achieve more
TRAINING LTD

Data Protection

Policy and Procedure

Document Status	Live & Current
Document Type	POL028
Version	5.0
Issue	1
Document Date	Jan 2025
Review Date	Jan 2027
Publication	Controlled Hard Copy and saved to cloud

Signed: 
Name/Role: Joe Havey / Director
Date: 20/01/2025

Signed: 
Name/Role: Matthew Hilliker
Date: 20/01/2025

Data Protection Policy

Introduction

Achieve More Training needs 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.

Why this policy exists

This data protection policy ensures that Achieve More Training Complies with data protection law and follow 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

Data protection law

The Data Protection Act 2018 describes how organisations — must collect, handle and store personal information.

Digital technology has transformed almost every aspect of our lives in the twenty years since the last Data Protection Act was passed.

Our new Data Protection Act:

- makes our data protection laws fit for the digital age in which an ever-increasing amount of data is being processed
- empowers people to take control of their data
- supports UK businesses and organisations through the change
- ensures that the UK is prepared for the future after we have left the EU
- The text of the Data Protection Act and related documents can be found here on legislation.gov.uk Historical documents relating to the passage of the Act can be found on the Parliament website.

People, risks and responsibilities

Policy scope

This policy applies to:

- All staff and volunteers of Achieve More Training
- All contractors, suppliers and other people working on behalf of Achieve More Training

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 2018. This can include:

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

Data protection risks

This policy helps to protect Achieve More 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.

Responsibilities

Everyone who works for or on behalf of the company has some responsibility for ensuring data is collected, stored and handled appropriately.

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

However, these people have key areas of responsibility:

- The **Director** is ultimately responsible for ensuring that Achieve More Training meets its legal obligations.
- All staff to be responsible for:
    - Keeping them 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 (where necessary.)
    - Handling data protection questions from staff and anyone else covered by this policy.

- Dealing with requests from individuals to see the data Achieve More 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 **Administration staff are** 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, cloud computing services.

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.
- 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.
- Personal data **should not be disclosed** to 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.
- When **collecting or sharing personal data / ID / information remotely**, encryption platforms should be used (Such as watts app / one drive / Egress)

Data storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the IT 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**.

- 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** should only be uploaded to the **approved cloud computing services**.

- Servers containing personal data should be **sited in a secure location**, away from general office space.

- 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 servers and computers containing data should be protected by **approved security software and a firewall**.

Data use

Personal data is of no value to Achieve More 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**. It should never be sent by email, as this form of communication is not secure.

- Sensitive Data must be **transferred securely encryption** platforms/software/applications should be used (Such as watts app / one drive / Egress / Filezilla)**.** Staff will be trained on how to send data to authorized 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.

- Pictures and personal information such as names, work places may be shared for marketing and publicity purposes with the consent of the individual at the application/referral stage: 'I **consent for the information contained in this application to be processed and shared with**

relevant host company and training provider, as required, in accordance with the principles of the Data Protection Act 1998.'

Data accuracy

The law requires Achieve More Training 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 Achieve More Training 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 learner's/customer's details when they call.
- 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.

Subject access requests

All individuals who are the subject of personal data held by Achieve More 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 the Director at info@achievemoretraining.com . The Director can supply a standard request form, although individuals do not have to use this.

Individuals will be charged £10 per subject access request. The Director will aim to provide the relevant data within 14 days.

The Director will always 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, Achieve More Training will disclose requested data. However, the Director will ensure the request is legitimate.

Providing information

Achieve More 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, the company has a GDPR Statement (available on request,) setting out how data relating to individuals is used by the company.