HEALTH AND SAFETY CONSULTANTS AND TRAINING SERVICES

Data Protection Policy

Policy Statement

NewStart 2001 Ltd (Company)is committed to a policy of protecting the rights and privacy of individuals (includes learners, staff, clients and others) in accordance with the General Data Protection Regulation 2018. The Company needs to process certain information about its staff, learners and other individuals it has dealings with for administrative purposes (e.g. to recruit and pay staff, and contractors to administer programmes of study, to record progress, to agree awards, to collect fees, and to comply with legal obligations to funding bodies and government, to provide consultancy services to our clients).

To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully.

The policy applies to all staff / contractors and learners of the Company or associated. Any breach of the General Data Protection Regulation 2018 is considered to be an offence, and, in that event, NewStart 2001 Ltd disciplinary procedures will apply.

In order to provide our services, we currently hold the following information:

- Company names and addresses
- Individual employee names and titles
- Contact phone numbers
- Email addresses
- Bank Details where applicable for accounting purposes
- For CITB Levy claiming course we hold securely delegates DOB, full address, email address, telephone numbers and National Insurance numbers

We gather this data from incoming enquiries, ongoing enquiries/contracts, new clients, suppliers, consultants, instructors and subcontractors

Your information will only be used for legitimate business purposes. We will not transmit your information to other parties unless it is required to fulfil contracted works. All data disclosures will only be relevant to the particular requirements of the contract works. This information will be handled in accordance with the guidelines of the GDPR and again will only be relevant to the requirements of providing our services

We do not allow third-party service providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes for training or consultancy reasons

NewStart 2001 Limited

HEALTH AND SAFETY CONSULTANTS AND TRAINING SERVICES

The General Data Protection Regulation (GDPR), was implemented on 25 May 2018.

Its purpose is to protect the rights and privacy of living individuals and to ensure that personal data is not processed without their knowledge, and, wherever possible, is processed with their consent.

Definitions:

Personal Data - Data relating to a living individual who can be identified from that information or from that data and other information in possession of the data controller. Includes name, address, telephone number, national insurance number and id number or other identification method. Also includes expression of opinion about the individual, and of the intentions of the data controller in respect of that individual.

Sensitive Data - Different from ordinary personal data (such as name, address, telephone) and relates to racial or ethnic origin, political opinions, religious beliefs, health, sex life, criminal convictions. Sensitive data are subject to much stricter conditions of processing.

Data Controller - Any person (or organisation) who makes decisions with regard to particular personal data, including decisions regarding the purposes for which personal data are processed and the way in which the personal data are processed.

Data Subject - Any living individual who is the subject of personal data held by an organisation.

Processing - Any operation related to organisation, retrieval, disclosure and deletion of data and includes: Obtaining and recording data accessing, altering, adding to, merging or deleting data.

Third Party - Any individual/organisation other than the data subject, the data controller (Company) or its agents.

Relevant Filing System - Any paper filing system or other manual filing system, which is structured so that information about an individual is readily accessible. Please note that this is the definition of "Relevant Filing System" in the regulations. Personal data as defined, and covered, by the Regulations can be held in any format, electronic (including websites and emails), paper-based, photographic etc. from which the individual's information can be readily extracted.

Responsibilities of the General Data Protection Regulation 2018

NewStart 2001 Ltd (Company) as a body corporate is the data controller under the new regulations. Compliance with data protection legislation is the responsibility of all members of the Company who process personal information. Members- employee/ contractors of the Company are responsible for ensuring that any personal data supplied to the Company are accurate and up-to-date.

Data Protection Principles

All processing of personal data must be done in accordance with the eight data protection principles.

1. Personal data shall be processed fairly and lawfully. Those responsible for processing personal data must make reasonable efforts to ensure that data subjects are informed of the identity of the data controller, the purpose(s) of the processing, any disclosures to third parties that are envisaged and an indication of the period for which the data will be kept.

2. Personal data shall be obtained for specific and lawful purposes and not processed in a manner incompatible with those purposes. Data obtained for specified purposes must not be used for a purpose that differs from those.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose for which it is held. If Information, which is not strictly necessary for the purpose for which it is obtained, should not be collected. If data is given or obtained which is excessive for the purpose, it should be immediately deleted or destroyed.

