Data Protection Policy

Context and overview

Key Details

Policy prepared by	David Riddell
Approved by board / management on:	30th March 2018
Policy became operational on:	31st March 2018
Reviewed on:	31st March 2021
Next review date:	31st March 2022

1. Introduction

Later Life Training Ltd need to gather and use certain information about individuals.

These can include customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the company's data protection standards — and to comply with the law.

2. Why this policy exists

This data protection policy ensures Later Life Training Ltd:

- Complies with data protection law and follows good practice.
- Protects the rights of staff, customers and partners.
- Is open about how it stores and processes individuals' data.
- Protects itself from the risks of a data breach.

3. Data protection law

The General Data Protection Regulation (GDPR) legislation which came into force on 25th May 2018 describes how organisations — including Later Life Training Ltd — must collect, handle and store personal information. These rules apply regardless of whether data is stored electronically, on paper or on other materials. To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully. GDPR expands the definition of "personal data" to include a much wider range of consumer information. Whereas the Data Protection Act only pertains to information used to identify an individual or their personal details, GDPR broadens that scope to include online identification markers, location data, genetic information and more.

The key principles of GDPR are as follows. Personal data shall be;

a) Processed lawfully, fairly and in a transparent manner in relation to individuals.

b) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for

archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

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

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

e) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.

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.

4. People, risks and responsibilities

Policy Scope

This policy applies to:

- The head office of Later Life Training Ltd.
- All branches of Later Life Training Ltd.
- All staff and volunteers of Later Life Training Ltd.
- All contractors, suppliers and other people working on behalf of Later Life Training Ltd.

It applies to all data that the company holds relating to identifiable individuals. This can include, but not limited to;

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- Plus any other information relating to individuals

5. Data protection risks

This policy helps to protect Later Life Training Ltd from some very real data security risks, including;

Breaches of confidentiality. For instance, information being given out inappropriately.

Failing to offer choice. For instance, all individuals should be free to choose how the company uses data relating to them.

Reputational damage. For instance, the company could suffer if hackers successfully gained access to sensitive data.

6. Responsibilities

Everyone who works for, or with Later Life Training Ltd, has some responsibility for ensuring data is collected, stored and handled appropriately.

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

However, the following people have key areas of responsibility:

The **board of directors** is ultimately responsible for ensuring that Later Life Training Ltd meets its legal obligations.

The **data protection officer**, **David Riddell**, is responsible for:

- Keeping the directors updated about data protection responsibilities, risks and issues.
- Reviewing all data protection procedures and related policies, in line with an agreed schedule.
- Arranging data protection training and advice for the people covered by this policy
- Handling data protection questions from staff and anyone else covered by this policy
- Dealing with requests from individuals to see the data Later Life Training Ltd holds about them (also called 'subject access requests').
- Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data

The **Office manager**, **David Riddell**, is responsible for:

- Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
- Performing regular checks and scans to ensure security hardware and software is functioning properly.
- Evaluating any third-party services the company is considering using to store or process data. For instance, Modus Scotland or Expert IT Solutions

7. 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**. When access to confidential information is required, employees can request it from their line managers.

Later Life Training Ltd **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

the guidelines below:

- In particular, **strong passwords must be used** and they should never be shared, apart from with the data protection who will store all passwords.
- Personal data **should not be disclosed** with unauthorised people, either within 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 and disposed of.
- Employees **should request help** from their line manager, or the data protection officer, if they are unsure about any aspect of data protection.

8. Data storage

These rules describe how, and where, data should be safely stored. Questions about storing data safely can be directed to the office manager or data controller. 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 or files should be kept **in a locked drawer or filing cabinet** and all keys stored in a locked box with the office manager keeping the master key.

Employees should make sure paper and printouts are **not left where unauthorised people could see them**, like on a printer.

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** (like a CD or DVD), 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 an **approved cloud computing services**. No sensitive information should be stored on an individual PC.
- Servers containing personal data should be **sited in a secure location**.
- Data should be **backed up frequently**. Those backups should be tested regularly, in line with the company's standard backup procedures.
- Data should **never be saved directly** to laptops or other mobile devices like tablets or smart phones.
- All mobile devices with access to the company's network should be protected by strong passwords or PIN numbers.
- All servers and computers containing data should be protected by **approved security software and a firewall**.

9. Data use

Personal data is of no value to Later Life Training Ltd 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.

Data must be **encrypted before being transferred electronically**. The office manager can explain how to send data to authorised external contacts.

Personal data should **never be transferred outside of the European Economic Area**.

Employees **should not save copies of personal data to their own computers**. Always access and update the central copy of any data.

10. Data accuracy

The law requires Later Life Training Ltd to take reasonable 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 Later Life Training Ltd should put into ensuring its accuracy.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as 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**. For instance, by confirming a customer's details when they call/email.
- Later Life Training Ltd will make it **easy for data subjects to update the information** Later Life Training Ltd holds about them. For instance, via a simple email request.
- Data should be **updated as inaccuracies are discovered**. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.

11. Subject access requests

All individuals who are the subject of personal data held by Later Life Training Ltd are entitled to:

- The right to request a copy of the personal data we hold.
- Withdraw consent for Later Life Training Ltd to use personal data for marketing purposes at any time.
- The right to request a correction to information that we hold.
- The right to lodge a complaint with a supervisory authority if we fail in our obligations to protect data.
- 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 the data controller at info@laterlifetraining.co.uk. The data controller does not require a standard request form. The data controller will aim to provide the relevant data within 28 days. The data controller will always verify the identity of anyone making a subject access request before handing over any information.

12. 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, Later Life Training Ltd will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers where necessary.

13. Providing information

Later Life Training Ltd 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, the company has a privacy policy, setting out how data relating to individuals is used by the company. This is available on the Later Life Training website.