



ACCEPTABLE USE OF TECHNOLOGY (AUT-04)

TABLE OF CONTENT

CHANGE HISTORY	3
INTRODUCTION	4
OVERVIEW	5
PURPOSE	5
SCOPE	5
DEFINITIONS	5
1. Ownership and Responsibilities	6
2. Security	7
3. Privacy	8
4. Prohibited Users	9
ENFORCEMENT	10

CHANGE HISTORY

Revision	Chapter	Description of Change	Date
1	All	Update of Handbook	01/02/2016
2	All	Update of Handbook	30/06/2018
3	All	Update of Handbook	30/07/2019
4	All	Update of Handbook	30/09/2020

INTRODUCTION

AIM	To set out the EIMF policy in relation to the acceptable use of technology.
RELATED POLICIES	Computer Usage Policy
APPROVED BY	Directors
DATE OF APPROVAL	July 2019
NEXT REVIEW DATE	July 2020
DISTRIBUTION	All staff via Shared Drive and all learners via email and notice board at EIMF.
APPLICABLE TO	All learners and staff.

OVERVIEW

EIMF provides and maintains information technology resources to support its training programs and administrative operations. These resources are provided to all EIMF employees, students, and authorised guests. EIMF seeks to ensure the integrity of information technology resources made available to prevent disruption to learning and administrative needs.

PURPOSE

This policy is intended to protect the users of EIMF information technology resources by ensuring a reliable and secure technology environment that supports the educational mission of xxx. The purpose of this policy is to provide guidelines for the appropriate use of information technology resources at EIMF and establish sanctions for violations of this policy. This policy is not intended to inhibit the culture of intellectual inquiry, discourse and academic freedom.

SCOPE

This policy applies to all EIMF employees, students and any other individual that is granted access to the information technology resources owned, managed, leased or otherwise provided by EIMF.

DEFINITIONS

EIMF employees: for the purpose of this document, includes all delivery, administrative staff, support staff, contract and temporary workers, and hired consultants.

Information Technology Resources: refers to all computer and communication facilities, services and resources, including but not limited to networking devices, telephony equipment, email services, wireless devices, computers, workstations, servers, and any associated peripherals and software that are owned, managed, maintained, leased or otherwise provided by EIMF.

Members: for the purpose of this document, includes the EIMF employees (as described above) and the Institutes clients.

1. Ownership and Responsibilities

EIMF owns and maintains the information stored in its information technology resources, and limits access to authorised users. Users of information technology resources have a responsibility to properly use and protect these resources, respect the rights and privacy of other users, and behave in a manner consistent with any law and regulation, as well as any EIMF policy. Information technology resources, including Internet bandwidth, are shared among its members and clients, and users will utilise resources with this understanding.

Users must respect all intellectual property rights, including any licensing agreements, applicable to information and resources made available by EIMF to its members and clients.

Any behaviour or activity that alters the normal functioning of the information technology resources or negatively impacts their use by any other member is strictly prohibited. EIMF retains the right to take any reasonable action necessary to protect the integrity and security of its information technology resources, to curtail illegal use of the resources, to ensure the resources are equitably shared, and to protect the rights and privacy of its users.

Information technology resources are provided to support the work of the learners and staff, therefore EIMF bears no responsibility for the loss of any non-EIMF information stored or located on any system.

EIMF reserves the right to make unannounced changes to the infrastructure or accessibility of any information technology resources in case of system instability or suspicion of possible criminal activity.

EIMF does not systematically monitor communications or files and cannot reasonably be aware of, or responsible for, material which members may post, send or publish using its network, servers, and other resources including the Web. However, EIMF is committed to educating the members in the responsible use of information technology resources and will respond as appropriate when notified of violations of this policy.

This policy has been approved by the Executive Management Team.

2. Security

EIMF seeks to protect the security of its information technology resources and of users' accounts, and to prevent unauthorised access by others.

Users of EIMF information technology resources have a responsibility to protect the confidentiality of the information to which they have access. Users shall only access information technology resources to which they have authorisation and shall protect the privacy of passwords and accounts to prevent unauthorised access by others. Users shall not use EIMF resources intentionally to distribute viruses or other items that have a destructive or deceptive nature, and shall not interfere with the use of information technology resources, alter, disable, or circumvent those resources, or use those resources in a manner not authorised by EIMF. Unauthorised access by any member of the EIMF members to any information technology resources will result in disciplinary action, up to and including termination, expulsion and/or legal action.

3. Privacy

EIMF strives to protect the privacy of this information, although it cannot guarantee confidentiality. Under certain circumstances, it may be necessary to disclose information in response to court orders or other legal action, disciplinary processes, health and safety emergencies or to protect the integrity of information technology resources. EIMF retains the right to use its discretion in reviewing and disclosing records in order to comply with these requirements.

Some data is protected by data protection legislation. EIMF seeks to fulfil its legal obligations in protecting any personally identifiable information managed on information technology resources. In addition, EIMF seeks to protect any additional confidential or sensitive information at its own discretion.

4. Prohibited Users

Use of another individual's account or other misrepresentation of one's identity via electronic means is strictly prohibited.

Users are prohibited from adding, removing or modifying equipment comprising the information technology resources at EIMF unless they have been explicitly authorised to make such changes by the Head of EIMF.

Users shall not add, delete or otherwise modify data in EIMF information technology resources unless authorised to do so. The system administrators facilitate authorised access; authorisation is determined by the Head of EIMF.

Users are prohibited from using information technology resources in a manner that is construed by another as hateful, threatening or harassing, or that otherwise might contribute to the creation of a hostile academic or work environment.

Users of EIMF information resources are expressly prohibited from engaging in any political activities or engaging in any personal commercial activity.

EIMF reserves the right to determine other prohibited activities not identified in this document.

ENFORCEMENT

Failure to comply with any of the above policies may result in suspension or termination of network services, appropriate disciplinary action, and termination in the case of employees or expulsion in the case of learners.