Ecological Land Trust

ECOLOGICAL LAND TRUST

Policy Document

Document Name:	**Data Protection and GDPR Policy**
Approved by Board of Trustees on	29/02/24
Review Schedule	Annual
Next review due	1/03/25

Document Description

We hold personal data about individuals for a variety of charitable purposes. This policy sets out how we seek to protect personal data and ensure that data controllers understand the rules governing the use of personal data to which they have access in the course of their work.

The policy applies to all the processing of personal data carried out by the Ecological Land Trust (ELT) including processing carried out by joint controllers, contractors, and processors.

Implementation & Quality Assurance

Implementation is immediate and this Policy shall stay in force until any alterations are formally agreed.

The Policy will be reviewed every year by the Board of Trustees, sooner if legislation, best practice, or other circumstances indicate this is necessary. All aspects of this Policy shall be open to review at any time.

Aim and Scope

This Policy sets out the obligations of the ELT regarding data protection and the rights of its employees ("data subjects") in respect of their personal data under EU Regulation 2016/679 General Data Protection Regulation ("GDPR"). The policy applies to all the processing of personal data carried out by the ELC including processing carried out by joint controllers, contractors, and processors.

The GDPR defines "personal data" as any information relating to an identified or identifiable natural person (a "data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

Related Legislation
Data Protection Act 2018
UK General Data Protection Regulation (UK GDPR)

Context
Organisations must comply with data protection legislation guided by the six Data Protection Principles.

1. Data protection principles

The ELC is committed to processing data in accordance with its responsibilities under the GDPR. Article 5 of the GDPR requires that personal data shall be:

- processed lawfully, fairly and in a transparent manner in relation to individuals

- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes

- adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed

- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased, or rectified without delay

- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures."

2. General provisions

This policy applies to all personal data processed by the ELT.

The Responsible Person shall take responsibility for the Charity's ongoing compliance with this policy. The Responsible Person for the ELT is Dylan Lindo Jones.

This policy shall be reviewed annually.

The ELT is registered with the Information Commissioner's Office as an organisation that processes personal data.

3. Lawful, fair, and transparent processing

To ensure its processing of data is lawful, fair, and transparent, the ELT shall maintain a Register of Systems. This is a register of all systems or contexts in which personal data is processed by the Charity.

The Register of Systems shall be reviewed annually.

Individuals have the right to access their personal data and any such requests made to the charity shall be dealt with in a timely manner.

4. Lawful purposes

All data processed by the charity must be done on one of the following lawful bases:
consent, contract, legal obligation, vital interests, public task, or legitimate interests.

Since the ELT has fewer than 250 employees, we will only document processing activities that:

- are not occasional; or
- could result in a risk to the rights and freedoms of individuals; or
- involve the processing of special categories of data or criminal conviction and offence data

Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data.

Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be clearly available and systems should be in place to ensure such revocation is reflected accurately in the Charity's systems.

- You must identify valid grounds under the GDPR (known as a 'lawful basis') for collecting and using personal data
- You must ensure that you do not do anything with the data in breach of any other laws
- You must use personal data in a way that is fair. This means you must not process the data in a way that is unduly detrimental, unexpected, or misleading to the individuals concerned
- You must be clear, open, and honest with people from the start about how you will use their personal data

4.1 Lawful Basis

The lawful bases for processing are set out in Article 6 of the UK GDPR. At least one of these must apply whenever you process personal data:

(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose. Consent must always be specific and informed, and reusing the data for a new purpose would unfairly undermine the original consent. You usually need to get fresh consent which specifically covers the new purpose.

(b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract

(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations)

(d) Vital interests: the processing is necessary to protect someone's life

(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law

(f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

For clarification, please refer to the ICO interactive tool to help determine lawful basis before collecting personal data: Lawful basis interactive guidance tool | ICO

5. Special Category Data

Special category data is personal data that needs more protection because it is sensitive. To lawfully process special category data, you must identify both a lawful basis under Article 6 of the UK GDPR **and** a separate condition for processing under Article 9. These do not have to be linked.

All staff must be aware of the risks of processing special category data and the additional rules for processing it.

