WLT Data Protection Policy

Introduction

World Land Trust (**WLT**) keeps and processes certain personal information in order to:

- fulfil our charitable objectives and responsibilities to supporters;
- operate day-to-day;
- maintain financial and administrative records; and
- comply with legal and regulatory obligations.

WLT treats all personal data with respect and in compliance with relevant laws and regulations. We are committed to ensuring that individuals' personal data is:

- processed lawfully, fairly and transparently;
- collected and processed for specified and legitimate purposes;
- adequate, relevant and limited to what is necessary for the purposes for which it is processed;
- accurate and kept as far as is possible up to date;
- kept only as long as is required according to WLT's Retention of Data Policy; and
- kept securely and safeguarded against unauthorised or unlawful processing, and accidental loss, destruction or damage.

This policy applies to all individuals who are handling personal data for which WLT is responsible. The aim of the policy is to ensure all individuals handling such data are fully aware of and act in accordance with WLT's data protection principles and procedures.

Key Definitions

Personal Data is any information (electronic or hard copy) relating to a living person who can be directly or indirectly identified from that information, such as a person's name, identification number, location data or online identifier. These examples are not exhaustive.

Special category data is Personal Data which requires special protection, and includes such data as an individual's race, ethnic origin, political opinion, religion or philosophical beliefs, trade union membership, genetics, biometrics (where used for ID purposes), health, sex life, sexual orientation or data relating to criminal convictions.

Processing means any operation(s) performed on Personal Data or on sets of data, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Data Subject is the person who is the subject of Personal Data. That person must be living, and identifiable from the data.

Data Controller is World Land Trust (**WLT**).

Data Processor is any individual or organisation that processes data on behalf of the Data Controller.

Data Protection by Design and Default

We will ensure that all of our operations have data protection at their heart and that appropriate technical and organisational measures are put into place to ensure that the rights and interests of data subjects are protected.

Data protection will be considered where projects are being developed which may have an impact on privacy (such as developing new IT systems or processing data for new purposes). Where appropriate, Data Protection Impact Assessments (**DPIA**), which are designed to assess the impact of Processing on the protection of Personal Data and the rights and freedoms of Data Subjects, will be undertaken.

Training

Training about the requirements of data protection law and how it is followed by WLT will take the following forms:

- We will make available to all staff and individuals a manual outlining our Data Protection Policy, guidelines and procedures;
- Ongoing training, awareness raising and mentoring will be provided as appropriate;
- Monitoring practice and updating training where gaps in knowledge or practice are identified;
- All staff or individuals responsible for processing Personal Data will undergo a data protection training programme; and
- All staff and individuals responsible for Processing Personal Data will be required to sign a receipt to show that they have read and understood the Data Protection Policy.

Resources for data protection training may include:

- Data Protection Manual;
- in-house presentations, regular information and updates to staff and individuals responsible for Processing Personal Data;
- use of online training resources and printable materials from the Information Commissioner's Office and other appropriate official sources; and
- formal training courses (online/personal attendance).

How Personal Data is collected, used, checked and retained

WLT must Process Personal Data fairly, lawfully and in a transparent manner. WLT must also have a lawful basis for Processing Personal Data. This could include, having the Data Subject's consent, the Processing being necessary for the purposes of a contract with the Data Subject or Processing being in the legitimate interests of WLT.

- We will only collect Personal Data that is necessary for a specific legal, business or commercial purpose relevant to WLT.
- We will not collect more Personal Data than we need.
- We will only Process Data Subject Personal Data where we have a lawful basis for doing so.
- We will ensure that Data Subjects have been told about how their Personal Data will be used by WLT.
- We will maintain a written record of all Processing activities for each category of Data Subject so that we can demonstrate that we comply with the requirements of data protection law.
- We will not retain Personal Data for any longer than is necessary in relation to the purpose(s) for which it is collected.
- We will not purchase third party lists of Personal Data for direct marketing purposes or sell such lists to third parties.
- We will not transfer personal data to Data Processors, unless the Data Processor has appropriate systems in place to safeguard the security and privacy of the Data Subjects' Personal Data.
- We will implement and document measures to ensure that Personal Data is accurate and kept up to date as far as possible; and
- We will only collect Personal Data when we know that we can collect and store it safely.

