



**Mangosuthu
University of Technology**

ACCEPTABLE EMAIL USE POLICY

Approved by Council on: **04/04/2012**

1 PURPOSE

The purpose of the policy on Acceptable Email Use is to provide a framework that will guide Mangosuthu University of Technology (MUT) staff, students, and service providers, in understanding the acceptable and appropriate use of the email system, and related services and facilities to accomplish the University's core activities (teaching, learning, research, community engagement, and the rendering of support services).

The policy will serve to define the accepted behaviour of email system users that will allow MUT:

- To ensure and maintain the integrity, security, reliability, and quality of the email services;
- To protect email users and email infrastructure from abuse; and
- To adhere to and comply with national laws and legislation.

2 RATIONALE

Email is an efficient and timely communications tool that is provided at MUT primarily for University business purposes, to employees, students and service providers to assist them in accomplishing the University's core activities. The use of email has to be managed for it to bring the maximum benefit to the University. Email creates a large potential for misuse and abuse and its use must be controlled. Acceptable and appropriate use of the email system can enhance productivity and efficiency, but inappropriate use can conflict with the University's vision, mission, and policies, and it can compromise availability of the email system for all.

This policy seeks to define requirements and prohibitions for acceptable and appropriate use of the University email system, related services, or any messaging system that uses the University's computer network.

3 OBJECTIVES

The objectives of the Acceptable Email Use Policy are:

- 3.1 To enforce appropriate use of email and related services and facilities to fulfil the University's core activities and the rendering of support services;
- 3.2 To guarantee appropriate use of the e-mail and related services and facilities, which are beneficial to the University's community of email users;
- 3.3 To protect the University's IT and Computer Systems and related resources, e-mail system, and data integrity against intrusion and malware;
- 3.4 To prevent unauthorized and unprotected connections to the University and e-mail systems;
- 3.5 To secure the IT and Computer Systems Security across the entire University network;
- 3.6 To urge Users of the University e-mail, related services and facilities to apply self-regulation in their use of the e-mail and that they acquaint themselves with the legal consequences of inappropriate use of such services and facilities; and
- 3.7 To maintain and apply appropriate monitoring arrangements to all e-mail and related services and facilities which it provides to all Users on a continual basis.

4 SCOPE

This policy covers acceptable and appropriate use of any email sent from and/or received through MUT email address and also applies to all email users who are MUT employees, students, service providers, and other authorised users of the University IT and email related services and facilities. It will be enforced for intended and unintended transmission of viruses, worms, malicious code, or otherwise unknown causes and prohibited usage.

5 DEFINITION OF TERMS

5.1 Email

Email is the Electronic mail which will be defined as a method of exchanging digital messages from an author to one or more recipients. It operates across the computer networks. Email systems are based on a store-and-forward model. Email servers accept, forward, deliver and store messages. Neither the users nor their computers are required to be online simultaneously; they need connect only briefly, typically to an email server, for so long as it takes to send or receive messages.

5.2. Email blast

An email blast will be defined as an electronic mailing, sent all at once to a large mailing list. This is commonly used by marketers who want to send email advertisements or promotions to their list of customers. It is usually done with the help of special software or through an email service provider. For the email blast to be effective, the people on the mailing list must have "opted-in", meaning that they have signed up to receive messages.

5.3. IT and Computer Systems

IT and Computer Systems will mean the computers, terminals, printers, networks, modem banks, online and offline storage media and related equipment, software, and data files that are owned, managed, and maintained by the University. These will include institutional and departmental information systems, faculty and/or research systems, desktop and laptop computers, the University's Campus network, and the University's general access computer clusters.

5.4 Malicious code

Malicious code will be used to describe any code in any part of a software system or script that is intended to cause undesired effects, security breaches or damage to a system. It describes a broad category system security terms that includes attack scripts, viruses, worms, Trojan horses, backdoors, and malicious active content.

5.5 MUT

MUT will mean Mangosuthu University of Technology.

5.6 Software

Software will mean all intangible programmes and systems intended for use or installation in IT and computer systems devices acquired for or/on behalf of the University, developed by the University, or contracted personnel on behalf of the University. Such software shall be deemed University property/assets. All such software will be used in compliance with applicable licenses, notices, contracts and agreements.

5.7 University

University will mean Mangosuthu University of Technology.

5.8 Users

Users will mean people, including University's employees, students and service providers who use the University's IT and Computer Systems (hardware, software) email, and programmes.

5.9 Unsolicited email

Unsolicited email will mean an unsought email that is sent to a recipient who has not requested it. If it is sent to a group of recipients who have not requested it, it is called the 'unsolicited bulk email (UBE) which is also known as email spam or junk email.

5.10 Virus

Virus will be defined as a programme or programming code that replicates by being copied or initiating its copying to another programme, computer boot sector or document. Viruses can be transmitted as attachments to an email note or in a downloaded file, or be present on a CD or diskette. The immediate source of the email note, downloaded file, or diskette received is usually unaware that it contains a virus. Some viruses wreak their effect as soon as their code is executed; other viruses lie dormant until circumstances cause their code to be executed by the computer. Some viruses are benign or playful in intent and effect and others can be quite harmful, erasing data or causing hard disk to require reformatting. A virus that replicates itself by resending itself as an email attachment or as part of a network message is known as a "worm".

