Purpose/Impact: **This policy applies to the processing of personal data in manual and electronic records kept by the company in connection with its human resources function as described below. It also covers the company's response to any data breach and other rights under the general data protection regulation (GDPR).**

This policy applies to the personal data of job applicants, existing and former employees, apprentices, volunteers, placement students, workers and self-employed contractors. These are referred to in this policy as relevant individuals.

"Personal data" is information that relates to an identifiable person who can be directly or indirectly identified from that information, for example, a person's name, identification number, location, online identifier. It can also include pseudonymised data.

"Special categories of personal data" is data which relates to an individual's health, sex life, sexual orientation, race, ethnic origin, political opinion, religion, and trade union membership. It also includes genetic and biometric data (where used for ID purposes).

"Criminal offence data" is data which relates to an individual's criminal convictions and offences.

"Data processing" is any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

The Company makes a commitment to ensuring that personal data, including special categories of personal data and criminal offence data (where appropriate) is processed in line with UK GDPR and domestic laws and all its employees conduct themselves in line with this, and other related, policies. Where third parties process data on behalf of the company, the company will ensure that the third party takes such measures in order to maintain the company's commitment to protecting data. In line with GDPR, the company understands that it will be accountable for the processing, management and regulation, and storage and retention of all personal data held in the form of manual records and on computers.

Types of data held

Personal data is kept in personnel files or within the Company's HR systems. The following types of data may be held by the company, as appropriate, on relevant individuals:

- Name, address, phone numbers - for individuals and next of kin.
- CVs and other information gathered during recruitment.
- References from former employers.
- National Insurance numbers.
- Job title, job descriptions and pay grades.
- Conduct issues such as letters of concern and disciplinary proceedings.
- Holiday records.

- Internal performance information.
- Medical or health information.
- Sickness absence records.
- Tax codes.
- Terms and conditions of employment.
- Training details.

Relevant individuals should refer to the company's privacy notice for more information on the reasons for its processing activities, the lawful bases it relies on for the processing and data retention periods.

Data protection principles

All personal data obtained and held by the company will:

- Be processed fairly, lawfully and in a transparent manner.
- Be collected for specific, explicit, and legitimate purposes.
- Be adequate, relevant and limited to what is necessary for the purposes of processing.
- Be kept accurate and up to date. Every reasonable effort will be made to ensure that inaccurate data is rectified or erased without delay.
- Not be kept for longer than is necessary for its given purpose.
- Be processed in a manner that ensures appropriate security of personal data including protection against unauthorised or unlawful processing, accidental loss, destruction or damage by using appropriate technical or organisation measures.
- Comply with any relevant UK GDPR procedures for international transferring of personal data where applicable.

In addition, personal data will be processed in recognition of an individuals' data protection rights, as follows:

- The right to be informed.
- The right of access.
- The right for any inaccuracies to be corrected (rectification).
- The right to have information deleted (erasure).
- The right to restrict the processing of the data.
- The right to portability.
- The right to object to the inclusion of any information.
- The right to regulate any automated decision-making and profiling of personal data.

Procedures

The company has taken the following steps to protect the personal data of relevant individuals, which it holds or to which it has access:

- It appoints or employs employees with specific responsibilities for:
    a. The processing and controlling of data.
    b. The comprehensive reviewing and auditing of its data protection systems and procedures.
    c. Overviewing the effectiveness and integrity of all the data that must be protected.

  There are clear lines of responsibility and accountability for these different roles.
- It provides information to its employees on their data protection rights, how it uses their personal data, and how it protects it. The information includes the actions relevant individuals can take if they think that their data has been compromised in any way.
- It provides its employees with information and training to make them aware of the importance of protecting personal data, to teach them how to do this, and to understand how to treat information confidentially
- It can account for all personal data it holds, where it comes from, who it is shared with and also who it might be shared with.
- It carries out risk assessments as part of its reviewing activities to identify any vulnerabilities in its personal data handling and processing, and to take measures to reduce the risks of mishandling and potential breaches of data security. The procedure includes an assessment of the impact of both use and potential misuse of personal data in and by the company.

- It recognises the importance of seeking individuals' consent for obtaining, recording, using, sharing, storing and retaining their personal data, and regularly reviews its procedures for doing so, including the audit trails that are needed and are followed for all consent decisions. The Company understands that consent must be freely given, specific, informed and unambiguous. The company will seek consent on a specific and individual basis where appropriate. Full information will be given regarding the activities about which consent is sought. Relevant individuals have the absolute and unimpeded right to withdraw that consent at any time.
- it has the appropriate mechanisms for detecting, reporting and investigating suspected or actual personal data breaches, including security breaches. It is aware of its duty to report significant breaches that cause significant harm to the affected individuals to the Information Commissioner, and is aware of the possible consequences.
- It will comply with any relevant UK GDPR procedures for international transferring of personal data where applicable.

