Bespoke Professional Development and Training Limited

Data Protection and Privacy Policy

Updated: June 2022
Next renew due: June 2023

Version Number	Last Amended	Amended By-
v1	July 2019	Tracey Carter
v2	July 2020	Tracey Carter
v3	June 2021	Tracey Carter
V4	June 2022	Bev Harland

Background

BePro needs to keep certain information on its employees, volunteers and service users to carry out its day-to-day operations, to meet its objectives and to comply with legal obligations.

The organisation is committed to ensuring any personal data will be dealt with in line with the Data Protection Act 2018 and General Data Protection Regulations 2018 (GDPR). To comply with the law, personal information will be processed lawfully, transparently, and for a specific purpose.

The aim of this policy is to ensure that everyone handling personal data is fully aware of the requirements and acts in accordance with data protection procedures. This document also highlights key data protection procedures within the organisation.

This policy covers employees and learners.

Definitions

In line with the Data Protection Act 2018 principles, BePro will ensure that personal data will:

- Be obtained fairly and lawfully and shall not be processed unless certain conditions are met
- Be obtained for a specific and lawful purpose
- Be adequate, relevant but not excessive
- Be accurate and kept up to date
- Not be held longer than necessary
- Be processed in accordance with the rights of data subjects
- Be subject to appropriate security measures
- Be subject to appropriate security measure

The definition of ‘Processing’ is obtaining, using, holding, amending, disclosing, destroying and deleting personal data. This includes some paper based personal data as well as that is kept on Microsoft SharePoint in an area that only BePro can access.

We will follow the data protection principles set out under the GDPR, including the following rights for individuals:

- The right to be informed
- The right of access
- The right to rectification
- The right to reassure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling

Type of information processed

BePro processes the following personal information: Employees: name, address, NI number, contact number, email address, DOB, bank details, next of kin, CV, references, appraisal notes.

Learners: name, address, contact number, email address, DOB, previous highest qualifications, any special needs, employment status, next of kin, employer name and invoice address (only if employer is paying).

Apprentices: name, address, contact number, email address, plus all information required by the Education & Skills Funding Agency (ESFA), including DOB, gender, NI number, nationality, home country, residency status and details, ethnicity, learning disabilities, employment and employer details, prior attainment, initial assessment details, course details and programme of learning, passport number and driving license number.

Personal information is kept in the following forms: electronically on Microsoft SharePoint, and paper based where a paper enrolment form is submitted. Paper based information is kept locked in filing cabinets when not in use.

Groups of people within the organisation who will process personal information are:

- Directors
- Employees
- Tutors and assessors

Responsibilities

Overall responsibility for personal data rests with the Directors. These are Val Swales, Managing Director, and Georgina Selmi, CEO.

All employees, trustees and volunteers who process personal information must ensure they not only understand but also act in line with this policy and the data protection and GDPR principles. Breach of this policy will result in disciplinary action.

Policy Implementation

To meet our responsibilities, employees, trustees and volunteers will:

- Ensure any personal data is collected in a transparent, fair and lawful way
- Explain why it is needed at the start
- Ensure that only the minimum amount of information needed is collected and used

- Ensure the information used is up to date and accurate
- Review the length of time information is held
- Ensure it is kept safely
- Ensure the rights people have in relation to their personal data can be exercised

We will ensure that:

- Everyone managing and handling personal information is trained to do so
- Anyone wanting to make enquiries about handling personal information, whether a member of staff or learner, knows what to do
- Any disclosure of personal data will be in line with our procedures
- Queries about handling personal information will be dealt with swiftly and politely.

Training

Training and awareness raising about the Data Protection Act and GDPR principles, and how these are followed in this organisation will take the following forms:

On induction: employees must read and understand this Data Protection Policy. Employees will receive training on how data protection and GDPR legislation affects the way we handle and process data.

General training/awareness raising covers:

- Collecting personal data in a transparent and lawful way
- Not sharing information unless necessary to the needs of the business and in line with the Data Protection Act and GDPR legislation.
- Only using information for the reason it was collected.
- Raising any concerns regarding data protection.
- The rights individuals have to access the information held on them and/or have their data removed.
- Disposing of personal data that is no longer relevant.
- Secure use of files and processing of information.
- Keeping passwords private and files secure.
- Keeping any keys safe.
- Keeping effective records on the data we hold.

Gathering and checking information

Before personal information is collected, we will consider:

- What data is needed to provide our services
- Who it will be shared with and for what purposes
- How long we will need to keep information

We will inform people whose information is gathered about the following:

- The reason we are collecting the information
- What the information will be used for
- Which, if any, third parties will have access to the information
- Their right of access and right to have their data deleted.

We will take the following measures to ensure that personal information kept is accurate and secure:

- Checking information gathered. We will ask if there have been any change in personal details annually, where necessary.
- Strictly enforcing the BePro Information Security Policy.

Personal sensitive information will not be used apart from the exact purpose for which permission was given.

