1. Purpose

Tyne North Training Limited ("the organisation") is required to collect and process certain information on apprenticeship candidates for the purpose of assessing their suitability for an apprenticeship and in securing apprenticeship employment. Once on programme as an apprentice the organisation is required to collect and process certain information on learners in order to facilitate the monitoring of performance, achievement, health and safety and employment status. It is also necessary to process and transfer information externally to maintain compliance with government funding body requirements.

The organisation also collects and processes certain information on organisations that recruit or may potentially recruit apprentices for the purposes of securing and administering apprenticeships for learners.

The organisation also collects and processes certain information on employees in order to maintain compliance with employment law. In some cases, it is necessary to transfer this information externally for the administration of payroll, pension and other human resources related purposes.

All of the organisation's staff have a statutory obligation to safeguard the confidentiality of personal information. The relevant legislation includes the General Data Protection Regulation 2018 (GDPR), the Human Rights Act 1988, common law and employment law. It is also central to professional codes of conduct. All staff must be aware that any breach of confidentiality may be a matter for disciplinary action or provide grounds for a complaint or private legal action against them by the individual(s) concerned.

The organisation is acting as a data controller for the purposes of collection, processing, storage, transfer and deletion of personal data and must comply with the General Data Protection Regulation 2018 (GDPR).

In summary this sets out seven principles that the organisation should adhere to when collecting and processing data.

1.1. **Lawfulness, fairness and transparency**. Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject.

1.2. **Purpose limitation**. Personal data must be collected only for specified, explicit and legitimate purposes. It must not be further processed in any manner incompatible with those purposes.

1.3. **Data minimisation**. Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

1.4. **Accuracy**. Personal data must be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that data which is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay.

1.5. **Storage limitation**. Personal data must not be kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed.

1.6. **Integrity and confidentiality**. Personal data must be processed in a manner that ensures its appropriate security.

1.7. **Accountability**. The data controller for the organisation is responsible for, and must be able to demonstrate, compliance with the other data protection principles.

2. Scope

This policy applies to all data collection and processing activities conducted at the organisation. Data subjects may include, candidates, learners, the organisation's staff and members of staff within employers of the organisation's learners or potential employers and subcontractors.

This policy does not form part of the contract of employment, or the Education and Skills Funding Agency (ESFA) training provider – employer contract, but it is a condition of these that the organisation's regulations and policies are adhered to. A failure by a member of the organisation's staff to follow the policy and procedures may result in disciplinary proceedings.

If a data subject has a complaint about the way the organisation has collected or processed their data they can contact us directly in the first instance using the contact details for the data controller below. However, if they are not satisfied with the response from the organisation then they can contact the Information Commissioner's Office https://ico.org.uk/concerns/

3. General Procedures for Data Collection and Processing

In order to comply with the principles of GDPR 2018 the organisation will undertake the following actions:

3.1. The data collected from data subjects will be reviewed on a regular basis to ensure that it is collected for a valid purpose, is necessary and is not in excess of that required for the organisation to fulfil its operational requirements and statutory obligations

3.2. The lawful basis for holding and processing the data will be identified from those listed in Article 6 of the GDPR regulations which are:

3.2.1. **Consent**: the individual has given clear consent for the data controller to process their personal data for a specific purpose.

3.2.2. **Contract**: the processing is necessary for a contract that the data controller has with the individual, or because they have asked the data controller to take specific steps before entering into a contract.

3.2.3. **Legal obligation**: the processing is necessary for the data controller to comply with the law (not including contractual obligations).

3.2.4. **Vital interests**: the processing is necessary to protect someone's life.

3.2.5. **Public task**: the processing is necessary for the data controller to perform a task in the public interest or for official functions, and the task or function has a clear basis in law.

3.2.6. **Legitimate interests**: the processing is necessary for the data controller's legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

3.3. Data subjects will be informed about which lawful basis the organisation has identified for the collection and processing of their data

3.3.1. In the cases where consent has been identified as the lawful basis this will be a positive opt-in, sought separately for each specific purpose and the mechanism for withdrawing consent will be identified.

3.3.2. In the cases that legitimate interest has been identified as the lawful basis, the mechanism for opting out of this processing and the consequences of opting out will be identified

3.4. Data subjects will be informed if their data falls into a Special Category of Data as listed in Article 9 of GDPR (information on ethnic origin, health/disability and criminal records)

3.4.1. In the case of special categories of data, the organisation will be required to identify a lawful basis under Article 6 and a separate condition under Article 9

3.4.2. In the case of special categories of data, the organisation may be required to seek explicit consent. In this case the mechanism for withdrawing consent will be identified

3.5. Data subjects will be informed about the processing and storage of their data

3.5.1. Processes will ensure that data is collected, and transferred accurately between different physical and electronic media. In the case that the organisation or a data subject identify any inaccuracy in the data held then the organisation will rectify this without delay. The procedure for a Data Rectification Request is detailed below.

