SBC Training – General Data Protection Regulation

SBC Training is fully committed to compliance with the requirements of the General Data Protection Regulation (GDPR) which came into force on the 25 May 2018. SBC Training will therefore follow procedures specified in the Regulation to ensure that all employees, learners, businesses, with whom training and/or assessment is contracted or sub-contracted, consultants and internal assessors and their learners, who have access to any personal data held by or on behalf of SBC Training, are fully aware and abide by their duties and responsibilities under the Regulation.

Statement of Policy

In order to operate efficiently, SBC Training has to collect and use information about people with whom it works. This may include members of the public/private citizens, community and charitable or aid organisations, businesses in which assessment and training takes place, local government agencies and projects. In addition, SBC Training is required to gather information which is used by government agencies such as the Education and Skills Funding Agency (ESFA). This personal information must be properly handled and dealt with, however it is collected and used, and whether it is recorded on paper, held on computerised systems or held by any other means, and there are safeguards within the Regulation to ensure this.

SBC Training regards the correct handling and treatment of data as being of paramount importance to its successful operation and to maintaining confidence between SBC Training and those service users and customers with whom it carries out its business. SBC Training will ensure that it deals with personal information lawfully and correctly. To this end, SBC Training fully endorses and adheres to the privacy principles as set out in the General Data Protection Regulation 25 May 2018.

The Regulation stipulates that anyone processing personal data must comply with the six privacy principles of good practice. These Principles are legally enforceable. The principles require that personal data shall be:

1 Processed lawfully, fairly and in a transparent manner in relation to individuals.

2 Collected for a specific purpose and only collect data for as long as necessary to complete that purpose. Processing that's done for archiving purposes in the public interest or for scientific, historical or statistical purposes is given more freedom.

3 Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

4 Accurate and kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay. Individuals have the right to request that inaccurate or incomplete data be erased or rectified within 30 days.

5 Similarly organisations need to delete personal data when it is no longer necessary. Data must be kept in a form which permits identification of data subjects for no longer than necessary for the purpose for which the personal data was processed. Personal data may be stored for longer periods insofar as it will

be processed solely for archiving purposes in the public interest and is subject to implementation of the measures required by the GDPR in order to safeguard the rights and freedoms of individuals.

6 Processed in a manner that ensures appropriate security of the personal data including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The Regulation provides conditions for the processing of any personal data. It also makes a distinction between personal data and "sensitive" personal data.

Personal data is defined as data relating to a living individual who can be identified from:

- That data
- That data and other information which is in the possession of or is likely to come into the possession of the data controller and includes an expression of opinion about the individual and any indication of the intentions of the data controller, or any other person in respect of the individual.

Sensitive personal data is defined as personal data consisting of information as to:

- Racial or ethnic origin
- Political opinion
- Religious or other beliefs
- Trade union membership
- Physical or mental health condition
- Sexual orientation

Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing.

Handling of personal/sensitive information

SBC Training will, through appropriate management and the use of strict criteria and controls:

- Observe fully, conditions regarding the fair collection and use of personal information.
- Meet its legal obligations to specify the purpose for which information is used.
- Collect and process appropriate information and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements.
- Ensure the quality of information used.
- Apply strict checks to determine the length of time information is held.
- Take appropriate technical and organisational security measures to safeguard personal information.
- Ensure that personal information is not transferred abroad without suitable safeguards.
- Ensure that the rights of people about whom the information is held can be fully exercised under the Regulation.

These include:

- The right to be informed that processing is being undertaken.
- The right of access to one's personal information within the statutory 40 days.
- The right to prevent processing in certain circumstances.
- The right to correct, rectify, block or erase information.

In addition, SBC Training will ensure that:

- There is someone with specific responsibility for data protection in the organisation.
- Everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice.
- Everyone managing and handling personal information is appropriately trained to do so.
- Everyone managing and handling personal information is appropriately supervised.
- Anyone wanting to make enquiries about handling personal information, whether a member of staff or a member of the public, knows what to do.
- Queries about handling personal information are promptly and courteously dealt with.
- Methods of handling personal information are regularly assessed and evaluated.
- Performance with handling personal information is regularly assessed and evaluated.
- Data sharing is carried out under a written agreement, setting out the scope and limits of the sharing.

All SBC Training's employees including associates, contracted and sub-contracted are to be made fully aware of this policy and of their duties and responsibilities under the Regulation.

All managers and professionals working across all disciplines and functional areas will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure and in particular will ensure that:

- Paper files and other records or documents containing personal/sensitive data are kept in a secure environment.
- Personal data held on computer and computerised systems is protected by the use of secure passwords, which where possible have periodic forced changes.
- Individual passwords should be such that they are not compromised.

All contractors and sub-contractors, consultants and associates of SBC Training must:

- Ensure that they and all of their staff who have access to personal data held or processed on behalf of SBC Training, are aware of this policy and are fully trained in and are aware of their duties and responsibilities under the Regulation. Any breach of any provision of the Regulation will be deemed as being a breach of any contract made between SBC Training and that individual, contractor, sub-contractor, partner, company or firm.
- Allow General Data Protection Audits by SBC Training if requested.

Implementation

SBC Training has appointed an Information Officer who will have responsibility for:

- For the development of best-practice guidelines.
- For carrying out compliance checks throughout the organisation, within the General Data Protection Regulation.
- Investigating any breach of confidentiality and carrying out a risk assessment as to the likelihood and severity of the risk to people's rights and freedoms following the breach. If there is a risk, then notifying the Information Commissioner's Office.

Notification to the Information Commissioner

The Information Commissioner maintains a public register of data protection. The General Data Protection Regulation 25 May 2018 requires every data controller who is processing personal data to notify and renew their notification annually. Failure to do so is a criminal offence.

To this end the designated officers will be responsible for reviewing and updating the Information Officer of the range of personal data collected.

Any changes must be notified to the Information Commissioner within 28 days. Any changes to data collected or held will be notified to the Information Officer immediately.

Signed: Rhian Chadwick Date: 8 April 2020

Quality manager