University of Mines and Technology, Tarkwa

ICT POLICY

June 2012

TABLE OF CONTENTS

Contents **Page**

1 Purpose and Scope

1.1 Purpose

This document defines the Information and Communication Technology (ICT) Policy of the University of Mines and Technology (UMaT), Tarkwa. The purpose of the UMaT ICT Policy is to:

1. Provide guidelines and standards to guide users and decision makers in the development and use of ICT Resources.
2. Ensure that ICT resources are used efficiently and appropriately in support of teaching, learning, research and administrative functions of the University.
3. Ensure that ICT resources are secured and protected against abuse, damage, loss or theft.

This Policy shall be publicised through a number of channels. These include:

1. ICT training of staff and students.
2. Orientation programmes for new staff and students.
3. UMaT staff and student mailing lists.
4. The University's website.
5. New users subscribing to UMaT Email facility.

The rules in this document are mandatory upon all users of the University's ICT resources. Users are responsible for making themselves familiar with the rules and regulations governing ICT resources and services.

The ICT Policy shall be approved by the Academic Board.

1.2 Scope

This ICT Policy provides the policy framework for:

1. Managing ICT services and facilities.
2. Secured and acceptable use of ICT facilities.
3. Use of Internet and Email.

4. Managing the website.
5. IT procurement.
6. IT project management.

This ICT Policy is NOT a procedure manual for handling or using ICT systems or facilities. Procedure manuals shall be developed for specific ICT systems by the relevant IT support units for running and managing such systems. Procedure manuals are detailed guidelines that provide steps for handling the day-to-day operation and management of ICT systems.

2 ICT Governance and Service Management

ICT services in the University shall be managed by the:

1. ICT Unit.
2. Planning and Quality Assurance Unit of the University.
3. ICT Management Committee.
4. ICT Help Desk.

2.1 The ICT Unit (ICTU)

The ICT Unit (ICTU) is mandated to provide leadership in the development, management and use of ICT in the University as follows:

1. Development and implementation of ICT Policies, Strategies and Standards.
2. Support of the University's ICT Infrastructure. This covers the management and day-to-day operation of the:
    a. Network Operating Centre.
    b. University's backbone network that interconnects the Local Area Networks (LANs).
    c. Computer laboratories (labs).
    d. Telephone system.

3. The setup, administration, troubleshooting and problem resolution of personal computers, printers, servers, networks and communications systems. The ICTU is responsible for:
    a. The University Email system.
    b. Internet access.
    c. Technical support of the University website.
    d. Promoting the use of e-learning tools.
    e. Basic ICT training for staff and students.
    f. ICT advisory services.
    g. Developing and generating reports.
    h. Technical support.

2.2 The Head of the ICTU

The Head of ICTU shall be responsible for the day-to-day management of the ICTU.

2.3 The Planning and Quality Assurance Unit of the University

The Planning and Quality Assurance Unit of the University shall be responsible for:

1. The strategic planning, management of quality assurance as well as management of information systems of the University.
2. Co-ordinating activities of the ICTU to ensure that the ICT facilities and services are managed and delivered at the highest level of quality.
3. Liaising with the ICTU to prepare and maintain an up to date database on staff and students as well as basic statistics in the University.

2.4 The ICT Management Committee

The functions of the ICT Management Committee shall be to:

1. Formulate policies and guidelines for the running of the ICTU.
2. Oversee the administration of the ICTU.
3. Make recommendations to the Academic Board on the use of ICT facilities in the University.

4. Offer advice on the development of ICT infrastructure and acquisition of computers and ICT equipment.

2.5 The ICT Help Desk

The ICT Help Desk shall be created by the ICTU and shall be the basis for managing problems and changes. Help Desk procedures shall be established for receiving user problems and requests, trouble ticketing and tracking, as well as problem resolution and escalation.

2.5.1 Objective

The objective of the ICT Help Desk is to provide customer-oriented ICT services to the UMaT user community by receiving problem calls, requests and enquiries, and arranging to have them resolved or addressed by the appropriate ICT personnel.

2.5.2 Service Availability

The Help Desk service shall be available during working hours. The Help Desk can be reached either through the University intercom phone number 264 or Email: helpdesk@umat.edu.gh.

3 ICT Infrastructure

3.1 Provision of ICT Infrastructure

The University shall develop, operate and maintain a computing and networking infrastructure as well as software systems to provide the following ICT facilities and services:

1. LCD projectors and laptops for lecture rooms.
2. Internet and Email services.
3. Access to library information resources.
4. Access to Management Information Systems (MIS).

5. Access to computer labs.
6. Other computing facilities and services as they become available.

3.2 Components of ICT Infrastructure

The ICT infrastructure of the University comprises:

1. The Campus Area Network that links the networks of Faculties, Departments, and Administration.
2. The Network Operating Centre which houses centralised equipment for Internet, Email and Intranet services.
3. Computer labs.
4. Computers at offices.
5. Application software.
6. Other ICT related systems.

4 Hardware, Software, and Data and Information Policies

The hardware, software, and data and information policies are aimed at ensuring that the ICT systems are protected from:

1. Unfavourable environmental conditions.
2. Unauthorised access.
3. Malicious attacks (virus, worms, Trojan horses, *etc*).
4. Inappropriate handling by IT personnel and users.

