Data Protection Policy

Policy information	
Organisation	**Care First Training Ltd**
Scope of policy	Care First Training Ltd is required to process relevant personal data regarding members of staff, volunteers, applicants, Employers, learners and their next of kin/parents and customers as part of its operation and shall take all reasonable steps to do so in accordance with this Policy.
Policy operational date	18/05/2018.
Policy prepared by	Dáre Akosile (DPA) Data Protection Officer.
Policy review date	To be reviewed every 3 years.

Introduction

The Organisation collects and processes personal information, or personal data, relating to its employees, workers and contractors to manage the working relationship. This personal information may be held by the Organisation on paper or in electronic format.

The Organisation is committed to being transparent about how it handles your personal information, to protecting the privacy and security of your personal information and to meeting its data protection obligations under the General Data Protection Regulation ("GDPR") and the Data Protection Act 2018. The purpose of this privacy notice is to make you aware of how and why we will collect and use your personal information both during and after your working relationship with the Company. We are required under the GDPR to notify you of the information contained in this privacy notice.

This privacy notice applies to all current and former employees, workers and contractors. It is non-contractual and does not form part of any employment contract, casual worker agreement, consultancy agreement or any other contract for services.

Purpose of policy

Care First Training Ltd shall so far as is reasonably practicable comply with the Data Protection Principles (the Principles) contained in the Data Protection Act to ensure all data is: -

- Fairly and lawfully processed
- Processed for a lawful purpose
- Adequate, relevant and not excessive
- Accurate and up to date
- Not kept for longer than necessary
- Processed in accordance with the data subject's rights
- Secure
- Not transferred to other countries without adequate protection

Types of data

"Personal data" is any information that relates to a living individual who can be identified from that information. Processing is any use that is made of data, including collecting, storing, amending, disclosing or destroying it.

"Special categories of personal data" means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and biometric data.

"Criminal records data" means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

Data protection principles

The organisation processes HR-related personal data in accordance with the following data protection principles:

- The organisation processes personal data lawfully, fairly and in a transparent manner.
- The organisation collects personal data only for specified, explicit and legitimate purposes.
- The organisation processes personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing.
- The organisation keeps accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.
- The organisation keeps personal data only for the period necessary for processing.
- The organisation adopts appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.

The organisation tells individuals the reasons for processing their personal data, how it uses such data and the legal basis for processing in its privacy notices. It will not process personal data of individuals for other reasons. Where the organisation relies on its legitimate interests as the basis for processing data, it will carry out an assessment to ensure that those interests are not overridden by the rights and freedoms of individuals.

Where the organisation processes special categories of personal data or criminal records data to perform obligations or to exercise rights in employment law, this is done in accordance with a policy on special categories of data and criminal records data.

The organisation will update HR-related personal data promptly if an individual advises that his/her information has changed or is inaccurate.

Personal data gathered during the [employment, worker, contractor or volunteer relationship, or apprenticeship or internship] is held in the individual's personnel file (in hard copy or electronic format, or both). The periods for which the organisation holds HR-related personal data are contained in its privacy notices to individuals.

The organisation keeps a record of its processing activities in respect of HR-related personal data in accordance with the requirements of the General Data Protection Regulation (GDPR).

Security

Security measures
Care First Training Ltd will take appropriate technical and organisational steps to ensure the security of personal data.
All staff will be made aware of this policy and their duties under the Act.

All staff are required to respect the personal data and privacy of others and must ensure that appropriate protection and security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to all personal data. An appropriate level of data security will be deployed for the type of data and the data processing being performed. In most cases, personal data will be stored in appropriate systems and be Data Protection Policy Lent 2017 encrypted when transported offsite. Other personal data may be for publication or limited publication within the organisation, therefore having a lower requirement for data security.
Attention is also drawn to the existence of the Information and Computing Technology (ICT) Policy, which provides more specific information on digital data protection within the ICT policy.

Responsibilities

Company Directors
Executive Directors:
Dáre Akosile
Kaminee Hirani
Data Protection Officer
The organisation has appointed Dáre Akosile as its data protection officer. His role is to inform and advise the organisation on its data protection obligations. He can be contacted at dare@carefirsttraining.co.uk . Questions about this policy, or requests for further information, should be directed to the data protection officer.

(DPC) will endeavour to ensure that all personal data is processed in compliance with this Policy and the Principles of the Data Protection Act 1998. The Freedom of Information Act 2000 and the Protection of Freedoms Act 2012 are also relevant to parts of this policy. Care First Training Ltd recognises The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) adopted 27 April 2016.
Employees & Volunteers
All staff and volunteers are required to read, understand and accept any policies and procedures that relate to the personal data they may handle in the course of their work. (From now on, where 'employees' is used, this includes both paid employees and volunteers.)

Right of Access

Procedure

Individuals have the right to make a subject access request. If an individual makes a subject access request, the organisation will tell him/her:

- whether or not his/her data is processed and if so why, the categories of personal data concerned and the source of the data if it is not collected from the individual;
- to whom his/her data is or may be disclosed, including to recipients located outside the European Economic Area (EEA) and the safeguards that apply to such transfers;
- for how long his/her personal data is stored (or how that period is decided);
- his/her rights to rectification or erasure of data, or to restrict or object to processing;
- his/her right to complain to the Information Commissioner if he/she thinks the organisation has failed to comply with his/her data protection rights; and
- whether or not the organisation carries out automated decision-making and the logic involved in any such decision-making.

The organisation will also provide the individual with a copy of the personal data undergoing processing. This will normally be in electronic form if the individual has made a request electronically, unless he/she agrees otherwise.

[If the individual wants additional copies, the organisation will charge a fee, which will be based on the administrative cost to the organisation of providing the additional copies.

To make a subject access request, the individual should send the request to [email address] or use the organisation's form for making a subject access request. In some cases, the organisation may need to ask for proof of identification before the request can be processed. The organisation will inform the individual if it needs to verify his/her identity and the documents it requires.

The organisation will normally respond to a request within a period of one month from the date it is received. In some cases, such as where the organisation processes large amounts of the individual's data, it may respond within three months of the date the request is received. The organisation will write to the individual within one month of receiving the original request to tell him/her if this is the case.

If a subject access request is manifestly unfounded or excessive, the organisation is not obliged to comply with it. Alternatively, the organisation can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request. A subject access request is likely to be manifestly unfounded or excessive where it repeats a request to which the organisation has already responded. If an individual submits a request that is unfounded or excessive, the organisation will notify him/her that this is the case and whether it will respond to it.CVs are kept for

no more than 6 months. In an event that we need to keep it for longer, we shall express permission from the candidates.

Provision for verifying identity
Where the person managing the access, procedure does not know the individual personally, before handing over any information we may request to see an acceptable identification to check their identity.

Procedure for granting access
If the request is made electronically, information will be provided in electronic format.

Where possible, Care First Training Ltd will provide remote access to a secure self-service system which would provide the individual with direct access to his or her information.

Security

Security measures
Care First Training Ltd will take appropriate technical and organisational steps to ensure the security of personal data.
All staff will be made aware of this policy and their duties under the Act.
All staff are required to respect the personal data and privacy of others and must ensure that appropriate protection and security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to all personal data.

An appropriate level of data security will be deployed for the type of data and the data processing being performed. In most cases, personal data must be stored in appropriate systems and be encrypted when transported offsite. Other personal data may be for publication or limited publication within the organisation, therefore having a lower requirement for data security.
Attention is also drawn to the existence of the information and Computing Technology (ICT) Policy, which provides more specific information on digital data protection within the ICT policy.