



Data Protection Policy

Introduction

London Electrical College Ltd is required to keep certain information about employees, students and other users to allow it to monitor performance, achievements, health and safety, recruitment etc. LEC also has legal obligations to submit data to government funding bodies / agencies. To comply with the law, information must be used fairly, stored safely and not be disclosed to any person unlawfully. To do this, LEC must comply with the Data Protection Principles which are set out in the Data Protection Act 1998 (the 1998 Act).

This policy is operated in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. Where this policy refers to data protection principles, rights or responsibilities, these are intended to reflect the requirements of current data protection legislation as amended or replaced from time to time.

In summary these state that personal data shall:

- Be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met.
- Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose.
- Be adequate, relevant and not excessive for those purposes.
- Be accurate and kept up to date.
- Not be kept for longer than is necessary for that purpose.
- Be processed in accordance with the data subject's rights.
- Be kept safe from unauthorised access, accidental loss or destruction.
- Not be transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data.

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

Status of the Policy

This policy does not form part of the formal contract of employment, but it is a condition of employment that employees will abide by the rules and policies made by LEC from time to time. Any failure to follow the policy can therefore result in disciplinary proceedings.

Any member of staff who considers that the policy has not been followed in respect of personal data about themselves should raise the matter with the Data Controller initially. If the matter is not resolved it should be raised as a formal grievance.

Notification of Data Held and Processed

All staff, students and other users are entitled to

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

LEC will update staff data at least annually. Students' data is updated annually through the enrolment process.

Responsibilities of Staff

- To check that any information that they provide to LEC in connection with their employment is accurate and up to date.
- To inform LEC of any changes to information, which they have provided. i.e. changes of address.
- Checking the information that LEC will send out from time to time, giving details of information kept and processed about staff.
- To inform LEC of any errors or changes. LEC cannot be held responsible for any errors that have not been notified.

If and when, as part of their responsibilities, staff collect information about other people, (e.g. about students' course work, opinions about ability, references to other academic institutions, or details of personal circumstances), they must comply with the guidelines for staff.

Training and Staff Awareness

All staff who handle or process personal data are required to complete data protection and information security awareness training as appropriate to their role.

Training will include data protection principles, secure data handling, and reporting of data breaches. Refresher training and updates will be provided where legislation, systems or procedures change.

Data Security

All staff are responsible for ensuring that:

- Any personal data which they hold is kept securely.

- Personal information is not disclosed either orally or in writing or 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.

Personal information should be

- kept in a locked filing cabinet; or
- in a locked drawer; or
- if it is computerised, be password protected; or
- stored only on disk which is itself secure.

Any actual or suspected personal data breach, including loss, unauthorised access, disclosure or destruction of personal data, must be reported immediately to the Data Protection Officer. The College will assess all reported incidents and take appropriate action, including containment, investigation and notification where required in line with UK GDPR requirements.

Monitoring and Review

Compliance with this Data Protection Policy is monitored by the Data Protection Officer and senior management through routine oversight, incident review and periodic checks.

This policy is reviewed annually, or sooner where required, to ensure it remains effective, compliant with legislation, and aligned with awarding organisation and regulatory requirements.

Student Obligations

Students must ensure that all personal data provided to LEC is accurate and up to date. They must ensure that changes of address, etc are notified to the administrators or other person as appropriate.

Rights to Access Information

Staff, students and other users of LEC have the right to access any personal data that is being kept about them either on computer or in certain files. Any person who wishes to exercise this right should complete the college "Access to Information" form and hand it in to the main office, who will forward it to the Data Protection Officer.

In order to gain access, an individual may wish to receive notification of the information currently being held. This request should be made in writing using the standard form attached.

LEC will make no charge for the first occasion that access is requested, but may make a charge of £10 per each subsequent request at its discretion.

LEC 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.

Publication of LEC Information

Information that is already in the public domain is exempt from the 1998 Act. It is LEC policy to make as much information public as possible, and in particular the following information will be available to the public for inspection:

- Names of LEC governors and senior staff with significant financial responsibilities (for inspection during office hours only)
- List of key staff
- Photographs of key staff
- Information on examination results

The Colleges internal phone list is not a public document.

Subject Consent

In many cases, LEC can only process personal data with the consent of the individual. In some cases, if the data is sensitive, **express consent** must be obtained. Agreement to LEC 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 criminal convictions.

Some jobs or courses will bring the applicants into contact with children, including young people between the ages of 16 and 18. LEC has a duty under the Children Act and other enactments to ensure that staffs are suitable for the job, and students for the courses offered. LEC also has a duty of care to all staff and students and must therefore make sure that employees and those who use LEC facilities do not pose a threat or danger to other users.

LEC 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. LEC 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.

Processing Sensitive Information

Sometimes it is necessary to process information about a person's health, criminal convictions, race and gender and family details. This may be to ensure LEC is a safe place for everyone, or to operate other LEC policies, such as the sick pay policy or equal

opportunities policy. Because this information is considered sensitive, and it is recognised that the processing of it may cause particular concern or distress to individuals, staff and students will be asked to give express consent for LEC to do this. Offers of employment or course places may be withdrawn if an individual refuses to consent to this, without good reason. More information about this is available from the Data Controller.

