INFORMATION TECHNOLOGY POLICY

FOR

STUDENTS & EMPLOYEES

APPROVED BY

VICE CHAIRMAN

MURDOCH UNIVERSITY INTERNATIONAL STUDY CENTRE DUBAI.

Murdoch UNIVERSITY
INTERNATIONAL STUDY CENTRE DUBAI

TABLE OF CONTENTS

Introduction

This document describes the general policies covering the use of the Information Technology facilities. "Information Technology" means any use of University-owned/purchased computing machinery (Printers, Terminals, Media Equipments and other types of peripheral equipment), software related to teaching, learning and research activities, and related facilities (computing rooms, VPN access, Internet resources).

Every student or staff (Hereafter called "User") of university computing resources is expected to understand and follow these guidelines. To accomplish this, it is very important that the computer systems (Computers, network equipment, telecommunication systems, email facilities and the internet) is used and managed according to specific rules or governance to ensure that the system as well as the information that resides within it is available on demand as well as secure.

The policies set out in this document are applicable to all users of Murdoch University International study center Dubai ("MUISCD") and Global Institute Middle East Limited ("GIMEL").

1. Computers and Network Access

A user gain access to the computer network (dedicated PC, library PC or computer Lab PC) by assigned personal "username". Possession of a computer username allows users to access the personal folder ("T:"), network share(S:,P:,Q:) internet, network software and other network devices such as printer, scanners etc..

1.1 General Use of Account

- In general, no user may use, or attempt to use, any computer account(s) other than his/her own assigned account(s).
- In general, no user may lend his/her account(s) to other students or colleagues.
- A user should only access, or attempt to access, files in his/her own account(s), or files which have been made accessible to him/her.
- Any exception to the access policies stated above must be approved in writing by the University Management.

1.2 General Use of Computing Resources

All users of computing facilities at MUISCD must abide by the University's Code of Practice these include, but are not limited to:

- It is the policy of the MUISCD that it's computing and networking facilities are intended for use for teaching, learning, research and administration in support of the University's mission. Although recognizing the increasing importance of these facilities to the activities of user, the University reserves the right to limit, restrict, or extend access to them.

- Users of the computing and networking facilities recognize that when they cease to be formally associated with the MUISCD (e.g. no longer an employee or enrolled student), their information

may be removed from University computing and networking facilities without notice. Users must remove their information or make arrangements for its retention prior to leaving the University.

- All persons using the computing and networking facilities shall be responsible for the appropriate use of the facilities provided as specified by the "Codes of Practice" of this policy, and shall observe conditions and times of usage of the internet.

- It is the policy of the University that it's computing and associated network facilities are not to be used for commercial purposes or non-University-related activities without written authorization from the University. In any dispute as to whether work carried out on the computing and networking facilities is internal work, the decision of the Vice Chairman or his delegate shall be final.

- The University will endeavor to protect the confidentiality of information and material furnished by the user and will instruct all computing personnel to protect the confidentiality of such information and material, but the University shall be under no liability in the event of any improper disclosure.

- MUISCD and GIMEL will endeavor to safeguard the possibility of loss of information within the University's computing and networking facilities but will not be liable to the user in the event of any such loss. The user must take all reasonable measures to further safeguard against any loss of information within the University's computing and networking facilities.

- The MUISCD and GIMEL reserves the right to limit permanently or restrict any user's usage of the computing and networking facilities; to copy, remove, or otherwise alter any information or system that may undermine the authorized use of the computing and networking facilities; and to do so with or without notice to the user in order to protect the integrity of the computing and networking facilities against unauthorized or improper use, and to protect authorized users from the effects of unauthorized or improper usage.

- MUISCD and GIMEL, through authorized individuals, reserves the right to periodically check and monitor the computing and networking facilities, and reserves any other rights necessary to protect them.

- MUISCD and GIMEL reserves the right to take emergency action to safeguard the integrity and security of the computing and networking facilities. This includes but is not limited to the termination of a program, job, or on-line session, or the temporary alteration of user account names and passwords. The taking of emergency action does not waive the rights of the University to take additional actions under this policy.