3.5.2. Access to data will be limited to those individuals who have a legitimate reason for using the data. Physical and electronic data will be stored in such a way that is protected from unauthorised or unlawful access. It will not be stored for longer than necessary and when it is no longer needed it will be securely destroyed. Further details of storage are provided in the procedure for the Secure and Confidential Handling of Data which is detailed below. In the situation where it is believed that data has been lost or subject to unauthorised access the organisation will follow its procedure for reporting a Data Breach detailed below will be followed.

3.5.3. Data will only be transferred out of the organisation for limited specified purposes and to identified external organisations. Data subjects will be informed about any transfers of their data that will take place. The organisation will obtain assurance from any external organisations of their GDPR compliance.

3.5.4. The organisation will maintain up to date records of how and where data is collected, processed and stored. The reasons for this processing and the lawful basis for doing so will also be documented. Data subjects will be able to request a copy of all the data that is held upon them by making a Subject Access Request, the procedure for which is set out below

3.6. Data subjects will have the right to request that their data be permanently erased (the “right to be forgotten”). However, this right will be balanced against the organisation’s lawful basis for holding the data and the data subject will be made aware of the decision that has been made and the reasons behind it. The procedure to be followed when the Data Subject Requests the Right to Erasure is detailed below.

3.7. For all collection and processing activities data subjects will be provided with a privacy notice which will contain:

3.7.1. The organisation’s purpose for collecting and processing data.

3.7.2. The lawful basis that the organisation has identified for collecting and processing the data.

3.7.3. Positive opt-in consent mechanisms for any data where we have identified consent as the lawful basis for collecting and processing the data

3.7.4. Positive opt-in consent mechanisms if required for any special categories of data

3.7.5. Information on any transfers of data to external organisations

3.7.6. Information on the storage mechanisms and the period of retention

3.7.7. Information on how to make a request for rectification, a subject access request, or a request to be forgotten

3.7.8. The contact details of the Data controller

3.7.9. The organisation's contact details for making a complaint about any data processing or collection and the contact details for the Information Commissioners' Office (ICO) if the complaint is to be taken further

4. Procedure for Data Rectification

4.1. Rectification of data may be required in two situations:

4.1.1. The circumstances of a data subject may change resulting in previously held data becoming out of date and requiring updating.

4.1.2. Correct data may have been recorded or transferred inaccurately at some time in the past into another medium and this inaccuracy with the data held on a data subject may be identified internally by a member of the organisation's staff or externally by a data subject themselves.

4.2. In the instance of data requiring updating:

4.2.1. The organisation requires that all data subjects inform the organisation of any change in personal data as soon as this occurs. This should be communicated in writing to tnt@tynenorthtraining.co.uk

4.2.2. If necessary the orginisation may seek verification from the person making the request that they are the data subject.

4.2.3. Confirmation that the change has been made will be sent via return email to the data subject.

4.3. In the instance of an identified inaccuracy with the data:

4.3.1. If identified externally by the data subject, the data subject should inform the organisation of an inaccuracy as soon as this is identified. This should be communicated in writing to tnt@tynenorthtraining.co.uk.

4.3.2. If necessary the organisation may seek verification from the person making the request that they are the data subject.

4.3.3. Confirmation that the change has been made will be sent via return email

4.3.4. If identified internally by a member of the organisation's staff, the staff member should inform the admin office via email of an inaccuracy as soon as this is identified.

4.3.5. If necessary the organisation may seek verification from the data subject of the accuracy of the proposed amendment.

4.3.6. Confirmation that the change has been made will be sent via return email

5. Procedure for a Subject Access Request

5.1. When a data subject makes a subject access request the following procedure will be followed:

5.1.1. The time and date of the request will be recorded in the data access and erasure log

5.1.2. A response acknowledging the request will be sent to the data subject within 5 working days

5.1.3. If necessary the organisation may seek verification from the person making the request that they are the data subject

5.1.4. If necessary the organisation may seek further clarification from the data subject as to the nature of the request

5.1.5. The organisation will use its data mapping to identify the location and nature of all personal data held on a data subject

5.1.6. The organisation will provide copies of all the personal data held on a data subject within 30 days of the request (subject to verification of the subject and clarification)

5.1.7. Copies of physical data will be provided in the form of photocopies. Electronic data will be provided in a common readable format (e.g. pdf, MS Office, Open Office)

6. Exemptions to the Right of Subject Access

In certain circumstances we may be exempt from providing some or all of the personal data requested. These exemptions are described below and should only be applied on a case-by-case basis after a careful consideration of all the facts.

