BALTIC APPRENTICESHIPS

DATA PROTECTION POLICY

POL 028

V8 | 2021/2022

BE THE FUTURE

DATA PROTECTION POLICY

Introduction

This Policy together with related procedures and documents detailed below support an information governance Framework compliant with the Data Protection Act 2018, the UK's implementation of the General Data Protection Regulation (GDPR).

Related Policies & Procedures:

- Privacy Policy and Notices
- Subject Access Request Procedure
- Data Breach Procedure
- Data Retention and Deletion Procedure
- Transmission, Storage & Handling Guidelines
- The Rules – Using Personal Equipment for Business Use
- Data Protection Audit Procedure
- Staff Communication Policy
- IT Acceptable Use Policy
- Social Media Policy
- Information Security & Risk Management Policy

Baltic Training needs to hold and to process personal data about its employers, learners, employees, candidates, contractors and other individuals in order to carry out its business and organisational functions.

GDPR defines personal data as any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Examples of personal data

- Date of Birth
- Online IDs
- IP address

Examples of Sensitive Personal Data (Special Categories)

- Ethnic origin
- Health data
- Biometric data

Purpose

Compliance with legislation will be achieved through the implementation of controls and responsibilities including measures to ensure that:

1. personal data is processed lawfully, fairly and transparently. This includes the provision of appropriate information to individuals upon collection of their data by Baltic Training in the form of privacy notices. Baltic Training must also have a legal basis to process personal data.

2. personal data is processed only for the purposes for which it was collected;

3. personal data is adequate, relevant and not excessive for the purposes for which it was collected;

4. personal data is accurate and where necessary kept up to date;

5. personal data is not kept for longer than necessary;

6. personal data is processed in accordance with integrity and confidentiality principles; this includes physical and organisational measures to ensure that personal data, both manual and digital, are subject to an appropriate level of security when stored, used and communicated by Baltic Training, in order to protect against unlawful or malicious processing and accidental loss, destruction or damage. It also includes measures to ensure that personal data transferred to or otherwise shared with third parties have appropriate contractual provisions applied;

7. personal data is processed in accordance with the rights of individuals, where applicable. These rights are:

- the right to be informed;
- the right of access to the information held about them by Baltic Training (through a subject access request);
- the right to rectification;
- the right to erase;
- the right to restrict processing;
- the right to data portability;
- the right to object; and
- rights in relation to automated decision making and profiling;

8. The design and implementation of Baltic Training systems and processes must make provision for the security and privacy of personal data;

9. Personal data will not be transferred outside of the European Economic Area (EEA) without the appropriate safeguards in place

10. Additional conditions and safeguards must be applied to ensure that more sensitive personal data (defined as Special Category data in the legislation), is handled appropriately by Baltic Training. Special category personal data is personal data relating to an individual's:

- race or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- genetic data;
- biometric data (where used for identification purposes);
- health; or
- sex life or sexual orientation.

In addition, similar extra conditions and safeguards also apply to the processing of the personal data relating to criminal convictions and offences.

Scope

This Policy applies to:

- all personal data held and processed by Baltic Training. This includes expressions of opinion about the individual and of the intentions of Baltic Training in respect of that individual. It includes data held in any system or format, whether electronic or paper;
- all employees, management, contractors, associates, business partners and other parties who have access to company data.
- all locations from which personal data is accessed including away from Baltic Offices

Roles and Responsibilities

Baltic Training Managing Director is the Accountable Officer who has ultimate responsibility for compliance with the Data Protection Act.

The Director of Support Services, Sales Director and Head of Operations are responsible for ensuring that personal data within their areas is processed in line with this Policy and established procedures.

Baltic Training Services permanent and temporary employees and associates are responsible for incorporating this policy and its associated procedures into their own working practices to ensure compliance.

All staff and other approved users of Baltic Training systems must:

- complete data protection training as part of their mandatory induction learning
- complete refresher data protection training as a minimum annually or when an audit or data breach may trigger the requirement for further training.
- seek advice and guidance from the Director of Support Services if clarification is required in any areas relating to data protection governance framework;
- comply with related procedures including Data transmission, storage and handling guidelines, Use of personal equipment for business use and data retention and deletion procedure;
- immediately report to the Director of Support Services any actual or suspected misuse, unauthorised disclosure or exposure of personal data, "near misses" or working practices which jeopardise the security of personal data held by Baltic Training.

The Director of Support Services is responsible for overseeing Baltic Training's compliance with the data protection legislation.

Staff must note that any breach of this Policy may be treated as misconduct under the disciplinary procedure and could lead to disciplinary action or sanctions. Serious breaches of this Policy may constitute gross misconduct and lead to summary dismissal or termination of contract.

Monitoring

This policy will be monitored by Data Protection audit procedure.

Policy review.

This policy will be reviewed annually or when changes are required.

- PROMOTING EQUALITY AND DIVERSITY -

BE THE FUTURE

POLICY NUMBER: **POL028**
VERSION NUMBER: **V8**
DATE ISSUED: **01.09.2021**
REVIEW DATE: **31.07.2022**
AUTHOR: **DEBBIE PARK**