4.1 Hardware Policy

The hardware components cover:

1. Computers: Servers, desktop computers, portable computers (laptops, notebooks), *etc*.
2. Output, input and storage equipment: Disk storage systems, printers, scanners, *etc*.
3. Networking equipment: Routers, switches, modems, *etc*.
4. Communication systems: Very Small Aperture Terminal (VSAT), cabling systems, *etc*.

4.1.1 Environmental Conditions

The policy guidelines on environmental conditions are aimed at ensuring that the environment within which the ICT systems operate is protected against inappropriate levels of power, temperature, humidity, and also against fire and dirt. Consequently, the following are to be noted:

1. Power

   Power supply to computers and accessory equipment shall be clean, safe and uninterruptible. This will involve the provision of:

   a. Standby generators/battery banks, especially for centralised systems.
   b. Uninterruptible Power Supply (UPS).
   c. Stabilisers.
   d. Power protection devices against surges and lightning strikes.

2. Air Conditioning

   The server room and computer labs shall have air conditioning systems that operate at all times. The air conditioning systems shall keep the room within the equipment manufacturers' recommended specifications for temperature and humidity throughout the year.

3. Lighting

   Adequate lighting shall be provided in the server room and computer labs.

4. Fire

   a. Computer labs and server rooms shall be protected by smoke detectors and fire alarm systems.
   b. Fire extinguisher(s) shall be provided for computer labs and server rooms. They shall be periodically tested to ensure that they are in good working condition.
   c. IT personnel in charge shall periodically be made to undergo fire prevention drills.

5. Cleaning

   a. The server room, computer labs and computers shall at all times be kept clean of dust, dirt and rubbish.
   b. Eating and drinking shall be prohibited at the computer labs and server rooms.
   c. The computers shall be kept clean and free from contamination.

4.1.2 Access Control

1. Physical Control
    a. Server Room and Computer Laboratories
        i. Server room and computer labs shall be adequately secured at the doors and windows with locks and burglar proofs.
        ii. A logbook or electronic system shall be maintained at the sever room to record entries and departures by IT personnel, visitors and service providers. Details of date, time, personnel/student/staff, purpose, and exit time shall be recorded in the logbook.
        iii. Provision (*eg*, pigeon holes) shall be made for safe keeping of student bags in the computer labs; bags shall not be allowed into the computer labs.
        iv. All students who use the computer labs shall be duly authorised through a registration process.
        v. At the end of each day of work, Lab Technicians or IT personnel in charge shall check all equipment to ensure that they are intact and in good operating condition.
        vi. A log book shall be maintained to record incidents, events and problems at the computer labs.
        vii. Anyone in possession of the keys to the server room or computer labs is totally responsible for that key. His/her responsibilities shall include not handing over the key to anyone else while the key is signed out to them and not making duplicates of the key.
        viii. Any irresponsibility on the part of anyone in possession of the keys to the server room or computer labs that results in loss of any item or improper use of the facilities shall attract sanctions such as prohibition to use the facilities and payment for the loss of any item.
    b. Asset Management
        i. User Departments shall track their computer systems through the use of an Asset Register. The Asset Register may be a notebook but preferably a spreadsheet with the following basic information: *Type of Equipment, Serial Number, Model, Specification, Date Purchased,*

Location (Room, Office), Cost, Life-Cycle (In Years), *Status (in operation, faulty or under repairs)*.

ii. The ICTU shall provide a template for the Asset Register and make it available to user departments through the website.

iii. Asset Identification: All IT equipment shall be identified by an Asset Number in line with the University's asset naming and identification scheme. The asset number shall be engraved on the equipment casing.

c. Tracking movement of equipment

i. An equipment movement log book shall be maintained to track movement of ICT equipment. Details shall include equipment specifications, name of user, where the equipment is being moved from and to, why it is being moved and the date of removal and replacement. A template shall be provided by the ICTU through the website.

ii. Any IT equipment other than the individual's laptop taken off site shall have the IT Officer in charge's authorisation for removal. Failure to comply with this directive shall result in disciplinary actions against the person. The person shall be held liable for any damage to equipment or loss of equipment.

iii. Removal of any IT equipment other than laptops from its normal place of use, *eg,* from one computer lab to the other for any reason, shall be authorised by the IT Officer in charge and logged in the equipment movement log book.

iv. Unauthorized removal of any IT equipment from its normal place of use without permission by any person shall attract sanctions including withdrawal of access privileges, payment for loss or damage to ICT facilities and suspension or expulsion from the University. The University also reserves the right to report any illegal activities to the appropriate legal authorities, *eg,* the Police.

d. Lost or stolen ICT equipment shall be reported to the appropriate Head of Department and the Chief Security Officer.

e. Costs/charges due to damage or otherwise as a result of negligence on the part of users shall be borne by the user in question.

f. Security breaches shall be reported to the appropriate Head of Department and the Chief Security Officer. These include but are not limited to:

unauthorised entry, doors left open or unlocked, faulty locks, broken window glass, windows left open, *etc*.

g. Cabling shall be kept tidy and neatly arranged to prevent any work hazards. Cabinets for devices shall be used where possible. Cables shall also be terminated in all cabinets and labelled for easy identification.