The Data Controller

The College as a body corporate is the Data Controller under the Act, and the board is therefore ultimately responsible for implementation. However, there is a designated Data Protection Officer that deals with data protection issues and requests. The first point of contact for enquiries is

Ardita Zeka
London Electrical College,
North Finchley Library,
Ravensdale Ave, North Finchley
N12 9HP

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

Retention of Data

LEC will keep some forms of information for longer than others. Because of data retention legislation, information about students will not be kept indefinitely, unless there are specific requests to do so. LEC will retain student information, student work and other material used through the duration of the student's course for a minimum of 3 years as per EAL policy.

Assessment and Examination Record Retention

In line with awarding organisation and regulatory requirements, London Electrical College will ensure that:

- Accurate assessment records are retained for a minimum of **three (3) years**;
- Internal assessment records are retained for **a minimum of twelve (12) months following certification**; and
- Examination records are retained for a minimum of **two (2) years**.

These arrangements operate alongside the wider retention schedule set out in Appendix 2.

Disposal of Data

When personal data is no longer required, or has passed its retention date, paper records must be shredded. If there is a significant amount of material which cannot be dealt with by normal shredding machines, academy helpdesk should be contacted for a secure shredding bag which can be topped up and shredded by LEC agreed third party. Computerised records must be permanently deleted, with particular care taken that 'hidden' data cannot be recovered. The IT team can advise on permanent deletion of computerised records.

CybSafe and Cyber Security Policy

Introduction

In today's digital age, ensuring the security of our information and systems is paramount. This section outlines our commitment to cyber security and the measures we take to protect our digital assets.

CybSafe

CybSafe is our chosen platform for cyber security awareness and training. It provides comprehensive resources and tools to help our employees understand and mitigate cyber threats. All employees are required to complete CybSafe training modules and stay updated with the latest security practices.

Cyber Security Measures

1. **Access Control:** We implement strict access control measures to ensure that only authorized personnel have access to sensitive information.
2. **Data Protection:** All data, both in transit and at rest, is encrypted to prevent unauthorized access.
3. **Incident Response:** We have a robust incident response plan in place to quickly address and mitigate any security breaches.
4. **Regular Audits:** Regular security audits are conducted to identify and address potential vulnerabilities.
5. **Employee Training:** Continuous training and awareness programs are conducted to keep employees informed about the latest cyber threats and best practices.

Compliance

We adhere to all relevant laws and regulations regarding cyber security and data protection. Our policies are regularly reviewed and updated to ensure compliance with the latest standards.

Conclusion

Compliance with the 1998 Act is the responsibility of all members of the College. Any deliberate breach of the data protection policy may lead to disciplinary action being taken, or access to London Electrical College facilities being withdrawn, or even a criminal prosecution. Any questions or concerns about the interpretation or operation of this policy should be taken up with the Data Protection Officer.

COLLEGE POLICY DATA PROTECTION Appendices

- 1 Staff Guidelines for Data Protection (including checklist for recording data)
- 2 Guidelines for archiving

IMPACT ASSESSMENT			
<i>Equality Strand</i>	<i>Carried out by:</i>	<i>Completed (date)</i>	<i>Comment</i>
<i>Age</i>			
<i>Disability</i>			
<i>Gender</i>			
<i>Race</i>			

LEC POLICY DATA PROTECTION

Appendix 1 to the Data Protection Policy: Staff Guidelines for Data Protection

1. All staff will process data about students on a regular basis, when marking registers, or LEC work, writing reports or references, or as part of a pastoral or academic supervisory role. LEC will ensure, through registration procedures, that all students give their consent to this sort of processing, and are notified of the categories of

processing, as required by the 1998 Act. The information that staff deal with on day-to-day basis will be 'standard' and will cover categories such as:

- General personal details such as name and address,
 - Details about class attendance, course work marks and grades and associated comments.
 - Notes of personal supervision, including matters about behaviour discipline.
2. Information about a student's physical or mental health; sexual life; political or religious views; trade union membership or ethnicity or race is sensitive and can only be collected and processed with the student's consent.

Examples : recording information about dietary needs, for religious or health reasons prior to taking students on a field trip; recording information that a student is pregnant, as part of personal duties.

3. All staff has a duty to make sure that they comply with the data protection principles, which are set out in LEC Data Protection Policy. In particular, staff must ensure that records are:

- accurate;
- up-to-date;
- fair;
- Stored and disposed of safely, and in accordance with LEC policy.

4. LEC will designate staff as 'authorised staff'. These are the only staff authorised to hold or process data that are :

- not standard data; or
- sensitive data

The only exception to this will be if a non-authorised staff member is satisfied that the processing of the data is necessary :

- in the best interests of the student or staff member, or a third person, or LEC; AND
- He or she has either informed the authorised person of this, or has been unable to do so and processing is urgent and necessary in all the circumstances.

This should only happen in very limited circumstances.

