WATER OF LEITH CONSERVATION TRUST DATA PROTECTION POLICY 2018 – Version 1

Introduction
Water of Leith Conservation Trust (WOLCT) needs to gather and use certain information about individuals. These can include members, volunteers, customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact. This policy describes how this personal data must be collected, handled and stored to meet the Trust's data protection standards and to comply with the law.
This data protection policy ensures the Water of Leith Conservation Trust

- Complies with data protection law and follows good practice
- Protects the rights of staff, volunteers, customers and partners
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach.

Data Protection Law
The Data Protection Act 1998 and General Data Protection Regulation (GDPR) (EU) 2016/679 describe how organisations must collect, handle and store personal information. These rules apply regardless of whether data is stored electronically, on paper or on other materials. To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully. The Data Protection Act is underpinned by eight important principles. These say that personal data must:
1. Be processed fairly and lawfully
2. Be obtained only for specific, lawful purposes
3. Be adequate, relevant and not excessive
4. Be accurate and kept up to date
5. Not be held for any longer than necessary
6. Processed in accordance with the rights of data subjects
7. Be protected in appropriate ways
8. Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection

Lawful Basis for Processing
The nature of business and actions conducted by WOLCT require that we process data under the following legal bases as set out in Article 6 of the GDPR:

- Consent: the individual has given clear consent for you to process their personal data for a specific purpose.
- 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.
- 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.
- 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.

People, Risks and Responsibilities
The policy applies to all staff, trustees and volunteers with WOLCT
It applies to all data that the Trust holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 1998 or General Data Protection Regulation (GDPR) (EU) 2016/679.
This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- Plus any other information relating to individuals

Data protection risks

This policy helps to protect the WOLCT from some very real data security risks, including:

- Breaches of confidentiality. For instance, information being given out inappropriately.
- Failing to offer choice. For instance, all individuals should be free to choose how the company uses data relating to them.
- Reputational damage. For instance, the company could suffer if hackers successfully gained access to sensitive data.

Responsibilities

Everyone who works for or with the WOLCT has some responsibility for ensuring data is collected, stored and handled appropriately. Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles. However, these people have key areas of responsibility:

- The board of Trustees is ultimately responsible for ensuring that WOLCT meets its legal obligations.
- The privacy monitoring shall be jointly shared between the Trust Manager and Trust Administrator Their responsibilities are detailed below.

The Administrator, is responsible for:

- Keeping the Trust Manager updated about data protection responsibilities, risks and issues.
- Reviewing all data protection procedures and related policies, in line with an agreed schedule.
- Arranging data protection training and advice for the people covered by this policy.
- Handling data protection questions from staff and anyone else covered by this policy.
- Dealing with requests from individuals to see the data WOLCT holds about them (also called 'subject access requests').

The Trust Manager is responsible for:

- Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
- Performing regular checks and scans to ensure security hardware and software is functioning properly.
- Evaluating any third-party services the company is considering using to store or process data. For instance, cloud computing services.
- Approving any data protection statements attached to communications such as emails and letters.
- Addressing any data protection queries from journalists or media outlets like newspapers.
- Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

General Staff Guidelines

The only people able to access data covered by this policy should be those who need it for their work. Data should not be shared informally. WOLCT will provide training to all employees to help them understand their responsibilities when handling data. Employees should keep all data secure, by taking sensible precautions and following the guidelines below. In particular, strong passwords must be used and they should never be shared. Personal data should not be disclosed to unauthorised people, either within the company or externally. Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.

Data storage and Retention

The following rules describe how and where data should be safely stored.

When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it. These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept in a locked drawer or filing cabinet.
- Employees should make sure paper and printouts are not left where unauthorised people could see them, like on a printer.
- Data printouts should be shredded and disposed of securely when no longer required.

When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data should be protected by strong passwords that are changed periodically .
- If data is stored on removable media (like a flash drive), these should be kept locked away securely when not being used.
- Data should only be stored on designated drives and servers, and should only be uploaded to approved cloud computing services.
- Servers containing personal data should be sited in a secure location and the office is locked when un attended.
- Data should never be saved directly to laptops or other mobile devices like tablets or smart phones.
- All servers and computers containing data should be protected by approved security software and a firewall.

Data accuracy

The law requires the WOLCT to take reasonable steps to ensure data is kept accurate and up to date. The more important it is that the personal data is accurate, the greater the effort the WOLCT should put into ensuring its accuracy. It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets.
- Staff should take every opportunity to ensure data is updated. For instance, by confirming a members details when they call.
- WOLCT will make it easy for data subjects to update the information the WOLCT holds about them and data should be updated immediately should inaccuracies be discovered

Individual Rights

Individual Rights General Data Protection Regulation (GDPR) (EU) 2016/679 also guarantees individuals the following rights with regard to their personal information:

- Individuals have the right to be informed about the collection and use of their personal data.
- Individuals have the right to access their personal data and supplementary information.
- Individuals have the right to have inaccurate personal data rectified, or completed if it is incomplete.
- Individuals have the right to have personal data erased (‘the right to be forgotten’).
- Individuals have the right to request the restriction or suppression of their personal data. (This is not an absolute right and only applies in certain circumstances.)
- Individuals have the right to obtain and reuse their personal data for their own purposes across different services.
- Individuals have the right to object to: processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling); direct marketing (including profiling); and processing for purposes of scientific/historical research and statistic

Subject Access Request

If an individual contacts the company requesting this information, this is called a subject access request. Subject access requests from individuals should be made by email,

addressed to the Trust Manager admin@waterofleith.org.uk. The Trust Manager or Administrator can supply a standard request form, although individuals do not have to use this. The data controller will always verify the identity of anyone making a subject access request before handing over any information.

Disclosing data for other reasons

In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject. Under these circumstances, WOLCT will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers where necessary.

Providing information

WOLCT aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used
- How to exercise their rights

To these ends, the company has a privacy statement, setting out how data relating to individuals is used by the company. This is called Water of Leith Conservation Trust Privacy Policy 2018 and is stored on office server and is on our website http://www.waterofleith.org.uk/do/

CCTV

The trust does operate a CCTV system to prevent or detect crime and to monitor the Visitor Centre buildings and grounds in order to provide a safe and secure environment for its staff and visitors, and to prevent loss or damage to property. It was installed in 2016 following a prolongued period of break-ins, vandalism, theft of property and damage to the building. We have a separate CCTV policy available on office server or on request.

Produced in May 2018 by Helen Brown and Sandie Boyle

Agreed by Trustees at the meeting held on 4th June 2018.

To be reviewed no later than 4th June 2019.