Transferring Personal Data abroad

Where permitted by data protection law, WLT may transfer Personal Data to a Data Processor or NGO in another country (located outside of the EEA). Where the countries or territories to which Personal Data is being transferred may not offer an equivalent level of protection, WLT will take steps to ensure that the Personal Data and the rights of Data Subjects are adequately protected.

Transparency and respecting individuals' rights

We are committed to the principle of transparency in collecting and processing Personal Data.

We will inform Data Subjects in clear and concise language:

- why their Personal Data is being collected;
- how it will be used and kept up to date;
- the lawful basis for the Processing their Personal Data;
- who will have access to their Personal Data; and
- what their rights of access are and methods of redress should they have any concerns about the collection and use of their Personal Data.

We will inform Data Subjects should we intend to use their Personal Data for any additional purposes, including the lawful basis for doing so. As far as is practical this information will be provided at the point of collection, but we will ensure that appropriate privacy notices are made available to all Data Subjects.

Data Subjects may access and update their Personal Data by registering for an online account on our webportal https://portal.worldlandtrust.org/portal/public/login/login.aspx.

Data Subjects have certain rights under data protection law in relation to their Personal Data, including:

- the right to request confirmation as to whether WLT has Personal Data relating to them;
- the right to access the Personal Data that is being processed by WLT;
- the right to require WLT to rectify any inaccurate or incomplete Personal Data;
- in certain circumstances, the right to require WLT to erase their Personal Data;
- in certain circumstances, the right to restrict WLT from Processing Personal Data or object to the Processing;
- the right to receive their Personal Data in a format that can be processed by a computer; and
- the right to lodge a complaint to relation to WLT's Processing of their Personal Data with the Information Commissioner's Office..

Any Data Subject wishing to exercise their rights in relation to their Personal Data should apply in writing to the Company Secretary, or complete the form available on our website. Before access is granted we will require proof of identity.

Collecting and using Personal Data of children

We are committed to safeguarding the rights and interests of children whose Personal Data we may Process, in line with our Safeguarding Policy.

How we collect children's Personal Data

- We will only collect Personal Data which is freely given by young people aged 16 or over. Young people under the age of 16 must seek consent or authorisation from a parent or legal guardian before making a donation or supplying Personal Data.
- Where a young person under the age of 16 discloses their age to us, it will be noted in their record on the WLT database to ensure appropriate safeguards are observed.

The lawful basis for processing children's Personal Data

- We will inform the young person and, where possible, their parent(s) or legal guardian of the lawful basis for Processing their Personal Data, as detailed in the Privacy Policy on our website.

The extent of processing of children's Personal Data

- We will not knowingly send a young person under the age of 16 fundraising appeals.
- Where we have reason to be concerned about the source of a donation from a young person under the age of 16, we may make further enquiries before accepting the donation.
- We will require consent from a parent or legal guardian before knowingly accepting direct debit instructions from a young person under the age of 16.
- We will only take and use photographs of young persons under the age of 16 with the express written authorisation of the parent or legal guardian, obtained via the school or association. Any related publicity material will normally be submitted in advance to the school or association for comment/correction.

Privacy statements

We will use our best endeavours to ensure that any privacy statements directed towards children will be written in clear and understandable language.

