**DATA PROTECTION POLICY**

THE TARN MOOR ESTATE

**Introduction**

The Tarn Moor Estate needs to collect and use certain types of information about the Data Subjects who come into contact with it in order to carry on its activities. This personal information must be collected and dealt with appropriately– whether on paper, in a computer, or recorded in other material - and there are safeguards to ensure this under the GDPR 2018 and Data Protection Act 2018.

The following list below gives definitions of the technical terms we have used and is intended to aid understanding of this policy.

**Consent** – must be freely given, specific, informed, unambiguous and able to be withdrawn by a Data Subject to the processing of personal information about her/him.

**Data Controller** – The person who (either alone or with others) decides what personal information is held and how it will be held or used.

**Data Protection Act 2018** – The UK legislation that provides a framework for responsible behaviour by those using personal information.

**Data Subject/Service User** – The individual whose personal information is being held or processed by the charity (for example: a client, a volunteer, contractor or adviser)

**General Data Protection Regulation (GDPR) 25 May 2018 –** givesrights and protections to individuals for use of their personal data by organisations

**Information Commissioner** – The UK Information Commissioner responsible for implementing and overseeing the Data Protection Act 1998. Organisations are required to pay a data protection fee to the ICO on an annual basis.

**Processing –** means collecting, amending, handling, storing or disclosing personal information

**Personal Information** – Information about living individuals that enables them to be identified – e.g. name and address. It does not apply to information about organisations, companies and agencies but applies to named persons, such as individual volunteers or contractors working on behalf of the charity.

Sensitive or special category data – means data about:

* Racial or ethnic origin
* Political opinions
* Religious or similar beliefs
* Trade union membership
* Physical or mental health
* Sexual life
* Criminal record
* Criminal proceedings relating to a data subject’s offences

**GDPR Requirements**

|  |  |
| --- | --- |
| **Record Keeping** | Each Data Controller must maintain a record of processing activities under its responsibility. Data Processors must also keep a record of the processing activities they carry out on behalf of a Data Controller. The log can be requested at any time by the ICO. |
| **Privacy Notices** | Under the GDPR, privacy notices must contain information tp be transparent, use clear and plain language, and must be easily accessible.  |
| **Consent** | Individuals have rights to decide how their data is processed. The types of processing activities which require the consent of an individual need to be identified and consents must be captured in a GDPR compliant manner. Where processing personal data is based on consent, an organisation must be able to evidence the consent. Consent must be by an “opt in” method. |
| **Breaches** | Data Controllers must report personal certain types of data breaches to the ICO without ‘undue delay’, and where possible no later than 72 hours after having become aware of the breach. An individual who has suffered damage as a result of a breach can claim compensation from the Data Controller or the Data Processor.  |
| **Right of Access (Subject Access Requests)** | The time limit to comply with a Subject Access Request (“SAR”) is one calendar month. SARs are free of charge. |
| **Data Privacy Impact Assessments (“DPIA”)** | The GDPR makes it mandatory for DPIAs to be carried out in certain situations, eg where new technologies are introduced for high risk processing activities or where there is extensive use of automated processing. DPIAs will need to contain a description of the processing and the purpose of the processing and need to identify any risks to the personal data and the rights and freedoms of individuals, and the measures and safeguards implemented to mitigate these risks.  |
| **Privacy by Design** | When developing, designing or using services or applications which involve processing personal data, Data Controllers and Processors should adopt internal policies and measures to ensure personal data is protected. |
| **Right to Object to processing** | Individuals must be advised of their right to opt out of processing activities, including marketing. Any reasonable requests to object to processing should be stored and evidenced.  |
| **Right to Erasure** | An individual has a right to request that their personal data is deleted. A Data Controller must delete personal data unless there is a legal obligation to retain the personal data. |
| **Profiling** | An individual has the right not to be subject to a decision based solely on “automated processing”, including profiling. This is where a computer, or computer software rather than a human makes a decision about an individual. |
| **Data Protection Officer** | A Data Protection Officer (DPO) may need to be appointed where personal data is processed for regular monitoring of individuals, or any sensitive personal data, on a large scale. The DPO should report to the highest level of management (i.e. the Board) and must be informed about all data protection issues within the organisation. |
| **Right of Portability** | The GDPR introduces a new right of data portability. This right allows for the data which an individual provided to the Data Controller to be provided to the individual in a structured format, to allow it to be provided to another Data Controller. |

**Principles**

## The GDPR has a number of underlying principles. Personal data:

#### Must be processed **lawfully, fairly and transparently**.

#### Should only be used for a **specific processing purpose** that the data subject has been made aware of and no other, without further consent.

