Internet, Electronic Communication and Web Management Policy

1. PREAMBLE

This policy applies to all users who have access to and/or use UNISA's communication facilities or equipment. It provides rules, standards and guidelines on the use of UNISA's communication facilities and equipment to ensure the value and integrity of UNISA's equipment and network(s).

2. DEFINITIONS AND ABBREVIATIONS

CCM means Department of Corporate Communication and Marketing;

ICT means Information and Communications Technology;

Communication facilities include internet access, email access and the use of any equipment made available by UNISA for purposes of:

a) accessing, creating, copying, distributing, sharing and deleting records

b) initiating, creating, receiving or storing communications;

Communications include

a) written text and verbal utterances of a user in or during a meeting where the business of UNISA or related matters are discussed,

b) the transfer of any information whether speech, data, text or images in any format through communication facilities,

c) access to or use of the services available on the internet, including email, websites, file transfer, video conferencing, voice over Internet Protocol, chat rooms and bulletin boards by users through the equipment;

Content manager is a person responsible for the content management of a website which, in the UNISA environment, may be either a departmental website, a website belonging to an organisational unity or any subsection of the UNISA website;

Discriminatory means offensive, untrue or provocative material based on race, gender, sex, pregnancy, marital status, ethnic or social origin, colour, sexual orientation, age, disability, religion, conscience, belief, culture, language and birth;

Email is the exchange of electronic text messages and computer file attachments between computers over a communications network, such as a local area network or the internet;

Equipment means computers, desktops, servers, routers, laptops, telephones, cellphones, electronic handheld devices, facsimile machines, pagers, software, hardware and/or similar equipment owned by, licensed to or rented by UNISA;

EWCD means Electronic and Web Communication Directorate;

© 2009 UNISA
All rights reserved

Front line departments
Student Admissions and Registrations, Student Assessment Administration, Finance, Contact Centre, Graduations and Records Management;

Illegal content
refers to material that is

- pornographic,
- discriminatory,
- oppressive,
- racist, including hate speech,
- sexist or defamatory against any user or third party,
- offensive to any user or group,
- a violation of a user's or a third party's privacy, identity or personality,
- an infringement on copyright,
- contains malicious codes such as viruses and Trojan horses containing content of any personal information of third parties without their express consent, and
- includes hyperlinks or other directions to such content;

Intercept
means filter, scan, block, redirect, access, disrupt, copy, print, disclose, retain, use, collect, delete and/or record, in any format and in any manner;

Internet
refers to a cooperative system linking computer networks worldwide which include intranets, mobile networks, wireless access areas, email, world wide web, news groups, ftp, and so on;

Multimedia
refers to the use of several media, such as movies, slides, music and lighting in combination normally for the purpose of education or entertainment;

Online advertising
is a form of advertising that uses the internet and world wide web in order to deliver marketing messages and attract customers;

Personal information
means personal information as defined in the Promotion of Access to Information Act, 2000;

Policy
means this Internet and Electronic Communication Policy;

Pornographic
means all the content and actions, simulated or real, graphic or written detailed in Schedules 1, 2, 6, 7 and 11 of the Films and Publications Act 65 of 1996;

PowerPoint
is a Microsoft Office Presentation Software that allows one to create slides, handouts, notes and outlines[1];

Record
means any content, document, record, file, data, information, picture, download, graphic depiction, representation or software that is created, used, accessed, disclosed, copied, stored, received or delivered by a user, regardless of the format thereof;

User(s)
mean all persons who have access to or use of UNISA's equipment, communication facilities or communications;

[1] www.gslis.utexas.edu/~vlibrary/glossary/

© 2009 UNISA
All rights reserved

World wide web	is a client-server information system that uses the internet to access computers containing millions of hypertext documents.

3. SCOPE OF APPLICATION

This policy applies to all users, which also includes third parties, who have temporary access to and/or use of UNISA's communication facilities or equipment.

4. PURPOSE

The purpose of this policy is to

4.1. inform and educate users on the access to and use of UNISA's communication facilities and equipment;

4.2. create rules for the access to and use of UNISA's communication facilities and equipment;

4.3. provide for the interception of communications;

4.4. provide for disciplinary action against users who fail to comply with this policy;

4.5. ensure and maintain the value and integrity of UNISA's equipment and network(s).