- The Management of the Technical Department may suspend any person from using the computing and networking facilities for a period not exceeding 28 days (and may recommend additional penalties to the General Manager Finance & Administration) if after appropriate investigation that person is found to be:-

    - responsible for willful physical damage to any of the computing and networking facilities;
    - in possession of confidential information obtained improperly;
    - responsible for willful destruction of information;

- responsible for deliberate interruption of normal services provided by the Computing Centre;
- responsible for the infringement of any patent or the breach of any copyright;
- gaining or attempting to gain unauthorized access to accounts and passwords;
- gaining or attempting to gain access to restricted areas without the permission of the IT Management;
- responsible for inappropriate use of the facilities.

- External work or use of the computing and networking facilities shall not be undertaken which would prevent University users from having their usual access to the facilities.

- MUISCD and GIMEL computing resources may not be used for any activities which intimidate, threaten or harass individuals, or which violate the campus policies concerning relationships between campus constituencies.

- No person may possess or use programs that violate or hamper another person's use of computing resources. Examples of such programs are those that attempt to control terminals or PCs obtain another user's passwords, acquire another user's files, viruses, etc.

- Where the use of Computer Systems to engage in personal e-commerce transactions (for example, internet banking and on-line purchasing) the company shall not be held responsible for any loss or liability that may follow as a result of any failure of the Computer Systems. Any costs, debts, or losses incurred by an student as a result of an aforementioned transaction, or failure of a transaction, shall be for the student personal account only.

- Abuse or improper use of the Computer Systems is not permitted. Unacceptable usage includes, but is not limited to, the transmitting, retrieving, storage or display of the following:

    - Material of a discriminatory nature
    - Obscene or pornographic materials
    - Derogatory or inflammatory remarks of any nature
    - Abusive, profane or offensive language
    - Chain letters and petitions
    - Political or religious viewpoints
    - Material or language that might be deemed to constitute harassment
    - Video, voice clips and/or files unconnected to our business
    - Advertising/soliciting for personal gain

2. Code of Practice in the Use of Computing & Network Facilities

Standards for the use of the MUISCD & GIMEL's computing and networking facilities derive directly from standards of common sense and common decency that apply to the use of any shared resource. The University community depends on a spirit of mutual respect and cooperation to resolve differences and resolve problems that arise from time to time. This code of practice is published in that spirit. Its purpose is

to specify user responsibilities and to promote the appropriate use of IT for the protection of all users of the MUISCD and GIMEL.

2.1 Appropriate and Reasonable Use

Appropriate and responsible use of the MUISCD & GIMEL's computing and networking facilities is defined as use that is consistent with the teaching, learning, research and administrative objectives of the University and with the specific objectives of the project or task for which such use was authorized. All uses inconsistent with these objectives are considered to be inappropriate use.

2.2 Responsibilities

Users of the MUISCD and GIMEL's computing and networking facilities accept the following specific responsibilities:

- **Security**
  - To safeguard their data, personal information, passwords and authorization codes, and confidential data;
  - To take full advantage of file security mechanisms built into the computing systems;
  - To choose their passwords wisely and to change them periodically;
  - To follow the security policies and procedures established to control access to and use of administrative data.
- **Confidentiality:**
  - To respect the privacy of other users; for example, not to intentionally seek information on, obtain copies of, or modify files, tapes, or passwords belonging to other users or the University;
  - Not to represent others, unless authorized to do so explicitly by those users;
  - Not to divulge sensitive personal data to which they have access concerning staff or students without explicit authorization to do so.
- To respect the rights of other users; for example, to comply with all University policies regarding sexual, racial, and other forms of harassment. The University is committed to being a racially, ethnically, and religiously heterogeneous community.
- To respect the legal protection provided by copyright and licensing of programs and data; for example, not to make copies of a licensed computer program to avoid paying additional license fees or to share with other users.