4. Personal data shall be accurate and, where necessary, kept up to date. Data, kept for a long time, must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume accurate. It is the responsibility of individuals to ensure that data held by the Company is accurate and up-to-date. Completion of an appropriate registration or application form, service agreements etc. will be taken, as an indication that the data contained therein is accurate. Individuals should notify the Company of any changes in circumstance to enable personal records to be updated accordingly. It is the responsibility of the Company to ensure that any notification regarding change of circumstances is noted and acted upon.

5. Personal data shall be kept only for as long as necessary. In accordance with any awarding body requirements, client working relationships.

6. Personal data shall be processed in accordance with the rights of data subjects under the General Data Protection Regulation 2018.

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of data.

8. Personal data shall not be transferred to a country or a territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data. Data must not be transferred outside of the European Economic Area (EEA) - the EU Member States together with Iceland, Liechtenstein and Norway - without the explicit consent of the individual. Members of the Company should be particularly aware of this when publishing information on the Internet, which can be accessed from anywhere in the globe. This is because transfer includes placing data on a web site that can be accessed from outside the EEA.

Data Subject Rights Data

Subjects have the following rights regarding data processing, and the data that are recorded about them:

- To make subject access requests regarding the nature of information held and to whom it has been disclosed.
- To prevent processing likely to cause damage or distress.
- To prevent processing for purposes of direct marketing.
- To be informed about mechanics of automated decision-making process that will significantly affect them.
- To take action to rectify, block, erase or destroy inaccurate data.

Consent

Wherever possible, personal data or sensitive data should not be obtained, held, used or disclosed unless the individual has given consent. The Company understands "consent" to mean that the data subject has been fully informed of the intended processing and has signified their agreement, whilst being in a fit state of mind to do so and without pressure being exerted upon them.

Consent obtained under duress or on the basis of misleading information will not be a valid basis for processing. There must be some active communication between the parties such as signing a form and the individual must sign the form freely of their own accord. Consent cannot be inferred from non-response to a communication.

For sensitive data, explicit written consent of data subjects must be obtained unless an alternative legitimate basis for processing exists. In most instances consent to process personal and sensitive data is obtained routinely by the Company (e.g. when a student signs a registration form or when a new member of staff or contractor signs a contract of employment or service). Any Company forms (whether paper-based or web-based) that gather data on an individual should contain a statement explaining what the information is to be used for and to whom it may be disclosed. It is particularly important to obtain specific consent if an individual's data are to be published on the Internet as such data can be accessed from all over the globe. Therefore, not gaining consent could contravene the data protection principle. If an individual does not consent to certain types of processing (e.g. direct marketing), appropriate action must be taken to ensure that the processing does not take place. If any member of the Company is in any doubt about these matters, they should consult the Company Data Protection Officer.

Security of Data

All staff are responsible for ensuring that any personal data (on others), which they hold, are kept securely and that they are not disclosed to any unauthorised third party. All personal data should be accessible only to those who need to use it. You should form a judgement based upon the sensitivity and value of the information in question, but always consider keeping personal data: In a lockable room with controlled access, or in a locked drawer or filing cabinet, or If computerised, password protected, or Kept on disks which themselves are kept securely. Care should be taken to ensure that PCs and terminals are not visible except to authorised staff and that computer passwords are kept confidential. PC screens should not be

left unattended without password protected screen-savers and manual records should not be left where they can be accessed by unauthorised personnel.

Care must be taken to ensure that appropriate security measures are in place for the deletion or disposal of personal data. Manual records should be shredded or disposed of as "confidential waste". Hard drives of redundant PCs should be wiped clean before disposal. This policy also applies to staff / contractors and learners who process personal data "off-site". Off-site processing presents a potentially greater risk of loss, theft or damage to personal data. Staff and learners should take particular care when processing personal data at home or in other locations outside the Company office. Rights of Access to Data Members of the Company have the right to access any personal data, which are held by the Company in electronic format and manual records, which form part of a relevant filing system. This includes the right to inspect confidential personal references received by the Company about that person. Any individual who wishes to exercise this right should apply in writing to the Data Protection Officer. The Company reserves the right to charge a fee for data subject access requests (currently £10). Any such request will normally be complied with within 40 days of receipt of the written request and, where appropriate, the fee. In order to respond efficiently to subject access requests, the Company needs to have in place appropriate records management practices.