5. RESPONSIBILITIES OF USERS AND DEPARTMENTS

5.1 Users are personally responsible for:

5.1.1 abiding by the rules created in this policy and other related policies;

5.1.2 the creation, provision, updating and maintenance of information, data and communication using the infrastructure provided by the ICT Department.

5.2 The ICT Department is responsible for:

5.2.1 the technical issues related to the access to and use of UNISA's communication facilities and equipment;

5.2.2 assisting UNISA's management in intercepting communications and investigating breaches of the provisions of this policy;

5.2.3 causing all outgoing email messages to contain UNISA's official email legal notice;

5.2.4 scanning, filtering and blocking all electronic communications for damaging code such as viruses.

© 2009 UNISA
All rights reserved

5.3 Corporate Communication and Marketing Department is responsible for:

5.3.1 managing and maintaining the corporate websites;

5.3.2 implementing the corporate image, marketing and communication elements on the internet mediums;

5.3.3 coordinating content provision by information providers;

5.3.4 providing specialised hypertext authoring;

5.3.5 ensuring quality assurance of the content and presentation of information.

5.4 The Colleges, with the assistance of the Directorate: Curriculum and Learning Development, are responsible for:

5.4.1 researching, teaching and learning via the internet;

5.4.2 coordinating teaching and learning via the internet;

5.4.3 developing and implementing support and the enhancement of distance learning with internet communication tools and resources;

5.4.4 developing and implementing fully online delivered courses;

5.4.5 ensuring quality assurance of learning materials on the internet.

5.5 The Management Committee is responsible for:

5.5.1 ensuring that the Internet, Electronic Communications and Web Management Policy is formulated, implemented, updated and enforced;

5.5.2 ensuring that the electronic communication facilities are used to support the vision and mission of the University;

5.5.3 instituting disciplinary action if the policy is not adhered to.

5.6 Heads of operational units are responsible for:

5.6.1 ensuring that employees use the electronic communication facilities as prescribed in this policy;

5.6.2 ensuring that information relevant to their operational units is correct, supplied in good time for dissemination and conforms to University standards;

5.6.3 providing facilities where students may access the internet;

5.6.4 informing the students of this Policy and taking appropriate action when students do not adhere to the guidelines for acceptable use.

© 2009 UNISA
All rights reserved

SECTION A

USE OF THE INTERNET (ICT)

6. RATIONALE

UNISA has a legal right and duty to:

6.1 secure and maintain its computer network, equipment and communication facilities;

6.2 ensure the confidentiality of its trade secrets, client/student information, employee information and confidential information generally;

6.3 protect the privacy of its clients/students;

6.4 identify and address the potential risks associated with the use of technology and communication facilities in the workplace;

6.5 promote employee productivity;

6.6 comply with the provisions of laws and regulations that govern the access, use and interception of communications;

6.7 investigate and institute disciplinary action for illegal or unauthorised use of its communication facilities and/or equipment;

6.8 respect and protect every employee’s right to privacy, free speech and the right to receive and impart with information as detailed, amongst others, in the South African Constitution, 1996;

6.9 to successfully discharge the abovementioned obligations UNISA needs to:

- regulate employee use of equipment and communication facilities,
- monitor and intercept employee communications, and
- secure and maintain the equipment and communication facilities.

7. RIGHT TO MONITOR

7.1 UNISA reserves the right to intercept any communication and/or record any such interception if reasonably required and justified for one or more of the following purposes:

7.1.1 Compliance with UNISA’s rights and obligations detailed in paragraph 6 above.

7.1.2 Investigating, preventing or detecting unauthorised access or use.

7.1.3 Investigating, preventing or detecting breach of the provisions of this policy.

7.1.4 Maintenance of the security of any equipment or communication facilities.

7.1.5 Disaster recovery or similar emergency measures.

7.1.6 Prevention of loss or destruction of UNISA assets or data.

7.1.7 Investigating or detecting illegal activities.

© 2009 UNISA
All rights reserved

UNISA's right to intercept any communication will:

7.1.8 only commence with the prior written authority of the Principal or the Executive Director: Legal Services;

7.1.9 be implemented with due regard to the privacy and constitutional freedoms of users.

