DATA PROTECTION POLICY

DATA PROTECTION POLICY

1 Policy Statement

Local Education and Development is required to retain certain information about its employees, learners and other users in order to facilitate the monitoring of performance, achievements, and health and safety. It is also necessary to process information so that staff can be recruited and paid, courses organised and legal obligations to funding bodies and government complied with. To comply with the law, information stored in files (either paper based or electronically including on a computer including e-mail, internet, intranet or portable storage device) covered by the data protection legislation must be collected and used fairly, stored and disposed of safely, and not disclosed to any other person unlawfully. To do this, LEAD must comply with the Data Protection Principles, which are set out in the Data Protection Act 1998 (the 1998 Act).

In summary these state that personal data shall:

1.1 Be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met.

1.2 Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose.

1.3 Be adequate, relevant and not excessive for those purposes.

1.4 Be accurate and kept up to date.

1.5 Not to be kept for longer than is necessary for that purpose.

1.6 Be processed in accordance with the data subject's rights.

1.7 Be safe from unauthorised access, accidental loss or destruction.

1.8 Not be transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data.

LEAD and all staff or others who process or use any personal information must ensure that they follow these principles at all times. In order to ensure that this happens, LEAD has developed the Data Protection policy.

2 Scope

This policy applies to all members of LEAD community (staff (including agency workers), governors, learners, contractors/suppliers and members of the public).

This policy does not form part of the formal staff contract of employment nor of the student contract with LEAD, but it is a condition of both contracts that LEAD regulations and policies must be adhered to. A failure to follow the policy may result in disciplinary proceedings.

Any members of staff or learners who consider that the policy has not been followed in respect of personal data about themselves or about other data subjects should raise the matter with the designated data controller initially (learners may wish to do this through their lecturer or course tutor). If the matter is not resolved it should be raised as a formal complaint or grievance or through LEAD 's Complaints Procedure where appropriate.

Notification of Data Held and Processed

2.1 All staff, learners and other data subjects are entitled to

- Know what information LEAD holds and processes about them and why
- Know how to gain access to it
- Know how to keep it up to date
- Know what LEAD is doing to comply with its obligations under the 1998 Act

2.2 LEAD will advise staff and learners and other relevant data subjects about the types of data LEAD holds and processes about them, and the reasons for which it is processed. This will be notified via application/enrolment or other documentation.

3 Legislation

- General Data Protection Regulation 2018
- Data Protection Act 1998
- Freedom of Information Act 2000
- Computer Misuse Act 1990
- Education Act 2002

4 Responsibilities

4.1 LEAD staff have responsibility for

i. Checking that information they provide to LEAD in connection with their employment is accurate and up to date.
ii. Informing LEAD of changes to information which they have provided, e.g. change of address.

iii. Checking the information that LEAD will send to them from time to time, which gives details of information kept and processed about them.
iv. Informing LEAD of any errors or changes. LEAD cannot be held responsible for any errors which staff members have had the opportunity to correct.

4.2 If and when, as part of their responsibilities, staff collect information about other people, (i.e. about learners' course work, opinions about ability, references to other academic institutions, or details of personal circumstances) they need to follow the data collection principles

4.3 The Data Controller and the Designated Data Controller ultimately are responsible for ensuring implementation of this policy. They will also deal with day-to-day matters.

The Director is the designated data controller.

5 Actions to Implement and Develop Policy

5.1 Data Security

All staff have responsibility for ensuring that:

- Any personal data which they hold is stored and disposed of securely.
- Personal information is not disclosed orally, in writing, accidentally, or otherwise to any unauthorised third party

Staff should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases.

The Data Security Policy contains requirements for the encryption of data being transferred to approved third parties.

Personal information should be stored securely, usually this means

- In a locked office, or
- In a locked filing cabinet, or
- In a locked drawer, or
- If it is computerised, be password protected, or
- If it is kept on portable storage (i.e. USB, laptop etc..) be encrypted and itself kept securely

5.2 Unauthorised Access

Any member of staff or student who deliberately gains or attempts to gain unauthorised access to personal data on any data subject or discloses such data to any third party may be disciplined in accordance to LEAD procedures.

5.3 Student Obligations

Learners must ensure that all personal data provided to LEAD are accurate and up to date. Learners must ensure that changes of address, etc, are notified to MIS and admin office.

Learners who use LEAD facilities may wish, from time to time, to process personal data. If they do they must obtain the prior permission of their course tutor.

5.4 Rights of Access to Information

Staff, learners and other data subjects have the right of access to any personal data that are being kept about them either on computer or in certain other files. Any person who wishes to exercise this right should complete LEAD "Access to Information" form and give it to the designated data controller or, in the case of a student, to her/his course tutor or lecturer. Forms are available from the finance office

LEAD aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 21 days unless there is good reason for delay. In such cases, the reason for delay will be explained in writing to the data subject making the request.

5.5 Public Domain

Information that is already in the public domain is exempt from the 1998 Act.

5.6 Subject Consent

In many cases, LEAD can only process personal data with the consent of the individual. In some cases, if the data are sensitive, express consent must be obtained. Data is considered sensitive if it is about an individual's race; political opinions; religious beliefs; trade union membership; health; sex life or criminal record.

Agreement to LEAD processing some specified classes of personal data is a condition of acceptance of a student onto any course, and a condition of employment for staff. This includes information about previous convictions.

Some jobs or courses will bring the applicants into contact with children, including young people between the ages of 14 and 17. LEAD has a duty under the Education Act 2002 and other enactments to ensure that staff are suitable for the job, and learners for the courses offered. LEAD also has a duty of care to all staff and learners and must therefore make sure those employees, and those who use LEAD facilities, do not pose a threat or danger to other users.

LEAD will also ask for information about particular health needs, such as allergies to particular forms of medication or any conditions such as asthma or diabetes. LEAD will only use the information in the protection of the health and safety of the individual, but will need consent to process in the event of a medical emergency, for example.

Therefore, all prospective staff and learners will be asked to sign a 'Consent to Process' clause in any application forms, regarding particular types of information when an offer of employment or a course place is made. A refusal to sign such a form can result in the offer being withdrawn.

5.7 Examination Marks

Learners will be entitled to information about their marks for both coursework and examinations. However, this may take longer than other information to provide. LEAD may withhold certificates, accreditation or references in the event that the full course fees have not been paid, or all books and equipment returned.

5.8 Retention of Data

A full list of information with retention times is available from the designated data controller and detailed in the Archive policy.

LEAD will keep some forms of information for longer than others. In general information about learners will be kept for a maximum of ten years after they leave LEAD.

Some information, including information about health, or disciplinary matters will be destroyed within 3 years of the learners leaving LEAD.

LEAD will need to keep information about staff for six years after the member of staff leaves. Some information however will be kept for much longer. This will include information necessary in respect of pensions, taxation, health, potential or current disputes or litigation regarding the employment and information required for job references.