- To respect the intended usage of resources; for example, to use only the account name and password, funds, transactions, data, and processes assigned by service providers, unit heads, or project directors for the purposes specified, and not to access or use other account names and passwords, funds, transactions, data, or processes unless explicitly authorized to do so by the appropriate authority.
- To respect the intended usage of systems for electronic exchange (such as e-mail, Usenet News, World Wide Web, etc.); for example, not to send forged electronic mail, mail that will intimidate or harass other users, chain messages that can interfere with the efficiency of the system, or promotional mail for profit-making purposes. Also, not to break into another user's electronic mailbox or read someone else's electronic mail without their permission.
- To respect the integrity of the computing and networking facilities; for example, not to intentionally develop or use programs, transactions, data, or processes that harass other users or infiltrate the system or damage or alter the software or data components of a system. Alterations to any system or network software or data component are to be made only under specific instructions from authorized academic staff, unit heads, project directors, or management staff.
- To respect the financial structure of the computing and networking facilities; for example, not to intentionally develop or use any unauthorized mechanisms to alter or avoid charges levied by the University or GIMEL for computing, network, and data processing services.
- To adhere to all general University policies and procedures including, but not limited to, policies on proper use of information resources and computing and networking facilities; the acquisition, use, and disposal of GIMEL owned computer equipment; use of telecommunications equipment; legal use of software; and legal use of administrative data.
- To report any information concerning instances in which the MUISCD and GIMEL IT Security Policy or any of its standards and codes of practice has been or is being violated. In general, reports about violations should be directed initially to the administration of the school, area or unit where the violation has occurred whereupon it will be passed on to the Custodian of the system. If it is not clear where to report the problem, it may be sent to the Information Technology Help Desk which will redirect the incident to the appropriate person(s) for action or will handle it directly.

3. Code of Practice for Specific Activities

The following apply to specific activities.

3.1 Illegal Activity

In general, it is inappropriate use to store and/or give access to Information on the MUISCD computing and networking facilities that could result in legal action against the University.

3.2 Objectionable Material

The MUISCD's and GIMEL's computing and networking facilities must not be used for the transmission, obtaining possession, demonstration, advertisement or requesting the transmission of objectionable material knowing it to be objectionable material; namely:

- A film classified refused classification, a computer game classified refused classification, or a refused publication;
- Child pornography;
- An article that promotes crime or violence, or incites or instructs in matters of crime or violence; or
- An article that describes or depicts, in a manner that is likely to cause offense to a reasonable adult e.g.

    - The use of violence or coercion to compel any person to participate in, or submit to, sexual conduct;
    - The use of urine or excrement in association with degrading or dehumanizing conduct or sexual conduct;
    - Acts of torture or the infliction of extreme violence or extreme cruelty.

3.3 Restricted Software and Hardware

Users should not knowingly possess, give to another person, install on any of the computing and networking facilities, or run, programs or other Information which could result in the violation of any MUISCD's policy or the violation of any applicable license or contract. This is directed towards but not limited to software known as viruses, Trojan horses, worms, password breakers, and packet observers.

The unauthorized physical connection of monitoring devices to the computing and networking facilities which could result in the violation of MUISCD's policy or applicable licenses or contracts is inappropriate use. This includes but is not limited to the attachment of any electronic device to the computing and networking facilities for the purpose of monitoring data, packets, signals or other information. Authorization to possess and use such hardware for legitimate diagnostic purposes must be obtained from the management of the Information Technology.

3.4 Copying and Copyrights

- Users of the computing and networking facilities must abide by the MUISCD's copyright Policy, which covers copyright issues pertaining to MUISCD's & GIMEL's faculty, staff and students.

- Respect for intellectual labor and creativity is essential to academic discourse. This tenet applies to works of all authors and publishers in all media. It includes respect for the right to acknowledgment and right to determine the form, manner, and terms of publication and distribution. If copyright exists, as in most situations, it includes the right to determine whether the work may be reproduced at all. Because electronic information is volatile and easily reproduced or altered, respect for the work and personal expression of others is especially critical in computing and networking environments. Viewing, listening to or using another person's information without authorization is inappropriate use of the facilities. Standards of practice apply even when this information is left unprotected.

- In particular, users should be aware of and abide by the MUISCD's Policy on Copying and Using Computer Software. Most software that resides on the computing and networking facilities is owned by the MUISCD or GIMEL, and is protected by copyright and other laws, together with licenses and other contractual agreements. Users are required to respect and abide by the terms and conditions of software use and redistribution licenses. Such restrictions may include prohibitions against copying programs or data for use on the computing and networking facilities or for distribution outside the University; against the resale of data or programs, or the use of them for non-educational purposes or for financial gain; and against public disclosure of information about programs (e.g., source code) without the owner's authorization. MUISCD's or GIMEL's employees or students who develop new packages that include components subject to use, copying, or redistribution restrictions have the responsibility to make any such restrictions known to the users of those packages.

