

**STEP4TRAINING CENTRE****GENERAL DATA PROTECTION REGULATION POLICY**

Step4Training Centre acknowledges its obligations to comply with GDPR and the Data Protection principles in the correct storage, disposal and other administration of any sensitive personal details it holds about its students, staff, suppliers and any other external agencies. In summary, it commits that all data held by S4T will:

- Protect any data securely and it will only be used by S4T for the service that we provide
- Not sell data or give data to a third party without prior consent from the individual
- Keep your personal information/data safe & private
- Allow individuals to request access to any information/data that we may hold and if there are any mistakes, we will correct it
- Individuals may request for information/data to be removed or erased

**0. Objective**

The objective of this policy is to protect the personal information processed by or disclosed to staff or students of Step4Training Centre (hereafter referred to as “The Centre”) or other authorised persons (all hereinafter referred to as Data Owners and Data Users) ensuring its confidentiality, integrity and availability by processing it in accordance with current legislation.

**2. Responsibilities of Staff, Students, suppliers and Authorised Third Parties****2.1 Managing Director**

On behalf of The Centre, the Managing Director is responsible for approving the GDPR policy and for ensuring that it is discharged to all members of staff. The Managing Director is also responsible for appointing, on behalf of The Centre, a Data Controller as required by the GDPR.

**2.2 Centre Data Controller**

The Centre’s designated Data Controller has the responsibility, on behalf of the Managing Director:

- To ensure that staff, students, suppliers and authorised third parties comply with the data protection principles, as set out in GDPR, in respect of personal data under his/her control;
- To ensure that The Centre’s Policy and Codes of Practice are appropriate for the types of personal data being processed;

- To ensure that The Centre maintains an up-to-date notification of its use of personal data with the Information commissioner office.
- be the focal point for the administration of all subject access requests relating to personal data held by The Centre;
- audit annually The Centre's personal data processing activities to ensure that these are in accordance with The Centre's notification with the Information Commissioner (ICO).

### **2.3 Data Owner**

A Data Owner is responsible for:

- informing the Data Controller when a new dataset has been established or if the use or purpose of data stored in a dataset, which has already been registered, has changed
- ensuring that the data is kept up-to-date and that amendments are made promptly following notification of changes.
- ensuring that the security measures are appropriate for the types of personal data being processed;

### **2.4 Data Use**

All staff, students, suppliers and authorised third parties when processing personal data about others, whether held manually or electronically, are responsible for working in compliance with the Data Protection principles.

### **2.5 Data Subject**

As Data Subjects, all staff, students, suppliers and authorised third parties are responsible for:

- ensuring that any personal information that they provide to The Centre in connection with their employment, registration or other contractual agreement is accurate
- informing The Centre of any changes to any personal information which they have provided, e.g., changes of address
- responding to requests to check the accuracy of the personal information held on them and processed by The Centre, details of which will be sent out from time to time, and informing The Centre of any errors or changes to be made.

- If staff, students, suppliers and any external third part organisation request access to any of the personal data held on file that they complete the appropriate data request form (Appendix 1)

## **2. Data Security**

It is the responsibility of all staff, students, suppliers and any third parties authorised to access The Centre's personal data sets to ensure that those data, whether held electronically or manually, are kept securely and not disclosed unlawfully, in accordance with The Centre's Data Protection Policy.

Unauthorised disclosure will usually be treated as a disciplinary matter, and could be considered as constituting gross misconduct in some cases.

## **4. Subject Consent to Processing**

The Centre will observe the conditions for processing personal information as laid down by the General Data protection regulation and with this policy

It will be assumed that consent has been given by the Data Subject for his/her personal data to be used for the purposes advised at the point of collection of that data but, where the data is defined as sensitive personal data under the Act, explicit consent must be obtained from the Data Subject by the Data User before processing can proceed.

## **5. Rights of Access to Personal Information**

The Centre respects the right of individuals to access and check the accuracy of any personal data that is being kept about them, either on computer or in a relevant filing system. Procedures for access to this data-by-data subjects and to data relating to their examination scripts and marks and confidential references are set out in S4T policies and procedures.