Live chat function

We use a live chat service on our website provided by a third party called Chat Heroes. Their privacy policy is available here: http://chatheroes.com/privacy-policy/

When you use our live chat service, we automatically collect the following information: IP address, browser type and operating system.

We will also collect your name, phone number, email address and any other information which you provide to us in order to follow up on an enquiry. If your enquiry is dependent on location, we may also need to confirm a postcode.

Transfer and storage of your information:

The information collected by our live chat service is processed by Chat Heroes and their third party chat service provider, SnapEngage, the privacy policy of which is available here: https://snapengage.com/privacy-policy/. SnapEngage stores your information for 60 days.

A transcript of your live chat is forwarded to us by SnapEngage via email and stored on our email

provider's servers. Our email provider is Microsoft Outlook and their privacy policy is available here https://privacy.microsoft.com/engb/privacystatement.

Live Chat Cookies:

Our live chat service uses functional cookies to allow it to function properly.

Legal basis for processing:

Our legitimate interests (Article 6(1)(f) of the General Data Protection Regulation).

Legitimate interests:

We have a legitimate interest in collecting your IP address, browser information and device to better understand our customers as they access our website and live chat service. We have a legitimate interest in collecting your name, email address, phone number and any additional information you provide in order to be able to respond to your enquiry and messages you submit via our live chat service. We ask for your phone number and email address in case we are unable to reach you on one of those means and to ensure that we are able to respond to your enquiry as quickly and effectively as possible. We ask for your name so that we know who we will be contacting, to allow us to ensure we are contacting the correct person and for legal and evidential purposes so that we can identify what we have said to whom and when.

Legal basis for processing:

Necessary to perform a contract or to take steps at your request to enter into a contract with you (Article 6(1)(b) of the General Data Protection Regulation).

Reason why necessary to perform a contract:

Where your message or enquiry relates to our goods and services, we will collect your information in order to enter into a contract with you or take steps to enter into a contract with you. This includes the collection of your name, email address and phone number so we know who we are contracting with and so that we can provide you with the information you need in order to be able to enter into a contract with you.

How long we retain your information live chat transcripts:

We store the information from our live chat service for a maximum period of seven (7) years in order to defend against legal claims. This period is the maximum period in which a claim form can be issued and served in respect of contract and tort claims under the Limitation Act 1980 under English law.

Transfers of your information outside the European Economic Area

Live chat Information you submit to us by email is transferred outside the EEA and stored on SnapEngage's servers in the United States of America.

Country of storage:

United States of America. This country is not subject to an adequacy decision by the European Commission.

Safeguard(s) used:

Our SnapEngage has self-certified its compliance with the EU-U.S. Privacy Shield which is available https://www.privacyshield.gov/. The EU-U.S. Privacy Shield is an approved certification mechanism under Article 42 of the General Data Protection Regulation, which is permitted under Article 46(2)(f) of the General Data Protection Regulation. You can access the European Commission decision on the adequacy of the EU-U.S. Privacy Shield https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/eu-us-privacy-shield_en

Data Security

BePro will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure. The following measures will be taken:

- Offices will be kept locked when not in use.
- Computers will be password protected, including office computers and any laptops used to conduct BePro business.
- Filing cabinets containing data will be kept locked when not in use.
- Personal data will not be allowed to be taken off site, except where necessary to provide our services (for example to classes).
- USB sticks must not be used; BePro provides secure cloud storage for all data.

Any unauthorised disclosure of personal data to a third party by an employee may result in disciplinary proceedings.

Subject access requests

Anyone whose personal information we process has the right to know:

- What information we hold and process on them
- How to gain access to this information
- How to keep it up to date
- What we are doing to comply with legislation.

They also have the right to prevent processing of their personal data in some circumstances and the right to correct, rectify, block or erase information regarded as wrong, and to request BePro deletes all the data held on them.

Individuals have the right to access the personal data held on them. Any person wishing to exercise this right should apply in writing to Georgina Selmi, CEO, Bespoke Professional Development and Training Ltd, Springboard Centre, Stokesley Business Park, 24 Ellerbeck Way, Middlesbrough, TS9 5JZ.

The following information will be required before access is granted:

- Full name and contact details of the person making the request
- Their relationship with the organisation

We may also require proof of identity before access is granted. The following forms of ID will be accepted:

- Passport
- Birth certificate
- Driving License

Queries about handling personal information will be dealt with swiftly and politely.

We will aim to comply with requests for access to personal information as soon as possible but will ensure it is provided within the 40 days required by the Act from receiving the written request.

Retention

All records of learners including training records and personal details will be kept for 7 years as required by the ESFA. One the learner has completed/withdrawn the paper version will be destroyed and the electronic version retained for this period.

Review

This policy will be reviewed at intervals of 1 year to ensure it remains up to date and compliant with the law.

The policy was last updated June 2022 and is due for review June 2023
The policy may also be reviewed if legislation changes or if monitoring information suggests that policy or practices should be altered.

GSelmi

Georgina Selmi
CEO