2. Logical Control (User IDs and Passwords)
   a. Generally all users of computing and networking facilities shall be authorised through the assignment of User IDs and Passwords.
   b. All guests and visitors to the University shall sign-up for Guest User Accounts. The essential 'dos and don'ts' shall be explained to such visitors and guests, prior to their use of the University's computer facilities.
   c. Users are advised not to disclose their personal passwords to anybody. Users are responsible for protecting their personal password and for the consequences of their password being known by others.
   d. Users may not sign on to any University system using a User ID other than that assigned to them.
   e. Users are accountable for all system activities that occur using their User ID and password.
   f. Initially assigned passwords for any users shall be changed upon first login.
   g. Good practice with passwords shall largely be enforced by the system settings. However, users are advised to follow these guidelines:
      i. Passwords shall be a minimum of eight characters in length and they shall either contain both alphabetic and numeric characters or be a phrase of two or more unrelated words.
      ii. If Password change is prompted by the system, please do so when requested to.
      iii. Passwords shall be changed immediately if the user believes he or she has been compromised or noticed anything unusual.
      iv. The standard password protected screen saver shall be activated when the PC is left unattended.
      v. Users shall log off when leaving their personal computers for a period of 30 minutes or more.

vi. The PC shall always be logged off and switched off before being left overnight unless it is running an overnight process, in which case the screen saver shall be activated.

4.1.3 Network Control

1. UMaT's networking facilities are intended for teaching, learning, research and administrative support purposes.
2. Configuration of personal computers, printers, *etc,* for network access shall be done by the ICTU or under the ICTU's direction.
3. The University network infrastructure shall be secured against:
   a. Email Spam: These are unsolicited Emails that users receive through the Internet.
   b. Intruder or Hacker Break-ins: The University's network like all networks connected to the Internet is susceptible to attacks or intrusion by eternal users.
   c. Virus, worms, spyware which create various dysfunctions in computer systems.
4. To avoid interoperability or poor network connectivity problems, User Departments are advised to contact the ICTU before installing or making any changes in their Local Area Networks (LANs) as well as workstations.
5. Users or User Departments shall seek clearance from the ICTU for any third-party network connections to the Internet or any external networks.

4.1.4 Troubleshooting, Repairs and Maintenance

1. Desktop computers, Portables (laptops, notebooks, and Personal Digital Assistants (PDAs)) and Printers that develop faults may be sent to the ICTU for repairs and maintenance.
2. IT personnel shall document and keep system settings and drawings up to-date.
3. User Departments may contract an external ICT service provider to maintain such hardware equipment. User Departments shall liaise with the ICTU to conclude maintenance agreements with external ICT Service Providers.

4. The ICTU shall provide templates for maintenance contracts and make them available to user departments through the website.

4.1.5 Disaster Recovery and Contingencies

Disaster recovery procedures and contingencies shall be defined and established for Mission Critical Systems such as the Internet, Email, MIS systems and Library Information Resources. The objective is to create capacity to restore services within an acceptable period of time after a disaster such as major hardware or system failures or failures resulting from fire, flood and earthquakes.

4.1.6 Other User Responsibilities

1. Users shall be responsible for the appropriate use of the facilities provided as specified in this Policy, and shall observe conditions and times of usage as published by the University.
2. Users shall take all reasonable steps to ensure that computer equipment in their possession or under their control are protected at all times against theft, accidental or deliberate damage by others and damage by natural elements.
3. In all cases users shall exercise good judgment and take reasonable care to safeguard the equipment, *eg,* equipment shall be physically secured when not in use and shall never be left unattended when not in use.
4. Only the University's staff and students are allowed to use the University's ICT facilities. Visitors and guests shall obtain authorisation from the IT Officer in charge before use.
5. Unauthorised or improper use of the University's ICT facilities and equipment by any person shall attract sanctions against the person. The sanctions shall include withdrawal of access privileges, payment for loss or damage to ICT facilities and suspension or expulsion from the University. The University also reserves the right to report any illegal activities to the appropriate legal authorities, *eg,* the Police.

4.2 Software Policy

Software refers to both system and application software. The following shall govern the appropriate use of software:

1. Pirated or Unlicensed Software: No pirated or unlicensed software shall be installed on individual workstations or on servers.
2. Copying of Software: Users shall not allow UMaT licensed software and/or associated documentation to be copied by outsiders and may not themselves make copies other than those provided for in the relevant licensing agreements.

   Appropriate disciplinary action including criminal penalties shall be prescribed by the Head of ICTU for the breach of this directive.
3. Application Development Approach: Standard Software Development Life-Cycle (SDLC) methodology shall be applied to planning, analysis and design as well as management and implementation of custom-built software.
4. Faculty/Department/Centre Software Applications: In order to benefit from volume discounts and common installation and setups, the ICTU shall coordinate the procurement and implementation of common software applications used by the academic units. Such software applications shall be run at the faculty/department level where it is used.
5. Software Configurations: Software configurations shall be documented for easier reference.

   Note: a person who breaches this Policy faces disciplinary action including withdrawal of access privileges, payment for loss or damage to ICT facilities and suspension or expulsion from the University. The University also reserves the right to report any illegal activities to the appropriate legal authorities, *eg,* the Police.

