LOUTH COUNTY ENTERPRISE FUND (LCEF)

Data Protection Policy

Introduction

LCEF needs to gather and use certain information about individuals. These can include clients, suppliers, business contacts, employees and other people the Fund may have a relationship with or may need to contact.
This policy describes how this data may be collected, handled and stored to meet the Fund's data protection standards – and to comply with applicable data protection laws.

Why this policy exists

This data protection policy ensures LCEF:

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

This policy does not form part of any employee's contract of employment and it may be amended at any time. Any breach of this policy will be taken seriously and may result in disciplinary action up to and including dismissal.

Data Protection Law

The General Data Protection Regulation and the Data Protection Act 2018 describes how organisations, including LCEF, must collect, handle and store personal data.
These rules apply regardless of whether data is stored electronically, in paper files 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 the following principles;

Personal data must be;

1. Processed fairly and lawfully.
2. Processed for limited purposes and in an appropriate way.
3. Adequate, relevant and not excessive for the purpose.
4. Accurate, complete and up to date.
5. Not kept longer than necessary for the stated purpose.

6. Processed in line with data subjects' rights i.e. access and amendment rights.
7. Secure.
8. Not transferred to people or organisations situated in countries without adequate protection.

Policy scope

This policy sets out the Fund's rules on data protection and the legal conditions that must be satisfied in relation to the collecting, obtaining, handling, processing, storage, transportation and destruction of personal and sensitive information.

This policy applies to all data that the Fund holds relating to identifiable individuals. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- IP addresses
- Telephone numbers
- Personnel/employment files
- Client correspondence (email and hard copy)
- Application forms
- Financial information
- Records of telephone calls
- Records of websites visited

Data Protection risks

This policy helps to protect LCEF from some very real data security risks, including;

- **Breaches of confidentiality**
- **Reputational damage**

Responsibilities

Everyone who works for LCEF has some responsibility for ensuring data is collected, stored and handled appropriately.

Each person/team that handles personal data must ensure that it is handled and processed in line with this policy and the data protection principles.

- The *Board of Directors* are ultimately responsible for ensuring that LCEF meets its legal obligations by;
  - Appointing a data protection officer (where required to under law)
  - Keeping the employees 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 for the people covered by this policy
  - Dealing with requests from individuals to see the data LCEF holds about them ("subject access requests").
  - Checking and approving any contracts or agreements with third parties that may handle the Fund's sensitive data.
  - 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.
  -

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**. When access to confidential information is required, employees can request it

from their supervisor/manager

- **LCEF 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 Fund 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. **See file retention and destruction policy**.
- Employees **should request help** from a director or the data protection officer if they are unsure about any aspect of data protection

Data Storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the IT manager/data controller/directors.

- When data is stored on **paper,** the paper or **files** should be kept in a locked drawer or filing cabinet.
- Employees should ensure paper/printouts/files 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. In this regard, the Fund has the following policies in place;

- Information Systems Security policy
- Password policy

- Computer back-up policy
- General email, intranet, internet and computer usage policy

Data use

Personal data should only be collected to the extent that it is required for the specific purpose notified to the data subject. Any data which is not necessary for that purpose should not be collected in the first place.

Data accuracy

The law requires LCEF to take reasonable steps to ensure data is kept accurate and up to date. Information which is incorrect or misleading is not accurate and steps should be taken to check the accuracy of any personal data at the point of collection and at regular intervals afterwards. Inaccurate or out-of-date data should be destroyed. Employees should ensure that they notify their manager/supervisor of any relevant changes to their personal information so that it can be updated and maintained accurately. Examples of relevant changes to data would include a change of address.

.

Obtaining and processing data

Data protection legislation is not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject. The data subject must be told who the data controller is - in our case it is LCEF - the purpose for which the data is to be processed by the Fund and the identities of anyone to whom the data may be disclosed or transferred.

For personal data to be processed lawfully, certain conditions have to be met. These may include, among other things, requirements that the data subject has consented to the processing or that the processing is necessary for the legitimate interest of the data controller or the party to whom the data is disclosed. When special categories of data (previously referred to as sensitive personal data) are being processed, more than one condition must be met.

