
MANTRA LEARNING LIMITED DATA PROTECTION POLICY

A) INTRODUCTION

Mantra Learning Limited is fully committed to compliance with the requirements of the Data Protection Act 2018 including the European Union's General Data Protection Regulation (GDPR). To this end Mantra Learning Limited fully endorses and adheres to and complies with the eight principles of the Act that states personal information held by them will be: -

- fairly and lawfully processed.
- processed for limited purposes.
- adequate, relevant, and not excessive.
- accurate and up to date.
- not kept for longer than is necessary.
- processed in line with employer/employee rights.
- secure; and
- Not transferred to other countries without adequate protection.

In order to operate efficiently, Mantra Learning Limited has to collect and use information about people with whom it works. These may include employees, sub-contractors, learners, employers, and suppliers.

Personal information will only be processed in line with established regulations. Personal data will be collected, recorded, and used fairly, stored safely and securely and not disclosed to any third party unlawfully.

As the lawful and correct treatment of personal information is critical to our successful operations and to maintaining confidence, Mantra Learning Limited is committed to: -

- protecting learners and staff's personal details, records, and assessment outcomes.
- keeping learners, staff, and other individuals' personal data up to date and confidential.
- maintaining personal data only for the time period required.
- releasing personal data only to authorised individuals / parties and will not do so unless permission is given.
- collecting accurate and relevant data only for specified lawful purposes; and
- adhering to regulations and related procedures to ensure that all employees who have access to any personal data held by or on behalf of Mantra Learning Limited are fully aware of and abide by their duties under the Data Protection Act 2018.

Because Mantra Learning Limited is a training provider, learners' personal information may need to be shared at some point. By providing personal information learners are deemed to consent to your personal information being shared outside Mantra Learning Limited in the following circumstances: -

- where Mantra Learning Limited needs to share learner information to provide the service they have requested.
- where Mantra Learning Limited needs to send the information to companies who work on behalf of Mantra Learning Limited to provide a service to the learner (we will only provide those companies with the information they need to deliver the service, and they are prohibited from using that information for any other purpose); and
- Mantra Learning Limited will also disclose learners' personal information if required to do so by law in urgent circumstances, to protect personal safety, the public or our website.
- Sometimes it is necessary to process information about a person's health, criminal convictions, race, gender, and family details. This may be to ensure that Mantra Learning is a safe place for everyone, or to operate other policies such as the safeguarding policy. Offers of employment or course places may be withdrawn if an individual refuses to consent to this, without good reason.

Mantra Learning Limited data is stored in controlled servers with limited access. All personal information is stored and processed in the United Kingdom where Mantra Learning Limited, or its business partners, are located.

The Company website does not target, and is not intended to attract, children under the age of 14. Mantra Learning Limited does not knowingly solicit personal information from children under the age of 14 or send them requests for personal information.

Mantra Learning Limited may amend this policy from time to time. If we make any substantial changes in the way, we use your personal information we will make that information available.

B) RETENTION OF DATA

Mantra Learning Limited will keep some forms of information for longer than others. Because of storage problems, information about learners cannot be kept indefinitely, unless there are specific requests to do so for the funding and/or awarding body organisations. Please refer to the documentation retention policy for specific timescales on data storage.

C) STAFF GUIDELINES FOR DATA PROTECTION

1. All staff will process data about learners on a regular basis. Mantra Learning will ensure through registration procedures that all learners give their consent to this processing, and are notified of the categories of processing, as required by the 2018 data protection act. The information that staff deal with on a day-to-day basis will be standard and will cover categories such as:

- General personal details such as name and address
- Details about course attendance, course work and associated comments
- Notes of personal supervision, including matters about behaviour and discipline

2. All staff have a duty to make sure they comply with the data protection principles. In particular, staff must ensure that records are:

- Accurate
- Up to date
- Fair
- Kept and disposed of safely and in accordance with Mantra Learning's policies

3. Staff will be responsible for ensuring that all data is always kept securely.

4. Staff must not disclose personal data, without authorisation or in line with Mantra Learning's policy.

5. Personal information, whether electronic or paper based, should be stored securely and in keeping with Mantra Learning's procedures. Information should only be removed from its storage location when operationally necessary and with appropriate security measures in place.

