Data Protection Policy

Policy Reference	LT-POL05
Approval Date	September 2025
Next Review Date	September 2026
Version Number	1
Owner	Quality Coordinator/Data Protection Officer

Contents

1. Purpose 3
2. Scope 3
3. Definitions 3
4. Policy Statement 3
4.1) Types of data held 4
4.2) Data protection principles 4
5. Responsibilities and Procedures 5
6. Clear Desk Initiative 6
7. Compliance 7
7.1) Access to data – Subject Access Request 7
7.2) Data disclosures 9
7.3) Data security 10
7.4) International data transfers 11
8. Data Breach 11
8.1) Definition/Types of Breach 11
8.2) Reporting an incident 11
8.3) Containment and Recovery 12
8.4) Investigation and Risk Assessment 12
8.5) Evaluation and Response 13
9. Training/Awareness 14
10. Records 14
11. Cyber Essentials Plus 15

1. Purpose

This policy applies to the processing of all personal data processed by HETA, including manual and electronic records kept by the company. It also covers the company's response to any data subject access request or data breach and other rights under the General Data Protection regulation (GDPR) 2018.

2. Scope

This policy applies to the personal data processed at all three of HETA's sites, such as but not limited to data of job applicants, learner applicants, existing and former employees, learners, apprentices, volunteers, placement students, workers and self-employed contractors. This includes temporary, casual or agency staff and contractors, consultants, suppliers and data processors working for, or on behalf of HETA.

3. Definitions

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 but not limited to collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, partner sharing, alignment or combination, restriction, erasure or destruction.

4. Policy Statement

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,

regulation, storage and retention of all personal data held in the form of manual records and on computers and related systems.

4.1) Types of data held

Personal data of staff employed by HETA 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 all 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.

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

Personal data of Learners applying for and obtaining a place at HETA

- Name, address, phone numbers - for individuals and next of kin.
- CVs and other information gathered during recruitment.
- References from schools/colleges.
- 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.
- Terms and conditions of employment.
- Training details.

4.2) 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 minimised to what is necessary for the intended purposes of processing and not further processed in a way that is incompatible with those purposes.
- 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. Once data is no longer needed it will be securely deleted or anonymised.
- 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.
- Shared with partners linked to HETA and the delivery of curriculum or provision of alternative offers to provide our users with a range of alternative educational options

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.

5. Responsibilities and Procedures

HETA promotes within the organisation that all members of staff have a duty to read, understand and follow the guidance within this policy.

The company takes the following steps to protect by default the personal data of all individuals, which it holds, processes or to which it has access:

It appoints or employs members of staff 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 highlighted within job descriptions.

It provides information to its stakeholders on their data protection rights, upon request or via its website on how it uses their personal data, and how it is protected.

The information includes the actions all 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 within their role and at all times.

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 to individuals regarding the activities about which consent is sought. All 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.

Any personal data that is to be transported will be done using confidential files and lockboxes, and follow the organisational sign in and out process to track ownership at all times.

It will comply with any relevant UK GDPR procedures for international transferring of personal data where applicable.

6. Clear Desk Initiative

HETA promotes a culture of security and trust within the organisation.

To protect staff and information that is processed a clear desk initiative has been put in place this involves the participation and support of all Staff taking

responsibility for their workspace and the documentation that they might process whilst carrying out their role.

Department Managers are responsible for promoting this initiative to their staff.

All staff should familiarise themselves with the following guidelines for the Clear Desk Initiative.

The main reasons for ensuring a clear desk when away from the office are:

- A clear desk can produce a positive image when people visit the company.
- It reduces the threat of a security incident as confidential information will be locked away when unattended.
- Sensitive information left on desks or in trays can be lost, stolen or copied.

Scope

At known extended periods away from work areas, such as a lunch break, sensitive working papers are expected to be placed in locked drawers.

At the end of the working day staff are expected to tidy their desk and to put away all office papers. HETA provide locking desks and filing cabinets for this purpose.

- Always clear your workspace before leaving for long-periods of time.
- If you are unsure of whether a duplicate piece of sensitive documentation should be kept - it will probably be better to place it in the confidential waste bin.
- Consider scanning paper items and filing them electronically. Store the information in a safe area electronically and if discarding of the sensitive data, ensure that this is disposed of in the confidential waste bin provided at all sites.
- Use the confidential waste bins for bulk sensitive documents when they are no longer needed.
- Lock desks and filing cabinets at the end of the day.
- Lock away portable computing devices such as laptops or PDA devices.
- Treat mass storage devices such as CDROM, DVD or USB drives as sensitive and secure them in a locked drawer.
- Always lock terminals and / or ~~your~~ laptop screens when leaving desks / offices for any length of time.

Staff not complying with the clear desk initiative may be subject to HETA's disciplinary procedure, if sensitive data is left at risk of causing a GDPR incident.

7. Compliance

7.1) Access to data – Subject Access Request

All individuals have a right to request access to the personal data the company holds relating to them and to understand the reason for the data being collected.

Requests for access to this data will be dealt in accordance with this policy and the rules laid out by the GDPR act 2018.