4.2.1 Antivirus

1. All computers in the University shall have the University's standard antivirus software installed.

2. The ICTU shall ensure that the relevant Antivirus is installed on all computers once notified. It is the responsibility of every user to avail their machines for the installation of the antivirus software.
3. The ICTU shall provide automatic updates of the antivirus through the network for computers connected to the network once a first-time installation is done.
4. For computers not connected to the network, the officer in charge at the Department shall liaise with the ICTU to have the updates done regularly.
5. Any software or data received from any external source, including the original manufacturer and the Internet, shall be treated as suspect and not installed, executed or used in any other fashion until it has been scanned for viruses using the University's standard virus detection software.
6. Users shall call the attention of the Departmental IT personnel immediately for assistance if a virus incident or activity is noticed and cannot be cleaned by the user. The problem shall be reported to the ICT Help Desk if problem persists.

4.3 Data and Information Policy

1. The University shall endeavour to protect the confidentiality of information and material furnished by the user and shall 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.
2. Recording or processing information which infringes any patent or breaches any copyright shall be avoided. Individual persons, not the University, shall be held responsible for any patent or copyright breaches.
3. All information acquired or created by user while carrying out the University's business, except that which is specifically exempted as private or personal, is a general University resource. However, each User Department shall have individual ownership of its own data resource.
4. Single Source Principle: Data shall be captured at source to avoid data re-input error and duplication.
5. Data Accuracy: Each user shall be responsible for the accuracy of the data that they enter into the system and they shall own it.
6. Users accept the following specific responsibilities:
   a. Security

i. To safeguard their data, personal information and confidential data.
ii. To take full advantage of file security mechanisms built into the computing systems.
iii. To follow the security policies and procedures established to control access to and use of data.

b. Confidentiality
   i. To respect the privacy of other users; for example, not to intentionally seek or access information on, obtain copies of, or modify data belonging to other users.
   ii. Not to divulge sensitive personal data concerning staff or users to which they have access without explicit authorisation to do so.
   iii. Not to access information and data without proper authority, nor make unauthorised modifications to the contents of any computer system, including deleting or changing data.
   iv. Not to disclose or use computerised personal data for any purpose which contravenes national or international legislation.

Individuals who violate any of these directives stated above are subject to discipline up to and including termination from employment, in accordance with employment contract, professional discipline or criminal prosecution in accordance with the laws of the country. At the discretion of the Vice Chancellor, the University may terminate an employee or student for the first, substantiated breach of its confidentiality and security policy if warranted by the seriousness of that breach.

Any employee or student who believes that another staff member, student or employee has breached the confidentiality or integrity of one's information or the University's information or data shall immediately report that breach to the appropriate authority.

The Head of ICTU shall instruct to be conducted a thorough and confidential investigation of the allegation and recommend corrective action to the Vice Chancellor.

The Head of ICTU shall inform the complainant of the results of the investigation and any corrective action taken.

The University shall not retaliate against or permit reprisals against any staff or student who reports a suspected violation of its policies protecting the confidentiality and integrity of personnel or University's information and data.

7. Data Backups Strategy
    a. A backup strategy and procedures shall be established to allow computer systems to recover from effects, which impair availability of and access to system functions and data. The chosen backup strategy shall aim to restore services within a specified acceptable period of downtime, driven by UMaT business objective, economic and justifiable recovery environment.
    b. In order to ensure prompt and easy recovery from data loss/corruption it is necessary to keep reliable backups of all documents and data.
    c. Both on-site and off-site backups need to be kept.
    d. Regularly test the backup media to ensure that the media can be read and can be relied upon for emergency use when necessary.
    e. All data backup tapes/CDs/disks shall be stored in a secure location (*eg,* fireproof safe) and this environment shall be conducive to storage of magnetic media. Documents will be archived on a monthly basis.

4.4 Policy and Rules on Privacy and Access to Electronic Records

UMaT reserves the right to interrogate electronic records held by UMaT, but this shall not be exercised without the written permission of the Vice Chancellor following due process involving consultation by the Vice Chancellor, or the Vice Chancellor's nominee.

5 Email Policy

The Email facility has been provided to enhance the business of the University through easier, faster communications and interaction among the user community.

This Policy provides guidance to users to use the facility in an appropriate and beneficial manner.

5.1 Subscription to Email Facility

5.1.1 Subscription by Staff

1. All staff of the University are entitled to an Email account.
2. An Email address shall be created for staff within 2 days, on applying to the ICTU.
3. Staff may apply by calling the Help Desk or writing a memo addressed to the ICTU. The details required for the Email address are: *Name, Department, Category (Senior Member, Senior Staff, Junior Staff) and Contact Phone.*
4. Applicant will be required to change the assigned password on his/her first login.

5.1.2 Subscription by Student

1. Email addresses shall be created for students when they register to use the ICTU facilities and services.
2. Alternatively, students may apply for Email address through their respective Departments.

5.1.3 Closure of Staff Email Account

1. The office of the Registrar shall notify the ICTU when a staff leaves the services of the University.
2. The ICTU shall disable the staff account/Email address. But before this is done, the ICTU shall confirm that all official documents and correspondences received through the mailbox of the staff have been printed and filed by the user departments.
3. The staff account/Email address shall be deleted three months after the staff has left the services of the University.

5.1.4 Closure of Student Email Account

1. Email accounts of all final year students shall automatically be deleted one month after completion of programme.
2. Students requiring more than one-month retention of Email account after completion of programme shall submit request through their Head of Department.

