Lift-it Training Company

Data Protection Policy

Lift-it Training Company
Unit 50,
Holmebank Business Park,
Station Road,
Mirfield,
West Yorkshire,
WF14 8NA

The GDPR Act 2018 requires every data controller who is processing personal data to notify unless they are exempt. Failure to notify is a criminal offence.

Lift-it Training Company (LTC) will set up a direct debit to renew our notification each year for the following purposes if the Business changes significantly:

- Staff administration
- Advertising, marketing and public relations
- Accounts and records
- Advertising, marketing and public relations for others
- Consultancy and advisory services
- Education
- Information and databank administration
- Journalism and media
- Legal services
- Research
- Trading/sharing in personal information

If Lift-It Training Company needs to collect data for any purpose not stated above we will notify the Information Commissioner before collecting that data.

Lift-It Training Company is a controller of data in respect of personal files of employees and a Data processor in respect of the Data we process for our funders that is then handed and controlled by them.

Six Data Protection Principles

Whenever collecting information about people LTC agrees to apply the Six Data Protection Principles set out by GDPR:

1. Personal data should be processed fairly, lawfully and be transparent
2. Personal data should be obtained only for the purpose specified under the limitation principle.
3. Data collected should be adequate, relevant and not excessive for the purposes required.
4. Data must be aaccurate and kept up-to-date including 3rd parties

5. All candidates/Learners have the right to withdraw their permission to have their personal date stored by LTC or the RTITB at any point in time, notification will be needed via email or in righting to the below companies address's
6. Lift-it Training, Unit 50, Holmebank Business Park, Station Road West Yorkshire WF14 8NA
7. RTITB, HQ, Access House, Halesfield 17, Telford TF7 4PW
8. Data should not be kept for longer than is necessary for purpose unless legislation alters or our awarding body requests.
9. Security: appropriate technical and organizational measures should be taken unauthorized or unlawful processing of personal data and against accidental loss or destruction or damage to personal data.

Notes for Your Org:

- Data controller (for employees) and Processor (RTITB for Operators) must provide their identityty, people should be told exactly what the information is being collected for and any other information necessary. We must get their consent.
- We should think in advance about what we wish to do with personal data – i.e. – if we get names and addresses for a specific campaign we should only use that info for that campaign – we should from now on add other purposes to forms – e.g. I wish to be kept up-to-date with LTC activities.
- Individuals have a right to see what data is being kept on them, and for what purpose in 30 days
- Personal data should never be taken out of the office/ Training centre
- If we buy in a mailing list we cannot use it for any other purpose than the original Data Controller specified – we must check original use.
- Data subjects must be made aware of Third party involvements
- Data subjects must be told access and correction rights
- Data subjects must be told about the right to be forgotten
- Data subjects must be told about the right to withdraw
- Data subjects must be to about the Mechanism of how their data will be used

Working from home

- Employees must never take any personal data from the office
- Employees must not use personal Laptops, Phones and e-mails for company business

Security Statement

LTC has taken measures to guard against unauthorized or unlawful processing of personal data and against accidental loss, destruction or damage.

This includes:

- Adopting an information security policy (this document is our policy)
- Taking steps to control physical security (projects and staff records are all kept in a locked filing cabinet)
- Establishing a business continuity/disaster recovery plan (LTC takes regular back-ups of its computer data files and this is stored away from the office at a safe location)
- Training all staff on security systems and procedures
- Detecting and investigating breaches of security should they occur
- No data to be held on Laptops / Computers except in relation to training via our company and the NORS data base with consent from our trainees/company's.
- Data to be encrypted and password protected on USB drive
- All laptops to use Vera Crypt encryption software as and when required
- USB drives to be kept in a locked secure safe
- The safe is to be secured to an outside wall
- A lock is to be put on the office to secure data inside and must be locked when the office is not in use, all files that contain personal data to be returned to the office when not in use.
- Screens are to be used on laptops so only the user can see data.
- Any data breaches to be reported to ICO within 72 hours

This document is controlled by the Managing Director of Lift-it Training Company Mr. R H. Wadsworth and will be the nominated person for the above policy.

Signed……R. Wadsworth……/Date……..10th May 2018……

Name Richard Wadsworth ……/Date……10th May 2018……

To be reviewed as and when the business/regulations alter.