- With a greater emphasis on computer based assignments, students need to be especially cognizant of the appropriate use of computing and networking facilities. In particular, academic dishonesty or plagiarism in a student assignment may be suspected if the assignment calling for independent work results in two or more solutions so similar that one can be converted to another by a mechanical transformation. Academic dishonesty in an assignment may also be suspected if a student who was to complete an assignment independently cannot explain both the intricacies of the solution and the techniques used to generate that solution. Suspected occurrences of academic dishonesty are referred to the DEAN of the University & to the General Manager of GIMEL.

3.5 Harassment

- MUISCD's and GIMEL's policy prohibits sexual and discriminatory harassment. University's computing and networking facilities are not to be used to libel, slander, or harass any other person. The following constitute examples of Computer Harassment:

    - Intentionally using the computer to annoy, harass, terrify, intimidate, threaten, offend or bother another person by conveying obscene language, pictures, or other materials or threats of bodily harm to the recipient or the recipient's immediate family;

- Intentionally using the computer to contact another person repeatedly with the intent to annoy, harass, or bother, whether or not any actual message is communicated, and/or where no purpose of legitimate communication exists, and where the recipient has expressed a desire for the communication to cease;

- Intentionally using the computer to contact another person repeatedly regarding a matter for which one does not have a legal right to communicate, once the recipient has provided reasonable notice that he or she desires such communication to cease (such as debt collection);

- 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 otherwise, of another or the threatened invasion of the privacy of another.

- The display of offensive material in any publicly accessible area is likely to violate MUISCD's & GIMEL's harassment policy. There are materials available on the Internet and elsewhere that some members of the University community will find offensive. One example is sexually explicit graphics. The MUISCD and GIMEL cannot restrict the availability of such material, but it considers its display in a publicly accessible area to be inappropriate. Public display includes, but is not limited to, publicly accessible computer screens and printers.

3.6 Wasting Resources

- It is inappropriate use to deliberately perform any act which will impair the operation of any part of the computing and networking facilities or deny access by legitimate users to any part of them. This includes but is not limited to wasting resources, tampering with components or reducing the operational readiness of the facilities.

- The willful wasting of computing and networking facilities resources is inappropriate use. Wastefulness includes but is not limited to passing chain letters, willful generation of large volumes of unnecessary printed output or disk space, willful creation of unnecessary multiple jobs or processes, or willful creation of heavy network traffic. In particular, the practice of willfully using the MUISCD's and GIMEL's computing and networking facilities for the establishment of frivolous and unnecessary chains of communication connections is an inappropriate waste of resources.

- The sending of random mailings ("junk mail") is discouraged but generally permitted in so far as such activities do not violate the other guidelines set out in this document. It is poor etiquette at best, and harassment at worst, to deliberately send unwanted mail messages to strangers. Recipients who find such junk mail objectionable should contact the sender of the mail, and

request to be removed from the mailing list. If the junk mail continues, the recipient should contact the IT Helpdesk.

3.7 Game Playing

Limited recreational game playing, that is not part of an authorized and assigned research or instructional activity, is tolerated (within the parameters of each department's rules). MUISCD's and GIMEL's computing and network services are not to be used for recreational game playing.

3.8 Commercial & Personal Business Use

MUISCD's and GIMEL's computing and network facilities are provided by the MUISCD and GIMEL for the support of its mission. It is inappropriate to use the computing and networking facilities for:

- Commercial gain or placing a third party in a position of commercial advantage
- Any non-university related activity, including non-university related communications
- Commercial advertising or sponsorship except where such advertising or sponsorship is clearly related to or supports the mission of the University or the service being provided.

MUISCD's and GIMEL's computing and network facilities may not be used in connection with compensated outside work nor for the benefit of organizations not related to MUISCD or GIMEL, except in connection with scholarly pursuits (such as academic publishing activities), in accordance with the University Consulting Policy or in a purely incidental way. This and any other incidental use (such as electronic communications or storing data on single-user machines) must not interfere with other users' access to resources (computer cycles, network bandwidth, disk space, printers, etc.) and must not be excessive.