5.2 Email Address Naming Convention and Account Types

5.2.1 Naming Convention

The University's Email address convention is:

i. Individual Email Address: *Initial(s)surname@umat.edu.gh*
   Example 1: *jbrobbey@umat.edu.gh* (Juliet Brobbey).
   Example 2: *jabrobbey@umat.edu.gh* (Juliet Akua Brobbey).
   Where there are duplicate Email address names, sequential numbers shall be used to differentiate the Email addresses:
   Example: *jbrobbey1@umat.edu.gh; jbrobbey2@umat.edu.gh*
ii. Departmental Email Address: *deptname@umat.edu.gh*
   Example: *mn@umat.edu.gh* (Mining Engineering)

5.2.2 Sub Domain Email Accounts

Faculties and Departments may request for a sub domain to be created by applying to the ICTU. An Email address with a sub domain will look like: *Initiallastname@subdomainName.umat.edu.gh*
Example: *jbrobbey@finance.umat.edu.gh* (Finance Department).

5.2.3 Faculty/Unit/Section/Department/Special Purpose Email Accounts

Faculties, Departments, Units, Sections or groups may apply to create a *Faculty/Departmental/Unit/Section/Group* Email account to send, receive and store official Emails. Special Email accounts could be setup for a specific purpose.
Example: *registrar@umat.edu.gh* or *grasag@umat.edu.gh*

5.3 Email Policy Guidelines

5.3.1 Security and Confidentiality

1. The University does not guarantee the confidentiality of electronic mail since it could be intercepted within or outside the University's network.
2. Except as provided elsewhere in this Policy, ICT personnel are not permitted to see or read intentionally, the contents of Email messages except where necessary to ensure proper functioning of University Email services, or to disclose or otherwise use what they have seen.

5.3.2 Legal Implications

Users are to note that Email has the same standing in law as any other document and that insulting someone in an Email may be considered defamatory and may leave the University and/or the individual user open to legal action.

5.3.3 Email Disclaimer

Users may not transmit personal opinions as those of UMaT. The following disclaimer will automatically be included as a suffix to all Email messages to addresses external to UMaT.

---------- DISCLAIMER -------

The information contained in this electronic mail transmission is confidential. It may also contain privileged work product or proprietary information. If you are not the intended recipient, you are hereby notified that any disclosure, copying, distribution or use of any of the information contained in or attached to this transmission is STRICTLY PROHIBITED. If you have received this transmission in error, please disregard it and reply to the sender, then delete it from all directories and destroy all copies of it. Thank you.

5.3.4 Use of Third-Party Email Systems

Third party Email systems such as *Hotmail* and *Yahoo* shall be restricted during working hours. This Policy is aimed at preserving the Internet Bandwidth.

5.3.5 Leave, Vacation, Travel

In order to ensure that official information held in a staff's mail box is available when staff takes leave, vacation or travels, the following measures shall be taken:

1. For staff about to take leave, vacation or travel, the Email shall be set to automatically inform senders of their *out-of-office status*, with an advice to send the message to an alternative Email address if it is official.
2. Staff travelling outside or within the country, have the option of setting the Email to forward mail messages to an alternative Email system where it would be easier to retrieve.

5.3.6 Email Data Backup and Storage Management

1. The size of mailboxes on the Email server shall be limited by quotas on the server. When a user's mailbox reaches the quota, a message will be displayed requesting the user to clear the mailbox. The user will not be able to send messages, but will be able to receive them.
2. It is the responsibility of the user to backup mails already received in their mailboxes. The central storage Email system shall hold pending Emails for users till they are retrieved by users.
3. The following guidelines are recommended for managing Emails:
   a. Save your mails as files on your disk regularly and delete from mail box.
   b. Use departmental mailboxes to store official Emails.
   c. Adopt the practice of sending copies of official Emails to the departmental mailboxes. Such mailboxes shall be backed up periodically. Occasionally, depending on storage, print Email and then purge.

5.3.7 Sending and Receiving Emails

1. Responsibility: Users are responsible for Emails they send and for contacts made.
2. Composing: Email shall be written carefully and politely. As messages may be forwarded, Email is best regarded as public property.
3. Carbon copying (cc'ing): Before carbon copying (cc'ing) anyone, consider whether or not it is necessary for the individual to be receiving the message. Email as a medium has increased communication capabilities, but the abuse of copying everyone in the UMaT or outside on messages reduces this benefit when users simply delete messages where they are on the 'cc' list as opposed to being directly addressed.
4. Attachments to Email Messages: Attachment to Email messages shall be used sensibly. Transmission of large volumes of data in a message can have a drastic effect on the general level of service provided to all other users. If it is necessary to include attachments then these shall be restricted to less than 20 Mbytes in size when using internal mail, and 10 Mbytes in size when sending to any Internet addresses. Files larger than recommended above should be broken into separate "chunks" (usually zipped) and then transmitted as separate Email messages.
5. Attachments are sources of virus attacks. Users should not activate attachments unless they are from a trusted source.
6. The following are forbidden:
    a. Sending of unsolicited bulk mail messages of personal nature.
    b. Anonymous messages and chain letters should not be sent.
    c. Advertising of personal items.
    d. Transmitting any material either as the message or as attachments to a message that is unlawful, obscene, malicious, threatening, abusive, libellous, or hateful, or encourages conduct that would constitute a criminal act or give rise to civil liability or unrest or a breach of the University's policies. Among those which are considered offensive are any messages which contain sexual implications, racial slurs, gender specific comments, defamatory statements or any other comment that offensively addresses

someone's age, sexual orientation, religious or political beliefs, national origin or disability.

e. Users are not authorised to retrieve or read any Email messages that are not addressed to them. Employee shall not use any password or code, access a file, or retrieve any stored information, unless authorised to do so.

