

Introduction

LA Training data protection policy sets out our commitment to protecting personal data and how we implement that commitment with regards to the collection and use of personal data.

Data Protection Act

The Data Protection Act 1998 describes how organisations, including LA Training, must collect, handle and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or by other means.

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 eight important principles. These say that personal data must:

1. Be processed fairly and lawfully
2. Be obtained only for specific, lawful purposes
3. Be adequate, relevant and not excessive
4. Be accurate and kept up to date
5. Not be held for any longer than necessary
6. Processed in accordance with the right of data subjects
7. Be protected in appropriate ways
8. Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection.

Policy Scope

The policy applies to all staff who are employed by LA Training, as well as all contractors, supplier and other people working on behalf of the company.

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside the Data Protection Act 1998. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone Numbers

Data Protection Risks

This policy helps to protect LA Training from some very real security data risks, including:

- Breaches of confidentiality (e.g. information being given out inappropriately.)
- Failing to offer choice (e.g. all individuals should be free to choose how the company uses data in relating to them.)
- Reputational damage (e.g. the company could suffer if hackers successfully gained access to sensitive data.)

Responsibilities

Everyone who works for or with LA Training has a responsibility to ensure data is collected and handled appropriately.

Each member of staff that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, the managing directors have these key areas of responsibilities:

- They are ultimately responsible for ensuring that LA Training meet its legal obligation.
- They keep all staff updated about data protection responsibilities, risks and issues.
- They review all data protection procedures and related policies, in line with an agreed schedule.
- They arrange data protection training and advice for the people included in this policy.
- They must handle data protection questions from all staff.
- They deal with requests from individuals to see the data LA training holds about them.
- They check and approve any contracts or agreements with third parties that may include the companies sensitive data.
- They ensure all IT systems, services and equipment used for storing data, meet acceptable security standards.

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.
- LA Training 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 company guidelines.
- Strong passwords must be used and never be shared.
- Personal data should not be disclosed to unauthorised people, with the company 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 or disposed of.

Data Storage

These rules describe how and where data should be safely stored, Questions about storing data safely can be directed to the managing directors.

When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper of files should be kept in a locked drawer or filing cabinet.
- Employees should make sure paper and printouts are not left where unauthorised people could see them.
- 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.

- Data should be protected by strong passwords that are changed regularly and never shared between employees.
- If data is stored on removable media (CD), these should be kept locked away securely when not being used.
- Data should only be stored on designated drives and servers, and should only be uploaded to approved cloud computing services.
- Data should be backed up frequently and those backups should be tested regularly, in line with the company's standard backup process.
- All servers and computers containing data should be protected by approved security software and a firewall.

Data use

Personal data is of no value to LA training unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, employees should ensure the screens of their computers are always locked when left unattended.
- Personal data should not be shared informally. In particular, it should never be sent by email, as this form of communication is not secure.
- Personal data should never be transferred outside of the EEA.
- Employees should not save copies of personal data to their own computers.

Data accuracy

The law requires LA Training to take responsible steps to ensure data is kept accurate and up to date.

The more important it is that the personal data is accurate, the greater the effort LA Training should put in to ensuring its accuracy.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept accurate and up to date as possible.

- Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets.
- Staff should take every opportunity to ensure data is updated.
- LA Training will make it easy for data subjects to update the information LA Training holds about them.
- Data should be updated as inaccuracies.

Subject access requests

All individuals who are subject of personal data held by LA Training are entitled to:

- Ask what information the company holds about them and why.
- Ask how to gain access to it.
- Be informed how to keep it up to date.
- Be informed how the company is meeting its data protection obligations.

If an individual contacts the company requesting this information, this is called a subject access request. Subject access requests from individuals should be made by email, addressed to LA Training at the company's e-mail address. Individuals will be charged £10 per subject access request. LA Training will aim to provide the relevant data within 14 days. LA Training will also verify the identity of anyone making a subject access request, before handing over any information.

Disclosing data for other reasons

In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, LA Training will disclose requested data. However, LA Training will ensure the request is legitimate seeking assistance from the company's legal advisers when necessary.

Providing Information

LA Training 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 their rights.

To these ends, LA training has a privacy statement, setting out how data relating to individuals is used by the company.

Signed..... Daniel Bevan (Managing Director)

Signed..... Dominic Ham (Managing Director)

Reviewed: 20/08/18