LEAD
ASD Diagnosis

DATA PROTECTION POLICY

Document Detail	
Effective from	28/08/2020
Last reviewed	10/06/2024
Date of next review	June 2026
Version	1.3
Owner	LEAD Manager

Data Protection Policy

1. Introduction and Scope

1 Introduction

The Privacy and Data Protection Policy of LEAD is to protect the personal data of those various

stakeholders connected to the organisation, and is created in accordance to the European Union's General Data Protection Regulation (GDPR)

1.2. Definition of Data

In its everyday business LEAD makes use of a variety of data about identifiable individuals ('natural persons'), including data about:

- Patients and their guardians
- Current, past and prospective staff
- Users of its websites
- Other relevant stakeholders (e.g. referrers, SENCOs,)

In collecting and using this data, the organisation is subject to a variety of legislation controlling how such activities may be carried out and the safeguards that must be put in place to protect it.

The purpose of this policy is to set out the relevant legislation and to describe the steps LEAD is taking to ensure that it complies with it.

2. Definitions

Articles 4 and 9 of the GDPR define key terms which are relevant to this policy and include:

Personal data

Any information that relates to a living individual who can be identified (either directly or indirectly) from that information. Examples include name, telephone number and email address.

Special category data

This type of data under data protection law requires more protection because it is sensitive.

Special categories of personal data include:

- Personal data revealing - racial or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership
- Genetic data
- Biometric data (where used for identification purposes, such as fingerprints or facial recognition)

Additionally, while they are not considered “special category data”, children’s data and also data relating to criminal convictions are afforded further protections.

Data subject

An identified, or identifiable natural person.

Processing

Any operation (or set of) which is performed on personal data.

Pseudonymisation

Processing 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.

Data Controller

The natural or legal person, public authority, agency or body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Processor

A natural or legal person, public authority, agency or body which processes personal data on behalf of the controller.

Recipient

A natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not.

Third party

A body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

Personal data breach

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.

3. Principles

To ensure our obligations under information law are met, the processing of personal information must comply with the principles of the GDPR. Accordingly, personal data will be:

a. Processed lawfully, fairly and in a transparent manner in relation to the data subject.

b. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. LEAD uses the personal confidential data supplied by you for your personal care and we do not disclose this information to third parties for any other uses.

c. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation').

d. Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purpose for which they are processed, are erased or rectified without delay.

e. Kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. We do not process or disclose personal and confidential data for any other use.

f. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

4. Lawfulness of Processing Data

There are six data protection principles defined in Article 5 of the GDPR. These require that all personal data be:

- processed in a **lawful**, **fair** and **transparent** manner.
- collected only for **specific**, **explicit** and **limited** purposes ('purpose limitation').
- **adequate**, **relevant** and **not excessive** ('data minimisation').
- **accurate** and kept **up-to-date** where necessary.
- kept for **no longer than necessary** ('retention').
- handled with appropriate **security** and **confidentiality**.

We are committed to upholding the data protection principles. All personal data under our control will be processed in accordance with these principles.

All processing of personal data must meet one of the six lawful bases defined in Article 6(2) of the GDPR:

- Where we have the **consent** of the data subject
- Where it is in our **legitimate interests** and this is not overridden by the rights and freedoms of the data subject.
- Where necessary to meet a **legal obligation**.
- Where necessary to fulfil a **contract**, or pre-contractual obligations.
- Where we are protecting someone's **vital interests**.
- Where we are fulfilling a **public task,** or acting under official authority.

Special category data (sensitive types of personal data as defined in Article 9(1) of the GDPR) is prohibited from being processed and can only be processed if conditions are satisfied as specified in Article 9(2).

Processing shall be lawful only if and to the extent that at least one of the following applies:

- (a) the data subject has given **consent** to the processing of his or her personal data for one or more specific purposes;
- (b) **processing is necessary for the performance of a contract** to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- (c) processing is **necessary for compliance with a legal obligation** to which the controller is subject;
- (d) processing is necessary in order to **protect the vital interests of the data subject** or of another natural person;
- (e) processing is necessary for the performance of a task carried out in the **public interest** or in the exercise of official authority vested in the controller;
- (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.
- Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.

The most appropriate lawful basis will be noted in our Data Processing Register.

Where processing is based on consent, the data subject has the option to easily withdraw their consent.

5. Responsibilities

The GDPR states that the data controller shall be responsible for, and be able to demonstrate compliance with the above principles ("accountability"). This means that we must:

maintain relevant documentation on all data processing activities

implement appropriate technical and organisational measures that ensure and demonstrate that we comply;

implement measures that meet the principles of privacy by design and by, such as:

- data minimisation;
- pseudonymisation;
- transparency; and
- creating and improving security features on an ongoing basis.
- use data protection impact assessments where appropriate.
- record all data security breaches

LEAD has overall responsibility for ensuring compliance with the Data Protection Acts. However, all staff who process personal data in the course of their employment are also responsible for ensuring compliance with the Data Protection Acts.

The LEAD Manager will assist the staff in complying with the Data Protection legislation.

Specifically, the following roles and responsibilities apply in relation to this Policy:

All staff members and users of LEAD information:

- Should take all necessary steps to ensure that no breaches of information security result from their actions;
- Must report all suspected and actual data security breaches to the LEAD manager, so that appropriate action can be taken to minimise harm;
- Must inform LEAD of any changes to the information that they have provided to LEAD in connection with their employment (e.g. changes of address or bank account details).
- acquaint themselves with, and abide by, the rules of Data Protection set out in this Policy;
- read and understand this policy document;
- understand what is meant by 'personal data' and 'special categories of personal data' and know how to handle such data;
- understand the lawful basis for processing personal data;
- not jeopardise individuals' rights or risk a contravention of the Act;
- report all data security breaches to the manager immediately;
- contact the LEAD manager if in any doubt.

