



The Petroleum Institute

Student's IT Policy

TABLE OF CONTENTS

Policy Statement And Purpose	3
Who Should Read And Follow This Policy	3
Related Documents.....	3
Policies And Guidelines.....	4
Student Acceptable Use Policy	4
Network Data Storage Policy	5
Student-Owned Technology Policy.....	5
Printing Policy	5
Prohibited Actions.....	5
Computing Lab Policies	6
Prohibited Actions.....	6
Computer Open Labs Schedules	6
Confidentiality And Privacy Policies.....	6
Actions Taken For Policy Violations	7
Contacts.....	8
Definitions	9



POLICY STATEMENT AND PURPOSE

The Petroleum Institute (PI) provides extensive computing and network communication services to registered students. Information Technology services are part of the campus infrastructure and their purpose are to support the institute's academic service missions. These policies apply to all computing and network communications equipment within the PI campus.

WHO SHOULD READ AND FOLLOW THIS POLICY

The student IT Policy (including the UAE information Technology Crimes Law) applies to all registered students of the Petroleum Institute.

RELATED DOCUMENTS

UAE Information Technology Crimes Law attached.

POLICIES AND GUIDELINES

STUDENT ACCEPTABLE USE POLICY

1. You are the only person who can use your assigned IT resources.
 - Never give your password to anyone, even people you trust, such as your friends or relatives or someone who has offered to help fix a problem.
 - You are responsible for all charges accrued using the computing account or computing resources assigned to you, even if a friend using your account without your permission runs up the charges.
 - You will also be held responsible for activities done by someone to whom you gave access.
 - You are responsible for the security of your computer accounts, including the changing of passwords on a regular basis.
 - The password expires automatically every 45 days, a time interval that is enforced by IT policy and subject to be changed.
 - If you forget your password, you should present your ID card to the authorized personnel.
 - No password is given through telephone, external email, fax, etc.
2. You may not promote commercial activity or make any profit from the use of PI provided computing resources or from any output produced using them.
3. Never use any PI provided computing resource to do illegal, threatening, or deliberately destructive activities not even as a joke. All complaints will be investigated. Violations can result in disciplinary action, criminal charges, or both. The police and the Directorate Security investigate violations of Emirate or Federal Law.
 - Never intentionally install any malicious code on the PI network.
 - Never intentionally be involved or use any hacking methods, including flooding, ping attacks (ICMP attacks), or other denial of service attacks.
 - Never destroy, modify, damage hardware, software, or any IT-related equipments.
 - You are only allowed to connect your PC or laptop in the authorized PI campus connection points.
 - Ignorance is no excuse. For more information, refer to U.A.E Information Technology Crimes Law.
4. Be careful of copyright infringement. Copyrighted materials include, but are not limited to, computer software, audio and video recordings, photographs, and e-books. It is a violation to use PI computers to copy, display or distribute copyrighted materials such as software, MP3 files, or MPEG files illegally.



5. Never try to get around login procedures on any computer system or otherwise attempt to gain access where you are not allowed. Such activities are not acceptable under any circumstances and can result in serious consequences, including disciplinary action.

NETWORK DATA STORAGE POLICY

1. Network drive space is an institutional resource provided for the purpose of storing academic-related documents and files.
2. The institution's responsibility for managing students' network drive space includes setting quotas and maintaining data availability.
3. Students have a responsibility for managing this space, which includes deleting non-essential or obsolete files to keep space utilization at a minimum.
4. Never store your data on the local hard disks. The IT department will not be responsible for any loss of data stored on local hard drives.

STUDENT-OWNED TECHNOLOGY POLICY

1. The IT Department will provide assistance to on-campus students connecting personal computers to the campus network. The IT Support Team does not repair faulty student-owned equipment, software, or operating system files.
2. Students are responsible for keeping personal computers virus-free. Students who are knowingly or unknowingly propagating viruses on the network will be disconnected from the campus network.

PRINTING POLICY

The IT department recognizes that students need to print in the course of doing academic work. The IT department also recognizes its responsibility to discourage waste and to reduce some of the cost of printing on campus.

PROHIBITED ACTIONS:



1. Printing material that is offensive to others.
2. Printing material for business-related purposes or financial gain.
3. Removing paper jams, using the printer console and turning printer off.
4. Using the manual feed tray to print special documents (labels, envelopes, etc.) without IT assistance.

Ask for IT assistance if you need to have any special printing requirements or face any printing problems.

COMPUTING LAB POLICIES

Computing and Network Services provides IBM-compatible microcomputers and high-speed laser printing. There are several Computer Open Labs available on male and female campuses for free use by PI students, faculty, and staff. The software on the PCs is only available on the lab workstations.

Some PI academic departments have private computing labs and other resources such as scanners and laser printers. These labs are usually reserved for students majoring in the departments' courses of study.

PROHIBITED ACTIONS:

1. Equipment use is restricted to students with a valid Petroleum Institute ID.
2. Students exhibiting disruptive or destructive behavior will be asked to leave the facilities.
3. "No Food and Drink" policy is applied in all computing labs.
4. Non-academic computing activities are prohibited in all labs. Umm Al Nar Club's Cyber Café is dedicated for all non-academic activities.

COMPUTER OPEN LABS SCHEDULES:

1. Labs are available during specific operating periods. Those periods are usually posted on each lab entrance.
2. Opening times might be subject to change, an email notification will be sent to students at an earlier time.
3. All labs are closed during official holidays and maintenance periods.
4. These labs have a priority for student orientations, special events, or other academic courses without previous notification.

CONFIDENTIALITY AND PRIVACY POLICIES



In general, the PI regards information stored on network drives and email as confidential. E-mail and data stored on PI network of computers may be accessed by the Institute for the following purposes¹:

1. Investigating reports of violation of this policy, local or federal law.
2. Complying with legal requests for information.

ACTIONS TAKEN FOR POLICY VIOLATIONS

Punishment for infractions includes, but is not limited to:

- verbal warnings
- revocation of access privileges
- warning letter
- suspension/termination from PI
- criminal prosecution

If your activity breaks the law, you can be prosecuted. Even if you are not charged criminally, you can still be suspended or terminated from the PI.

The PI reserves the right to protect its electronic resources from threats of immediate harm. This may include activities such as disconnecting an offending computer system from the campus network, terminating a running job on a computer system, or taking other actions.

If you are unsure whether an action you are considering is an acceptable use of electronic resources, contact us before you act. Representatives from IT department will be glad to work with you to prevent problems.

¹ The system administrator will need specific approval from the IT manager or the appropriate designee to access these items. The extent of the access will be limited to what is essentially necessary to acquire the information.



CONTACTS

For more information please contact the IT Department through helpdesk@pi.ac.ae or visit our IT offices.



DEFINITIONS

Email Account An email account issued by the PI, which is based on a person's first name, middle initial, and last name, and ends in the domain name "pi.ac.ae".

Computer Resource Any physical or virtual component of limited availability within a computer system

Malicious Code Includes all and any programs (including macros and scripts) which are deliberately coded in order to cause an unexpected (and usually, unwanted) event on a user's PC.

Newsgroup A repository usually within the Usenet system, for messages posted from many users at different locations

Network Drive A disk or tape drive connected to a server in the network that is shared by multiple users or a single user. Also known as a "remote drive"

PDA Personal digital assistants (PDAs) are handheld computers that were originally designed as personal organizers, but became much more versatile over the years. PDAs are also known as pocket computers or palmtop computers.