In most cases the data subject's explicit consent to the processing of such data will be required.

We have inserted relevant consents to such processing in our template terms of engagement

Personal data may only be processed for the specific purposes notified to the data subject when the data was first collected or for any other purposes specifically permitted by the Data Protection Acts. This means that personal data must not be collected for one purpose and then used for another. If it becomes necessary to change the purpose for which the data is processed, the data subject must be informed of the new purpose before any processing occurs. Any employee personal data collected by the Fund is used for ordinary Human Resources purposes. Where there is a need to collect employee data for another purpose, the Fund will notify the employee of this and where it is appropriate will get employee consent to such processing.

Data Retention

Personal data should not be kept longer than is necessary for the purpose.

Processing in line with Data Subjects Rights

Data must be processed in line with data subject's rights. Data subjects have a right to:

- Request access to any data held about them by a data controller.
- Prevent the processing of their data for direct-marketing purposes.
- Ask to have inaccurate data amended.
- Prevent processing that is likely to cause damage or distress to themselves or anyone else.

Dealing with Subject Access Requests

The Fund has a Data Subject Access request protocol in place.

Providing information over the telephone

Any employee dealing with telephone enquiries should be careful about disclosing any personal information held by the Fund over the phone. In particular the employee should:

- Check the identity of the caller to ensure that information is only given to a person entitled to that information.
- Suggest that the caller put their request in writing if the employee is not sure about the identity of the caller and in circumstances where the identity of the caller cannot be verified.

- Refer the request to their departmental manager for assistance in difficult situations. No employee should feel forced into disclosing personal information.

Transfer of Data outside the EEA

If any personal data is being transferred outside the EEA, they must be compliant with EU law. Such transfer is required to be subject to "an adequate standard of protection" and an appropriate data transfer mechanism will be required to transfer personal data outside the EEA.

The requisite contractual provisions must be in place and the client/employee /data subject must be notified of such a transfer.

Providing information

LCEF 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 those rights

REVIEW OF POLICY

The Fund will continue to review the effectiveness of this policy to ensure it is achieving its stated objectives on at least an annual basis and more frequently if required taking into account any changes to current data protection laws.

Signed: **LOUTH COUNTY ENTERPRISE FUND**

Dated:

Appendix 1

Definition of Data Protection terms
(as defined by the General Data Protection Regulation)

1. **Personal data** means any information relating to an identified or identifiable natural person ('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.

2. **Sensitive personal data** means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation.

3. **Data controller** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

4. **Data processor** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

5. **Processing** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, 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;

6. **Profiling** means any form of automate automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person in particular to analyse or predict aspects concerning the natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

7. **Pseudonymisation** means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified of identifiable natural person.

8. **Personal data breach** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to, personal data transmitted, stored or otherwise processed.

Appendix 2

LOUTH COUNTY ENTERPRISE FUND
Ardee Business Park
Hale Street
Ardee
County Louth
www.thefund.ie

Data Protection Statement

Information which you provide to us and information which Louth County Enterprise Fund (The Fund) already holds may be used by The Fund in assessing your application for loan funding.
Your information will only be used and disclosed in circumstances where there is an obligation to do so, as the law permits, or where you have given your consent.
If your application is unsuccessful, your personal data will be deleted within 30 days of the Fund's decision date.
If your application is successful, your personal data will be deleted eight (8) years after the loan has been cleared.
Occasionally The Fund may wish to contact you about supports, similar to the type it already provides, or with information which may be useful to you and/or your business.

The Enterprise Fund manages the NURTURE FUND, the result of an Alliance between the Enterprise Fund and Dundalk Credit Union (DCU). The Fund may suggest that your Application be referred to DCU for loan funding. Your specific approval will be required by The Fund before such a referral is made.

If you agree with the statements contained herein and if you are content to receive information from The Fund as described above, please sign below

Signed _____ **Date** _____