DATA PROTECTION POLICY

Contents

Introduction

The aim of this policy is to comply with relevant legislation in regard to the keeping of employment records and customer data. HIL Liverpool ("The Company") requires personal information relating to each individual in order to manage its business in an efficient and effective manner; this data is subject to the Data Protection Act 2018 and the principles of the General Data Protection Regulation ("GDPR") (Regulation (EU) 2016/679). The Company is committed to working within the rules, guidelines and principles of this legislation. We are committed to respecting and protecting the rights and information of our customers who access our services as well as our staff and volunteers.

Any breach of this policy will be considered to be a disciplinary offence.

Definitions

Data: includes computerised data, manual data and any other form of accessible record that includes personal information held by the Company.
Personal data: is that which relates to a living individual who could be identified by the data.
Data Subject: A data subject is an individual that is the subject of any personal data.

Legal Requirements

Data is protected by the Data Protection Act 2018. Its purpose is to protect the rights and privacy of individuals and to ensure that personal data are not processed without their knowledge, and, wherever possible, is processed with their consent.

The Act requires us to register the fact that we hold personal data and to acknowledge the right of 'subject access' – anyone who we hold information about has the right to copies of their own data.

Purpose of data held by HIL LIVERPOOL

Data may be held by us for the following purposes:

1. Staff Administration
2. Student and Customer Administration
2. Accounts & Records
3. Advertising, Marketing & Public Relations
4. Information and Database administration
5. Journalism and Media
6. Reporting and monitoring for our investors
7. Research
8. Volunteer administration

Policy

It is the intention of this Company to adhere to the principles of the Data Protection Act and GDPR. Therefore the data protection policy applies to all employees and to any other party that handles data for or on behalf of the Company.

Any personal data collected will:

- Be used by the Company in accordance with the Data Protection Act.
- Be obtained and processed fairly and lawfully, in particular, shall not be processed unless specific conditions are met.
- Be relevant and not excessive in relation to the purpose for which it was collected.
- Be accurate and, if necessary, kept up to date.
- Not be kept for longer than necessary for the specified purpose.
- Be processed in accordance with the rights of the data subject in accordance with the Act.
- Be stored safely to avoid unauthorised access, loss and/or damage.
- Not be transferred to a country outside the European Economic Area unless it ensures an adequate level of protection for the rights of the data subjects.

The Company will inform any data subjects:

- What information the Company holds about them.
- How to gain access to the data.
- How to keep data held up-to-date.

The data protection principles

There are eight data protection principles that are central to the Act. HIL LIVERPOOL and all its employees must comply with these principles at all times in its information-handling practices. In brief, the principles say that personal data must be:

1. **Processed fairly and lawfully**. - This means that the individual must consent to their personal data being held about them. Sensitive personal data may only be processed with the explicit consent of the individual and consists of information relating to:
    - race or ethnic origin
    - political opinions and trade union membership
    - religious or other beliefs
    - physical or mental health or condition
    - criminal offences, both committed and alleged.

2. **Obtained only for one or more specified and lawful purposes, and not processed in a manner incompatible with those purposes.** - In HIL LIVERPOOL this means that data can only be held for the reasons we specify e.g. administration reports, tracking and monitoring. We can't then use this information for any other purpose.

3. **Adequate, relevant and not excessive** – The data we hold needs to be relevant to HIL LIVERPOOL work. There is no need to ask for unnecessary information which isn't relevant to our purposes.

4. **Accurate and kept up-to-date** - If your personal information changes, ie. your address, you must inform your line manager as soon as practicable so that HIL LIVERPOOL records can be updated. HIL LIVERPOOL cannot be held responsible for any errors unless you have notified HIL LIVERPOOL of the relevant change. The same is true of information we hold about service users e.g. if someone changes addresses delete the old one – it is no longer accurate or up to date.

5. **Not kept for longer than is necessary** – Different departments will require us to keep records for different lengths of time. Generally the records we need to keep are reports, administration and evidence that we have achieved the outcomes and results stated. HIL LIVERPOOL will retain information about staff for 6 years after they leave the organisation.

6. **Processed in accordance with the rights of employees under the Act** – every individual who HIL LIVERPOOL holds personal data about has the right to request and see the information we hold.

7. **Secure, technical and organisational measures will be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, data** – Personnel files are confidential and are stored in locked filing cabinets. Only authorised staff have access to these files. Files will not be removed from their normal place of storage without good reason. Data stored on memory stick or other removable media will be kept in locked filing cabinets. Data held on computer will be stored confidentially by means of password protection, encryption or coding and again only authorised employees have access to that data. The Company has network backup procedures to ensure that data on computer cannot be accidentally lost or destroyed.

