

Policy: **Appropriate Use of Technology Resources**

Code: **07HS04**

Reviewed/ Revised: **28/07/2022**

Date of Next Review: **February 2024**

Policy Owner: **Assistant IT Manager**

Target audience: **All EAHM Students, EAHM Staff and Faculty members**

PURPOSE:

Computing and network resources are provided to The Emirates Academy of Hospitality Management (EAHM) community for educational, research and professional purposes. Misuse of these facilities interferes with the legitimate and necessary functions of EAHM. This policy describes inappropriate use of computing and network facilities and how misuse is handled.

SCOPE:

This policy applies to all members of EAHM community, including students, Faculty, and staff.

The policy covers all hardware, software and networking facilities provided by EAHM.

DEFINITIONS:

In this context, **“student”** includes full- and part-time degree students and exchange students, as well as participants in short courses and professional development. Access rights to computing and network facilities differ with the type of student but the guidelines for use are the same for all users.

POLICY STATEMENT:

Appropriate use

Appropriate use of computing and networking resources include instruction, independent and classroom study, professional research, communication and official work for students, Faculty and staff. For staff, personal email and limited activities related to job seeking or personal study are also acceptable but are subject to monitoring and limitation by line managers.

Authorized users:

Authorized users are currently Faculty, staff, and students (including Professional Training & Development students) of EAHM only. External visitors to the library may use designated computers to access the internet under supervision of library staff. Same applied to the use of classrooms and all included equipment e.g., Projector, workstation, presenter, printer, etc.

A user must be specifically authorized to use a particular computing or network resource by EAHM unit responsible for operating the resource. Computer systems are protected by access controls to ensure that only authorized users have access. This access is restricted to only those capabilities that are appropriate to each user, as specified by an individual’s department head.

Sharing of access

Login accounts are assigned to individual users and must not be shared with others. You are responsible for any use of your own account. However, generic account can be used by multiple users but with basic access and should not be shared without an EAHM representative’s approval.

Termination of access

When a user changes status, terminates employment, graduates, retires or changes position, the individual’s department head is responsible for notifying the IT Department of the

necessary disabling and enabling of accounts. A user may not use facilities, accounts, access, privileges or information for which he/she is not authorized.

When a staff member leaves EAHM, all hardware must be returned, accounts must be disabled but kept in the system for reference purposes required by the staff line manager.

Unauthorized network or file access

Users of computing and network facilities may not

- damage computer systems, for example by hacking or intentionally infecting the system with a virus
- gain unauthorized access to systems
- share passwords with other users
- deprive another user of authorized access.
- remove or install software without approval of the IT Department.
- change the configuration of systems or set-up
- use EAHM computing resources for unauthorized monitoring of electronic communications.
- use EAHM computing or network resources in connection with outside work or for the benefit of organizations not related to The Emirates Academy of Hospitality Management or Jumeirah.
- Use EAHM computing resources to communicate confidential or proprietary information, or trade secrets

Unauthorized use of hardware

Users of computing and network facilities owned by the campus may not

- Move a computer
- Move a printer
- Connect or disconnect items of equipment.
- intentionally damage a computer, printer or associated equipment
- Computers that belong to classrooms should not be taken outside the class unless there is an official approval from the IT department.
- Students should not take any EAHM computer outside the campus unless it is officially loaned by the IT department.
- Connected cables should not be disconnected without advice from an IT staff.

Privacy (Applicable to all)

To the greatest extent possible the EAHM IT department seeks to preserve user privacy. All records and files maintained by EAHM are confidential and remain the property of EAHM. All content residing on the system is subject to inspection by the IT Department. Personal information is subject to inspection if stored on the EAHM network/Shared folders.

EAHM reserves the right to access the contents of any messages sent over its facilities if it believes, in its sole judgment, that it has official need to do so. If for example IT administrators discover that circulation of a large file through the network by email is slowing down network transmissions generally, they will investigate until they discover the source of the file.

Unauthorized individuals are prohibited from looking at, copying, altering or destroying anyone else's files.

The ability of an unauthorized user to access a file or other information does not imply permission to do so.

