



The Lisa Project CIC Data Protection Policy

Policy brief & purpose

Our Company Data Protection Policy refers to our commitment to treat information of employees, customers, service users and other interested parties with the utmost care and confidentiality. With this policy, we ensure that we gather, store and handle data fairly, transparently and with respect towards individual rights.

Scope

This policy refers to all parties (employees, job candidates, customers, service users, suppliers etc.) who provide any amount of information to us.

Who is covered under the Data Protection Policy?

Employees of our company and its subsidiaries must follow this policy. Contractors, consultants, partners and any other external entity are also covered. Most importantly this covers the personal details of any of our service users data that we hold. Generally, our policy refers to anyone we collaborate with or acts on our behalf and may need occasional access to data.

Policy elements

As part of our operations, we need to obtain and process information. This information includes any offline or online data that makes a person identifiable such as names, addresses, usernames and passwords, digital footprints, photographs, social security numbers, financial data etc.

Our company collects this information in a transparent way and only with the full cooperation and knowledge of interested parties. Once this information is available to us, the following rules apply.

Our data will be:

- Accurate and kept up-to-date
- Collected fairly and for lawful purposes only
- Processed by the company within its legal and moral boundaries
- Protected against any unauthorized or illegal access by internal or external parties
- Our data will not be:
- Communicated informally
- Stored for more than a specified amount of time
- Transferred to organizations, states or countries that do not have adequate data protection
- Policies

Distributed to any party other than the ones agreed upon by the data's owner (exempting legitimate requests from law enforcement authorities)

In addition to ways of handling the data the company has direct obligations towards people to whom the data belongs. Specifically, we must:

- Let people know which of their data is collected
- Inform people about how we'll process their data
- Inform people about who has access to their information
- Have provisions in cases of lost, corrupted or compromised data
- Allow people to request that we modify, erase, reduce or correct data contained in our databases

Storage of paperwork

Our community work involves collecting paperwork such as feedback forms, registration forms and other personal data from our community's service user. We will;

- Only ask for personal details we need and keep it to a minimal.
- Store paperwork in a locked filing cabinet in a locked office.
- Keep any electronic documents under password protection.
- We will destroy all documents after three years.



Actions

To exercise data protection, we're committed to:

Restrict and monitor access to sensitive data

Develop transparent data collection procedures

Train employees in online privacy and security measures

Build secure networks to protect online data from [cyberattacks](#)

Establish clear procedures for reporting privacy breaches or data misuse

Include contract clauses or communicate statements on how we handle data

Establish data protection practices (document shredding, secure locks, data encryption, frequent backups, access authorization etc.)

Our data protection provisions will appear on our website.

Disciplinary Consequences

All principles described in this policy must be strictly followed. A breach of data protection guidelines will invoke disciplinary and possibly legal action.

Disclaimer: This policy template is meant to provide general guidelines and should be used as a reference. It may not take into account all relevant local, state or federal laws and is not a legal document. Neither the author nor Workable will assume any legal liability that may arise from the use of this policy.

Further reading:

[Data Protection Act of 1998 \(UK\)](#)

[Data protection in United States](#)

Policy reviewed every May

Last reviewed by Natasha Storey, Senior Director 18/06/2025