

## Data Protection Policy

The Data Protection Act 2018 ('Act') and General Data Protection Regulation (GDPR) (Regulation EU 2016/679) places obligations on those that control and process information relating to individuals.

Data refers to information about an individual (referred to as a "data subject") that may be used or processed by Focal Point Training (referred to as a "data controller") in order to carry out its function as a training provider.

There are two categories of data:

### Personal Data

Personal data is data that relates to a living individual (data subject) who can be identified from those data or other information which is already in the possession of or is likely to come into the possession of the data controller.

### Special Categories of Personal Data

This is data that relates to a data subjects racial or ethnic origin, political opinion, religious belief or beliefs of a similar nature, trade union membership, physical or mental health or condition, sexual life, the commission or alleged commission of any offence, criminal proceedings or the sentence of any court/convictions.

### Data Protection Principles

Focal Point Training and Consultancy Ltd is committed to managing, securing and protecting information in line with the seven principles of the GDPR as set out below:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

### Staff Responsibilities

Tracy Powley, Director of Operations, is responsible for overseeing the data protection policy and the processes which support it and reviewing it on an annual basis.

All staff and Consultants within Focal Point have a responsibility to manage and use personal data appropriately according to the principles and procedures set out in this policy and the IT security policy. Failure to do so may result in disciplinary action or termination of contract.

Special Category Data - Due to the sensitive nature of this type of personal data, it is imperative that additional levels of security and safeguards are followed. All staff and consultants are to be responsible for being able to identify these types of data and ensure the appropriate level of security is provided.

### **Security**

All Consultants must follow the Information Security procedures defined in this policy, the Internal Quality Assurance Policy, the Information Security policy and guidelines and their contractual obligations. All Consultants must attest annually that they comply with the standards and procedures outlined in these policies and their contractual terms.

Focal Point Training has appropriate technical and organisational measures in place to protect and ensure the safety of stored data to prevent unauthorised disclosure or use.

All Focal Point documents and materials should be accessed by consultants via MS Teams, our cloud base file sharing system. Information should only be downloaded from Teams where there is a valid reason to do so- such as working with a client where there is no internet access. In these instances, information should be downloaded to an encrypted data stick and deleted after the session. All devices must be password protected.

### **Data Storage**

Data provided to Focal Point is stored using either cloud based systems such as our CRM, systems which are password protected and backed up on secure servers in the UK, or on the secure servers of a third party we have entered into a contract with, to provide services to us (details are contained in our Information asset log as part of our business continuity plan).

Consultants must ensure records containing personal data are stored on the appropriate, centralised Focal Point systems, not on personal devices.

### **Data Sharing and Transfer**

Personal data may be shared with third parties for the purposes of administration and to deliver products or services where elements of these are provided by suppliers, sub-contractors or events organisers other than those with which you have directly contracted.

It may also be shared with government authorities and/or law enforcement officials if mandated by law or if needed for the legal protection of our legitimate interests in compliance with applicable laws.

In the event that our business or any part of it is sold or integrated with another business, your details will be disclosed to our advisers and those of any prospective purchaser and will be passed to the new owners of the business.

No transfers of data shall be made outside of the EEA without prior authorisation of Tracy Powley or another authorised data privacy agent for Focal Point Training.

## **Data Breach**

On discovery of any form of security breach an employee or consultant must notify Support Manager immediately. A data breach is defined as any loss of data, or potential for loss of data, including but not limited to:

- loss or misplacement of physical documents or files;
- verbal transfer of information to inappropriate parties;
- loss or misplacement of a data stick;
- loss of mobile device, phone or computer;
- inappropriate access to data or systems by either internal or external users (whether accidental or intentional)

In the event of a security breach Focal Point will implement its procedures for assessing the risk associated by the breach, notifying the ICO and individuals affected by the breach, as required, and reviewing/updating security measures as mitigation. See more detail in our IT security policy.

## **Record Retention**

We operate a retention policy based on our obligations. Please contact us for details outlined in our Data Register.

After these time periods the data will be destroyed (electronic data will be deleted from our systems; paper copies will be destroyed through incineration, cross shredding or use of confidential waste bags.)

## **Subject Access Requests**

Data subjects have a number of rights under data protection legislation, including:

- Right to be informed
- Right to rectification
- Right to erasure
- Right to restrict processing
- Right to data portability
- Right to object

If any consultant retains data outside of our systems relating to the data subject, this must also be disclosed at the time of the request, the disclosure must include all relevant information, including what data is stored where and how it is stored and for what purposes.

If a Consultant receives a request from a data subject to exercise any of the above rights they must pass this immediately to [dstanfield@focalpointtraining.com](mailto:dstanfield@focalpointtraining.com) who is responsible for

handling our data subject access request (DSAR) process. DSAR requests must normally be completed within one month of receipt so it is imperative there is no delay in passing on requests. We will always verify the identity of anyone making a subject access request before providing any information.

### **Communicating the Policy**

All new consultants, employees, suppliers, clients, learners and contacts will be provided with a privacy notice at the point of collecting personal data. This will identify the types of data collected, the legal basis for processing as well as other key elements such as storage locations, data sharing and data storage.

We ensure that all learners and specifically those enrolling on an ILM (City and Guilds) programme with us have access to a copy of our Privacy Notice for Clients (usually as part of their induction).

Learners taking part in a coaching programme will also receive a copy of our coaching agreement outlining confidentiality parameters.

We also ensure that all our Consultants and support team have a copy of this Data Protection Policy when they first join our team and annually thereafter. We particularly highlight to our Consultants involved in delivery of ILM qualifications and programmes, their responsibilities in holding and processing personal data on learners (this is also outlined in our IT Security Policy, internal quality assurance policy and individual contracts issued to Consultants). All Consultants will attest annually to their compliance with our data protection and IT Security Policy.

### **Reviewing the Policy**

This policy will be monitored and reviewed annually.