Data Protection (GDPR) and Confidentiality Policy

Introduction

NextStep Training Ltd takes its responsibilities with regard to the management of the requirements of the General Data Protection Regulation (GDPR) very seriously. This policy sets out how we manage those responsibilities.

NextStep Training Ltd obtains, uses, stores and otherwise processes personal data relating to potential staff and students (applicants), current staff and students, former staff and students, current and former workers, contractors, website users and contacts, collectively referred to in this policy as data subjects. When processing personal data, NextStep Training Ltd is obliged to fulfil individuals' reasonable expectations of privacy by complying with GDPR and other relevant data protection legislation (data protection law).

This policy therefore seeks to ensure that we:

- are clear about how personal data must be processed and our expectations for all those who process personal data on its behalf;
- comply with the data protection law and with good practice;
- protect our reputation by ensuring the personal data entrusted to us is processed in accordance with data subjects' rights
- protect us as an organisation from risks of personal data breaches and other breaches of data protection law.

Data Protection registered number **Z2884210**.

Introduction

NextStep Training Ltd within its organisation needs to gather and use certain information about individuals. These can include employers, learners, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact.

Purpose

This data protection policy ensures NextStep Training Ltd complies with data protection law and follows good practice. We endeavour to protects the rights of staff, customers and partners and are open about how we store and process individuals' data and protects ourselves from the risks of a data breach

The law

The Data Protection Act 1998 and subsequently the General Data Protection Regulation May 2018; describes how organisations must collect, handle and store personal information. These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The Data Protection Act is underpinned by eight important principles. These say that personal

data must:

- Be processed fairly and lawfully
- Be obtained only for specific, lawful purposes Be adequate, relevant and not excessive
- Be accurate and kept up to date
- Not be held for any longer than necessary
- Processed in accordance with the rights of data subjects Be protected in appropriate ways

Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection

Policy scope

This policy applies to:

- The head office and all other sites of NextStep Training Ltd
- All staff members, contractors, suppliers and volunteers working on behalf of NextStep Training Ltd
- All learners and clients involved with NextStep Training Ltd.

It applies to all data that the company holds relating to identifiable individuals. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers

… plus, any other information relating to individuals

Data protection risks

This policy is to protect NextStep Training Ltd from some very real data security risks, including:

- Breaches of confidentiality. For instance, information being given out inappropriately. Failing to offer choice. For instance, all individuals should be free to choose how the company uses data relating to them.
- Reputational damage. For instance, the company could suffer if hackers successfully gained access to sensitive data.

Responsibilities

Everyone who works for or with NextStep Training Ltd has some responsibility for ensuring data is collected, stored and handled appropriately.

Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:
The board of directors is ultimately responsible for ensuring that NextStep Training Ltd meets its legal obligations.

The Data protection officer, Sharon Butcher, is responsible for:

- Keeping the board updated about data protection responsibilities, risks and issues.

Reviewing all data protection procedures and related policies, in line with an agreed schedule.

- Arranging data protection training and advice for the people covered by this policy. Handling data protection questions from staff and anyone else covered by this policy.
- Dealing with requests from individuals to see the data NextStep Training Ltd holds about them (also called 'subject access requests').
- Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.

The IT manager/ Director, Ahmed Khan, is responsible for:

- Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
- Performing regular checks and scans to ensure security hardware and software is functioning properly.
- Evaluating any third-party services, the company is considering using to store or process data. For instance, cloud computing services.

The Directors, are responsible for:

- Approving any data protection statements attached to communications such as emails and letters, learner applications.
- Addressing any data protection queries
- Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

General staff guidelines

The only people able to access data covered by this policy should be those who need it for their work.

Data should not be shared informally. When access to confidential information is required, employees can request it from their line managers.

NextStep Training Ltd will provide training to all employees to help them understand their responsibilities when handling data.

Employees should keep all data secure, by taking sensible precautions and following the guidelines below:

- Strong passwords must be used and they should never be shared.
- Personal data should not be disclosed to unauthorised people, either within the company or externally.
- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Employees should request help from their line manager or the data protection officer if they are unsure about any aspect of data protection.

Data storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the IT manager or data controller.

When data is stored on paper, it will be kept in a secure place where unauthorised people cannot see it, this includes locked filing cabinets in head office.

All staff members should make sure paper and printouts are not left where unauthorised people could see them, like on a printer.

Data printouts should be shredded and disposed of securely when no longer required.

When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

Data should be protected by strong passwords that are changed regularly and never shared between employees.

If data is stored on removable media (like a CD or DVD), these should be kept locked away securely when not being used.

Data should only be stored on designated drives and servers, and should only be uploaded to an approved cloud computing service.

Servers containing personal data should be sited in a secure location, away from general office space.

Data should be backed up frequently. Those backups should be tested regularly, in line with the company's standard backup procedures.

Data should never be saved directly to laptops or other mobile devices like tablets or smart phones.

All servers and computers containing data should be protected by approved security software and a firewall.

Data use

When working with personal data, employees should ensure the screens of their computers are always locked when left unattended.

Personal data should not be shared informally. In particular, it should never be sent by email, as this form of communication is not secure.

Data must be encrypted before being transferred electronically. The IT manager can explain how to send data to authorised external contacts.

Personal data should never be transferred outside of the European Economic Area.

Data accuracy

NextStep Training Ltd is required by law to take reasonable steps to ensure data is kept accurate and up to date.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets.

Staff should take every opportunity to ensure data is updated. For instance, by confirming learners details when they call.

Data should be updated as inaccuracies are discovered. For instance, if a learner can no longer be reached on their stored telephone number, it should be removed from the database.

It is the marketing manager's responsibility to ensure marketing databases are checked against industry suppression files every six months.

Subject access requests

All individuals who are the subject of personal data held by NextStep Training Ltd are entitled to:

- Ask what information the company holds about them and why.
- Ask how to gain access to it.
- Be informed how to keep it up to date.
- Be informed how the company is meeting its data protection obligations.

If an individual contacts the company requesting this information, this is called a subject access request.

Subject access requests from individuals should be made by email, addressed to the data controller at; info@nextsteptrainingltd.co.uk

The data controller can supply a standard request form, although individuals do not have to use this.

Individuals will be charged £10 per subject access request. The data controller will aim to provide the relevant data within 14 days.

The data controller will always verify the identity of anyone making a subject access request before handing over any information.

Disclosing data for other reasons

In certain circumstances, the Data Protection Act allows personal data to be disclosed to law

enforcement agencies without the consent of the data subject.
Under these circumstances, NextStep Training Ltd will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers where necessary.

Providing information
NextStep Training Ltd aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used How to exercise their rights
- To these ends, the company has a privacy statement, setting out how data relating to individuals is used by the company.

Management Approval

Date: 21/09/2022

Ahmed Khan: Managing Director

[This is available on request. A version of this statement is also available on the company's website.]