Data Protection Policy and Procedures

Last updated: September 2026

Introduction

This policy outlines how Low Carbon Destinations directors manage data.

Low Carbon Destinations CIC (referred to here as "LCD") is committed to the protection of the personal data of members and other individuals about whom it might hold information. LCD recognises the General Data Protection Regulation (GDPR) as the primary statutory responsibility relating to data handling and processing. To this end every individual handling data collected or administered by LCD takes responsibility and has due consideration for its appropriate use in line with this policy.

This policy applies to all members, volunteers and other relevant parties who may have access to other's personal data.

This data protection policy ensures LCD:

- Complies with data protection law and follows good practice
- Protects the rights of members, volunteers and other individuals
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach
- Is proportionate to the scale, scope and capacity of the organisation.

What sort of data does LCD manage?

LCD as a research-led CIC generally manages data for two main reasons

1. Core contacts database
   For people with whom LCD has professional contact
2. Data about people and organisations with whom LCD works
   This includes projects. Some of these projects may be bound by contacts that have specific conditions relating to data storage, including the deletion of contacts at the end of the project. Any such contractual obligations would over-ride this policy.

The data that we keep involves contact details including name, address, phone numbers, email addresses, websites, social media handles.

This Policy should also be read in conjunction with relevant data protection law General Data Protection Regulation (GDPR) is set of EU regulations that strengthen the existing UK Data Protection Action 1998 (DPA). The DPA describes how organisations must collect, handle and store personal data. 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 DPA is underpinned by the following eight principles. According to these principles, personal data must be

- used fairly and lawfully
- used for limited, specifically stated purposes
- used in a way that is adequate, relevant and not excessive
- accurate
- kept for no longer than is absolutely necessary
- handled according to people's data protection rights
- kept safe and secure
- not transferred outside the European Economic Area without adequate protection.

Responsibilities

This policy applies to all operations of LCD and to all directors, volunteers and other associated individuals. It applies to all data LCD holds relating to identifiable individuals, even when technically these data fall outside the DPA. This can include names of individuals, postal and email addresses, telephone numbers, and any other information relating to individuals.

Contractors

All personal information from any recruitment – from the process of recruitment to ongoing employment of contractors - will be held on password protected Dropbox files with privacy and security key features of the system.

Any contractors must ensure that all personal data provided to LCD in the process of employment is accurate and up to date. They must ensure that changes of address etc are updated. In the course of day to day working it is likely that employees will process individual personal data. In addition, employees must maintain a current understanding of what is required of them under Data Protection law.

When handling personal data, LCD are required to follow the guidance set out in the Data Protection Guidance.

Data Breaches

The Information Commissioner's Office shall be notified within 72 hours of the breach where there is a risk to the rights and freedoms of individuals such as discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

Where there is a high risk to the rights and freedoms of individuals they shall also be notified directly.

A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means that a breach is more than just losing personal data.

Information Security

Data storage

These rules describe how and where data should be safely stored. Physical representation of data, such as paper forms, must be stored securely. When no longer needed, the e -copies should be deleted and any paper copies securely destroyed. Vital records for the purposes of business continuity must be protected from loss, destruction or falsification by LCD.

LCD will securely store data online using Dropbox. The only person with direct access to this is Alistair Kirkbride; anyone else who requires access will liaise with Alistair Kirkbride.

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

- use secure platforms for processing data
- maintain up to date antivirus and malware systems
- ensure secure destruction of IT equipment.

LCD will not use external storage devices such as external hard drives, memory sticks, pen drives etc. for storage of any sensitive LCD data other than for transfer of photos and data. Once such transfer has been effected, the relevant data will immediately be deleted from the device used for transfer.

Disposing of Data

LCD is committed to keeping data for the minimum time necessary to fulfil its purpose.

Paper based records shall be disposed of by shredding.

Electronic records will be deleted through the decommissioning of equipment by an IT specialist and digital records shall be deleted from databases at source.

Data use

Schedule 2 of the DPA lays down six conditions, at least one of which must be met, in order for any use of personal data to be fair. These are (in brief):

- With consent of the Data Subject
- If it is necessary for a contract involving the Data Subject
- To meet a legal obligation
- To protect the Data Subject's 'vital interests'
- In connection with government or other public functions
- In the Data Controller's 'legitimate interests' provided the Data Subject's interests are not infringed.

Personal data is at the greatest risk of loss, corruption or theft when it is accessed and used:

- When working with personal data, LCD should ensure the screens of their computers are always locked when left unattended
- Personal data should not be shared informally - in particular it should never be sent by email as this form of communication is not secure – all volunteers and committee members to be made aware of this.
- Data must be encrypted before being transferred electronically
- Personal data should never be transferred outside the European Economic Area

Data accuracy

The law requires LCD to take reasonable steps to ensure data is kept accurate and up to date. It is the responsibility of all who work with data to make reasonable steps to ensure it is kept as accurate and up to date as possible:

- Data will be held in a limited number of known places, and LCD should not create any unnecessary additional data sets
- LCD should take every opportunity to ensure data is updated

Subject access requests

All individuals who are the subject of personal data held by LCD are entitled to:

- Ask what information LCD holds about them and why
- Ask how to gain access to it
- Be informed how to keep it up to date
- Be informed how LCD is meeting its data protection obligations.
- Request for their data to be removed and for LCD to agree to this by default.