Data Protection Policy

September 2020
Version 1

Further Training Limited TA
Further EPAO
European Business Park, Taylors Lane, Oldbury, West Midlands, B69 2BN
0845 600 6690
assessments@furtherepao.co.uk

Introduction

This policy is aimed at Further EPAO staff and customers and outlines our commitment and procedures for the handling of data. All staff must read, understand, and comply with this policy when data processing on our behalf.

The policy will be reviewed annually unless the need arises for it to be completed sooner.

Further EPAO is committed to preserving the privacy of its staff and customers and takes the necessary steps to protect any personal and sensitive information that we have collected by adhering to the General Data Protection Regulation (GDPR).

Types of information we collect:
Further EPAO collects and processes personal data from its staff, customers, employers and apprentices which are stored electronically. The personal data we collect is information that can directly or indirectly identify a person such as a person's name, date of birth, national insurance number, address, contact details etc. We also collect some special categories data in relation to ethnicity and health.

All information we collect, and process is in accordance with the following principles;

- It is processed lawfully, fairly and in a transparent manner in relation to individuals
- It is collected for specified, explicit and legitimate purposes
- It is adequate, relevant and limited to what is necessary in relation to the purposes for which it is being processed
- It is accurate and, where necessary, kept up to date
- It is kept in a form which permits identification of data subjects for no longer than necessary for the purposed for which the data is processed
- It is processed in a manner that ensures the appropriate security of the personal data
- It is not transferred to a country outside of the European Economic Area, unless that country has equivalent levels of protection for personal data as defined by the ICO

Further EPAO will only process special categories of data where the following conditions apply:

- The processing relates to personal data which has already been made public by the individual
- The processing is necessary for the establishment, exercise, or defence of legal claims
- The processing is specifically authorised or required by law
- The processing is necessary to protect the vital interests of the individual or of another person where the individual is physically or legally incapable of giving consent

GDPR allows processing for specific purposes, the most relevant to Further EPAO are set our below:

- The individual has given their consent
- The processing is necessary for the performance of a contract relating to the individual
- To meet our legal compliance obligations
- To pursue our legitimate interests for purposes where they are not overridden because the processing prejudices the interests or fundamental rights and freedoms of data subjects.

Individuals can withdraw their consent to processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if it is intended that data is processed for a different purpose which was not disclosed when the individual first consented.

Further EPAO will only collect and process personal data required for the job or purpose and we will not collect excessive data.

Further EPAO shares specific information about staff, customers, and apprentices with the following organisations:

Staff

- Payroll
- The External Quality Assurance Body

Customers and apprentices

- The Education and Skills Funding Agency
- The External Quality Assurance Body

Further EPAO do not share data to any third parties other than those specified above. All third parties listed have a need to know the information for the purposes of providing contracted services.

Protecting personal data

Any personal data that is collected is either stored electronically on the restricted company server or secure portal used for delivering our services or kept in a locked storage cupboard which is only accessed by senior managers.

All staff, customers, employers and apprentices have the right of access to their data and are entitled to:

- Withdraw their consent at any time
- Receive certain information about processing activities
- Request access to their personal data that we hold
- Prevent the use of their personal data for direct marketing purposes
- Ask us to erase personal data if it is no longer necessary in relation to the purposes for which it was collected or processed or to rectify inaccurate data or to complete incomplete data
- Restrict processing in specific circumstances
- Challenge processing which has been justified on the basis of our legitimate interests or in the public interest
- Prevent processing that is likely to cause damage or distress to the individual or anyone else
- Be notified of a personal data breach which is likely to result in a high risk to their rights and freedoms
- Make a complaint to the supervisory authority and in limited circumstances, receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format

Further EPAO takes reasonable steps to delete personal data when it is no longer needed. We are bound by the Education and Skills Funding Agency (ESFA) and the Data Protection Act to retain personal data for six years for audit purposes and to be able to respond to any complaints or appeals. When ensuring the information we hold is accurate, we will correct or delete the inaccurate or out of date data without delay.

Data breaches
Suspected data breaches must be reported to the Director of Business Services at jemma.sutton@furtherepao.co.uk without delay where the claims will be investigated in full. In proven incidents of a data breach the Director of Business Services will record any lessons learnt from the investigation and pass these onto relevant internal colleagues to help Further EPAO prevent the same instances from reoccurring.