## **6. Publication of Centre Information**

It is Centre policy to make as much information public as possible and, in particular, the following type of information may be available to the public through The Centre's publications or otherwise by inspection:

- List of staff, their internal telephone numbers and Centre e-mail addresses
- Photographs of staff
- Photographs of students registered with The Centre
- Publication's dataset
- Academic qualifications and certifications
- Job title and grade of staff
- Research expertise of academic staff

Any individual who has good reason for wishing details in these lists or categories or other personal data to remain confidential should contact The Data Controller.

## **7. Retention of Data**

Personal data processed for any purpose shall not be kept for longer than is necessary for those purposes or as required to comply with other legislation. Personal information relating to students and suppliers will normally be kept on file for the duration of the contract specifications or archiving purposes as set out by government funded organisations.

## **8. Policy Awareness**

A copy of the Policy Statement will be given to all new members of staff and all new students on becoming members of The Centre and to newly-authorized third parties. All staff and students of The Centre and authorized third parties will be advised of the existence of this policy which will be posted on The Centre website, as will any subsequent revision of the policy. All staff, students and authorized third parties are to be familiar with and comply with the policy at all times.

## **9. Information/data held by Step4Training Centre**

Step4Training Centre are responsible for ensuring that all personal data/information held either electronically or manually is accurate, if when processing data to a third party it is identified that the data is incorrect. S4T must inform the Third Party in order that they can correct their records

## **10. Privacy Notice**

All information/data held by Step4Training Centre regarding personal & sensitive data will be shared with various external agencies, here is a list (this list is not exhaustive)

- Education & skills funding Agency (ESFA)
- Connexions
- Department of Education
- Department of Energy & Industrial strategy
- Other agencies dealing with research & statistical work that is being done on behalf of ESFA or Third Party
- Under Apprenticeship skills the Children's & learning Act 2009

Any Data Subject who considers that the policy has not been followed in respect of personal data about themselves, should raise the matter with the Data Controller.

## **11. Status of the Policy**

This policy does not form part of the formal contract of employment, but it is a condition of employment that members of staff whether freelance, self-employed or temporary will abide by the rules and policies made by The Centre from time to time. Likewise, the policy is an integral part of the Code of Conduct for Students.

Compliance with the Data Protection Regulation is the responsibility of all staff, students and authorised third parties. Any breach of the DPR may lead to disciplinary action being taken, access to Centre information facilities being withdrawn, or even a criminal prosecution. Any questions or concerns about the interpretation or operation of this policy should be taken up initially with The Centre's Data Controller.

## **12. Individual Rights**

At Step4Training Centre all individuals have the right to access or have their data/information erased Any individual who wishes to have one of these rights actioned by do the following:

- a) Firstly, complete the appropriate document 1) Appendix 1 – Access and 2) Appendix 2 – Deletion/erase
- b) Once the appropriate document has been completed, they pass it onto the Data Controller, who will have authorisation to carry out the request
- c) The report that contains the data/information will be produced in a format that is suitable for the individual and there will be mechanisms in place to ensure that only the data/information requested is provided
- d) A record will be kept with the following information – when the request was made, by whom the request was made and the date and when the request was actioned including the date it was given to the individual
- e) Once the information/data has been submitted to the individual they will sign to say that it was received and date the document
- f) If the request identified that the information was incorrect, the Data Controller will amend the information/data within 7 working days and the individual will be notified in writing that the change has been made
- g) All individuals must give at least 28 days' notice to the Data controller when making any request for information/data. Failure to do this could result in a delay of providing the information/data or in some instances result in a disciplinary as failure to follow S4T procedures
- h) If S4T refuses a request, we will inform the individual why & that they have the right to make a complaint to supervisory authority (referring to S4T complaint procedure) who will deal with the complaint with one month of the request.

### 13. Data Breach

In the event of a breach of data/information, depending on the severity Step4Training Centre will do the following:

- Carryout a full investigation of the breach, this will be done initially by the Data Controller, if the breach is considered to be serious (loss of substantial data or access to data without authorisation) then the investigation will be carried out by the Data Compliance Officer.

Managing Director: \_\_\_\_\_

Signature: \_\_\_\_\_ Date: \_\_\_\_\_

Data Controller: \_\_\_\_\_

Signature: \_\_\_\_\_ Date: \_\_\_\_\_

To be reviewed on: \_\_\_\_\_