6. Staff must ensure that learners are aware of the need to keep their own data secure around Mantra Learning premises for example, saving their CV to the learner computers.

7. Staff must ensure all data is stored in a lockable room and/or lockable cabinets.

8. Any staff member or learner wishing to access their information stored by Mantra Learning must do so in writing by completing the 'Access to information request form'.

9. Staff must report any data potential and/or breaches of data protection.

D) REMOTE / HOME WORKING

Remote working may involve paper records or use of electronic devices to access Mantra Learning's network outside of the offices. Examples of remote working may include:

- Home working
- Working when 'on the move' (e.g. on a train, during site visits)
- Working from the premises of customers, companies, delivery partners, contractors, and other organisations.

All Mantra Learning staff working at home or remotely are responsible for ensuring that all data, both paper and electronic, is kept confidential and secure to prevent access by a third party regardless of the environment.

Key principles specific to remote and home working are:

- For home working it is recommended that the work area of the house should be separate from the rest of the household.
- Laptops and other electronic devices should be locked when leaving unattended.

- When leaving the house (even for a short period), laptops and electronic devices must be shut down and all paperwork put securely away and out of sight.
- Paper files must be locked away in a secure cabinet when not in use.
- Do not email or divert emails to a personal email address in order to work remotely.
- Do not create or attempt to transfer data to you own home computer, mobile and/or any other devices including emails.
- Do not use USB data sticks, CD's or other removable media as portable temporary storage for electronic files and documents unless they have been appropriately encrypted.

When working in public locations, it is requested that this is only done if there are no other alternatives. Extra care should be taken to ensure that no bystander could overlook any information displayed on devices or paper documentation.

E) DATA AND DEVICES IN TRANSIT

When moving any data away from Mantra learning premises the following must be followed:

- Always shut down any device when in transit, regardless of the length of journey, this is to ensure encryption is engaged and the device is properly protected.
- Don't leave bags or cases containing paper files and/or devices visible in a vehicle.
- Never leave a device or papers unattended in a vehicle.
- Any paper files should not be visible from the vehicle and should be kept hidden when moving
- When travelling on public transport keep bags/cases containing paper files and/or devices close by at all times. Items should not be placed in luggage racks or storage areas as this increases the possibility of theft or the misplacing of the item.

F) CCTV

Mantra Learning will follow guidance in the Information Commission's code of conduct for users of CCTV and similar surveillance equipment monitoring spaces to which the public, learners and employees have access.

G) RIGHT TO INFORMATION

Learners and employees can request access to the information that Mantra Learning hold. To access this information an Access to information request form must be completed and returned to Mantra Learning by emailing dataprotection@mantralearning.co.uk. Mantra Learning have up to 10 working days to respond to the request.

The Data Protection Act gives individuals the right to know what personal information is held about them on computer and paper records.

Should any employee or learner of Mantra Learning Limited feel they have been denied access to personal information they are entitled to view or feel their information has not been handled according to the eight principles, they can contact the Information Commissioner's Office by writing to, Wycliffe House, Water lane, Wilmslow, Cheshire, SK9 5AF, or via telephone on 01625 545700.

If you have any questions or concerns about the collection, use, or disclosure of your or others personal information, please contact the HR & Quality Department or email dataprotection@mantralearning.co.uk.

H) DATA BREACHES

In the event of a data breach, it must be reported within 24 hours to the data protection persons within Mantra Learning by emailing Dataprotection@mantralearning.co.uk.

Details of the breach must be provided in full and logged onto the data breach log.

Individual's who are or may be affected by the breach must be contacted within 24 hours of the breach being reported, and if required, their employer informed.

Where the breach is deemed a risk to individual's data then Mantra Learning must report this to the Information Commissioner's office within 72 hours of the breach.

For further guidance, please refer to the data breach log guidance.

I) CONTRAVENTION OF THIS POLICY

Failure to comply with any of the requirements of this policy is a disciplinary offence and may result in disciplinary action being taken under Mantra Learning Limited's disciplinary procedure.

Signed:



Mark Currie, Chief Executive

Date: May 2022

Review Date: May 2023

Version: 1