Example: A student is injured and unconscious, but in need of medical attention, and a staff tutor tells the hospital that the student is pregnant or a Jehovah's Witness.

5. Authorised staff will be responsible for ensuring that all data is kept securely.

6. Staff must not disclose personal data to any student, unless for normal academic or pastoral purposes, without authorisation or agreement from the data protection officer, or in line with LEC policy.
7. Staff shall not disclose personal data to any other staff member except with the authorisation or agreement of the designated data controller, or in line with LEC policy.
8. Before processing any personal data, all staff should consider the checklist.

Staff Checklist for Recording Data

- Do you really need to record the information?
- Is the information 'standard' or is it 'sensitive'?
- If it is sensitive, do you have the data subject's express consent?
- Has the student been told that this type of data will be processed?
- Are you authorised to collect/store/process the data?
- If yes, have you checked with the data subject that the data is accurate?
- Are you sure that the data is secure?
- If you do not have the data subject's consent to process, are you satisfied it is in the best interests of the student or the staff member to collect and retain the data?
- Have you reported the fact of data collection to the authorised person within the required time?

LEC POLICY DATA PROTECTION

Appendix 2 to the Data Protection Policy: Guidelines for Archiving

Department	Type of Data	Reason for retention	To be maintained by:	Period of Retention	Location of Records

Centre Coordinator / Human Resources	• Personnel files	Provision of references and limitation period for litigation.	Head of Human Resources	6 years from the end of employment.	Centre Manager secure computerised file
Centre Coordinator / Human Resources	• Training records	Limitation period for litigation.		6 months from interview date	
Centre Coordinator / Human Resources	• Notes of grievance	Limitation period for litigation		6 years from the date of redundancies.	
Centre Coordinator / Human Resources	• Disciplinary hearings	Limitation period for litigation		12 years from the date of redundancies	
Centre Coordinator / Human Resources	• Staff applications form, interview notes.	Limitation period for personal injury claims.		3 years.	
Centre Coordinator / Human Resources	• Facts relating to redundancies (less than 20).	Management of health and safety at work regulations 1982.		40 years.	
Centre Coordinator / Human Resources	• Facts relating to redundancies (20 or more).				
Centre Coordinator / Human Resources	• Health records where reason for termination of employment is concerned with health incl. stress related illness.				
Centre Coordinator / Human Resources	• Health records.				
Centre Coordinator / Finance	• Income tax and NI returns: correspondence with Tax Office.	Income Tax (Employment) Regulations 1993.	Head of Finance	3 years after the end of the financial year to which the records relate. 3 years after the end of the financial year to which the records relate. 3 years after the end of the financial year to which the records relate. 6 years from the last date of employment. 6(?) years.	Main archive storage.
	• Statutory Maternity Pay records and calculations.	Statutory Maternity Pay (General) Regulations 1986.		6 years.	
	• Statutory Sick Pay records and calculations.	Statutory Sick Pay (General) Regulations 1982.		7 years.	
	• Wages and salary records.	Taxes Management Act 1970.		20 years.	
	• Invoices, receipts and copies of ledgers and accounts. (Hardcopy and electronic)			10 years.	
	• Official purchase orders, accounts raised bank statements and paid cheques.	Internal historical records.			
	• Tenders and timeexpired contracts.	Internal historical records.			
	• Employer's liability certificate.	Internal Historical records.			
	• Data protection registration				

Health and safety	Records and reports of accidents	RIDDOR 1985 COSHH 1994	H&S Manager	10 years after the date of the last entry. 40 years.	Collate info to include in the Human Resources archive.
	- Medical records kept by reason of the COSHH. - Risk assessments, asbestos register etc.				
Student Data Team	Student records including LPAs / LPDs / Registers and electronic data.	Limitation period for negligence.	Head of CIS.	6 years from the last day of the course. 10 years with the consent of the student for personal and academic references.	Main archive room.
Clerk to the Corporation.	- Minutes of the Board of the Corporation and its committees. - Agenda, papers and other records of the Board of the Corporation. - Internal and external audit reports.	Internal historical records. Internal historical records. Internal historical records.	Clerk to the Corporation	Never dispose. 10 years. 7 years.	
Examinations	- Exam and assessment records – entries and result files. - Student coursework sent to external examining bodies.	Internal historical records.	Head of Registry.	3 years from the date of claim. No longer than appeal period.	Main archive room. None expected as course work will be sent back to student.
Student Services	- Confidential student counselling records. - Student counselling, A and G, New Deal, EMA, Access fund and childcare.	Internal historical records.	Head of Registry.	2 years. Duration of student's enrolment then archived for 3 years.	
Quality Development	- Internal quality audit files. - Document control records.	Internal historical records. Internal historical records.	Quality Manager.	5 years. 5 years.	
CTS	Software licenses and hardware registers.	Internal historical records.	Head of CTS.	5 years.	
Academic Schools	- Student files (ILP's, timetables, course logs, course reviews, staff timetable) - Student examination scripts (internal). Student coursework / portfolios.	Internal inspection records. Evidence of achievement. Evidence of achievement.	Head of School.	3 years. 6 years. 3 years.	Academic area.