6.1. **Crime detection and prevention**: We do not have to disclose any personal data which we are processing for the purposes of preventing or detecting crime; apprehending or prosecuting offenders; or assessing or collecting any tax or duty. This is not an absolute exemption. It only applies to the extent to which the giving of subject access would be likely to prejudice any of these purposes. We are still required to provide as much of the personal data as we able to. For example, if the disclosure of the personal data could alert the individual to the fact that he or she is being investigated for an illegal activity (i.e. by us or by the police) then we do not have to disclose the data since the disclosure would be likely to prejudice the prevention or detection of crime, or the apprehension or prosecution of offenders.

6.2. **Protection of rights of others**: We do not have to disclose personal data to the extent that doing so would involve disclosing information relating to another individual (including information identifying the other individual as the source of information) who can be identified from the information (or that information and any other information that we reasonably believe the data subject is likely to possess or obtain), unless:

6.2.1. that other individual has consented to the disclosure of the information to the individual making the request; or

6.2.2. it is reasonable to disclose the information to the individual making the request without the other individual's consent, having regard to:

- the type of information that would be disclosed;
- any duty of confidentiality owed to the other individual;
- any steps taken by the controller with a view to seeking the consent of the other individual;
- whether the other individual is capable of giving consent; and
- any express refusal of consent by the other individual.

6.3. **Confidential references**: We do not have to disclose any confidential references that we have given to third parties for the purpose of actual or prospective:

- education, training or employment of the individual;
- appointment of the individual to any office; or
- provision by the individual of any service

This exemption does not apply to confidential references that we receive from third parties. However, in this situation, granting access to the reference may disclose the personal data of another individual (i.e. the person giving the reference), which means you must consider the rules regarding disclosure of third-party data set out above.

6.4. **Legal professional privilege**: We do not have to disclose any personal data which are subject to legal professional privilege. There are two types of legal professional privilege:

6.4.1. 'Advice privilege' covers confidential communications between the Company and our lawyers where the dominant purpose of the communication is the seeking or giving of legal advice;

6.4.2. 'Litigation privilege' covers any document which was created with the dominant purpose of being used in actual or anticipated litigation (eg legal proceedings before a court or tribunal). Once a bona fide claim to litigation privilege ends, the documents in the file which were subject to litigation privilege become available if a data subject access request is received.

6.5. **Corporate finance**: We do not have to disclose any personal data which we process for the purposes of, or in connection with, a corporate finance service if:

6.5.1. disclosing the personal data would be likely to affect the price of an instrument; or

6.5.2. disclosing the personal data would have a prejudicial effect on the orderly functioning of financial markets or the efficient allocation of capital within the economy and we believe that it could affect a person's decision:

- whether to deal in, subscribe for or issue an instrument;

- whether to act in a way likely to have an effect on a business activity, e.g. on the industrial strategy of a person, the capital structure of an undertaking or the legal or beneficial ownership of a business or asset

6.6. **Management forecasting**: We do not have to disclose any personal data which we process for the purposes of management forecasting or management planning to assist us in the conduct of any business or any other activity. Examples of management forecasting and planning activities include staff relocations, redundancies, succession planning, promotions and demotions. This exemption must be considered on a case-by-case basis and must only be applied to the extent to which disclosing the personal data would be likely to prejudice the conduct of that business or activity.

6.7. **Negotiations**: We do not have to disclose any personal data consisting of records of our intentions in relation to any negotiations with the individual where doing so would be likely to prejudice those negotiations. For example, if the organisation is negotiating with an employee in order to agree the terms of a redundancy package and the employee makes a data subject access request, the organisation can legitimately withhold giving access to information which would prejudice those redundancy negotiations. The organisation must, however, disclose all other personal data relating to the individual unless those other personal data are also exempt from disclosure.

7. Procedure for Requesting the Right to Erasure (The right to be forgotten)

The right to erasure does not provide an absolute “right to be forgotten”. Individuals have a right to have personal data erased and to prevent processing in specific circumstances

When a data subject makes a data erasure request the following procedure will be followed:

7.1. The time and date of the request will be recorded in the data access and erasure log

7.2. A response acknowledging the request will be sent to the data subject within 5 working days

7.3. The Senior or Lead Administrator and the designated member of the management team will review the request and the data that is held and being processed on the data subject

7.3.1. If the organisation’s lawful basis for processing the data is consent then the erasure request will be treated as if consent has been withdrawn. Processing of the data will be stopped immediately and electronic and physical copies of the data will be destroyed within 30 days

7.3.2. If the organisation’s lawful basis for processing the data is legitimate interest then the data subject will be informed of the consequences of opting out of the processing and the erasure of their personal data. If the data subject still wishes to proceed with the request then processing of the data will be stopped immediately and electronic and physical copies of the data will be destroyed within 30 days