6 POLICY PRINCIPLES

This policy is guided by the following principles:

6.1 Liability of users or the University

The University will not accept liability for negligence or otherwise; for dissemination of any content, information, images or data that encourages practices, which are prohibited by law and/or that, are the consequences of misuse of the , e-mail and related services and facilities. It will not accept liability for infringement of intellectual property rights and/or for any practices that do not constitute acceptable and appropriate use of the University e-mail and related services and facilities, except when they are legal and there is a demonstrable University business need to access or distribute such content:

6.1.1 Intellectual property

Any user who uses email to send or receive any material that infringes the intellectual property rights of a third party may be liable to that third party if such use is not authorised by them;

6.1.2 Defamation

Legal responsibility for the transmission of any defamatory, obscene or rude remarks which discredit an identifiable individual or the University will rest mainly with the sender of the email and may lead to appropriate disciplinary action being taken or substantial financial penalties being imposed;

6.1.3 Discrimination

Any material disseminated which is discriminatory or encourages discrimination is unlawful and shall not be accepted by the University;

6.1.4 Data protection

Processing information, including photographs, which contains personal data about the individuals, requires the express written consent of those individuals; and

6.1.5 Disclaimer

The University may arrange for an appropriate disclaimer to be appended to all email messages that are sent to external addresses from the University, in order to provide necessary legal protection.

6.2 Privacy

MUT email is public, not private communication, not only because its principal purpose is the conduct of the University business, but also because the email system permits forwarding and other wide distribution of messages without the consent of the sender. Therefore, senders and receivers of email can have no expectation of privacy with respect to MUT email (messages) system.

6.3 Property of the University

The email system is the property of the University. All passwords, user IDs, and messages created and transmitted are a property of the University.

6.4 Writing style

The University's emails are the equivalent of letters sent on official letterhead, and must therefore be written in a professional and courteous tone. They should be treated as formal business documents, the style, spelling, grammar, language, and punctuation should be business-appropriate and accurate.

6.5 Monitoring arrangements

6.5.1 The University reserves the right to use monitoring software in order to check upon the use and content of emails; to monitor messages without prior notice; inspect, copy, review any data recorded in the University's email systems and any and/or all files, information, software, and other content created, sent, received, downloaded, uploaded, accessed, or stored in connection with employee usage; and

6.5.2 The University may, at its discretion, apply automatic message monitoring, filtering and rejection systems as appropriate, and deny transmission of messages with content that is unacceptable in terms of this policy.

6.6 Interception

The MUT email users must acknowledge that the University is lawfully required to intercept communications in accordance with the provisions of the Regulation of Interception of Communications and Provision of Communication – related Information Act No: 70 of 2002, as amended. Any interception of communications shall be strictly in accordance with the requirements of the Act, as and when required under the Act.

6.7 Laws and Legislation

6.7.1 The University's email infrastructure will be used only for lawful purposes. Users may not violate any applicable laws or regulations of South Africa within the territory of South Africa. Should the user reside outside of South Africa, the laws of the country in which the user resides shall apply; and

6.7.2 Transmission, distribution or storage of any material on or through the University's email infrastructure in violation of any applicable law or regulation is prohibited. This includes, without limitation, material protected by copyright, trademark, trade secret or other intellectual property right used without proper authorisation, and material that is obscene, defamatory, constitutes an illegal threat, or violates export control laws.

6.8 Authorised personal use of the email system

The University permits the use of email system by employees, students, service providers, and other authorised users for personal use, subject to the following limitations:

- 6.8.1 A level of use must be reasonable and not detrimental to the main purpose for which the facilities are provided;
- 6.8.2 Priority must be given to use of resources for the main purpose for which they are provided;
- 6.8.3 Personal use must not be of a commercial or profit-making nature, or for any other form of personal financial gain;
- 6.8.4 Personal use must not be of a nature that competes with the University in business;
- 6.8.5 Personal use must not be connected with any use or application that conflicts with an employee's obligations to MUT as his/her employer;
- 6.8.6 Personal use must not be connected to any purpose or application that conflicts with the University's policies, procedures, rules and regulations; and
- 6.8.7 Personal use must comply with the University's vision, mission, and policies, in particular this Acceptable Email Use Policy;

6.9 Prohibited email use system and facilities

Email system and related facilities provided by the University should not be used for:

- 6.9.1 Personal use other than as specified under section 6.8 above;
- 6.9.2 Transmission of unsolicited commercial or advertising material, chain letters, press releases, or other junk-mail of any kind;
- 6.9.3 Campaigning for political causes or candidacy;
- 6.9.4 Promoting or soliciting funds for religious or other personal causes;
- 6.9.5 Using email system to play online games, visit chat rooms, shop online or engage in illegal activities including but not limited to gambling and drug dealing;
- 6.9.6 Unauthorised transmission to a third party of confidential material concerning the activities of the University;
- 6.9.7 The transmission of material such that this infringes the copyright of another person, including intellectual property rights;
- 6.9.8 The unauthorised provision of access to University services and facilities by third parties;

- 6.9.9 Activities that unreasonably waste staff effort or networked resources, or activities that unreasonably serve to deny service to other users;
- 6.9.10 Activities that corrupt or destroy other users' data;
- 6.9.11 Activities that disrupt the work of other users;
- 6.9.12 Using email language that has offensive content; that is harassing, and contains discriminatory activities: University employees, students, and service providers have the right to work, and learn in an environment that is free from hostility of any kind. They are prohibited from using the email system to engage in activities or transmit content that is harassing, discriminatory, menacing, threatening, obscene, defamatory, or in any way objectionable or offensive.