A breach of overuse of megabytes and any aspect of this directive on sending and receiving Emails shall result in: disciplinary action including withdrawal of access privileges, payment for loss or damage to ICT facility and suspension or expulsion from the University. The University also reserves the right to report any illegal activities to the appropriate legal authorities, *eg,* the Police.

5.3.8 Types of Mailing Lists

Mailing lists shall be created to facilitate communications and dissemination of information in the University. A mailing list may be moderated or non-moderated. When a list is moderated, messages sent to the list shall first be checked by a moderator before it is released to the list members. For a non-moderated list, messages are sent to the list members without any checks by someone.

For the purpose of this Policy mailing lists are categorised into two types:

1. UMaT Staff and Student Mailing Lists; and
2. Other Mailing Lists.

1. UMaT Staff and Student Mailing Lists
   a. The UMaT Staff Mailing List shall be created and used for disseminating University-wide announcements, events and news.
   b. The list shall be restricted to staff of the University.
   c. All subscribers to the University Email system are automatic members of the list.
   d. The List shall be moderated by the Webmaster.
   e. The Webmaster is mandated to reject messages sent to the list for circulation based on the following grounds:

i. When message is of personal nature.
ii. When message is defamatory or insulting.

2. Other Mailing Lists

Based on requests from users, the ICTU shall create on the Email server, other mailing lists for Faculties, Departments or groups that have some common interest or subject matter to share. For instance, a mailing list could be created for senior members of a Faculty.

5.3.9 Creating a Mailing List

Applicant shall send an Email to helpdesk@umat.edu.gh with the following information:

1. Name of Applicant.
2. Department.
3. Contact Phone.
4. Name of List.
5. Description of List.
6. Name and Email Address of Moderator (if list will be moderated).

The mailing list will be created and the applicant notified either by Email or phone. This will normally be done within a day by the ICTU.

6 Internet Policy

The Internet facility is primarily provided to enhance learning, teaching, research and administrative functions of the University. The Internet complements the University's library for researching materials and ideas from a variety of sources both national and international. The facility shall not be used to download personal collection of music, movies or pirated software. Any person that uses the Internet to download personal collections of music, movies or pirated software shall be liable to disciplinary action including withdrawal of access privileges, payment for loss or damage to ICT facilities and suspension or expulsion from the University. The University also reserves the right to report any illegal activities to the appropriate legal authorities, *eg,* the Police.

6.1 Monitoring and Control

1. Since the Internet is an unregulated medium it is highly subject to abuse. The ICTU shall regularly inspect Internet files held on computers connected to the University's network, to ensure users have not accessed inappropriate sites or sites that have been expressly forbidden.
2. Inappropriate sites will be filtered or blocked to ensure that users do not access their materials. Inappropriate sites are those with materials relating to pornography, offensive on grounds including but not limited to ethnic origin, religion, politics and gender.
3. Any user who finds a possible abuse as well as security lapse on any system shall report the event to the ICTU.
4. Users who deliberately access inappropriate material or send inappropriate messages to others shall also have their Internet access withdrawn and shall be dealt with in accordance with University's disciplinary procedures.

   Misuse of the Internet facility by users who deliberately access inappropriate material or send inappropriate messages to others shall result in disciplinary action, including written warnings, withdrawal of access privileges and suspension or expulsion from the University. The University also reserves the right to report any illegal activities to the appropriate authorities, *eg,* the Police.

6.2 Disclaimer of Liability for Use of the Internet

1. The University is not responsible for material viewed or downloaded by users from the Internet.
2. Users are cautioned that some materials from the Internet could be offensive and inappropriate.
3. In general, it is difficult to avoid contact with these undesirable materials while using the Internet. Users accessing the Internet do so at their own risk.
4. Users are to note that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is expected.

6.3 Downloading

1. Information that is downloaded from the Internet shall be used for official or academic purposes. Copyright laws shall be respected and the appropriate credit given to the author or source of the information.
2. The downloading of text or images which contain material of an offensive, indecent or obscene nature is prohibited.
3. Any software or files downloaded via the Internet onto the University's computers may be used only in ways that are consistent with their licenses or copyrights.
4. No user may use the University's facilities knowingly to download or distribute illegal software or material.
5. No user may use the University's Internet services to propagate deliberately any virus.

Any breach of these directives may result in disciplinary action, including written warnings, withdrawal of access privileges to the Internet facility and suspension. Also individual persons shall be held liable for any infringement of copyright laws as a result of downloaded information from the Internet or distribution of illegal software or material.

6.4 Peer-to-Peer (P2P)

1. Use of P2P applications (bittorent) for file sharing and entertainment is deemed to be inappropriate use and shall not be permitted.
2. P2P usage enable sharing and distribution of copyrighted works, and the Copyright Act makes it illegal to make or distribute copyright materials without proper authorization from the copyright owner. The University shall enforce protocol or port level restrictions to prevent P2P activities.
3. Individual persons shall be held liable for any infringement of copyright laws as a result of sharing and distribution of copyrighted works without proper authorisation from the copyright owner.