GDPR clarifies that the reason for allowing individuals to access their personal data is so that they are aware of and can verify the lawfulness of the processing.

We will provide a copy of the data held by us free of charge. However, we will charge a reasonable fee when a request is manifestly unfounded or excessive, particularly if it is repetitive. We will also charge a reasonable fee to comply with requests for further copies of the same information. The fee will be based on the administrative cost of providing the information. Information will be provided without delay and at the latest within 30 days of receipt of request.

We will extend the period of compliance by a further two months when requests are complex or numerous. If this is the case, we will inform the individual within one month of receipt of the request and explain why the extension is necessary.

When responding to a request we may refuse to divulge whether we do or do not hold the information or we may withhold some, or all, of the personal information that we hold.

When we refuse to divulge or withhold information, we will explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy without undue delay and at the latest within one month.

We will always verify the identity of the person making the request, If the request is made by someone other than the individual who's information we hold, their consent to allow us to divulge the information has to be obtained in writing with a signed declaration using our Subject Access Request form. If a request is made electronically, we will try to provide the information in a commonly used electronic format after verifying the identity of the person making the request.

If the personal data provided is incorrect and needs to be rectified it will be corrected upon receipt of the amended information, within 30 days. HETA will not rectify data if the information is provided by someone other than the individual who's information we hold, their consent to allow us to rectify the information has to be obtained in writing with a signed declaration as to the authenticity of the data to be rectified.

The individual will be informed of the correction once it has been completed. If we have disclosed the personal data in question to third parties, we will inform them of the rectification where possible. We will also inform the individuals about the third parties to whom the data has been disclosed where appropriate.

All requests from HETA Staff or HETA Apprentices/Trainees/learners should be made via email or in writing, clearly identifying the personal data they require.

All requests for CCTV footage must be made using the formal Internal Subject Access Request form (LT-H05.01) and be approved by the respective Centre

Manager.

All requests for personal data from an external party should be accompanied by the Subject Access Request Form and proof of identity.

On no account will a member of HETA staff relay any personal information to an external party, except those designated as partners and holding a Strategic Alliance Agreement or Memorandum of Understanding dealing with specific contracted delivery or alternative offers, without approval and a completed Subject Access Request Form.

The sharing of such information should be made by the Quality Coordinator/Data Protection Officer, IT Manager or a member of the Senior Leadership Team.

Where information has been shared and the recipient of the information believes the data is inaccurate, they must inform the company immediately ~~if~~ The company will take immediate steps to rectify the information as quickly as is deemed possible.

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

7.2) 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 or whilst in training.
- Individuals' health data - to comply with health and safety or occupational health obligations.
- For statutory sick pay purposes.
- Management and administration - to consider how an individual's health affects his or her ability to do their job or how it affects their ability to attend the training or courses they are enrolled on, or to carry out an exam or practical assignment.
- The smooth operation of any employee insurance policies or pension plans.
- Awarding organisations with regards to sharing CPD information, 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.
- Learner information to local authorities as and when required.

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

7.3) 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 for as long as is deemed necessary.
- 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.
- Obtain authorisation from the data owner before transferring any sensitive data.
- Ensure that all sensitive hard copies of documentation is disposed of adequately using confidential waste bins.

Personal data relating to individuals should not be kept or transported on laptops, USB sticks (prohibited), or similar devices.

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 are not left lying around where they can be stolen and information on the laptop accessed without the use of passwords.

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 risk of data being exposed or failure to follow the company's rules.

7.4) International data transfers

The Company does not transfer personal data to any recipients outside of the UK.

8. Data Breach

HETA holds, processes, and shares a large amount of personal data; a valuable asset that needs to be suitably protected. Every care is taken to protect personal data from incidents (either accidentally or deliberately) to avoid a data protection breach that could compromise security.

Compromise of information, confidentiality, integrity, or availability may result in harm to individual(s), reputational damage, detrimental effect on service provision, legislative non-compliance, and/or financial costs.

The objective of this policy is to contain any breaches, to minimise the risk associated with the breach and consider what action is necessary to secure personal data and prevent further breaches.

For the purpose of this Policy, data security breaches include both confirmed and suspected incidents. An incident in the context of this policy is an event or action which may compromise the confidentiality, integrity or availability of systems or data, either accidentally or deliberately, and has caused or has the potential to cause damage to HETA's information assets and/or reputation.

8.1) Definition/Types of Breach

An incident includes but is not restricted to, the following:

- Loss or theft of confidential or sensitive data or equipment on which such data is stored (e.g. loss of laptop, iPad/tablet device, mobile phone or paper record).
- Equipment theft or failure.
- Unauthorised use of, access to, or modification of data or information systems.
- Attempts (failed or successful) to gain unauthorised access to information or IT system(s).
- Unauthorised disclosure of sensitive/confidential data.
- Website defacement.
- Hacking attack.
- Unforeseen circumstances such as a fire or flood.
- Human error.
- 'phishing' offences where information is obtained by deceiving the organisation who holds it.