3.9 Use of Desktop Systems

Users are responsible for the security and integrity of University information stored on their personal desktop system. This responsibility includes making regular disk backups, controlling physical and network access to the machine, and installing and using virus protection software. Users should avoid storing passwords or other information that can be used to gain access to other campus computing resources. Users should not store University passwords or any other confidential data or information on their laptop or home PC or associated floppy disks or CD's.

4.0 Ownership of Software

All software developed using Office of Information Technology facilities and/or stored on a campus computing system is the property of GIMEL. Any exception to this policy must be arranged with the Management of Technical Department.

5.0 Ownership of Intellectual Property

Except as otherwise agreed in writing by an authorized person of the MUISCD and GIMEL, or stated in this policy, the MUISCD & GIMEL asserts legal and beneficial ownership of intellectual property,

Created by the students or staff of the university where:

- Generation of the intellectual property has resulted from the use of pre-existing intellectual property owned by the MUISCD or GIMEL ; or
- The intellectual property belongs to a set of intellectual property generated by a team of which the student is a member; or
- The intellectual property has been generated as a result of funding provided by or obtained by MUISCD or GIMEL.

6.0 Maintenance of Computing/Data Resources

Technical department makes strong efforts to maintain the security of username, passwords and Users Data. Each user must take full advantage of password and file protection security mechanisms provided by the MUISCD & GIMEL.

6.1 File Server Storage

MUISCD and GIMEL provides data services on a secured file server for all users called personal folder (T:) & network share drives (S:,P:,R:), these folder can be accessible from any workstation by logging in with respective "username". Additional space can be purchased by filling the IT request form.

These directives apply to all users:

- Users shall only store relevant data to the data server.
- Users have to ensure the space is cleaned up regularly and files that are no longer required must be deleted.

6.2 Server Backups

Technical department will carry out regular data backup to maintain the data continuity, restoration and recovery of critical data and systems. Technology department will ensure that all critical data is backed up periodically and copies maintained at offsite location.

Regular testing of restoring data/software from the backup copies will be undertaken, to ensure that they can be relied upon for use in an emergency.

6.3 Notification of Changes in the Computing Environment

Technical department will announce all non-transparent changes in operating procedures, hardware and software at least one week before the change is to take place. Such announcements will be made using the University E-Mail Services or system broadcast messages.

7.0 Print Policy

Students can print to any assigned printer in the library/computer lab by using individual "username". Each student will be awarded 100 pages free printing.

7.1 General Use of Printer

- If a student print over 100 pages and student has enough credit on print account, the over-quota pages are simply charged to respective users print account.
- If a student print over 100 pages and don't have enough credit on print account, print job won't proceed. Student will need to add credit to respective print account in order to print more pages.

7.2 Printer Account

Print account can be refilled by purchasing print voucher from the book sales room. To add credit to print account by using print voucher login to http://GIMELFAP:9191/user and click on redeem card & enter the print voucher number. The amount will be credited to the respective users print account.

8.0 Email Policy

MUISCD and GIMEL provides E-mail services to support the academic, research, and administrative functions of the institution. Because of this, users should explicitly recognize their responsibility for the content, dissemination and management of the messages they send.

Email users must comply with law, MUISCD and GIMEL policies and normal standards of professional and personal courtesy and conduct.

8.1 General Use of Email

- The standard naming convention for all e-mail addresses is firstname.surname@murdochdubai.ac.ae, this standard is applicable to all students & employees of the MUISCD and GIMEL.
- Address messages to recipients who "need to know," rather than to everyone you know. Messages sent unnecessarily can lower system and user performance.
- Extreme caution should be used when attaching documents and/or any electronic files to an email. No files containing confidential information concerning or belonging to the university may be forwarded to any unauthorized persons.
- Students may not access and read messages or files clearly intended for or saved by other persons, unless they are specifically authorized to do so by the company or the owner/addressee.
- Employees may not send email under another employee's name, except where certain rights and privileges have been granted (e.g. secretary on behalf of manager).

