RECORDS POLICY AND PROCDURE

Policy Statement

The purpose of this document is to summarise the requirements in relation to the retention of records.

All staff have to adhere to this policy as the company can face potential fines for non-compliance e.g., fines from Government bodies etc.

1. Retention

Retaining personal data for longer than the purpose for which it was collected does not comply with Data Protection legislation. To ensure compliance AET has adopted the following procedure for retaining documentation.

- Where documents are stored electronically (and securely backed up) they are not duplicated unless there are legal or regulatory reasons to do so. As a result, any paper copies of these documents can and should be destroyed.
- It is recognised that there are certain documents need to be retained / archived as paper copies.
- For specific types of documents, the following guidelines are expected to be adhered to:
  - Certificates - As a general principle, certificates are to be sent to students on passing. Where records are kept in-house, to be retained a maximum of 3 years (shorter where relevant body allows)
  - Learners records (learning agreements, enrolment forms, amendments, evidence,
  - etc.) to be kept for 3 years following course/exam completion.
  - Folders containing learners course work / assignments are to be either returned to the student or destroyed at the end of the course. NB - following learner certification records must be kept of summative assessments, X200's and the associated verification documentation for three years (shorter where awarding bodies allow). Such records include assignment briefs, marking criteria, IV records, Marks, BTEC front sheets. It is acceptable to retain this data electronically. Note that this does not mean retaining learner work, which should be disposed of as soon as the learner has received their certificates.
  - All other records should not be archived but should be destroyed at end of course.

2. Archiving

All documents to be stored should be placed in an archive box and clearly marked at both ends with the following information:

- Brief description of contents
- Date of archiving (i.e., the current date)
- Date for destruction. This is expected to be in line with the above guidelines.

3. Deletion/Erasure

All documents in hard copy will be security shredded. All electronic format documents will be removed from our computers and all backup data removed in line the retention guidelines above.

4. Data Breaches

Data security breaches include both confirmed and suspected incidents. An incident is an event or action which may compromise the confidentiality, integrity or availability of systems or data, either accidentally or deliberately.

An incident includes but is not restricted to, the following:

- loss or theft of confidential or sensitive data or equipment on which such data is stored (e.g., loss of laptop, USB stick, iPad / tablet device, or paper record).
- equipment theft or failure.
- system failure.
- unauthorised use of access to or modification of data or information systems.
- attempts (failed or successful) to gain unauthorised access to information or IT system(s).
- unauthorised disclosure of sensitive / confidential data.
- website defacement.
- hacking attack.
- unforeseen circumstances such as a fire or flood.
- human error.
- 'blagging' offences where information is obtained by deceiving the organisation who holds it.

4.1 Reporting an incident

Any individual who accesses, uses, or manages the Company's information is responsible for reporting data breach and information security incidents immediately to the Director.

5. Investigation

An investigation will be undertaken by the Director immediately and wherever possible, within 24 hours of the breach being discovered / reported. The risk associated with it will be assessed, for example, the potential adverse consequences for individuals, how serious or substantial those are and how likely they are to occur.

6. Notification

6.1 The Director will establish whether the Information Commissioner's Office will need to be notified of the breach, and if so, notify them within 72 hours of becoming aware of the breach, where feasible.

6.2 Individuals whose personal data has been affected by the incident, and where it has been considered likely to result in a high risk of adversely affecting that individual's rights and freedoms, will be informed without undue delay. Specific and clear advice will be given on what they can do to protect themselves and include what action has already been taken to mitigate the risks.

6.3 A record will be kept of any personal data breach, regardless of whether notification was required.