Data Protection Policy

(General Data Protection Regulations)

Reviewed by Adam Davies, Quality Manager

Approved by Lynne Whitehouse, Operations Director

Version date: 3/8/21

Review schedule: 3/8/22 or in line with operating procedure and/or legislative updates/requirements

Person/s responsible: SLT, all management and staff

Signed Adam Davies

Signed

Policy owner

Contents

Introduction

This document sets out the obligations of Netcom Training ("the Company") with regards to data protection and the rights of individuals in respect of their personal data under the Data Protection Act 2018. The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR).

This Policy sets out procedures which are to be followed when handling personal data. The procedures set out herein must be followed by the Company, its employees, contractors, agents, consultants, partners or other parties working on behalf in conjunction with the Company.

The Company shall ensure that it handles and stores all personal data correctly and lawfully for the purposes for which it is intended.

The Data Protection Principles

This Policy aims to ensure compliance with the Act. The Act sets out the principles with which any party handling personal data must comply. All personal data and information must be:

1. Processed fairly, lawfully and transparently.

2. Must be obtained only for specified and explicit purposes and shall not be processed in any manner which is incompatible with those purposes

3. Must be adequate, relevant and limited to the necessary purposes for which it may be required

4. Must be accurate and, where appropriate, kept up to date

5. Must be kept for no longer than necessary considering the purpose(s) for which it is processed

6. Handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

Rights of Data Subjects

Under the Act, data subjects have the following rights:

- To be informed how their personal data is being used.
- To access any of their personal data held by the Company within a reasonable timescale.
- To have incorrect data updated
- To prevent the processing of their personal data in certain circumstances
- To rectify, block, erase or destroy incorrect personal data
- To object to how data is processed in certain circumstances

Personal Data

Personal data is defined by the Act as data which relates to a living individual who can be identified from that data or from 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 any 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.

The Act also defines “sensitive personal data” as personal data relating to the racial or ethnic origin of the data subject; their political opinions; their religious (or similar) beliefs; trade union membership; their physical or mental health condition; their sexual life; the commission or alleged commission by them or any offence; or any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings.

The Company only holds personal data which is directly relevant to its dealings with a given subject. That data will be held and processed in accordance with the data protection principles and with this Policy. The following data may be requested, collected, held or processed by the Company when recruiting staff or learners for courses/programmes:

- Personal contact details.
- National Insurance Details.
- Information relating to ID checks e.g., passports, driving licences, birth certificates and other evidence of identification including photographs of applicants where appropriate.
- DBS checks.
- Evidence of entitlement to work in the UK (if appropriate).
- References from former employers or schools/colleges.
- Copies of insurance policies for client companies and policies and assessments in respect of Health and Safety checks.
- Details of qualifications achieved and copies of any relevant certificates.
- Bank account details for staff.
- Copies of CV’s.
- Any other information which may be required for legitimate purposes.

Processing Personal Data

Any personal data collected by the Company is used solely in order to ensure that it can facilitate efficient transactions with third parties including, but not limited to, its customers, partners, associates and affiliates and efficiently manage its employees, contractors, agents and consultants. Personal data shall also be used by the Company in meeting any and all relevant obligations imposed by law.

Personal data may be disclosed within the Company and shared in accordance with the data protection principles and this Policy. Under no circumstances will personal data be passed to any department or any individual within the Company that does not reasonably require access to that personal data with respect to the purpose(s) for which it was collected and is being processed.

The Company shall ensure that:

- All personal data collected and processed for and on behalf of the Company by any party is collected and processed fairly and lawfully.
- Data subjects are made fully aware of the reasons for the collection of personal data and are given details of the purpose for which the data will be used.
- Personal data is only collected to the extent that is necessary to fulfil the stated purpose(s).
- All personal data is accurate at the time of collection and kept accurate and up-to-date whilst it is being held and / or processed.
- No personal data is held for any longer than necessary considering the stated purpose(s).
- All personal data is held in a safe and secure manner, taking all appropriate technical and organisational measures to protect the data.
- All personal data is transferred using secure means, electronically or otherwise.

Data Protection Procedures

The Company shall ensure that all of its employees, contractors, agents, consultants, partners or other parties working on behalf of the Company comply with the following when processing personal data:

- Personal data may be transmitted over secure networks only – transmission over unsecured networks is not permitted in any circumstances.
- Where personal data is to be transferred in hardcopy form it should be passed directly to the recipient.
- All hardcopies of personal data should be stored securely in a locked box, drawer, cabinet or similar and access limited to authorised personnel only.
- All electronic copies of personal data should be stored securely using passwords and access limited as above.
- All passwords used to protect personal data should be changed regularly and should not use words or phrases which can easily be guessed or otherwise compromised.