8.2 Email Restrictions

- Sending or forwarding chain e-mail, i.e., messages containing instructions to forward the message to others.
- Sending non-work related e-mail i.e. jokes or video clips.
- Conducting personal business using company resources must be limited to the minimum.
- Transmitting any content that is offensive, harassing or fraudulent

8.3 File Size and Disk Quotas

Individuals must be sensitive in using distribution lists and files that contain images such as photographs. Such images dramatically increase file size – and when large files are sent to many people via distribution lists, the cumulative impact on resources is significant. If a file being sent to a distribution list appears likely to exceed quotas, the e-mail administrator will contact the sender to explore other, more efficient strategies for conveying the information.

The college reserves the right to implement e-mail quotas for both employee and student accounts. Current quotas are 100 megabytes for employees and 50 megabytes for students. Individuals are responsible for regularly deleting old files from personal in-boxes and mail folders; failure to do so may result in temporary termination of e-mail privileges until the cumulative total of files can be reduced below the quota. Students will receive a warning message when their mailbox reaches to 40MB; whereas employee will receive warning message when their mailbox reached 90MB. Students will be unable to send any mail when their mailbox reaches to 50MB. Incoming mail will always be accepted. Additional mail space can be purchased by filling up the IT request form.

Each user has to archive the mail to their respective home folder, and user is responsible to use this allocated space to the optimum.

9.0 Internet Policy

MUISCD and GIMEL encourages the use of the Internet for academic, research & communication purposes if it is an inherent requirement of the student. This service can be described as access to the internet from library / lab computers with the following basic facilities enabled:

- Internet browsing for research and information
- Download of academic related documentation

9.1 General Internet Access Rules

Each student has a responsibility to maintain and enhance MUISCD's & GIMEL's public image and to use access to the Internet in a productive manner. The following rules govern the use of internet services:

- First and foremost, the Internet for this company is a business tool that means MUISCD expect you to use your Internet access primarily for academic related purposes. Unnecessary or unauthorized Internet usage causes network and server congestion. Unlawful Internet usage may also garner negative publicity for the company and expose to significant legal liabilities.

- MUISCD and GIMEL insist that you conduct yourself honestly and appropriately on the Internet, and respect the copyrights, software licensing rules, property rights, privacy and prerogatives of others, just as you would in any other business dealings. To be absolutely clear on this point, all existing company policies apply to your conduct on the Internet, especially (but not exclusively) those that deal with intellectual property protection, privacy, misuse of company resources, sexual harassment, information and data security, and confidentiality.

- MUISCD and GIMEL reserve the right to inspect any and all files stored in private areas of our network in order to assure compliance with policy.

- The display of any kind of sexually explicit image or document on any company system is a violation of our policy. In addition, sexually explicit material may not be archived, stored, distributed, edited or recorded using our network or computing resources.

- MUISCD's and GIMEL's internet facilities and computing resources must not be used knowingly to violate the laws and regulations of the United Arab Emirates or any other nation, or the laws and regulations of any state, city, or province in any material way.

- Any software or files downloaded via the Internet into the MUISCD & GIMEL network become the property of the company. Any such files or software may be used only in ways that are consistent with their licenses or copyrights.

- No student or employee may use company facilities knowingly to download or distribute pirated software or data.

- No student or employee may use the company's Internet facilities to deliberately propagate any virus, worm, Trojan horse, or trap-door type program code.

- No student or employee may use the company's Internet facilities knowingly to disable or overload any computer system or network, or to circumvent any system intended to protect the privacy or security of another user, system or network.

- Each employee using the Internet facilities of the company shall identify him or herself honestly, accurately and completely including one's company affiliation and function where requested.

- Only those employees or officials who are duly authorized to speak to the media, to analysts or in public gatherings on behalf of the company may speak/write in the name of the company through electronic media.

- The company retains the copyright to any material posted to any forum, newsgroup, chat or World Wide Web page by any employee in the course of his or her duties.

- Employees are reminded that e-mails, chats and newsgroups are public forums where it is inappropriate to reveal confidential company information, customer data, trade secrets, and any other material covered by existing company secrecy policies and procedures. Employees releasing protected information via e-mail, newsgroup or chat – whether or not the release is inadvertent – will be subject to all penalties under the existing company secrecy policies.