University employees, students, and service providers are prohibited from using the email system to:

- Conduct disputes and/or arguments using the University Email System and CC (carbon copy) other individuals;
- Send, receive, solicit, print or reply to text or images that disparage others based on their race, religion, colour, sex, sexual orientation, national origin, veteran status, disability, ancestry, or age;
- Send, receive, solicit, print or reply to jokes (text or images) based on their race, religion, sex, sexual orientation, national origin, veteran status, disability, ancestry, or age;
- Send, receive, solicit, print or reply to messages that are disparaging or defamatory;
- Spread gossip, rumours, and innuendos about employees, staff, students, suppliers, or other outside parties;
- Send, receive, solicit, print, copy or reply to sexually oriented message or images;
- Send, receive, solicit, print, copy, or reply to messages or images that contain foul, obscene, off-colour, or adult-oriented language; and
- Send, receive, solicit, print, copy, or reply to messages or images that are intended to alarm others, embarrass the University, negatively impact employee productivity, or harm employee morale;

6.9.13 **Handling Unsolicited Email that Violates University Policy**

The Acceptable Email Use Policy prohibits University employees, students, and service providers from sending inappropriate or offensive material. University employees, students, and service providers are also prohibited from receiving material that violates this policy.

In the event that an employee, a student or a service provider who is a University email user, receives email messages that violate this policy, he/she must take the following steps:

- **If You Know the Sender:** If an employee, a student or a service provider receives email that violates this policy, and he/she knows the sender, then he/she must immediately instruct the sender to stop sending this type of material; and
- **If You Don't Know the Sender:** If an employee, a student or a service provider receives email that violates this policy, and he/she does not know the sender, he/she must not respond or reply to the message. Instead, he/she must immediately notify the Senior Director: Information Technology and Networks, who will attempt to block receipt of this type of material in the future:

6.9.13.1 Passwords

The University email users are not permitted to use passwords or user IDs to access other email user's email messaging system without consent. Misuse of passwords and/or user IDs, the sharing of passwords and/or user IDs with unauthorized University email users will result in disciplinary action, up to and including termination; and

6.9.13.2 Email Blasts

Employees, students, or service providers are prohibited from sending University-wide email messages to all employees, students or service providers without approval and they are prohibited from sending email blasts (mass mailings) to external parties. Any such requirement could be requested from Senior Director: Marketing Communications. Only the Senior Director: Marketing Communications and the designated staff may generate University-wide email distribution lists (email blasts).

7 RESPONSIBILITY AND ACCOUNTABILITY

- 7.1 All **staff, students, and service providers** who are the University email users will familiarise themselves and comply with this policy;
- 7.2 The **Head of the Department/Unit or the Dean of the Faculty** will ensure that this policy is complied with in his/her departments or faculty. He or she will co-operate with Senior Director: Marketing and Communications, and the Senior Director: Information Technology and Networks;
- 7.3 The **Senior Director: Marketing and Communications**, and the **Senior Director: Information Technology and Networks (ITN)** will co-ordinate and administer the implementation of this policy; and
- 7.4 The **Vice-Chancellor** will take overall responsibility for ensuring that this policy on the acceptable email use remains a source of pride to the University.

8 CUSTODIANSHIP

The **Senior Director: ITN** department will be the custodian of this policy.

9 Violations

These guidelines are intended to provide all the University email users with general examples of acceptable and unacceptable use of the University's Email System. A violation of this policy may result in disciplinary action up to and including termination of service relations with the University.

10 POLICY CONTEXT

This policy is informed by the following documents:

- 10.1 The Constitution of the R.S.A, 1996 (Act No: 108 of 1996);
- 10.2 The Copyright Act, 1978 (Act No: 98 of 1978), as amended;
- 10.3 Employment Equity Act, 1998 (Act No: 55 of 1998);
- 10.4 Solutions: Acceptable Use Policy, 2011;
- 10.5.1 MUT Acceptable Use and Management of Information Technology and Computer Systems Policy, 2011;
- 10.5.2 MUT Intellectual Property Rights Policy, 2009;
- 10.6 Promotion of Equality and Prevention of Unfair Discrimination Act, 2000 (Act No: 4 of 2000);
- 10.7 Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002 (Act No: 70 of 2002), as amended;
- 10.8 Staffordshire University: University Policies and Regulations, 2005; and
- 10.9 University of Cape Town: Policy and Rules on Internet and Email Use, 2007.

11 POLICY REVIEW

This policy will be reviewed when it becomes necessary.