8. **Not transferred to a country or territory outside the European Economic Area unless that country ensures an adequate level of protection for the processing of personal data.**

The following is a general overview to enable staff to easily implement the principles into their work. The following key dos and don'ts must be followed by all staff processing personal data on individuals.

Key Dos & Don'ts

Do

- Comply with Data Protection Principles at all times;
- Treat other people's data as though it were your own data;
- Remember the Act applies to paper files, information held electronically, video/DVD, audiotapes, photographs and verbal communication;
- Get permission from the data subject to hold their personal data unless consent is obviously implied;
- Be particularly careful about sensitive data: concerning race, political opinion, religious belief, physical or mental health, criminal offences;

•Hold personal data about people only when necessary and make sure it is appropriately secured with restricted access;
•Delete personal data when it is no longer relevant;
•Tell people you hold personal data about them and tell them why you need to do so (fair processing);
•Be open with people about information held about them;
•Ensure that you have a contract (data processing agreement) in place when sharing personal data with other organisations;
•Be very careful about passing personal data to third parties;
•Respect confidentiality and the rights of the data subject;
•Review storage of confidential data at least annually;
•Ensure all personal data is disposed of as confidential waste;
•When writing documents, bear in mind that the data subject has a right to see information relating to them;
•Realise even deleted emails may be retrieved and revealed to those about whom they are written;
•Hold personal data in such a way that it can be collected for inspection at short notice;
•Where possible, make anonymous personal data for analysis;
•Direct any official requests to see personal data to HIL LIVERPOOL directors.

Do Not

•Circulate or transfer any confidential information unless for an agreed and legitimate business process (e.g. bank transfers). Where this occurs electronically data must be encrypted and accessed by a password sent independently of the data;
•Transfer physical data unless via a recognised and data protection compliant carrier (e.g. sending document for shredding);
•Worry about the complexities of the Act - the Data Protection Principles are simple;
•Reveal personal data to third parties without the data subject's permission or justification within the Act;
•Disclose any personal data over the telephone;
•Use personal data about a service user without their explicit consent;
•Leave personal data insecure in any way, whether it is physical files or information held electronically;
•Take work data out of HIL LIVERPOOL places of work without particular care for security;
•Process confidential data on a computer not owned, supplied or approved by HIL LIVERPOOL;
•Transfer electronically unencrypted personal data (such as through email), as it is relatively insecure;
•Use personal data held for one purpose for a different purpose without permission from the data subject.

Non Compliance
All employees have a role to play in enforcing the policy and are required to deal with any observed or reported breaches. Should employees feel apprehensive about their own safety in regard to addressing any breach, they should seek senior management support.

Failure to comply with this policy may lead to a lack of clarity over job role, learning needs or expected standards of performance, resulting in reduced effectiveness or efficiency, underperformance and putting service delivery at risk.

Any member of staff refusing to observe the policy will be liable to disciplinary action in accordance with the Company's Disciplinary Policy up to and including dismissal.

Implementation of the Policy
Overall responsibility for policy implementation and review rests with the Company senior management. However, all employees are required to adhere to and support the implementation of the policy. The Company will inform all existing employees about this policy and their role in the implementation of the policy. They will also give all new employees notice of the policy on induction to the Company.

This policy will be implemented through the development and maintenance of procedures for appraisals and one-to-one meetings, using template forms, and guidance given to both managers and employees on the process.

This Policy was approved & authorised by:

Name:	Rauni Da Mota
Position:	Director Principal
Date of first implementation:	02/05/2019
Review Date:	21/04/2025
Version:	4
Signature:	

Monitoring Policy
The policy will be monitored on an on-going basis, monitoring of the policy is essential to assess how effective the Company has been.

Reviewing Policy
This policy will be reviewed and, if necessary, revised in the light of legislative or codes of practice and organisational changes. Improvements will be made to the management by learning from experience and the use of established reviews.

Policy Renew Date: 21/04/2027

Policy Amendments
Should any amendments, revisions, or updates be made to this policy it is the responsibility of the Company senior management to see that all relevant employees receive notice. Written notice and/or training will be considered.

Additional Information
If you require any additional information or clarification regarding this policy, please contact your manager. In the unlikely event where you are unhappy with any decision made, you should use the Company's formal Grievance Procedure.

To the extent that the requirements of this policy reflect statutory provisions, they will alter automatically when and if those requirements are changed.