- Use of company Internet access facilities to commit infractions such as misuse of company assets or resources, sexual harassment, unauthorized public speaking and misappropriation or theft of intellectual property are also prohibited, and will be sanctioned under the relevant provisions of the personnel handbook.

- Some applications use the Winsock service on proxy server to download files. Access to the WINSOCK services on the proxy's servers will be limited to only the standard services like FTP, Telnet and POP3 etc. Substandard ports will be blocked. Users that require access to these ports can log a call and request this type of access and will be investigated.

- No music file downloads

- No movie file downloads

- No pornographic material downloads

- No game downloads

- Any software used for Internet connection sharing (Peer to Peer) is not allowed to be installed on a User's computer. This includes software like kazaa, imesh, morpeus, winmx, audiogalaxy, edonkey, napster etc. If this software if found on a users machine Internet access will be revoked pending the investigation.

9.2 File Transfers/Download

The corporate Internet link of University is reserved exclusively for academic use. As such it is against the policy to abuse the Internet bandwidth by using it for downloading non-work related data. If a user is found to be abusing the Internet bandwidth by downloading a substantial amount of data, the type of download will be investigated and if the type is non-work related the user's Internet access rights will be revoked.

Students may not use the university's Internet facility to download entertainment software or games, or to play games against opponents over the Internet.

9.3 Content filtering

The company uses independently supplied software and data to identify inappropriate or sexually explicit Internet sites. We may block access from within our networks to all such sites that we know of. If you find yourself connected incidentally to a site that contains sexually explicit or offensive material, you must disconnect from that site immediately, regardless of whether that site had been previously deemed acceptable by any screening or rating program.

10.0 Computer Virus Control Policy

To ensure MUISCD's and GIMEL's computers are not infected by any computer virus, the following procedure is to be followed,

- Computers are to be used for academic purposes only.
- Only software authorised by the Technical department is allowed on campus computers.
- All computers must have antivirus software installed.
- It is the responsibility of every computer user to ensure antivirus software is installed and updated.
- Computer users must notify the Technical department immediately if a virus warning is received.
- Technical department will assess the warning and inform computer users, as appropriate. Individual users are not to forward the warning to anyone else.
- Technical department will assist the computer user in taking the appropriate remedial action and advice on how to best communicate with the sender of the virus.
- Computer users must notify the Technical department immediately if they are advised they have unknowingly sent a virus to someone else.

11. Problem /Incident Escalation

Any incidents affecting the computer services (this include inappropriate use of computer/ Internet/ Email/ Company representation on the Internet/ Internet response problems) can be reported at the it.helpdesk@murdochdubai.ac.ae

Technical Department must be notified immediately when:

- Sensitive University's or GIMEL's information is lost, disclosed to unauthorized parties, or suspected of being lost or disclosed to unauthorized parties.
- Unauthorized use of University or GIMEL information systems has taken place, or is suspected of taking place.
- Passwords or other system access control mechanisms are lost, stolen, or disclosed, or are suspected of being lost, stolen, or disclosed.
- There is any unusual systems behavior, such as missing files, frequent system crashes, misrouted messages.

12. Glossary of Terms

Chain letters and petitions	Any email not directly related to our academic that requires recipients to forward the message to others, often with a promise of some reward or disaster.
Proprietary and confidential information	Propriety and confidential information of the University. This includes all academic, business and trade information.
Derogatory	Offending, injurious, contemptuous, disparaging conduct.
Email	An electronic message sent from or received by an individual computer.
Fraudulent	Conduct that deceives, that is dishonest, delusive and misleading.
Harassment	Conduct that torments, troubles or annoys.

Inflammatory	That arouses strong feelings or anger in people.
Logon	Connecting to a system/network that requires the username and password.
MS Operating System	The basic software that makes your computer work.
Network	An interconnected group of computers within an organization.
Password	A secret word, that entitles the holder thereof to access an electronic system.
Pornography	Obscene pictures, video clips or writing.
Profane	Blasphemous and disrespectful language.
Screensaver	A new screen that appears automatically on the computer, after a predetermined amount of time has elapsed with no keyboard or mouse input, The new screen will only disappear if the password is inserted.
Soliciting	Enticing immoral, indecent, lascivious or lewd conduct.
Virus	A computer virus is a computer program that can copy itself and infect a computer without permission or knowledge of the user.