HSB.	**PERSONNEL POLICY**
Reference: HR001 Version: 1.1	Number of Pages 5
TITLE: **General Data Protection & Privacy Policy (Learners)**	
Authorised by: **Russell Prince** Operations Director	Effective Date: 01/06/2023 Supersedes:

Introduction

HSB and its employee's will do everything within its power to ensure the safety and security of any material of a personal or sensitive nature.

It is the responsibility of all employees to take care when handling, using or transferring personal data that it cannot be accessed by anyone who does not:

- Have permission to access that data, and/or
- Need to have access to that data.

Data breaches can have serious effects on individuals and / or institutions concerned, can bring HSB into disrepute and may well result in disciplinary action, criminal prosecution and fines imposed by the Information Commissioners Office (ICO) - for HSB and the individuals involved. Particularly, all transfer of data is subject to risk of loss or contamination.

Anyone who has access to personal data must know, understand and adhere to this policy, which brings together the legal requirements contained in relevant data protection legislation and relevant regulations and guidance.

Policy Statements

HSB will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.

Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay. All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".

Data Protection Principles

The Data Protection Act 1998 establishes eight enforceable principles that must be adhered to at all times:

1. Personal data shall be processed fairly and lawfully.
2. Personal data shall be obtained only for one or more specified and lawful purposes.
3. Personal data shall be adequate, relevant and not excessive.
4. Personal data shall be accurate and where necessary kept up to date.
5. Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act 1998.

7. Personal data shall be kept secure i.e. protected by an appropriate degree of security.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection.

General Data Protection Regulation

The EU's General Data Protection Regulation (GDPR) will apply from 25 May 2018, when it supersedes the UK Data Protection Act 1998. Significant and wide-reaching in scope, the new law brings a 21st century approach to data protection. It expands the rights of individuals to control how their personal information is collected and processed, and places a range of new obligations on organisations to be more accountable for data protection.

- Same basic principles as current DP law, but strengthened
- Increased accountability
- New rights for individuals, and strengthening of existing rights
- Breach reporting
- Data Protection Impact Assessments
- Higher penalties for non-compliance

Personal Data

HSB and individuals will have access to a wide range of personal information and data. The data may be held in a digital format or on paper records. Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances. This will include:

- Personal information including *apprentices/learners*, members of staff and parents / carers e.g. names, addresses, contact details, legal guardianship contact details, health records, disciplinary records
- Curricular / academic data e.g. class lists, learner / student progress records, reports, references
- Professional records e.g. employment history, taxation and national insurance records, appraisal records and references
- Any other information that might be disclosed by parents / carers or by other agencies working with families or staff members.

Responsibilities

HSB's Audit and Compliance Manager advises staff that have any questions or concerns. This person will keep up to date with current legislation and guidance and will:

- Determine and take responsibility for the HSB's information risk policy and risk assessment

HSB will identify Information Asset Owners (IAOs) *for the various types of* data being held (e.g. learner information / staff information / assessment data etc.). The IAO's will manage and address risks to the information and will understand:

- What information is held, for how long and for what purpose.
- How information has been amended or added to over time, and
- Who has access to protected data and why.

Everyone in HSB has the responsibility of handling protected or sensitive data in a safe and secure manner. The main board of directors are required to comply fully with this policy in the event that they have access to and may be involved with personal data, when engaged in their role as Director.

Registration

HSB is registered as a Data Controller on the Data Protection Register held by the Information Commissioner.

Training & awareness

All staff will be made aware of their responsibilities that need to be followed in data handling/ data protection training and will be made, as described in this policy through:

- Induction training for new staff
- Staff meetings / briefings

Secure storage of and access to data

HSB from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them. Access to protected data will be controlled according to the role of the user. Members of staff will not, as a matter of course, be granted access to the whole management information system.

All users will use strong passwords which must be changed. User passwords must never be shared. Personal data may only be accessed on machines that are securely password protected. Any device that can be used to access data must be locked if left (even for very short periods).

All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation. Personal data can only be stored on HSB's equipment (this includes computers and portable storage media (where allowed). Private equipment (i.e. owned by the users) must not be used for the storage of personal data.

When personal data is stored on any portable computer system, USB flash drive or any other removable media:

- The data must be encrypted and password protected,
- The device must be password protected the device must offer approved virus and malware checking software, and
- The data must be securely deleted from the device, in line with HSB's policy (below) once it has been transferred or its use is complete.

HSB **must not** use any unprotected USB flash drives to carry data that contains any personal / confidential information. HSB has clear policies and procedures for the automatic backing up, accessing and restoring all data held on SETA's systems, including off-site backups for MIS data.

As a Data Controller, HSB is responsible for the security of any data passed to a "third party". Data Protection clauses will be included in all contracts where data is likely to be passed to a third party. All paper based Protected and Restricted (or higher) material must be held in lockable storage, whether on or off site.

Secure transfer of data and access out of HSB

HSB recognises that personal data may be accessed by users out of HSB, or transferred to any agencies. In these circumstances:

- Users may not remove or copy sensitive or restricted or protected personal data from HSB or authorised premises without permission and unless the media is encrypted and password protected and is transported securely for storage in a secure location.
- Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (e.g. family members) when out of HSB.
- When restricted or protected personal data is required by an authorised user from outside the organisation's premises (for example, by a member of staff to work from their home), they should preferably have secure remote access to the management information system or learning platform;
- If secure remote access is not possible, users must only remove or copy personal or sensitive data from the organisation or authorised premises if the storage media, portable or mobile device is encrypted and is transported securely for storage in a secure location;
- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software; and
- Particular care should be taken if data is taken or transferred to another country, particularly outside Europe, and advice should be taken from the local authority or the Information Commissioner's Office (if relevant) in this event.

Disposal of data

HSB will comply with the requirements for the safe destruction of personal data when it is no longer required. The disposal of personal data, in either paper or electronic form, must be conducted in a way that makes reconstruction highly unlikely (any printed materials that contain any personal / sensitive / confidential information should be placed in the Safe Shred room in the Accounts archives room).

Data Breach

If any data (paper or electronic) is lost, it needs to be reported to the Audit and Compliance Manager immediately, so it can be determined if it is necessary to report to the ICO.
All significant data protection incidents must be reported through the Audit and Compliance Manager to the Information Commissioner's Office based upon the Seta incident handling policy.

Complaints and removal of data

We take any complaints about our collection and use of personal information very seriously.

If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance.

To make a complaint or require your data to be removed, please contact our Audit and Compliance Manager.

Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at https://ico.org.uk/concerns/
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Contact us

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact our Operations Director

- Tel: 0161 818 6118