Any request to collect special data information must be made to the designated Responsible Person who will decide if this is appropriate. If this is allowed, they will ensure the correct procedures are followed for deciding, recording, and processing special category data, including completing a data protection impact assessment (DPIA).

The UK GDPR defines special category data as:

- personal data revealing **racial or ethnic origin**
- personal data revealing **political opinions**
- personal data revealing **religious or philosophical beliefs**
- personal data revealing **trade union membership**
- **genetic data**
- **biometric data** (where used for identification purposes)
- data concerning **health**
- data concerning a person's **sex life**; and
- data concerning a person's **sexual orientation**

This does not include personal data about criminal allegations, proceedings or convictions, as separate rules apply.

6. Data minimisation

The ELT shall ensure that personal data is adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.

7. Accuracy

The ELT shall take reasonable steps to ensure personal data is accurate.

Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date.

8. Individual Rights of Data Subjects

Individuals may ask the ELT to restrict using their information or to stop using it altogether. There are also rights concerning data portability and using data for automatically making decisions.

The GDPR sets out the following rights applicable to all data subjects:

- The right to be informed - being told about the type of information we collect and how we use and look after it
- The right of access - (Subject Access Requests) – being given a copy of the personal data we hold about the individual
- The right to rectification – having inaccurate personal data corrected
- The right to erasure (also known as the 'right to be forgotten') – having personal data deleted from records or records deleted entirely
- The right to restrict processing– requiring us to store but not use personal data concerning the individual
- The right to data portability – being provided with an electronic copy of certain records to use for a different purpose
- The right to object – to put a case forward for stopping processing including marketing
- Rights with respect to automated decision-making and profiling – to have a human reconsider automated decisions and profiling

Some of these rights depend on why the information is being used and considerations can be complex. For this reason, such requests are managed solely by the designated Responsible Person.

9. Subject Access Requests

A subject access request (SAR) is the right of an individual to request a copy of any personal information you may hold on them. The request:

- can be verbal or in writing
- can be submitted by any means, e.g., via web form, email, letter, phone call
- can be made to any part of your business, not just a specific department
- doesn't have to explicitly state the phrase 'subject access request', but must be clear that the individual is requesting their own personal data

Individuals will only be able to request access to their own personal data, unless:

- they are authorised to act on behalf of someone
- the data that relates to another person also happens to relate to them

The ELT will always ask individuals to provide proof of identity complying with their request. This helps avoid third parties gaining unlawful access to personal data. This will only be the minimum information necessary to confirm who they are.

The ELT will reply to a SAR within a calendar month, as per the ICO guidelines. The timescale will begin once proof of identity has been established.

This can be extended if:

- We need to ask for additional clarity about a request. The request for more information will be made within a week of receiving the SAR and the one-month mark for responding will begin when the additional information is received

- the SAR is complex or is part of several requests from the same individual then the timescale can be extended by a further two months

The ELT will respond in an electronic format, unless specifically requested otherwise. Any information given will be concise, transparent, intelligible, using clear and plain language.

The ELT reserves the right to refuse the request under the following circumstance:

- If it is not possible to disclose the information without identifying another individual. If this person does not consent to the disclosure, then it may not be possible to comply with the original request.

- If the request is deemed manifestly unfounded or excessive. If a request is refused for this reason, then a clear explanation will be recorded to support this.

In most cases, the ELT will not charge a fee to comply with a subject access request. However, we may charge a 'reasonable fee' for the administrative costs of complying with the request:

- if the request is manifestly unfounded or excessive
- if an individual requests further copies of their data following a request

10. Archiving / Removal

To ensure that personal data is kept for no longer than necessary, the ELT shall put in place an archiving policy for each area in which personal data is processed and review this process annually.

The archiving policy shall consider what data should/must be retained, for how long, and why.

11. Security

The ELT shall ensure that personal data is stored securely using modern software that is kept-up to date.

Access to personal data shall be limited to personnel who need access and appropriate security should be in place to avoid unauthorised sharing of information.

When personal data is deleted, this should be done safely such that the data is irrecoverable. Appropriate back-up and disaster recovery solutions shall be in place.

12. Breach

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, the Ecological Land Trust shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the ICO (more information on the ICO website).