Information Security Policy

Definition

The use of the term “institution” is in reference to the following organization: Empire Education Corp. and Mildred Elley College.

Purpose

The purpose of this policy is to safeguard information belonging to the institution and its stakeholders (third parties, clients or customers and the general public), within a secure environment.

This policy informs the institution’s staff, students, and other individuals entitled to use institution facilities, of the principles governing the holding, use and disposal of information.

It is the goal of the institution that:

- Information will be protected against unauthorized access or misuse.
- Confidentiality of information will be secured.
- Integrity of information will be maintained.
- Availability of information / information systems is maintained for service delivery.
- Business continuity planning processes will be maintained.
- Regulatory, contractual and legal requirements will be complied with.
- Physical, logical, environmental and communications security will be maintained.
- Infringement of this policy may result in disciplinary action or criminal prosecution.
- When information is no longer of use, it is disposed of in a suitable manner.
- All information security incidents will be reported to the Director of Information Technology, and investigated through the appropriate management channel.

Information relates to:

- Electronic information systems (software, computers, and peripherals) owned by the institution whether deployed or accessed on or off campus.
- The institution’s computer network used either directly or indirectly.
- Hardware, software and data owned by the institution.
- Paper-based materials.
- Electronic recording devices (video, audio, CCTV systems).

Policy

The institution requires all users to exercise a duty of care in relation to the operation and use of its information systems.

1. Authorized users of information systems

   With the exception of information published for public consumption, all users of institution's information systems must be formally authorized by appointment as a member of staff, by enrolment as a student, or by other process specifically authorized by the Human Resources Department. Authorized users will be in possession of a unique user identity. Any password associated with a user identity must not be disclosed to any other person. The "Network password policy" describes these principles in greater detail.

   Authorized users will pay due care and attention to protect institution information in their personal possession. Confidential, personal or private information must not be copied or transported without consideration of:
   - permission of the information owner
   - the risks associated with loss or falling into the wrong hands
   - how the information will be secured during transport and at its destination.

2. Acceptable use of information systems

   Use of the institution's information systems by authorized users will be lawful, honest and decent and shall have regard to the rights and sensitivities of other people. The detail of acceptable use in specific areas may be found in the list of subsidiary policies detailed in the Appendix.

3. Information System Owners

   Institution Directors who are responsible for information systems are required to ensure that:

   I. Systems are adequately protected from unauthorized access.
   II. Systems are secured against theft and damage to a level that is cost-effective.
   III. Adequate steps are taken to ensure the availability of the information system, commensurate with its importance (Business Continuity).
   IV. Electronic data can be recovered in the event of loss of the primary source. I.e. failure or loss of a computer system. It is incumbent on all system owners to backup data and to be able to restore data to a level commensurate with its importance (Disaster Recovery).
   V. Data is maintained with a high degree of accuracy.

VI. Systems are used for their intended purpose and that procedures are in place to rectify discovered or notified misuse.
VII. Any electronic access logs are only retained for a justifiable period to ensure compliance with the data protection, investigatory powers and freedom of information acts.
VIII. Any third parties entrusted with institution data understand their responsibilities with respect to maintaining its security.

4. Personal Information

   Authorized users of information systems are not given rights of privacy in relation to their use of institution information systems. Duly authorized officers of the institution may access or monitor personal data contained in any institution information system (mailboxes, web access logs, file-store etc).

5. Individuals in breach of this policy are subject to disciplinary procedures (staff or student) at the instigation of the Dean/Director with responsibility for the relevant information system, including referral to the Police where appropriate.

   The institution will take legal action to ensure that its information systems are not used by unauthorized persons.

Ownership

The Director of Information Technology has direct responsibility for maintaining this policy and providing guidance and advice on its implementation.

Information system owners are responsible for the implementation of this policy within their area, and to ensure adherence.

Appendix: Subsidiary Policies

The detail of acceptable use in specific areas may be found in the following list of subsidiary polices:

1. Acceptable Use policy
2. Computer Password Policy