Disclosure of Data

The Company must ensure that personal data are not disclosed to unauthorised third parties which includes family members, friends etc without there consent. All staff and learners should exercise caution when asked to disclose personal data held on another individual to a third party. For instance, it would usually be deemed appropriate to disclose a colleague's work contact details in response to an enquiry regarding a particular function for which they are responsible. However, it would not usually be appropriate to disclose a colleague's work details to someone who wished to contact them regarding a non-work-related matter. The important thing to bear in mind is whether or not disclosure of the information is relevant to, and necessary for, the conduct of Company business. Best practice, however, would be to take the contact details of the person making the enquiry and pass them onto the member of the Company concerned.

This policy determines that personal data may be legitimately disclosed where one of the following conditions apply:

1. The individual has given their consent (e.g. a student/member/ contractor or staff has consented to the Company corresponding with a named third party);
2. Where the disclosure is in the legitimate interests of the company (e.g. disclosure to staff - personal information can be disclosed to other Company employees if it is clear that those members of staff require the information to enable them to perform their jobs);
3. Where the institution is legally obliged to disclose the data
4. Where disclosure of data is required for the performance of a contract (e.g. sponsor of course changes/withdrawal etc.).

The regulations permit certain disclosures without consent so long as the information is requested for one or more of the following purposes:

- To safeguard national security;
- Prevention or detection of crime including the apprehension or prosecution of offenders;
- Assessment or collection of tax duty;
- Discharge of regulatory functions (includes health, safety and welfare of persons at work);
- To prevent serious harm to a third party;
- To protect the vital interests of the individual, this refers to life and death situations.

Requests must be supported by appropriate paperwork. When members of staff / contractors receive enquiries as to whether a named individual is a member of the Company, the enquirer should be asked why the information is required. If consent for disclosure has not been given and the reason is not one detailed above (i.e. consent not required), the member of staff / contractor should decline to comment. Even confirming whether or not an individual is a member of the Company may constitute an unauthorised disclosure. Unless consent has been obtained from the data subject, information should not be disclosed over the telephone. Instead, the enquirer should be asked to provide documentary evidence to support their request. Ideally a statement from the data subject consenting to disclosure to the third party should accompany the request.

As an alternative to disclosing personal data, the Company may offer to do one of the followings:

- Pass a message to the data subject asking them to contact the enquirer;
- Accept a sealed envelope/incoming email message and attempt to forward it to the data subject.

Please remember to inform the enquirer that such action will be taken conditionally: i.e. "if the person is a member of the Company" to avoid confirming their membership of, their presence in or their absence from the institution.

Retention and Disposal of Data

The Company discourages the retention of personal data for longer than they are required. Considerable amounts of data are collected on current staff, contractors and learners. However, once a member of staff or student/ learner has left the institution, it will not be necessary to retain all the information held on them. Some data will be kept for longer periods than others. Learners In general, electronic student records containing information about individual learners are kept indefinitely and information would typically include name and address on entry and completion, email address, national insurance number, date of birth, telephone number, programmes taken, examination results, awards obtained.

The Company should regularly review the personal files of individual learners in accordance with the Company's Records Retention Schedule. Staff In general, electronic staff / contractor records containing information about individual members of staff / contractors are kept indefinitely and information would typically include name and address, positions held, email address, national insurance number, date of

birth, telephone number, Other information relating to individual members of staff will be kept by the Personnel Department for 6 years from the end of employment.

Information relating to unsuccessful applicants in connection with recruitment to a post must be kept for 12 months from the interview date. Personnel may keep a record of names of individuals that have applied for, be short-listed, or interviewed, for posts indefinitely. This is to aid management of the recruitment process.

Disposal of Records Personal data must be disposed of in a way that protects the rights and privacy of data subjects (e.g., shredding, disposal as confidential waste, secure electronic deletion).

Publication of Company Information

It is recognised that there might be occasions when a member of staff, a student, or a lay member of the Company, requests that their personal details in some of these categories remain confidential or are restricted to internal access.

All individuals should be offered an opportunity to opt-out of the publication of the above (and other) data. In such instances, the Company should comply with the request and ensure that appropriate action is taken.

Direct Marketing

Any department or section that uses personal data for direct marketing purposes must inform data subjects of this at the time of collection of the data. Individuals must be provided with the opportunity to object to the use of their data for direct marketing purposes (e.g. an opt-out box on a form).

This policy applies to NewStart 2001 Ltd

Managing Director

Date: 6th June 2018