8.2) Reporting an incident

Any individual who accesses, uses or manages HETA's information is responsible for reporting data breach and information security incidents immediately to the Data Protection Officer (DPO)/Quality Coordinator (data.protection@heta.co.uk) and IT Services (adrian.saxby@heta.co.uk). If the breach occurs or is discovered outside normal working hours, it must be reported as soon as is practicable.

The incident should be reported via email or verbally, and a HETA Data Breach Report Form (LT-H05.02) is started by the Departmental Manager of the person reporting the incident and sent to the IT Manager and the DPO/Quality Coordinator.

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.

8.3) Containment and Recovery

The DPO will firstly determine if the breach is still occurring. If so, the appropriate steps will be taken immediately to minimise the effect of the breach.

An initial assessment will be made by the DPO in liaison with relevant managers to establish the severity of the breach.

If it is an electronic breach, advice and guidance will be sought from the IT Department in putting short term measures in place prior to resolving the incident/issue.

The relevant manager and DPO will establish whether there is anything that can be done to recover any losses and limit the damage the breach could cause. They will establish who may need to be notified as part of the initial containment and will inform the police, where appropriate.

8.4) Investigation and Risk Assessment

An investigation will be undertaken by the DPO and/or the IT Manager immediately and wherever possible within 24 hours of the breach being discovered/reported.

The DPO along with the IT Manager will investigate the breach and assess the risks associated with it, for example, the potential adverse consequences for individuals, how serious or substantial those are and how likely they are to occur. The investigation will consider the following:

- The type of data involved.
- It's sensitivity.

- The protections are in place (e.g. encryption).
- What's happened to the data, has it been lost or stolen?
- Whether the data could be put to any illegal or inappropriate use.
- Who the individuals are, the number of individuals involved and the potential effects on those data subject(s).
- Whether there are wider consequences to the breach notification.

The DPO, in liaison with the IT Manager and relevant manager(s) will determine a suitable course of action to be taken to ensure a resolution to the incident and will determine who needs to be notified.

Every incident will be assessed on a case-by-case basis; however, the following will be considered:

- Whether there are any legal/contractual notification requirements.
- Whether notification would assist the individual affected – could they act on the information to mitigate risks?
- Whether notification would help prevent the unauthorised or unlawful use of personal data.
- Would notification help HETA meet its obligations under the seventh data protection principle (Accountability).

If many people are affected, or there are very serious consequences, considerations should be made as to whether the Information Commissioner's Office (ICO) should be notified. The ICO will only be notified if personal data is involved.

Guidance on when and how to notify ICO is available from their website at: https://ico.org.uk/for-organisations/report-a-breach/

Notification to the individuals whose personal data has been affected by the incident will include a description of how and when the breach occurred, and the data involved. Specific and clear advice will be given on what they can do to protect themselves and include what action has already been taken to mitigate the risks. Individuals will also be provided with a way in which they can contact HETA for further information or to ask questions regarding what has occurred.

Once informed of a Data Breach the Chief Executive Office (CEO) should consider whether it is necessary to make a press release and must be ready to handle any incoming press enquiries.

The CEO will consider notifying third parties such as the police, insurers, bank or credit card companies, and funding agencies. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future

All actions will be recorded by the DPO.

8.5) Evaluation and Response

Once the incident has been investigated and controlled, the DPO will carry out a full review of the causes of the breach, the effectiveness of the response(s) and whether any changes to systems, policies and procedures should be undertaken.

Existing controls will be reviewed to determine their adequacy, and whether any corrective action should be taken to minimise the risk of similar incidents occurring.

The review will consider:

- Where and how personal data is held and where and how it is stored.
- Where the biggest risks lie and will identify any further potential weak points within its existing measures.
- Whether methods of transmission are secure, sharing minimum amount of data necessary.
- Identifying weak points within existing security measures.
- Staff awareness.
- Implementing a data breach plan and identifying a group of individuals responsible for reacting to reported breaches of security.
- If deemed necessary a report recommending any changes to systems, policies and procedures will be considered by the DPO, IT Manager and the senior leadership team.

Please use the Data Breach Reporting Form to report any data breaches and email it to the DPO and the IT Manager.

9. Training/Awareness

This policy is shared on the Company's intranet page, together with all of HETA's policies and procedures.

New members of staff are shown where to find policies and procedures as part of the induction process.

Members of staff are notified by way of news updates via the intranet, of changes to policies and procedures.

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.

10. Records

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

11. Cyber Essentials Plus

HETA holds the Cyber Essentials Plus certification and will maintain and continually improve its commitment to ensuring it has the best data protection processes in place.

Related Policies, Documents and Links

- **HETA generic data sharing agreement**
- QA-POL03 Documents & Records Policy
- QA-POL04 Data Retention and Destruction Policy
- LT-H05.01 Subject Data Access Request Form.docx
- ICO Data Sharing Agreement Guidance
- LT-H05.02 HETA Data Breach Report Form
- ICO Data Breach Reporting Guidance
- ICO Data Breach Reporting Form
- https://ico.org.uk/for-organisations/report-a-breach/