of the individual concerned, unless this is required by law, or if there is reason to believe that a vulnerable adult, child, or any other person might be at serious risk of harm if that information is not shared

The trust may also disclose data without consent if that data is publicly available

Data access and accuracy

All data subjects have the right to:

- Access the personal data we hold about them.
- Have inaccurate or incomplete personal data corrected, completed, or removed
- Request that the Trust stop processing their data if this processing is likely to cause unwarranted damage or distress to the individual or to anyone else
- Object to the processing of their personal data for direct marketing purposes, for the purpose of the legitimate interests of the data controller, or where processing is deemed to be in the public interest. In this circumstance, the Trust would have to suspend the processing of data until they are able to demonstrate 'compelling legitimate grounds' for processing which override the rights of the data subject.

Any individual wishing to access their information should submit a Data Subject Access Request in writing to the organisation, using a Data Subject Access Request form. Personal information will only be released to the individual to whom it relates, unless there is a legal obligation to release additional information. The requested data must be provided to the data subject within one month of the request.

Staff responsibilities

All employees, trustees, and volunteers are responsible for helping the Trust to comply with its DPA and GDPR obligations.

- Any employees, trustee, or volunteer who becomes aware of any breach of this policy must bring it to the attention of their supervisor
- Any breach may render employees liable to disciplinary action, including dismissal for gross misconduct, or in the case of volunteers, termination of their voluntary position.

Additionally, the Trust needs to hold certain data about its trustees, employees, and volunteers, pertinent to their employment/voluntary involvement. All employees, trustees, and volunteers are responsible for ensuring that personal data provided to us is accurate and up to date, and informing the Trust of any changes.

Breaches of data

A breach of data is defined as 'a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed'.

- If a data breach is unlikely to result in a risk for the data subjects, then the details of the breach simply need to be recorded in a Data Breach Log.
- If the data breach is likely to result in a risk for the data subjects, the Trust must inform the ICO of the breach within 72 hours of becoming aware of it.
- If the data breach poses a high risk to the data subjects, the Trust must inform the data subjects themselves of the breach as soon as possible.

The ICO can be informed of a data breach by telephone (0303 123 1113) or by online form.
https://ico.org.uk/for-organisations/report-a-breach/

Monitoring, review, updates

This policy will be reviewed in September 2018.

Other policies

This policy is to be read in conjunction with the Trust's:

- Confidentiality policy and agreement
- Disciplinary policy and procedure
- Grievance policy and procedure
- Volunteer policy
- Complaints policy and procedure
- Safeguarding policies
- Conflict of interest policy