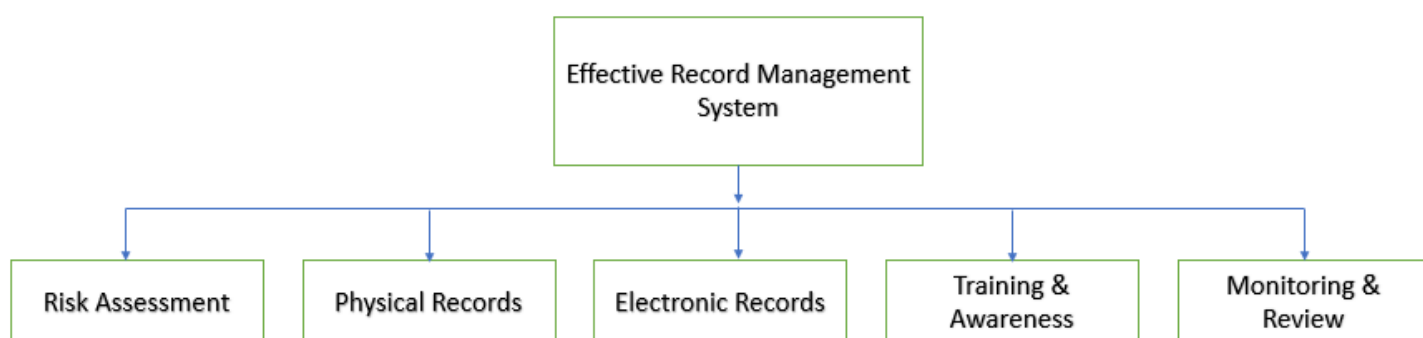




Policy No.:	P006
Name of Policy	Record Management Policy
Date of issue:	October 2022
Status:	Approved
Responsibility for policy:	Administration
Responsibility for implementation:	Office Manager



Overview

As part of our corporate governance responsibilities, our Record Management Policy is both for purposes of accountability and as a working document for staff.

IEU supports effective record keeping by:

- clear allocation of responsibilities for record management among staff;
- provision of clearly defined job descriptions outlining responsibilities in this area;
- effective support for good record management through investing in appropriate systems training;
- recruitment, where relevant on competencies and experience related to record management.

Governing Principles

We are committed to a record management system and practice which ensures corporate information, learner data, results and assessment records are:

- secured safely
- accurate and relevant
- up-to-date
- clearly organised using a commonly understood system
- accessible
- manageable for staff
- subject to clear guidelines on preservation

Key areas of practice

1. Security

- We ensure sensitive records such as learner data, results information, assessment material and examination scripts are managed securely, using the latest secure software and a clear system of password controls.
- We ensure all data is backed up on a secure external server and on storage devices which are then safely stored.
- We have clear audit trails used to manage records, for example in the development of examination scripts. Staffs are given different permissions in accessing records depending on their agreed roles and responsibilities.
- We recognise the use of USBs present a risk in terms of data security. We therefore limit the use of USBs and ensure they are encrypted.

2. Physical preservation/storage

IEU is responsible for storing its own records that are both of archival and of no Archival value. We store archival files in conditions that fully meet 'best practice' standards. We realise climatic conditions (such as temperature and relative humidity) could lead to deterioration of the records. Security controls and fire control systems are also areas taken into consideration.

Our on-site storage for both active and non active records is sufficiently secure. Electronic discs are kept in a room where temperatures are moderate and stored in a cabinet for security.

3. Preservation of electronic records

System back-ups of data are designed to provide another copy in the event of loss of data in the short/long-term and to provide physical maintenance of the records. These are not seen as spare copies but maintained as records that need to be treated accordingly, and managed over time. This includes web-site versions that are permanently preserved for future access.

We conduct an annual review on the management of hardcopy and softcopy records, and are mindful of the need to preserve records from any form of corruption/obsolescence.

4. Training and awareness raising

Another element of IEU 's approach to record management is an emphasis on training and development. We ensure all staff have the necessary training to use our IT systems effectively and manage hard and soft copy records in accordance with IEU guidelines and policy.

During assessment periods, IEU hires temporary data entry staff. To manage risks we ask temporary staff to save records into a temporary/transaction file. Permanent senior staff is then responsible for uploading records into the master files.

5. Monitoring and Review

We regularly monitor and evaluate our approach to record management. These reviews focus on ensuring we have effective controls in place (password protection for example) for high risk areas of record management system.

Other

(i) IEU Data Categories

In order to fulfil our assessment role and to function efficiently as an organisation, IEU has to hold and process a variety of personal data, which falls under four main categories, as follows:

- a. **Examinations** - assessment data, examination results, transcripts
- b. **Staff** – hourly rates, training and development needs, references, CVs, copies of qualifications.
- c. **Learner personal information** – exam numbers, contact details, reasonable adjustments, and examination disciplinary issues.
- d. **Center Information** – Center head contact details, Center disciplinary action, learner numbers, invoices, end of programme questionnaire, invigilation comments, incident reports, examination results, qualifications offered and annual reports.

The above examples are by no means exhaustive

Candidate records include the following information

- i. Exam registration details – examination application forms, educational qualification, learner photos
- ii. Candidate Examination Results
- iii. Reports/assessments in the area of special needs (Reasonable Adjustments / Special Considerations)
- iv. Serious accidents/incidents

(ii) Access to Records

The following will have access to records:

- a. Authorised members of staff
- b. Regulatory staff Under the Data Protection Acts 1988 and 2003
- c. Under the discovery process in legal proceedings

However, IEU reserves the right to refuse access to a record in exceptional circumstances, for example, a report on a candidate's record that includes details of a particularly sensitive family matter etc.

(iii) **The preservation of examination results and assessment material**
Electronic examination results will be retained indefinitely by IEU. Other information including assessment material produced by learners will be destroyed in a proper manner after an appropriate period as per IEU paper records retention policy outlined in IEU Management Handbook.

All personnel will be issued clear guidelines on their responsibilities in relation to the creation, maintenance, security, access and destruction of the records under their care. Staff will also be made aware of the statutory obligations in relation to the keeping of records.

This policy will be monitored and evaluated on a regular basis and will undergo a complete review five years after its implementation or after the implementation of any subsequent version of the policy.

(iv) **Data Protection Acts 1988 and 2003 (UK), FTCA 15 US Code 41, other US Federal privacy Laws, and Privacy Laws contained in The Constitution of Delaware 1897.**


The duties of IEU come under the eight data protection principles. Accordingly, we undertake to

1. Obtain and process the information fairly.
2. Keep it only for one or more specified and lawful purposes.
3. Process it only in ways compatible with the purposes for which it was given to initially.
4. Keep it safe and secure.
5. Keep it accurate and up to date.
6. Ensure that it is adequate, relevant and not excessive.
7. Retain it no longer that is necessary.
8. Give a copy of the candidate personal data on request.

IEU has a duty to treat all personal information held as confidential and will not disclose such information to third parties e.g. marketing organisations. Even within IEU itself, not all data is shared by across functional units. For example, the financial details of a candidate in relation to exam fees are a matter for the payments office and should not be exchanged with other members of staff. It is also IEU's policy to share personal information within the organisation only when it is strictly relevant.

Staff are made aware of the need to maintain confidentiality with regard to records and data to which they have legitimate access. Disclosure of such information outside the organisation will give rise to disciplinary action. However, there will be situations when personal information will need to be shared with other agencies; for example, in cases involving the police or other lawful authorities.

Approved October 4, 2022


Robert Clarke, CFA, PhD



Office of the President