DATA PROTECTION (GDPR) POLICY

Policy last reviewed: February 2020
Review Date: August 2020

Introduction

Purpose

North Lancs Training Group Limited (NLTG) is committed through this policy to being transparent about how it collects and uses the personal data of its employees, students, applicants, clients, suppliers, contractors, visitors and associates to meeting its data protection obligations. This policy sets out the company's' commitment to data protection, and individual rights and obligations in relation to personal data.

NLTG has appointed Gareth Lindsay, Managing Director, as the person with responsibility for data protection compliance within the company. Questions about this policy, or requests for further information, should be emailed to dataenquiries@nltg.co.uk. The policy will also be displayed on the NLTG website under publications.

Definitions

Personal data is any information that relates to an 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

NLTG processes personal data in accordance with the following data protection principles:

- NLTG processes personal data lawfully, fairly and in a transparent manner.
- NLTG collects personal data only for specified, explicit and legitimate purposes.
- NLTG processes personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing.
- NLTG keeps accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.
- NLTG keeps personal data only for the period necessary for processing.

- NLTG adopts appropriate measures to make sure that personal data is secure and protected (in line with its Data Security Policy and Data Security Arrangements) against unauthorised or unlawful processing, and accidental loss, destruction or damage.

NLTG will inform individuals how their personal data is processed and the legal basis for doing so through privacy notices. Privacy Notices are all available on Sharepoint and where applicable.

Where NLTG processes special categories of personal data or criminal records data to perform its legal obligations, i.e. safeguarding or to exercise rights in employment law, this is done in accordance with its policies such as Safeguarding, Recruitment and Equality and Diversity for the processing of such special category data and criminal records data.

NLTG will update personal data promptly if an individual advises that his/her information has changed or is inaccurate.

NLTG keeps a record of all its processing activities in respect of personal data in accordance with the requirements of the General Data Protection Regulation (GDPR) which is updated on an annual basis. Our use of the information you supply is governed by our registration under the 2018 General Data Protection Regulations and will be securely held.

Individual rights

As a data subject, individuals have a number of rights in relation to their personal data.

Subject access requests

Individuals have the right to make a subject access request. If an individual makes a subject access request, NLTG 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, 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 NLTG has failed to comply with his / her data protection rights; and
- whether or not NLTG carries out automated decision-making and the logic involved in any such decision-making.

NLTG 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.

To make a subject access request, the individual should complete the Subject Access Request form available on Sharepoint or (request in writing for external) and email or post the request to the Managing Director via (dataenquiries@nltg.co.uk). In some cases, NLTG may need to ask for proof of identification before the request can be processed. NLTG will inform the individual if it needs to verify his / her identity and the documents it requires.

NLTG will normally respond to a request within a period of one month from the date it is received. In some cases, such as where NLTG processes large amounts of the individual's data, it may respond within three months of the date the request is received. NLTG 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, NLTG is not obliged to comply with it. Alternatively, NLTG 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 NLTG has already responded. If an individual submits a request that is unfounded or excessive, NLTG will notify him / her that this is the case and whether or not it will respond to it.

Other rights

Individuals have a number of other rights in relation to their personal data. They can require NLTG to:

- rectify inaccurate data;
- stop processing or erase data that is no longer necessary for the purposes of processing;
- stop processing or erase data if the individual's interests override NLTG's legitimate grounds for processing data (where NLTG relies on its legitimate interests as a reason for processing data);
- stop processing or erase data if processing is unlawful; and
- stop processing data for a period if data is inaccurate or if there is a dispute about whether or not the individual's interests override NLTG's legitimate grounds for processing data.

To ask NLTG to take any of these steps, the individual should send the request to dataenquiries@nltg.co.uk

Data security

NLTG takes the security of personal data seriously. NLTG has internal policies and controls in place to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties. Please refer to NLTG's Data Security Policy.

Where NLTG engages third parties to process personal data on its behalf, such parties do so on the basis of written instructions and/or are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data. As such, NLTG will request such companies to provide their GDPR Policy which will be checked and held within the relevant folder the internal network – Sharepoint (GDPR)

Impact assessments

Some of the processing that NLTG carries out may result in risks to privacy. Where processing would result in a high risk to individual's rights and freedoms, NLTG will carry out a data protection impact assessment to determine the necessity and proportionality of processing. This will include considering the purposes for which the activity is carried out, the risks for individuals and the measures that can be put in place to mitigate those risks.

Data breaches

If NLTG discovers that there has been a breach of personal data that poses a risk to the rights and freedoms of individuals, it will report it to the Information Commissioner within 72 hours of discovery. NLTG will record all data breaches within a central register on SharePoint (GDPR) regardless of their effect.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, it will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures it has taken.

International data transfers

NLTG will not transfer personal data to countries outside the European Economic Area (EAA).

Individual responsibilities

Individuals are responsible for helping NLTG keep their personal data up to date. Individuals should inform the relevant department via a NL0529, i.e. Accounts if data provided to NLTG changes, for example if an individual moves to a new house or changes his / her bank details.

NLTG Employees may have access to the personal data of individuals in the course of their employment. Where this is the case, NLTG relies on its employees to help meet data protection obligations.

Any non NLTG Employee processing personnel data, such as volunteers or work experience personnel for example, will be required to sign a confidentiality agreement prior to processing which will held by the responsible manager in line with the company's retention policy.

Employees and those under a confidentiality agreement who have access to personal data are required:

- to access only data that they have authority to access and only for authorised purposes;
- not to disclose data except to individuals (whether inside or outside NLTG) who have appropriate authorisation;
- to keep data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction);
- not to remove personal data, or devices containing or that can be used to access personal data, from NLTG's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device;
- not to store personal data on local drives or on personal devices that are used for work purposes.
- To only access and process data on personal devices on a secure network and through the company's own internal infrastructure, i.e Office 365 etc.

Further details about NLTG's security procedures can be found in its Data Security Policy.

Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under NLTG's disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing employee or learner data without authorisation or a legitimate reason to do so, may constitute gross misconduct as listed within the companies' disciplinary procedure and could lead to dismissal without notice.

Training

NLTG will ensure **all** new staff are informed on the principles of GDPR compliance within their induction supplemented by additional training completed within four weeks of start. Records of this training is stored within the employees personnel file.

All existing staff at the point of the policy introduction will receive compliance training prior to the 1st May 2018 with refresher training bi-yearly to help them understand their duties and how to comply with them regardless of whether they have regular access to personal data, are responsible for implementing this policy, or responding to subject access requests under this policy.

Queries

Should anyone require additional information relating to Data Processing, then they can submit their query via dataenquiries@nltg.co.uk

Signed _____
GARETH LINDSAY
NLTG Managing Director