Data Protection Policy

Best Practice Training & Development keeps information about staff, learners and other parties to allow it to operate as a successful organisation and meet its legal obligations.

To comply with the Data Protection Act 2018 ("the Act) and the EU General Data Protection Regulation ("GDPR"), information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To do this, we comply with the following Data Protection Principles.

Data Protection Principles

Personal data must be processed in accordance with six 'Data Protection Principles'. It must:

- Be processed fairly, lawfully and transparently.
- Be collected and processed only for specified, explicit and legitimate purposes
- Be adequate, relevant and limited to what is necessary for the purposes for which it is processed.
- Be accurate and kept up to date. Any inaccurate data must be deleted or rectified without delay.
- Not be kept for longer than is necessary.
- Be processed securely.

Personal Data and Processing

Personal data is information relating to a living person who can be identified from the information, whether stored electronically or in paper-based filing systems or any other medium.

Processing, for the purpose of the Act, includes collection, accessing, altering, and adding to, using, changing, disclosing or merging data.

Requirement to Comply

Staff, learners or other parties who process personal data collected in the name of the Company must ensure that they follow the above principles.

Compliance with the Act is the responsibility of all staff and learners who access and process the data we hold. A breach of this Policy may lead to disciplinary action and/or access to Company facilities being withdrawn or even criminal prosecution.

Questions about the interpretation or operation of this policy should be raised to the Managing Director.

Staff, learners or other parties who believe that the Policy has not been followed in respect of their own personal data should raise the matter with the Managing Director. If the matter is not resolved it should be raised as a formal complaint or grievance, in accordance with Company procedures.

Responsibilities of Management and Staff

- Checking the information that they provide to the Company in connection with their employment is accurate and up to date.
- Informing the Company of changes to information they have provided.
- Checking information that the Company sends to them, detailing data stored and processed about them.
- Informing the Company of errors or changes to information stored.

Managers have a responsibility to ensure that their staff are aware of, and comply with the Data Protection Principles.

Data Subject Consent

In many cases, the Company can only process personal data with the consent of the individual concerned. In some cases, if the data is sensitive, express consent must be obtained. Agreement to the Company processing specified classes of personal data is a condition of acceptance of a learner onto a course and a condition of employment for staff. This includes information about previous criminal convictions.

The Company also asks for certain information about the health of staff and learners, which it will only use in connection with the health and safety of the individual and others, but needs consent to process.

Processing Sensitive Information

It is sometimes necessary to process sensitive information, such as about a person's health, criminal convictions, race, gender and family details.

This may be to ensure the Company is a safe place for everyone, or to operate other Company procedures, such as for sick pay or equal opportunities. Because this information is sensitive, and it is recognised that processing may cause concern, staff and learners are asked to give express consent for the Company to do this.
Offers of employment or course places may be withdrawn if consent is withheld without good reason.

Learner and Tutor Obligations

Learners must ensure that their personal data provided to the Company is accurate and up to date. They should notify changes of personal details to the company.

Learners who use Company computer facilities may process personal data. If they do so they must notify their tutor, who must notify the designated person. A learner who requires further clarification about this should contact the tutor or personal assessor.

Sharing Personal Information

Sometimes it is necessary to share personal data with other bodies or organisations in order to fulfil our services and legitimate interests. Where this is the case, it will be made clear in 'privacy statements' provided to our staff and/or learners.

When we share personal data, we require those companies to keep the data confidential and secure and to protect it in accordance with the law and data protection principles.

Data Security

Staff are responsible for ensuring that personal data they hold on behalf of the Company is (a) secure and (b) is not disclosed to an unauthorised third party.

Personal information should be physically secure and, if it is computerised, it should be password protected or kept only on a disk or computer that is stored securely.

Unauthorised disclosure will be a disciplinary matter, and may be considered gross misconduct.

The Company's main electronic data is stored on a dedicated file server which is backed up daily. All systems are password-protected to guard against unauthorised access.

The backup server is located on a secure network.

Paper-based data is stored securely in filing facilities in our head office. Only authorised personnel have access to paper-based data.

All equipment, systems and services are protected from unauthorised access, theft, interference or damage, through our security processes and adherence to the Data Protection Act.

All equipment used at training delivery sites is kept securely when not in use and cannot be accessed by unauthorised personnel.

Retention of Data

The Company keeps some types of information for longer than others. Information about learners that could be subject to audit must be kept for up to seven years but other information will be destroyed within three years after the learner completes their training with the Company.

The Company needs to retain information about staff, generally for two years after staff leave the Company. Some information, including information for pensions, taxation or for legal or audit reasons. will be kept for seven years.

See 'Data Retention Policy' for further details.

Subject Access Requests

Staff, learners and persons ("Data subjects") have the right to access their personal data that is stored by the Company by making a 'subject access request' ("SAR"). Anybody wishing to access such data must make their request in writing to the Managing Director.

The Company aims to comply with requests for access to personal information within 30 days of the date of receipt of the request by the designated person. If this timescale cannot be met, the reason for delay will be explained in writing to the person making the request.

Data Breaches

We have robust measures in place to minimise and prevent data breaches from taking place. Should a breach of personal data occur, we will keep records and evidence of the breach. If the breach is likely to result in a risk to the rights and freedoms of individuals then we will notify the Information Commissioner's Office within 72 hours.

Information Commissioners Office
Best Practice Training & Development Ltd is registered with the Information Commissioner's Office under registration reference:

Z5866412

Registration Start Date – 26th July 2011
Registration Expiry Date – 25th July 2019

Signed on behalf of Best Practice Training & Development Ltd

D S Allenstein
Managing Director

Date of Policy - 25.08.2018
Review date - 25.08.2019