Staff Privacy Policy

Introduction

We hold personal data about our employees, clients, suppliers and other individuals for a variety of valid purposes.

This policy sets out how we work to protect personal data and ensure that staff understand the rules governing their use of personal data to which they have access in the course of their work. In particular, this policy requires staff to ensure that the data Protection Officer (DPO) be consulted before an significant new data processing activity in initiate to ensure that relevant compliance steps are addressed.

Definitions

Business purposes	The purposes of which personal data may be used by us: Personnel, administrative, financial, regulatory, payroll and business development purposes. Business purposes include the following: • Compliance with our legal, regulatory and corporate governance obligations and good practice • Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests • Ensuring business polices are adhered to (such as policies covering email and internet usage) • Operational reasons, such as recording transactions, training and quality control, ensuring confidentiality of commercially sensitive information. • Investigating complaints • Checking references, ensuring safe working practices, monitoring and managing staff access to systems and facilities and staff absences, administration and assessments • Monitoring staff conduct, disciplinary matters

	• Marketing our business • Improving services
Personal data	Information relating to identifiable individuals, such as job applicants, current and former employees. Personal data we gather may include: individual contact details, educational background, pay details, details of certificates and diplomas, education and skills, marital status, nationality, job title and CV.
Sensitive personal data	Personal data on individual's racial or ethnic origin, political opinions, religious or similar beliefs, physical or mental health or condition, criminal offences – any use of sensitive personal data should be strictly controlled in accordance with this policy.

Scope

This policy applies to all staff. You must be familiar with this policy and comply with its terms.

This policy supplements our other policies relating internet usage and email use. We may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be circulates to all staff.

Who is responsible for this policy?

Welcome Skills management Team has overall responsibility for the day to day of this policy.

Our procedures

Under GDPR, all personal data obtained and held by us must be processed according to a set of core principles. In accordance with these principles, we will ensure that:

a) processing is fair, lawful and transparent
b) data is collected for specific, explicit, and legitimate purposes
c) data collected is adequate, relevant and limited to what is necessary for the purposes of processing
d) data is kept accurate and up to date. Data which is found to be inaccurate will be rectified or erased without delay

e) data is not kept for longer than is necessary for its given purpose

f) data is 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 we comply with the relevant GDPR procedures for international transferring of personal data

Fair and lawful processing

We must process personal data fairly and lawfully in accordance with individual's rights. This generally means that we should not process personal data unless the individual whose details we are processing has consented to this happening.

Responsibilities of the DPO

- Keeping the Welcome Skills Management Team updated data protection responsibilities, risks and issues.
- Reviewing all data protection procedures and policies on a regular basis
- Arranging data protection training and advice for all staff members.
- Answering questions on data protection from staff, management and other stakeholders.
- Responding to individuals such as learners and employees who wish to know which data is held on them by Welcome Skills.

Sensitive personal data

In the cases we do process sensitive personal data, we will require the data subject's explicit consent to do this unless exceptional circumstances apply or we are required to do this by law. E.g. to comply with legal obligations to ensure health and safety at work. Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

Accuracy and relevance

We will ensure that any personal data we process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained.

Individuals may ask that we correct inaccurate personal data relating to them. If you believe that your data is inaccurate you should inform the DPO.

Your personal data

You must take reasonable steps to ensure that personal data we hold about you is accurate and updated as required. For example, if your personal circumstances change, please inform the Human Resources/DPO so that they can update your records.

Data Security

You must keep personal data secure against loss or misuse. Where other organisations process personal data as a service on our behalf, the DPO will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third-party organisations.

Storing data securely

- In cases when data is stored on printed paper, it should be kept in a secure place where unauthorized personnel cannot access it.
- Printed data should be shredded when it is no longer needed
- Data stored on a computer/laptop should be protected by strong passwords that are changed regularly
- Data stored on CD's or memory sticks must be locked away secure when they are not being used
- Data should be regularly backed up in line with the company's backup procedures
- Data should never be saved directly to mobile devices such as laptops, tablets or smartphones without the prior authority of Welcome Skills Management.
- All servers containing sensitive data must be approved and protected by security software and a strong firewall.

Data retention

We must retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, taking in to account that the personal data was obtained, but should be determined in a manner consistent with our data retention guidelines. Please refer to Welcome Skills Retention policy.

Transferring data internationally

There are restrictions on international transfers of personal data. You must not transfer personal data anywhere outside the UK without first consulting the DPO or Welcome Skills Management.

Subject Access Request

Please note that individuals are entitled, subject to certain exceptions, to request access to information we held/hold about them.

If you receive a subject access requested, you should refer that request immediately to the DPO.

Please contact the DPO if you would like to correct or request information that we hold about you. There are also restrictions on the information to which you are entitled under applicable law.

Processing data in accordance with the individual's rights

You should abide by any request from an individual not to use their personal data for direct marketing purposes and notify the DPO about any such request.

Do not send direct marketing material to someone directly unless you have an existing business relationship with them in relation to the services being marketed.

Please contact the DPO for advice on direct marketing before starting any new direct marketing activity.

Transparency of data protection

Being transparent and proving accessible information to individuals about how we will use their personal data is important for our organisation.

Monitoring

Everyone must observe this policy. The DPO has overall responsibility for this policy and will monitor it regularly to make sure it is being adhered to.

Training

All staff will receive training on this policy. New employees will received training as part of the induction process. Further training will be provided at least every 2 years or whenever there is a sustainable change in the law or our policy and procedure.

Training is provided through an in-house seminar on a regular basis.

It will cover:

The history of data protection and the introduction of GDPR and why it's needed. Dos and Don'ts of GDPR, principles to follow, handling data correctly, types of record, storing data, data breaches and penalties.

Completion of training is compulsory.

DOCUMENT NAME/LOCATION	Date Produced	Version Number	Authorised By:	Document review date
Staff Privacy Policy	July 2021	2	K.Hussin	June 2021

Consequences of failing to comply

We take compliance with this policy very seriously. Failure to comply puts both you and the organisation at risk.

The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under our procedures which may result in dismissal.

If you have any questions or concerns about anything in this policy, do not hesitate to contact the DPO.

Making a Complaint

If you think your data rights have been breached, you are able to raise a complaint with our Data Protection Officer (DPO). You can write to the following address:

Welcome Skills DPO
Sovereign House,
29-31, Limpsfield Road,
Sanderstead,
South Croydon,
CR2 9LA

If you are dis-satisfied with the reply given to you by our DPO, you can also contact the Information Commissioner (ICO) at:

Information Commissioner's Office,
Wycliffe House,
Water Lane,
Wilmslow,
Cheshire SK9 5AF

or by telephone on 0303 123 1113 (local rate) or 01625 545 745.