6.5 E-Commerce

1. The use of the University's Internet services to conduct business or e-commerce activities not related to the University is expressly prohibited.
2. The use of the University's Internet services to engage in hacking other sites, accessing unauthorised information within and outside the University; stealing and using credit cards are criminal and prosecutable in the law courts.
3. Inappropriate use of the University's Internet facility to conduct business or e-commerce activities not related to the University shall result in:
    a. Loss of access privilege to the Internet facility and the University reserves the right to surcharge the person for the use of the University's Internet facility to conduct business.
    b. Individual liability to any offence committed as a result of using the University's Internet facility to engage in any illegal activities such as hacking, accessing unauthorized information within and outside the University or stealing and using of credit cards.

6.6 Chat and Newsgroups

1. Users of any chat Internet facilities shall identify themselves honestly, accurately and completely when participating in chats or newsgroups.
2. Users may participate in newsgroups or chats in the course of their work or study, but they do so as individuals, speaking only for themselves. Only those users who are duly authorised to speak to the media on behalf of the University may write in the name of the University to any newsgroup or Website.

7 Website Policy

7.1 Website Governance

1. Website Manager (Webmaster): There shall be a Website Manager (Webmaster) who will provide quality assurance on the Content, Look and Feel of the University's Website ensuring that it is in tune with the University's mission, unique identity, core values and status.

2. The Webmaster shall be responsible for setting policies governing the nature, content, format, maintenance, timeliness and ownership of information contained on the official pages of the website.
3. Public Relations Unit (PRU): The Public Relations Unit (PRU) shall be responsible for maintaining the content of the Home and main web pages. Information to be put up on these main pages shall be routed through the PRU. The PRU shall then proof read and edit the content. It will have an officer designated as a Web Assistant. The Web Assistant shall be responsible for updating the website and responding to Emails.
4. ICT Unit: The ICT Unit shall provide technical and advisory support services for the website. The ICTU shall be responsible for maintaining the University's web server.

7.2 Website Structure and Content

The website shall be made up of the following web pages:

1. Main University Web Pages: These shall comprise the University Home Page and pages that provide:
    a. The profile of the University, *ie*, the governance structure, the courses and programmes of the Schools, Faculties, Institutes and Centres, as well as the administrative departments.
    b. Admission and registration processes and requirements.
    c. University Policies and Regulations.
    d. News, events and announcements.
2. Departmental Web Pages: These shall comprise the pages or website of the respective Schools, Faculties, Institutes and Centres of the University. These pages shall provide details of the courses, programmes as well as academic staff. Personal web pages of Staff may be set up under the Departmental websites.
3. Student Web Portal: This shall be made up of pages that capture the life, programmes and activities of students.
4. Affiliates Websites: These are the websites of the affiliates of the University that the University may choose at its own discretion to have links.

5. Others Website: These are sites that the University may have links to, for the purpose of collaboration.

7.3 Website Rules and Regulation

7.3.1 Main University Web Pages

1. The Public Relations Unit shall be responsible for updating and maintaining the content of the main University web pages.
2. The content of the main University web pages shall reside on the University web server.

7.3.2 Departmental Web Pages

1. By default, where a Department does not have a website, a minimum number of web pages on the University web server shall be allocated to publish information about the Department.
2. The PRU in conjunction with the ICTU shall create a standard set of pages for Department. However, responsibility for maintaining information on the website shall rest with the Department's Web Assistant.
3. Departments may choose to have a website of their own which may be hosted outside the University's web server. In this case a link will be established on the University's website to the Department's site. Based on the policy provisions in this document, the PRU in consultation with the ICTU shall approve of the establishment of links to departments that have established their own websites.
4. The web pages of Department-owned websites shall comply with the policy provisions in this document. Websites that do not comply may have their links removed. The decision shall be made by the Webmaster. This regulation applies to personal pages of Faculties.
5. The PRU shall ensure that information on all Departments, *ie*, Schools, Faculties, Departments, Institutes or Centres is available on the website.

7.3.3 Student Web Portal

1. The student web portal shall be managed by the Student Representative Council (SRC) under the auspices of the office of Dean of Students.
2. The student web portal shall be hosted by the University's web server.
3. For other student groups, the decision to link or host pages shall be at the discretion of the PRU.

7.3.4 Websites of Affiliates and Others

1. Links to the websites of Institutions affiliated to the University or otherwise shall be established at the discretion of the University.
2. The PRU shall conduct due diligence of the institution website using the provisions in this policy document and grant approval in consultation with the Webmaster.

7.3.5 Applications to link to University Website

1. Outside institutions or organisations that wish to establish a link on their website to that of the University's shall apply to the PRU.
2. The PRU shall conduct due diligence of the institution and their website using the provisions in this policy document and grant approval in consultation with the Webmaster.

7.3.6 General Guidelines for Web Pages

The following guidelines apply to all web pages under the control of the University:

1. Content Management System: All web pages or websites shall have a Content Management System (CMS) that provides the capability for a Web Assistant who has no web programming skills to update the information on the website.
2. Identification: All web pages shall be identified by the University logo or logotype.