Password policy (Applicable to all)

- Choose a secure yet memorable password. Passwords such as “password” and “1234” should not be used. It should be something like “changeme!199”.
- Avoid gibberish or bizarre character combinations. Combinations such as dfTe#2) might be hard to guess but are also very difficult to remember and are not encouraged.
- The password should be a minimum of eight characters and should include symbol, numbers and letters.
- Do not change the password too often, if passwords are changed too often users are more likely to forget them.
- Under no circumstances is a user allowed to give away their passwords to another user, including EAHM students, staff, Faculty, or any other third party.
- A password must be changed immediately if it is suspected that it has become known to others.
- Do not keep on trying a wrong password more than twice, if that happened, please refer to IT Department immediately in order to avoid accounts suspend.
- To change the password, press on (CTRL+ALT+DEL) then choose “Change password” from the list, to know the password criteria please refer to the first point.
- Users may contact the IT department if faced any challenges in changing the password.

Harassment (Applicable to all)

The following constitutes computer harassment:

- Intentionally using the computer to annoy, harass, terrify, intimidate, threaten, offend, or bother another person by conveying demeaning, defaming, sexually suggestive or obscene language, pictures, or other materials.
- Intentionally using the computer to disrupt or damage the academic, research, administrative, or related pursuits of another.
- Intentionally using the computer to invade the privacy, academic or personal pursuits of another, or threatening to invade someone’s privacy.

Copyright (Applicable to all)

All members of EAHM community are prohibited from using, inspecting, copying, storing and redistributing copyrighted programs, CD ROMs, web-based resources or any other material in violation of UAE and international copyright, trademark or patent laws. Failure to observe copyright or license agreements may result in disciplinary action by EAHM and legal action by the copyright owner.

Unlicensed software / Personal software (Applicable to all)

No software may be installed, copied or used on EAHM computer systems unless properly licensed. Installation of personal software will be subject to the IT Manager’s approval and will be carried out by the IT Department only if licensed and compatible with the operating system in use.

The user will have to sign an agreement stating that the software/drivers have been installed on personal request and the IT Department will not bear any responsibility for loss, damage or the non-functionality of the device after installation.

Any damage caused to the computer due to personal software will be the sole responsibility of the user.

Use of licensed database resources

The EAHM Library subscribes to a wide range of licensed electronic resources for the academic purposes of EAHM community. By the terms of the licenses, only authorized, current The Emirates Academy of Hospitality Management students and Faculty may use these resources. Login details and passwords may not be given to anyone outside EAHM. Jumeirah colleagues and EAHM Alumni may not access the licensed databases although library staff may perform searches on their behalf.

Students and Faculty must observe United Arab Emirates (UAE) and international copyright law in their use of licensed electronic resources.

Confidentiality (Applicable to IT staff)

Information about The Emirates Academy of Hospitality Management network setup, IT structure, and its employees, customers, suppliers and vendors are to be kept confidential, and divulged only to individuals within the company who need and are authorized to receive such information.

If in doubt whether information should be divulged, or not discuss the situation with your manager.

Under no circumstances can any member of staff disclose or give away the EAHM administrator or local administrator passwords.

For vendors there is a separate login ID and password available to access required systems after signing the Non-Disclosure Agreement.

Help desk policy (Applicable to IT)

Under normal operations, support will be given on a first come, first served basis and problems will be solved as soon as possible.

The following ranking scheme should be used to categorize priorities for assistance. During extraordinary situations, such as a natural disaster, prolonged power outage, or other disasters, contact and resolution time may be longer.

Priority	Problem	Contact	Resolution
A	Highest importance- Mission critical systems with a direct impact on the organization,	Immediate	30 minutes
B	Single user or group outage that is preventing user(s) from working (Examples: Classroom malfunction during a session, Failed OS or Hard disk, Login errors)	10-15 minutes	1 hour
C	Problems that can be permanently or temporarily solved with a work around (Examples: PDA sync, PC sound problem, Printer error)	30 minutes	Same day
D	Scheduled work (Examples: New desktop installation, office move and clean-ups, software installation, scheduled events)	1 hour	1-3 days

The help desk is available from 0900hrs to 1800hrs.

