BALTIC
APPRENTICESHIPS

DATA PROTECTION POLICY

2023

BE THE EXPERT
BE THE CUSTOMER
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
- Data Protection Audit Procedure
- IT Acceptable Use Policy
- Trusted Contact Policy
- Cyber Essentials Policy & Procedures

Baltic Training Ltd (trading as Baltic Apprenticeships) needs to hold and to process personal data, about its employers, learners, employees, candidates, contractors and other individuals (data subjects) in order to carry out its business and organisational functions, this may include sensitive personal data.

Definitions

Data breach – means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal information;

Data subject – means the individual to whom the personal information relates;

Personal information – (sometimes known as personal data) means information relating to an individual who can be identified (directly or indirectly) from that information;

Processing information – means obtaining, recording, organizing, storing, amending, retrieving, disclosing and / or destroying information, or using or doing anything with it;

Sensitive information – (sometimes known as ' special categories of personal data' or 'sensitive personal data') means personal information about an individual's race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-

membership), genetic information, biometric information (where used to identify an individual) and information concerning an individual's health, sex life or sexual orientation

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

The principles of Data Protection

Our use of information is governed by the principles of the General Data Protection Regulation. Under the regulations, personal data shall be:

1. processed lawfully, fairly and in a transparent manner;

2. collected for specified, explicit and legitimate purposes;

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

4. accurate and where necessary kept up to date;

5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;

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;

Individual Rights

Personal data shall be processed in accordance with the rights of individuals, where applicable. These rights are:

- the right to be informed about how and why and on what basis information is processed (Privacy Notice);
- the right of access to the information held about by Baltic Training (Subject Access Request)
- the right to rectification, to have data corrected if it is inaccurate or incomplete;
- the right to erase data if it is no longer necessary for the purpose for which it was originally collected (the right to be forgotten);
- the right to restrict processing where the accuracy of the information is contested, or the processing is unlawful);
- the right to data portability;
- the right to object; and
- rights in relation to automated decision making and profiling.

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 and Customer Success Director are responsible for ensuring that personal data within their areas is processed in line with this Policy and established procedures.

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

Staff Training

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.

Transfer of data

Personal data will not be transferred outside of the UK or European Economic Area (EEA). EEA comprises the countries in the European Union and Iceland, Liechtenstein and Norway.

Information Security

Baltic Training will use appropriate technical and organisational measures to keep personal information secure, and in particular to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.

Data Breaches

Baltic Training takes every care in protecting the personal information it holds and avoiding risks which could lead to a compromise of security and a potential data protect breach. Compromised security and/or data breaches can result in harm to the individual(s) involved, reputational damage to the Company, detrimental effect on service provision, legislative non-compliance, and/or financial costs. Staff should refer to Data Breach procedure to report a data breach.

Consequences of failing to comply

Any breach of this Policy by staff 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.

Documentation and Records

A record of processing activity (a data inventory) will be maintained and will include:

- the purpose of the data collection process;
- details of data subjects;
- types of personal data and special categories data collected

- the source of the data
- geographical storage location
- the legal justification for processing
- retention – how long

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 -