Data security

We will take steps to ensure that Personal Data is kept secure and that unauthorised disclosure, acquisition, access, destruction or alteration is prevented. The following measures will be taken:

- All staff members and any individuals who may process or have access to Personal Data held by WLT must sign confidentiality agreements.
- Appropriate contractual obligations will be placed on contractors or third party processors who may process or have access to Personal Data held by WLT.
- Access to Personal Data is limited to individuals who require access to carry out their work and access is controlled by internal authorisation processes.
- Paper records containing Personal Data are kept in lockable cupboards with restricted access.
- Computer systems that contain Personal Data are access-restricted and password-protected.
- Appropriate IT security awareness training is provided to staff whose roles involve processing Personal Data.
- Remote access to Personal Data is strictly controlled and Personal Data physically taken offsite is encrypted.
- Data (including Personal Data) stored on WLT servers is backed up and taken offsite for disaster recovery purposes.
- Appropriate technical security measures are maintained to provide protection and monitoring of attempted breaches from external sources.
- Physical access to computer systems, network infrastructure and server rooms is controlled.
- Removal of data (including Personal Data) through destruction is carried out using certified third-party contractors; and
- Data (including Personal Data) used and stored in cloud accounts is considered against regulations before implementation and access is restricted to only those who require it.

Unauthorised disclosure of Personal Data to a third party may result in sanctions as detailed below (*see section on **Responsibilities***). This applies to employees or any other individual or organisation who may have access to Personal Data controlled by WLT. In the case of employees this may include disciplinary proceedings and in serious cases may be considered gross misconduct.

Documentation

We will document our Processing activities so that we can demonstrate that we comply with the requirements of data protection law. The information recorded will include:

- information audits of data carried out;
- the lawful basis for Processing Personal Data (including how we assess the lawful basis for Processing);
- where and how Personal Data is stored;
- information required for privacy notices;
- records of any DPIA reports;
- records of any data breaches, related notifications and measures taken;
- controller–processor contracts; and
- details of persons within the organisation with responsibilities for data protection.

We will conduct regular reviews of our policies and procedures, and document them accordingly.

Notification of data breaches

The Information Commissioner's Office (**ICO**) is the independent supervisory authority with responsibility for promoting and overseeing data protection regulation in the UK.

In the event of a breach, we will carry out an assessment of whether the breach is likely to result in a risk to the rights and freedoms of the individuals concerned. Where we consider there to be a risk, we will notify the ICO as soon as possible and within 72 hours of discovery with details of the breach (including, where possible, categories and approximate number of individuals affected, categories and approximate number of Personal Data records concerned, likely impact of the breach, and the measures undertaken to deal with the breach).

Where the breach affects individuals in different jurisdictions, we will notify the supervising authorities in the relevant jurisdictions.

Where the breach is likely to have a serious impact on the individuals concerned, we will notify those individuals directly.

Where it is assessed that a risk is unlikely to result (and notification to the ICO is therefore not required) we will retain full documentation relating to the risk assessment.

Responsibilities

Overall responsibility for data protection rests with the Trustees, as WLT's governing body. The Trustees have delegated responsibility for management of WLT's data protection policies and procedures to the CEO, who is tasked with submitting relevant policies for approval and adoption by Trustees.

The CEO delegates to departmental Directors and senior managers, as appropriate, responsibility for:

- understanding and communicating WLT's obligations under applicable data protection law;
- ensuring that clear and effective procedures are implemented;
- undertaking reviews of policies and procedures as appropriate and required;
- ensuring measures are implemented to ensure data security; and
- identifying potential problem areas or risks.

The CEO is responsible for reporting on all data protection issues to Trustees, and notifying, as required, the ICO and other relevant supervisory authorities and individuals about any breaches of data security, along with the measures undertaken to address the breach(es).

All workers (paid, temporary or sub-contractors) and anyone working on WLT's behalf in whatever capacity who process Personal Data held by WLT must ensure they not only understand but also act in line with this policy and the data protection principles.

Breach of this policy by staff members may result in disciplinary procedures and in some circumstances may be considered gross misconduct.

Sanctions against other individuals in breach of this policy may include release from their roles in the case of volunteers and interns, and potential legal action in the case of data processors, contractors and sub-contractors who may have breached their contractual obligations. In the case of a breach by a Member of the Charity, Trustees may resolve to remove their membership in accordance with the provisions of WLT's constitution.

Review

This policy will be reviewed at intervals of two years to ensure it remains up to date and compliant with the law, and in any event in the case of a change in relevant legislation or regulation, or in the event of a serious concern or data breach.