7.3.3. If the organisation’s lawful basis for processing the data is for the performance of a contract then the organisation will assess whether the data is no longer necessary for the purpose for which it was originally collected. A decision will be made as to whether the erasure request can be implemented. The data subject will either be informed that the processing has to continue and the reasons behind this decision or that the erasure

request can be implemented. If the organisation determines that the request can be implemented the data subject will be informed of the consequences of opting out of the processing and the erasure of their personal data. If the data subject still wishes to proceed with the request then processing of the data will be stopped immediately and electronic and physical copies of the data will be destroyed within 30 days

7.3.4. If the organisation's lawful basis for processing the data is for the fulfilment of a legal obligation then the data subject will be informed that there is no right of erasure for this data. They will be informed of the rationale underpinning the use of legal obligation as the lawful basis for collecting and processing the data

7.4. In any situation where a request for data erasure is being implemented the organisation will use its data mapping to identify any transfers of data to external organisations. The organisation will inform external organisations of the requirement for data erasure and will take reasonable steps to confirm that this has been implemented

8. Procedure for a Data Breach

A personal data breach is defined in the GDPR as a security incident that has affected the confidentiality, integrity or availability of personal data. This could occur if data is lost, destroyed, corrupted or disclosed, if the data is accessed or passed on without proper authorisation, or if the data is made unavailable and this unavailability will have a significant negative effect on the data subject.

8.1. In the case that a member of staff identifies or suspects a potential data breach this must in the first instance be reported to the Senior or Lead Administrator and the designated member of the management team with responsibility for monitoring and reporting data breaches.

8.2. The Senior or Lead Administrator and the designated member of the management team will assess the breach identifying where possible:

- The categories of data involved
- The approximate number of individuals concerned and the approximate number of personal data records
- The level of the risk to the rights and freedoms of the individuals involved
- An early assessment of the measures to be taken to deal with the breach, including the mitigations to be put in place and the possible adverse effects
- Whether the breach represents a risk to the rights and freedoms of the data subjects involved and therefore must be reported to the ICO

8.3. Full details of the breach will be recorded in the data breach log, including the decision and rationale as to whether it is a reportable breach

8.4. If it is considered that there will be a risk to the rights and freedoms of the data subjects involved then the data breach will be reported to the ICO within 72 hours

8.5. If the appropriate actions and mitigations have already been identified then these will be included within the breach reporting

8.6. If the appropriate actions and mitigations had not been identified at the time of the breach reporting then a follow-up report will be issued to the ICO as soon as these have been identified

8.7. If it is considered that there will be a high risk to the rights and freedoms of the data subjects involved then the data subjects will be provided with details of the breach within 72 hours and support will be provided on the measures that they can take to protect themselves from the effects

9. Procedure for the Secure and Confidential Handling of Data

9.1. The organisation will identify the operational requirements for holding personal data and will ensure that access to data will be limited to those individuals who have a legitimate operational reason for using the data

9.2. When discussing data subjects, staff must ensure that they cannot be overheard by others who are not bound by the same requirements of confidentiality towards the data subject

9.3. Staff must not leave material containing personal data, either on paper or on a computer screen, where it can be seen by other learners, unauthorised staff or other on-site visitors

9.4. Staff are to keep all portable physical records containing personal data in designated filing and storage places. This storage should be locked at times when it is not directly controlled or supervised

9.5. Staff will ensure that electronic copies of personal data are held only on encrypted devices provided by the organisation

10. Disclosure Without Prior Consent

Circumstances in which information may be disclosed without prior notice to the data subject.

10.1. Disclosure of personal information without prior notification to the data subject may take place where failure to do so may expose the data subject or others to risk of serious harm. In this situation the organisation will be operating under legal obligation or in exceptional circumstances will be acting to protect the vital interests of the data subjects or others and this is the lawful basis for data processing. These circumstances include:

10.1.1. Child protection (Safeguarding)

10.1.2. Radicalisation and Extremism (Prevent Duty)

10.1.3. Protecting vulnerable adults (Safeguarding)

10.1.4. Life threatening or dangerous situations, for example, where a learner:

- Shows signs of physical, emotional or sexual damage
- Is at risk of significant harm or threatening suicide
- Is threatening to kill or severely harm another person

10.1.5. The prevention, detection or prosecution of crime

10.1.6. The requirement to provide information by a court or the police

11. Contact Details for Data Controller

Tyne North Training, Embleton Avenue, Tyne & Wear, NE28 9NJ
Phone: 0191 262 6860
Email: tnt@tynenorthtraining.co.uk

For Tyne North Training Limited

Ian Selkirk
Chairman of the Board