

## Data Protection Policy

### 1. Purpose

1.1 The purpose of this Policy is to ensure compliance with the Data Protection Act 1998.

### 2. SCOPE

2.1 This Policy applies to all staff and students.

### 3. PRINCIPLES

3.1 As a Training Centre we are required to take specific measures to ensure that all information ("personal data") held about living individuals, in either paper based or computer format, is processed according to eight Data Protection Principles.

These require that personal data must be:

- Processed fairly and lawfully
- Obtained and processed for specific purposes
- Adequate, relevant and not excessive
- Accurate
- Held for no longer than necessary or required by regulations
- Processed in accordance with people's data protection rights
- Kept secure
- Transferred outside EEA only if adequate safeguards exist

The Act allows individuals to obtain a copy of their own data, usually subject to a fee being paid (education records up to a certain size must be provided free of charge); to have inaccurate personal data corrected or erased; to prevent data being used for direct marketing; to have decisions made solely by automated means reviewed manually (and other rights in connection with automated decision making); and, where appropriate, to seek redress for any unwarranted damage or distress caused.

### 4. PROCEDURES

4.1 The Centre has a legal responsibility as an institution to operate within the terms of the above Act but each member of staff or student could also have a personal liability for any unauthorized disclosure they make.

Disclosing information outside the terms of the Centre Policy could result in disciplinary action.

4.2 Disclosure Data held by the Centre may only be disclosed to third parties in the following circumstances:

#### Internal requests

To Centre employees who require the information to carry out their normal duties within the scope of their agreed roles

#### External requests

With the written authority of the student In accordance with the Centre's Fair Processing Statement(s) or Data

#### Protection Statement(s)

When required by law or statutory instruction\*

When required to prevent or detect crime\*

As a general rule, the assumption now made is that information may only be given if there is a specific authority to do so, otherwise the concept of confidentiality should apply and the enquirers request declined.

Note: Requests made under headings \* must be referred to the Centre Manager's office prior to any information being supplied to the party /authority who have made the request.

#### 4.3 Specific Obligations

##### 4.3.1 Processing personal data that is not registered is a criminal offence.

Staff and students should ensure that any data which it is proposed to process are covered by the Centre's Data Protection Notification.

In the first instance, queries should be raised with Assessors (i.e. for students - their tutors) and then with the Centre Manager.

##### 4.3.2 Any person for whom personal data is obtained should not be deceived or misled as to the purposes for which such data are held, used or disclosed.

Staff and students must ensure that an indication of the purpose(s) should appear on any form used to collect data, and, where necessary, an explanation given as to why personal data is being collected.

No unfair pressure should be used in order to obtain any personal data.

Special care must be taken when collecting sensitive personal data. When proposing to process sensitive personal data confirmation must be obtained from the Centre Manager in order to ascertain that the correct conditions for processing have been met.

##### 4.3.3 All staff and students should observe strict control measures when handling all personal data, whether in computerised or paper-based form, and whether it relates to staff, students or members of the general public.

Failure of any member of staff to inform Centre management of a computerised database could result in disciplinary action.

The holding of a College-related database (computerised or paper-based) outside the Centre (however temporarily) also falls within these restrictions.

##### 4.3.4 Great care must be taken not to disclose personal data, either intentionally or accidentally, by:

Only allowing authorised access to computers (e.g. by not disclosing passwords).

Switching off (or logging off) your computer when you're not using it.

Keeping doors to rooms containing computers and/or personal papers locked when not in use.

Preventing unauthorised information being obtained from a

computer screen.

Not disclosing personal data over the telephone.

Ensuring that the written authority of the subject individual is obtained when required.

Only disclosing personal data where you are sure that it is being given to an individual/institution who is authorised to receive it.

Preventing unauthorised information being obtained from a computer printout or other paper-based material.

Ensuring proper disposal of all paper containing personal data, including computer-based printouts.

Not removing any Centre hardware or software from the Centre without prior authorisation.

Not sending any data outside the EEA without the specific written authority of the subject individual.

Any circumstances where a decision is required on whether to disclose information should be referred in the first instance to the Centre Manager.

4.3.5. It is recognised that on occasions it is necessary for members of staff to work from home. In these circumstances, additional care must be taken with regard to the increased risk of unauthorised disclosure of personal data through theft, loss or access by family members/friends. Members of staff must recognise that the conditions enforced by the Data Protection Act within the Centre environment apply equally when working from home. Great care must be taken to ensure that any personal data removed from the Centre or accessed from management information sources (whether on laptop, USB memory key or in paper form) is kept secure from theft and viewing by unauthorised persons.

## 5. DEFINITIONS

### 5.1 Data

Data can be in computer or paper form and is any system that is a “structured set of personal data” and the records can be “centralised, decentralised or dispersed”. In effect this means all our staff/student records.

#### Personal Data

Personal data is information that relates to an individual who can be identified from that information, either by itself, or when used in conjunction with other information in – or likely to come into – possession of the Data and Information Services staff.

#### Sensitive Personal Data

Sensitive personal data is personal data that could be used to discriminate against an individual or may cause them to be treated differently from others. Specifically this is: racial or ethnic origin; political opinions; religious beliefs or other beliefs of a similar nature; trade union membership; physical or mental health or condition; sexual life; commission or alleged commission of a crime; proceedings related to the commission or alleged commission of a crime, the disposal of any such proceedings or the sentence of a court in relation to such proceedings.



**Data Subject**

The Data Subject is the living individual who is the subject of the data. This will include staff, students, contractors, suppliers, visitors and anyone else about whom we collect personal data.

**Data Information Services Staff**

The Data Information Services Staff will determine the purposes for which data is collected.

**Processing**

Processing of data is the collection, storage, use and dispersal of data.

**Third Party**

A Third Party is anybody other than the Data Subject, Data and Information Services Staff or other person authorised to process personal data on behalf of the Centre.

**Centre Manager**

The Centre Manager is responsible for maintaining the Centre's registration with the Information Commissioner's Office and providing advice and guidance to assist in ensuring compliance with the Data Protection Act.

**Centre's Fair Processing Statement**

This is included on the Enrolment form and normally on other documents used to collect data to indicate how any data provided will be processed by the Centre.

**6. IMPLICATIONS FOR EQUALITY & DIVERSITY**

This policy plays a key part in the Centre's Equality & Diversity Strategy and due care will be given when handling sensitive data.

**7. IMPLICATIONS FOR PERFORMANCE & STANDARDS**

There are no implications for Performance & Standards

**8. IMPLICATIONS FOR STAFF DEVELOPMENT OR RESOURCES**

Staff are expected to ensure they read the guidance available and are fully conversant with the requirements of this policy. Further support is available through annual updates and regular Data Protection audits and from the Centre Manager.