



# Providence Training Ltd Data Protection Policy

## Introduction

Providence Training Ltd needs to gather and use information about individuals. This can include customers/delegates, suppliers, business contacts, employees and other people that the organisation has or may need to contact. This data protection policy describes how this data must be collected, handled, stored and disposed of in order to meet the legislative requirements of the General Data Protection Regulations (GDPR) on 25<sup>th</sup> May 2018.

## Purpose

This Data Protection Policy ensures that Providence Training Ltd will:

- Comply with the Regulations and follow good practice
- Protect the rights of staff, clients and partners
- Be transparent about how it collects, stores and processes an individual's data
- Protect itself from the risks of data breaches

## Data Protection Law

The Data Protection Act 1998 is being replaced by the General Data Protection Regulations on 25<sup>th</sup> May 2018 (following an EU directive). The Regulations describe how a company must collect, handle, store and dispose of personal information.

The Regulations apply whether the data is stored electronically or as hard copy. Any data kept will be: -

1. Collected fairly and legally
2. The individual will be made aware of the Data Protection Notice and must actively give consent
3. Relevant
4. Accurate and current
5. Held for no longer than necessary
6. Protected appropriately
7. Destroyed on request – right to be forgotten
8. Supplied on request to the relevant individual (free of charge)
9. Not shared with any other party without permission unless disclosed for legitimate reasons

## Scope

This policy applies to: -

- All employees of Providence Training Ltd including associate instructors
- All contractors, suppliers, associates and others working on behalf of Providence Training Ltd

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside GDPR 2018. This data will include:

- Names of individuals
- National Insurance Number
- Company name
- Postal addresses
- E-mail addresses
- Telephone numbers – landline and mobile
- Any other information relating to individuals e.g: Date of Birth

## **Risks**

This policy helps to protect Providence Training Ltd from security risks including:

- Breaches of confidentiality e.g. divulging information by mistake
- Failing to offer choice e.g. preventing the individual giving permission on holding data
- Reputational damage e.g. company servers being hacked and sensitive data being stolen

## **Responsibility**

All staff have responsibility for ensuring that data is collected, handled, stored and disposed of appropriately. Each employee must ensure that data is handled in line with GDPR 2018.

## **Key Stakeholders & Responsibilities**

Managing Director – is responsible for ensuring the company meets its legal requirements under GDPR 2018.

Data Protection Officer – is responsible for

- Keeping the director updated
- Reviewing GDPR procedures
- Arranging GDPR training for employees
- Handling data protection questions from staff and anyone else covered by the policy
- Dealing with requests from individuals who request to see data Providence Training Ltd holds on them
- Ensuring any third party conforms to Providence Training Ltd's Data Protection Policy

Data Controller – is responsible for

- Ensuring marketing initiatives conform to GDPR
- Approving any data protection statements attached to letters and email
- Ensuring that all systems, security (including physical security) and equipment used for storing data meet acceptable security standards
- Perform regular checks and scans to ensure security hardware and software is functioning correctly
- Evaluate any third-party services the company is considering using to store or process data e.g. cloud computing services

General Staff

- The only staff accessing data should need to do it for their work
- Data must not be shared informally
- Providence Training Ltd will provide training to staff where appropriate
- Staff should keep all data secure and take sensible reasonable precautions
- Staff should use strong passwords and change them regularly
- Personal data must not be disclosed to unauthorised people either internally or externally
- Staff should request help from their manager or Data Protection Officer if they are unsure of any aspect of GDPR

## Collection & Storage

- When data is collected it must be with the permission of the individual. Passive agreement is not agreement so the individual must be told we are keeping their data, what will be recorded, how it will be stored and give consent.
- Data will be stored in a secure place either electronically or as hard copy.
- Staff should ensure that they do not leave hard copy records where unauthorised people could see them
- Data should be disposed of securely – e.g. shredded when no longer required
- Where data is stored electronically it must be protected from unauthorised access, accidental deletion and malicious hacking attempts
- Data should be protected by strong passwords, changed regularly and never shared between staff
- Data will only be stored on designated servers drives and approved cloud computing services
- Portable drives will be kept securely
- Data will be backed up frequently, at the end of each day. The backup is removed from site
- Servers are protected with security software and appropriate firewalls

Where on review data is found to be no longer needed it should be disposed of appropriately.

## Use

Data is at the highest risk of loss corruption or theft when it is being used:

- Staff should ensure no data is visible on screens when they are unattended
- Personal data should not be shared informally, where possible it should not be sent by email which is not secure
- Staff should not save copies of personal data to their own computer

## Accuracy

Providence Training Ltd and all employees will take reasonable steps to ensure data is kept up to date and it is accurate and relevant: -

- Data will be held in as few places as possible. Unnecessary additional sets will not be created
- Staff should take the opportunity to update client personal data – by confirming client details when speaking to a client
- Data will be updated as inaccuracies are discovered e.g. if the client can no longer be reached on a specific phone number it should be deleted from the database

## Subject Access Request

The person whose data is held is referred to under GDPR as the data subject. The data subjects of Providence Training Ltd are entitled to:

- Ask what information is held on them
- Ask how to gain access to it
- Be informed how to keep it up to date
- Be informed how the company is meeting its legal obligations under GDPR 2018

Subject access requests should be made to the Data Controller formally in writing. Requests will be managed by the Data Protection Officer. Information will be supplied free of charge within 1 month of the request.

The Data Controller will always verify the identity of the person making the subject access request before handing over any information.

### **Disclosing Data for other reasons**

We may disclose information relating to your training and qualifications to site operators and other relevant bodies who wish to verify that you and other candidates have undertaken training with Providence Training Ltd qualifications, or are in the process of such training and/or are working towards qualifications that we offer . It is within our legitimate business interests and those of candidates, and the industry generally to use candidates' information in this way to protect the reputation of Providence Training Ltd's training courses and qualifications, and to enhance the value of such training and qualifications.

We may also pass on information relating to vocational qualifications to the relevant government bodies e.g police, HSE etc. in accordance with our legal obligations to such bodies. We will not disclose other information to third parties for any other purposes.

Under these circumstances the Data Controller will ensure the request is legitimate seeking legal advice where necessary.



David Warrell BSc  
Managing Director  
Date: 25 May 2018

**Objection to Data Disclosure  
&  
Request for Erasure Form**

1. Please complete the form below if you object to Providence Training Ltd using your data and training and qualification information for the purposes set out in our Privacy Notice **OR** you wish to request that previously supplied information is removed.
2. Please enter the following information in the form below:
  - a. The name and date of the course/test and the name of the Awarding Organisation.
  - b. Your name in BLOCK CAPITALS.
  - c. If you are employed by or associated with an employer “in scope” to Providence Training Ltd, the name of the employer and establishment.
  - d. Your signature.

Course / Test:	
Course / Test Date:	
Name (BLOCK CAPITALS):	
Employer & Establishment (if “in-scope” to Providence Training Ltd)	
Objection to collection of personal data	Request to remove personal data previously supplied

I have read the Providence Training Ltd Privacy Notice. I object to Providence Training Ltd using and sharing information about me including my personal details (which may include photograph) and details relating to my training, registration and achievement of qualifications). I fully understand that objection and/or request for deletion of personal information will prevent any future verification by Providence Training Ltd or production of the relevant product and/or service.

Signature:		Date:	
------------	--	-------	--

Providence Training Office Use Only:			
Date received		Action by & Date	