#### Should be **adequate, relevant and limited** i.e. only the minimum amount of data should be kept for specific processing.

#### Must be **accurate** and where necessary **kept up to date**.

#### Should **not be stored for longer than is necessary**, and that storage is safe and secure.

#### Should be processed in a manner that ensures **appropriate security and protection.**

**Processing of Data**

## The GDPR sets out six lawful bases for processing personal data. These are:

###### Consent

* A controller must be able to demonstrate that consent was given. Transparency is key: consents given in written declarations which also cover other matters must be clearly distinguishable, and must be intelligible, easily accessible and in clear and plain language.
* Consent is defined as any freely given, specific, informed and unambiguous indication of the data subject’s wishes – either by a statement or by a clear affirmative action.
* Additional criteria apply for consent to be given for the processing of sensitive data, including explicit consent by the data subject and reasons of substantial public interest.

###### Legitimate interests

* This involves a balancing test between the controller (or a third party’s) legitimate interests and the interests or fundamental rights of and freedoms of the data subject – in particular where the data subject is a child. The privacy policy of a controller must inform data subjects about the legitimate interests that are the basis for the balancing of interests.

###### Contractual necessity

* Personal data may be processed if the processing is necessary in order to enter into or perform a contract with the data subject (or to take steps prior to entering into a contract).

###### Compliance with legal obligation

* Personal data may be processed if the controller is legally required to perform such processing (e.g. complying with the requirements of legislation).

###### Vital Interests

* Personal data may be processed to protect the ‘vital interests’ of the data subject (e.g. in a life or death situation it is permissible to use a person’s medical or emergency contact information without their consent).

###### Public Interest

* Personal data may be processed if the processing is necessary for the performance of tasks carried out by a public authority or private organisation acting in the public interest.

**Data Controller**

Tarn Moor Estate is theData Controller under the Act, which means that it determines what purposes personal information held will be used for.

**Disclosure**

Tarn Moor Estate may share data with other bodies such asits agents and its professional advisers.

The Data Subject will be made aware how and with whom their information will be shared. There are circumstances where the law allows the charity to disclose data (including sensitive data) without the data subject’s consent.

The charity regards the lawful and correct treatment of personal information as very important to successful working, and to maintaining the confidence of those with whom we deal.

The charity intends to ensure that personal information is treated lawfully and correctly.

To this end, the charity will adhere to the Principles of Data Protection, as detailed in the GDPR 2018.

Data collection

Tarn Moor Estate will ensure that data is collected in accordance with the Principles of Data Protection, as detailed in the GDPR 2018, and within the boundaries defined in this policy. This applies to data that is collected in person, or by completing a form.

**Data Storage**

Information and records relating to data subjects will be stored securely and will only be accessible to authorised agents and volunteers.

Information will be stored for only as long as it is needed or required by statute and will be disposed of appropriately.

It is the charity’s responsibility to ensure all personal data is non-recoverable from any computer system previously used within the organisation, which has been passed on/sold to a third party.

**Data** **access and accuracy**

All Data Subjects have the right to access the information the charity holds about them. The charity will also take reasonable steps to ensure that this information is kept up to date.

In addition**,** the charity will ensure that:

* It complies with Data Protection principles,
* Everyone processing personal information understands that they are contractually responsible for following good data protection practice,
* Everyone processing personal information is appropriately trained to do so,
* Everyone processing personal information is appropriately supervised,
* Anybody wanting to make enquiries about handling personal information knows what to do,
* It deals promptly and courteously with any enquiries about handling personal information,
* It describes clearly how it handles personal information,
* It will regularly review and audit the ways it holds, manages and uses personal information
* It regularly assesses and evaluates its methods and performance in relation to handling personal information
* All agents and volunteers are aware that a breach of the rules and procedures identified in this policy may lead to disciplinary action being taken against them

This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments made to the Data Protection Act 2018.

In case of any queries or questions in relation to this policy please contact the Clerk to the Trustees.

**This policy is reviewed on an annual basis**