LEAD Manager:

- responsible for reviewing and approving this and for ensuring compliance with the Data Protection Acts and this policy.

  ensuring that appropriate policies and procedures are in place to support this Policy;

- ensuring that any data security breaches are properly dealt with.
- process and respond to formal Data Access Requests;
- respond to requests for rectification, erasure of data and restrictions or objections to processing of data;
- initiate regular reviews of data protection policies and procedures and ensure documentation is updated as appropriate;
- maintain a record of all personal data security breaches;
- provide advice and guidance to staff on data protection matters;
- maintain a centrally-held register of the categories of personal data held by LEAD;
- maintain records of UCC's compliance with the Data Protection Acts;

6. Data Protection Breeches

A 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.

All members of staff should be vigilant and able to identify a suspected personal data breach. A breach could include:

loss or theft of devices or data, including information stored on USB drives or on paper

hacking or other forms of unauthorised access to a device, email account, or the network

disclosing personal data to the wrong person, through wrongly addressed emails, or bulk emails that inappropriately reveal all recipients email addresses

alteration or destruction of personal data without permission

Where a member of staff discovers or suspects a personal data breach, this should be reported to the manager as soon as possible.

Where there is a likely risk to individuals' rights and freedoms, the manager will report the personal data breach to the ICO within 72 hours of the organisation being aware of the breach.

Where there is also a likely high risk to individuals' rights and freedoms, LEAD will inform those individuals without undue delay.

The manager will keep a record of all personal data breaches reported, and follow up with appropriate measures and improvements to reduce the risk of reoccurrence.

7. Rights of the Data Subject

The GDPR explicitly states its commitment to European citizens and data subjects early on in the legislation. Chapter 3 of the GDPR records those rights as the Rights of the Data Subject.

1. Under data protection laws, data subjects have certain rights:
    - **Right to be informed**. The right to be told how their personal data is used in clear and transparent language.
    - **Right of access**. The right to know and have access to the personal data we hold about them.
    - **Right to data portability**. The right to receive their data in a common and machine-readable electronic format.
    - **Right to be forgotten**. The right to have their personal data erased.
    - **Right to rectification**. The right to have their personal data corrected where it is inaccurate or incomplete.
    - **Right to object**. The right to complain and to object to processing.
    - **Right to purpose limitation**. The right to limit the extent of the processing of their personal data.
    - **Rights related to automated decision-making and profiling**. The right not to be subject to decisions without human involvement.
2. We will uphold individuals' rights under data protection laws and allow them to exercise their rights over the personal data we hold about them. Privacy information will acknowledge these rights and explain how individuals can exercise them. Most rights are not absolute, and the individual will be able to exercise them depending on the circumstances, and exemptions may apply in some cases.
3. Any request in respect of these rights should preferably be made in writing to contact@londonearlyautismdiagnosis.com.
4. There is no fee for facilitating a request, unless it is 'manifestly unfounded or excessive', in which case administrative costs can be recovered.
5. Requests that are 'manifestly unfounded or excessive' can be refused.
6. We will take reasonable measures to require individuals to prove their identity where it is not obvious that they are the data subject.
7. We will respond to the request within one month from the date of request or being able to identify the person, unless it is particularly complex (in which case we will respond in no longer than 90 days).

8. The manager will ensure that required actions are taken and that the appropriate response is facilitated within the deadline.
9. The manager will draw up procedures for responding to requests where necessary, for example, for facilitating Subject Access Requests.

8. Security and Record Keeping

Principle (f) of the GDPR states that organisations must ensure "appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures". With continual changes to both technology and the demand for ever-easier ways by which information can be accessed and shared, it is important that a consistent approach be adopted to safeguard information.

LEAD will ensure that appropriate technical and organisational measures are in place, supported by privacy impact and risk assessments, to ensure a high level of security for personal and confidential data, and a secure environment for information held both manually and electronically.

'Records Management' refers to a set of activities required for systematically controlling the creation, distribution, use, maintenance, and disposition of recorded information maintained as evidence of business activities and transactions. It is impossible to be compliant with information law without robust records management policies and practises.

Good records management practises ensure not only record quality, but that personal data is only kept for as long as necessary for its original purpose, and help support data minimisation. They are integral to information security methodology, and to ensuring the integrity and confidentiality of personal data. It is a key feature of risk management.

LEAD is committed to implementing robust records management policy, process and practises to ensure compliance with the GDPR.

9. Privacy by Design

LEAD has adopted the principle of privacy by design and will ensure that the definition and planning of all new or significantly changed systems that collect or process personal data will be subject to due consideration of privacy issues, including the completion of one or more data protection impact assessments.

The data protection impact assessment will include:

- Consideration of how personal data will be processed and for what purposes
- Assessment of whether the proposed processing of personal data is both necessary and proportionate to the purpose(s)

- Assessment of the risks to individuals in processing the personal data
- What controls are necessary to address the identified risks and demonstrate compliance with legislation. Use of techniques such as data minimization and pseudonymisation will be considered where applicable and appropriate.

10.Further Information

If you have any queries in relation to this policy, please contact:

LEAD Manager

contact@londonearlyautismdiagnosis.com

0203 759 4070