Organisational Measures

The Company shall ensure that the following measures are taken with respect to the collection, holding and processing of personal data:

- A designated officer (“the Designated Officer”) within the Company shall be appointed with the specific responsibility of overseeing data protection and ensuring compliance with the Act.
- All employees, contractors, agents, consultants, partners or other parties working on behalf of the Company are made fully aware of both their individual responsibilities under the Act and shall be provided with a copy of this Policy.
- All employees, contractors, agents, consultants, partners or other parties working on behalf of the Company handling personal data will be appropriately trained to do so and supervised where required. There will be a

requirement for all data users to complete an online module covering the essentials of Data Protection An Introduction to GDPR | Virtual College (virtual-college.co.uk)

- Methods of collecting, holding and processing personal data shall be regularly evaluated and reviewed.
- The performance of those employees, contractors, agents, consultants, partners or other parties working on behalf of the Company handing personal data shall be regularly evaluated and reviewed.
- All employees, contractors, agents, consultants, partners or other parties working on behalf of the Company handling personal data will be bound to do so in accordance with the principles of the Act and this Policy by contract. Failure by any employee to comply with the principles of this Policy shall constitute a disciplinary offence and will be subject to the company processes set out within the Malpractice and Maladministration policy. Failure by any contractor, agent, consultant, partner or other party to comply with the principles of this Policy shall constitute a breach of contract. In all cases, failure to comply with the principles of this Policy may also constitute a criminal offence under the Act.
- All contractors, agents, consultants, partners or other parties working on behalf of the Company handling personal data must ensure that any employees who are involved in the processing of personal data observe and adhere to the same requirements as relevant employees of the Company in terms of this Policy and those of the Act.
- Where any contractor, agent, consultant, partner or other party working on behalf of the Company handling personal data fails in their obligations under this Policy, that party shall take responsibility for and indemnify the Company against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

Access by Data Subjects

Data subjects may make a subject access request ("SAR") at any time to see the information which the Company holds about them. SARs must be made in writing, accompanied by the correct administrative fee if applicable.

Upon receipt of a SAR, the following information will be provided to the data subject:

- Whether or not the Company holds any personal data on the data subject.
- A description of any personal data held on the data subject
- Details of what that personal data is used for
- Details of any third-party organisations that personal data may be shared with

Notification to the Information Commissioner's Office

As a data controller, the Company is required to notify the Information Commissioner's Office that it is processing personal data. The Company is registered in the register of data controllers.

Data controllers must renew their notification with the Information Commissioner's Office on an annual basis. Failure to notify constitutes a criminal offence.

Any changes to the register must be notified to the Information Commissioner's Office within 28 days of it taking place.

The Designated Officer shall be responsible for notifying and updating the Information Commissioner's Office.

Monitoring

The policy and procedures will be reviewed at least annually or in the light of significant changes to processes or legal requirements or policy breaches. Any such changes will be communicated at the earliest opportunity to all relevant staff, learners and other parties that may be affected.

Addendum to Data Protection policy-June 2022

Policy implementation update to meet the technical and organisational requirements of the UK GDPR. The purpose of this addendum is to provide additional clarity on the measures the company continues to take to act in compliance with the requirements of the regulation. Their effectiveness is assessed and evaluated to ensure the security of data processing to prevent breaches and information security incidents. All company systems, processes and procedures are designed to protect and secure the processing and storing of personal information.

The scope and content of the company's Information Security policy is in line with the operational requirements of the business which includes procedures for asset management, remote access, password controls, acceptable use and cyber security measures. An IT service provider provides additional support and cloud backup.

The company's Business Continuity policy incorporates measures to protect personal information and adhere to the principles of the UK GDPR from data security and access to recovery and maintenance.

Effective and compliant data protection and document retention policies are in place and these have been made directly available to all staff and stored on the shared document management system. Policies are reviewed annually or in light of any organisational changes, security incidents or legal requirements. Refresher training takes place periodically to ensure data processors are kept abreast of their responsibilities. The use of strong passwords is promoted and employees are reminded not to share them and keep them secure at all times.

The company will take all necessary precautions as part of its due diligence to comply with the requirements of the UK GDPR. Background checks are made of all employees prior to employment as part of safer recruitment practices. Suppliers and third parties will also be asked as to their level of compliance with data protection legislation.

The company will also ensure the compliant disposal of paperwork and devices. Hard-copy records will be shredded or made available for collection by assured confidential waste management services. The IT department is responsible for any IT recycling or disposal in line with WEEE Regulations 2019 to guarantee effective and complete erasure of personal data or access.

A current Cyber Essentials certificate is held as recommended by the ICO.

ICO suggestions on measures designed to further strengthen technical and organisational controls are under consideration:

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/security