Users can request support in any of the following ways:

- Send an e-mail to EAHMITHelpdesk@emiratesacademy.edu
- Call the IT helpdesk on +971 4 315 **5111** to speak with an IT Specialist or leave a voice mail message
- Pass by the IT office in Phase I building – Student Service Centre of EAHM on the first floor
- Call Mobile **+971 55 1000 216** to speak to the IT Specialist on duty or to leave a voice mail message if immediate assistance is required

IT support is available outside these hours for urgent requests only. We consider a request urgent only if without immediate assistance EAHM would lose money or would cause significant customer dissatisfaction. Students cannot log calls after these hours.

Internet and use of external email

Internet and external email is provided to users for official work and to obtain information related to work /studies.

Users must not

- Use these facilities for purposes that are illegal, unethical, harmful to EAHM or Jumeirah, or non-productive.
- No user, including students, staff and Faculty, may send or forward chain emails, or browse or transmit any content that is offensive, illegal or harassing.
- Users cannot conduct personal business using EAHM/Jumeirah resources, including telephone, fax and computer networks.
- Program downloads from the Internet are not permitted unless specifically authorized by the IT Department.

The responsibilities of users are to

- Ensure that communications are for professional reasons and do not interfere with productivity.
- Be responsible for the content of all text, audio, or images that sent over the Internet.

RESPONSIBILITY:

The IT Manager is responsible for investigating initial violation reports and for bringing them to the attention of the Director of Operations.

The IT Manager is responsible for ensuring that this policy is kept up to date and is reviewed according to the agreed schedule.

IMPLEMENTATION OF THE POLICY:

Misuse or alleged misuse involving harassment using computing and network resources is handled according to EAHM **Bullying and harassment Policy 06ST27**.

Infringement of copyright using computing and network resources is handled under EAHM **Copyright and Intellectual Property Policy 10LP03**.

Misuse of computing or network resources by EAHM staff is handled under HR disciplinary policies.

HOW TO REPORT A VIOLATION

EAHM Students, Staff and Faculty are to report any suspected violation of the policy to the IT Manager within two days via email. A full description of the behaviour should be given, including proof if available.

When an offense is identified by a member of the IT Department, it should be referred to the IT Manager.

PROCESS

In either case, the IT Manager will investigate and determine whether there is evidence of an offense having been committed. If such evidence is found, or if one or more credible witnesses attest to having seen the alleged misconduct, the IT Manager will bring the case to the attention of the Director of Operations.

As a first step the Director of Operations and the IT Manager will meet with the accused. The case may be resolved, and sanctions imposed at this stage, if

- The accused is a first-time offender
- There is no damage to property or the reputation, of EAHM or Jumeirah, and no harm to others or their property

- The offender confesses:
- The offense does not contravene UAE or international law

Sanctions for minor offenses may include one or more of the following:

- A warning letter to the student's file
- A fine or "service charge" for IT staff time needed to deal with consequences of the offense
- Temporary suspension of computing or network privileges

The Director of Operations and IT Manager may decide to convene the Disciplinary Committee to deal with the instance of misconduct. The Committee will hold a hearing within five working days of receipt of the violation report and will tender its decision within 2 working days of the hearing. The accused may produce his or her own evidence and witnesses at the hearing and may be accompanied by a proponent from within EAHM (a friend, personal tutor, etc.).

The Disciplinary Committee will decide and will assign sanctions if the accused is found to be guilty. Sanctions for serious computing and network misuse may include one or more of the following, or other appropriate penalties:

- A warning letter to the student's file.
- A fine or "service charge" for IT staff time needed to deal with consequences of the offense, or to pay for repair to damages caused as a result of the misconduct.
- Probation status, meaning that subsequent misdemeanours of any type will receive full sanctions.
- "Community service", e.g., a specified number of hours helping in the library or working with the cleaners or gardeners.
- Temporary suspension of computing or network privileges.
- Suspension for a Trimester.
- Expulsion.

The accused has the right to appeal the committee's decision and/or sanctions once. A written appeal must be submitted to the Dean within 10 working days of receipt of the Disciplinary Committee decision.

The Dean or Managing Director will consider a written appeal and will make a final decision.

ASSOCIATED DOCUMENTS:

- 06ST13 EAHM Student Discipline
- 06ST27 Bullying and harassment
- 10LP03 Copyright and Intellectual Property

MENTIONS:

- Student Handbook
- Catalogue
- EAHM Policy and Procedure Handbook

DATE OF NEXT REVIEW:

This document should be reviewed by **February 2024**.

