PROMISE TRAINING CENTRE

DATA PROTECTION POLICY

Promise Training Centre acknowledges its obligations to comply with Data Protection Act (1998) in the correct storage, disposal and other administration of any sensitive personal details it holds about its students. In summary, it commits that all student details held will be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate and up to date
- Not kept for longer than is necessary
- Processed in line with the learner's rights
- Secure
- Not transferred to other countries without adequate protection

1. Objective

The objective of this policy is to protect the personal information processed by or disclosed to staff or students of Promise Training 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 and Authorized Third Parties

2.1Managing Director

On behalf of The Centre, the Managing Director is responsible for approving the Data Protection 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 Data Protection Act 1998 (DP Act 98).

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 and authorised third parties comply with the data protection principles, as set out in DPAct98, 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 Data Protection Commissioner.

- maintain a register of the purposes for which CAUs hold datasets and relevant filing systems and to use this to maintain The Centre's notification of its processing of personal information with the Information Commissioner;
- be the focal point for the administration of all subject access requests relating to personal data held by The Centre;
- with the policy.
- 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.

2.3 Data Owner

A Data Owner is responsible for:

- informing the CAU Data Protection Co-ordinator 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 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, as set out in Appendix 2 of this policy, and working in accordance with the Code of Practice on the "Handling of Personal Data" associated with this policy.

2.5 Data Subject

As Data Subjects, all staff, students 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.

3. Data Security

It is the responsibility of all staff, students 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 and associated Codes of Practice.

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 in Schedules 2 and 3 to DPAct98 and as set out in the Code of Practice associated 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, as defined in the DPAct98. 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 the Code of Practice on Access to Personal Information associated with this policy.

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 in CAUs
- Photographs of students registered with The Centre
- Publications dataset
- Academic qualifications and honours
- Job title and grade of staff
- Research expertise of academic staff
- Publication of Research Grants and Awards
- Supervisors of Higher Degrees
- Academic achievements

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. Some forms of information will be kept for longer than others and a guide to retention time will be found in the Guidelines associated with this policy.

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-authorised third parties. All staff and students of The Centre and authorised third parties will be advised of the existence of this policy and associated Codes of Practice which will be posted on The Centre website, as will any subsequent revision of the policy. All staff, students and authorised third parties are to be familiar with and comply with the policy at all times.

9. Policy Implementation and Review

This policy is issued by the authority of the Managing Director, who has delegated the implementation of it to all staff. The Managing Director will facilitate an annual review of the policy by the Data Protection Review Group, whose members will review it for completeness, effectiveness and usability and make any recommendations for change via the Information Security Group (ISG) to the appropriate Managing Director's Committee.

10. Redress

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 employees will abide by the rules and policies made by The Centre from time to time. Likewise the policy is an integral part of the Regulations for Students.

Compliance with the DPAct98 is the responsibility of all staff, students and authorised third parties. Any breach of this Data Protection Policy 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. Definitions of the terms used in this policy and its associated Codes of Practice are given at Appendix 1 and details of the eight Data Protection Principles are set out in Appendix