Access to data

Relevant individuals have a right to be informed whether the company processes personal data relating to them and to access the data that the company holds about them. Requests for access to this data will be dealt with under the following summary guidelines:

- A form on which to make a subject access request is available from the HR department. The request should be made to the HR Manager.
- The company will not charge for the supply of data unless the request is manifestly unfounded, excessive or repetitive, or unless a request is made for duplicate copies to be provided to parties other than the employee making the request.
- The company will respond to a request without delay. Access to data will be provided, subject to legally permitted exemptions, within one month as a maximum. This may be extended by a further two months where requests are complex or numerous.

Relevant individuals must inform the company immediately if they believe that the data is inaccurate, either as a result of a subject access request or otherwise. The company will take immediate steps to rectify the information.

For further information on making a subject access request, employees should refer to our subject access request policy, available from the HR Manager.

Data disclosures

The company may be required to disclose certain data/information to any person. The circumstances leading to such disclosures include:

- Any employee benefits operated by third parties.
- Disabled individuals - whether any reasonable adjustments are required to assist them at work.
- Individuals' health data - to comply with health and safety or occupational health obligations towards the employee.
- For statutory sick pay purposes.
- HR management and administration - to consider how an individual's health affects his or her ability to do their job.
- The smooth operation of any employee insurance policies or pension plans.
- With awarding organisations with regards to CV's, photographs and qualifications of staff.
- Learner information with awarding organisations for registration and certification purposes.
- Learner information with potential employers for contact and interview purposes.
- Learner Information with external databases for qualification, apprentice standards and ESFA funding requirements

These kinds of disclosures will only be made when strictly necessary for the purpose. More information can be found within the respective organisations privacy statements.

Data security

The Company adopts procedures designed to maintain the security of data when it is stored and transported.

Employees must:

- Ensure that all files or written information of a confidential or sensitive nature are stored in a secure manner and are only accessed by authorised people who have a need and a right to access them.
- Ensure that all files or written information of a sensitive or confidential nature are not left where they can be read by unauthorised people or discussed in public or unsecured environments.
- Check regularly on the accuracy of data being entered into computers.
- Always use confidential passwords to access computer systems and files that contain sensitive or confidential data. It is important that passwords remain confidential and are not passed on to people who should not have them.
- Ensure that encryption is enabled for all data transferred over networks using approved encryption algorithms and protocols, both within and outside the institution. Use strong, unique passwords or access controls to protect encrypted data during transfer.
- Use computer screen blanking to ensure that personal data is not left on screen when not in use.
- Obtain authorisation from the data owner before transferring any sensitive data.

Personal data relating to employees should not be kept or transported on laptops, USB sticks, or similar devices, unless authorised by the HR Manager. Where personal data is recorded on any such device it should be protected by:

- Ensuring that data is recorded on such devices only where absolutely necessary.
- Using an encrypted system — a folder should be created to store the files that need extra protection and all files created or moved to this folder should be automatically encrypted.
- Ensuring that laptops or USB drives are not left lying around where they can be stolen.

Failure to follow the company's rules on data security may be dealt with via the company's disciplinary procedure. Appropriate sanctions include dismissal with or without notice dependent on the severity of the failure.

International data transfers
The Company does not transfer personal data to any recipients outside of the EEA.

Breach notification
Where a data breach is likely to result in a risk to the rights and freedoms of individuals, it will be reported to the Information Commissioner within 72 hours of the company becoming aware of it and may be reported in more than one instalment.

Individuals will be informed directly in the event that the breach is likely to result in a high risk to the rights and freedoms of that individual.

If the breach is sufficient to warrant notification to the public, the company will do so without undue delay.

Training
New employees must read and understand the policies on data protection as part of their induction.

All employees receive training covering basic information about confidentiality, data protection and the actions to take upon identifying a potential data breach.

The nominated data controller/auditors/protection officers for the company are trained appropriately in their roles under the UK GDPR.

All employees who need to use the computer system are trained to protect individuals' private data, to ensure data security, and to understand the consequences to them as individuals and the company of any potential lapses and breaches of the company's policies and procedures.

Records
The company keeps records of its processing activities including the purpose for the processing and retention periods in its HR data record. These records will be kept up to date so that they reflect current processing activities.

Data protection compliance

The Quality Coordinator is the company's appointed compliance officer in respect of its data protection activities. They can be contacted at data.protection@heta.co.uk

Cyber Essentials Plus.

HETA hold the above certification and will maintain and continually improve its commitment to ensuring it has the best data protection processes in place.

- **HETA generic data sharing agreement**
- **ICO Data Sharing Agreement Guidance**