3. Contact Information: All web pages shall carry the Email address of the department or officer in charge for their upkeep. The Web Assistant/ Departmental Secretary shall check for Email and respond.
4. Legal Compliance: All pages may not violate the University's policy and statutes, copyright, libel, obscenity or other local or national laws.
5. Commercialisation: Web pages may not be used for commercial purposes, sales or money-making ventures except those authorised by the University administration.
6. Accuracy and Currency: All pages shall be accurate, well-written, concise, and free of spelling and grammatical errors, and shall otherwise present the University's mission and values in a positive light.
7. Monitoring: All pages shall be regularly monitored by the Web Assistants to ascertain that material is current or appropriate. Outdated or inappropriate materials shall be removed within five working days when they are noticed.
8. Enforcement of Website Policy:
    a. Any staff, student or individual that notices an error or considers content on the website to be inappropriate may bring it to the attention of the PRU or Web Assistant in charge of the page.
    b. The PRU or Web Assistant shall take measures to address the concern and give a feedback to the complainant.
    c. The following shall govern the escalation procedures if the issue has far-reaching implications:
        i. Head/Secretary/Web Assistant of a department shall escalate to PRU.
        ii. PRU escalates to Webmaster.
        iii. Webmaster escalates to Head of ICTU.
        iv. Head of ICTU escalates to ICT Management Committee.
    d. Where an individual who reported a problem on the site is not satisfied, the complaint may be escalated to the Academic Board.
    e. Any page on the University site that violates policy may be removed from the website immediately by the Web Assistant of the Department or PRU or the University Webmaster.

8 IT Procurement Guidelines

The following guidelines are provided for the procurement of IT hardware, software and networking products and services. When in doubt, user Departments shall consult the ICTU for clarification or advice. ICTU shall publish standards and specifications for computer equipment and software at its website.

8.1 Service Contract

1. User Departments are advised to consult the ICTU before any contract with any ICT service provider is consummated.
2. The ICTU shall publish Contract Templates that may be adopted for ICT service contracts.

8.2 Technology Acquisition Guidelines

1. Warranty: A minimum of two (2) years warranty shall be specified for all technology acquisitions.
2. Laptop and Desktop Computers: Computers purchased shall have sufficient capacity to run applications at satisfactory response time for at least the next 5 years.
3. Proven Technology: Only proven hardware and software with available and very well established support shall be acquired. Preference shall be on proven technology, not leading edge.
4. Industry Standards Based: Technologies that conform to international industry standards shall be adopted. This will apply to hardware, networks, operating systems, databases and portable software. Proprietary technology and tools shall be avoided where industry standard systems exist.
5. Compatibility: New technology components shall be compatible with one another and with the existing ICT systems.
6. Upgradeability and Scalability: Technology components acquired shall be upgradeable or scalable.
7. Security: The Technology component or system shall have industry standard security built in.

9 IT Project Management Guidelines

IT Projects are generally risky and shall therefore be managed using best Project Management practices.

9.1 Project Implementation Team

1. All IT Projects shall have a properly constituted Project Implementation Team (PIT).
2. For a University-wide project, the PIT shall be constituted by the Vice Chancellor
3. For a Faculty or Departmental project, the PIT shall be constituted by the Dean or Head of the Department that is the direct beneficiary of the IT project.
4. The PIT shall comprise:
    a. Project Sponsor – The Vice Chancellor, Dean, or Head where applicable.
    b. Project Manager – Preferably shall be appointed from the faculty or department that is the direct beneficiary of the project.
    c. Project Team – Depending on the nature and scope of the project, the team shall be cross-functional (*ie,* a mix of Faculty, ICTU, *etc*)
5. The following shall form the phases of the project:
    a. Project Initiation
        i. Project justification and approval process resulting in an approved budget.
        ii. There shall be a Project Definition Document that defines at least the goals, objectives, resources to be used, deliverables and time frame of the project.
        iii. Identification and selection of Project Team members.
        iv. Definition of roles and responsibilities.
    b. Project Planning
        i. Preparation of detailed plans for managing the project.
        ii. The planning phase shall be used to define the project infrastructure – project filing and documentations and the various procedures for managing the issues, quality, risks, reporting and communications.

c. Project Execution
    i. Monitoring and controlling the project plan.
    ii. Issuing status reports.
d. Project Closure: Formally handing over deliverables and issuing Project Completion Report.

10 Policy Enforcement

1. The ICTU in conjunction with the Audit Unit, and Planning and Quality Assurance Unit of the University shall audit compliance with this Policy from time to time. The outcome of the audit shall be a rating of the User Department compliance which will be published.
2. The ICTU and Planning and Quality Assurance Unit shall be audited by an appointed external IT auditor twice in a year.
3. Users who flout the policy provisions shall be sanctioned according to the regulations of the University or the policy sanctions specified in this Policy.

10.1 Sanctions

1. Any student, staff or employee who contravenes the rules and regulations, guidelines or procedures spelt out in this policy document shall be liable to sanctions.
2. Appropriate sanctions shall be prescribed by the officer in charge or by a disciplinary committee constituted by the Vice Chancellor or his/her representative.
3. For the avoidance of doubt, the appropriate sanctions shall include withdrawal of access privileges, payment for loss or damage to ICT facilities and suspension or expulsion from the University. The University also reserves the right to report any illegal activities to the appropriate legal authorities, *eg,* the Police, Copyright Administration Authority, National Communication Authority, National Information Technology Agency, *etc*.

10.2 Amendments to Policy

1. An amendment could be a modification of an existing policy guideline or an addition to the Policy.
2. A member of the user community shall write to the ICTU to propose an amendment to the Policy.
3. The ICTU shall in consultation with the ICT Management Committee study the proposal.
4. If the proposed amendment is found to be meritorious, it shall be forwarded to the Academic Board through the Vice Chancellor.