7.2 Any person who actually intercepts communications or has access to intercepted communications will sign a non-disclosure agreement prior to such interception and undertake not to disclose the interception process, the identity of the person or subject and/or any related information, unless authorised to do so by due legal process or for the purposes of disciplinary or legal action.

UNISA will not share or disclose the following information to third parties:

7.2.1 private, personal and confidential information collected through the interception of communications, or

7.2.2 the identity of users whose communications are or were the subject of interception

unless such disclosure is authorised by due legal process or for the purpose of disciplinary or legal action.

8. ACCEPTABLE USE

This paragraph details general guidelines for the access and use of UNISA'S equipment and communication facilities:

8.1 UNISA has the right to limit the size of incoming and outgoing email messages and attachments, downloads and other files, and may block and delete email messages, downloads, attachments or other files that are larger than the set maximum size. It is the responsibility of users to limit the size of attachments and other files to prevent overloading of equipment.

8.2 Virus warnings or pop-ups that result from incoming email or file downloads must be reported to the ICT Department Help Desk immediately as indicated in the *Guidelines and Procedures for Electronic Communication and the Web*.

8.3 All outgoing emails must have UNISA's standard email legal notice at the bottom of the message. This email disclaimer may not be removed or tampered with by users.

8.4 Users should log-off or use screensavers with passwords in times of absence from a computer terminal to avoid improper and/or illegal use.

8.5 Notebook and/or offline users should load and update the "address book", if any, regularly.

8.6 Employees must ensure that they save or archive email.[2]

[2] See the *Guidelines and Procedures for Electronic Communication and the Web* document regarding the retention time of email.

© 2009 UNISA
All rights reserved

9. NON-ACCEPTABLE USE

The following communications, actions or forms of content are prohibited and will be sanctioned:

9.1 Sharing logon usernames with or disclosing passwords to anyone, accept ICT technical staff when technical work is being done. Directly after such disclosure, the user should change his/her password.

9.2 Intentionally bypassing the security mechanisms of the equipment or any third party security system or website.

9.3 Modifying the internal mail transport mechanism to forge a routing path that a message takes through the internet.

9.4 Downloading, receiving and/or installing software applications not approved by the ICT Department.

9.5 Knowingly burdening UNISA's equipment or communication facilities with data unrelated to UNISA's official business (e.g. forwarding, downloading or accessing large video clips or graphics to or from a distribution list or file-sharing server).

9.6 Sending or forwarding messages and attachments that are infected with malicious codes such as viruses.

9.7 Using discs that may be infected with malicious code.

9.8 Using any encryption, authentication and/or digital signatures not authorised by the ICT Department in writing.

9.9 Downloading, reproducing, sharing, retaining and/or creating records that contain music, images, sound or video if such record is not reasonably required for the user's official UNISA services[3].

9.10 Accessing and using internet relay chat if such actions burden UNISA's equipment or communication facilities.

9.11 Any actions that knowingly prevent other users from using and accessing equipment or communication facilities.

9.12 Taking any of the steps or actions criminalised and detailed in Chapter XIII of the Electronic Communications and Transactions Act 25 of 2002, including but not limited to hacking or developing, downloading and using any technology that may circumvent IT security measures.

9.13 Any destructive and disruptive practices on, through or with equipment or communication facilities.

9.14 Indiscriminate storage and/or forwarding of email, files, websites and attachments for which permission has not been obtained from the originator or copyright holder.

9.15 Any purposes that could reasonably be expected to cause, directly or indirectly, excessive strain on any computing facilities, or unwarranted or unsolicited interference with others.

[3] Personal files created or retained in computer software that is supported and maintained by the ICT Department e.g. MS Word, Excel etc. will be allowed, provided that the personal files use reasonable space. Pictures and video/sound recordings, MP3, etc. will only be allowed if it does not interfere with the hard disk space of the PC or any other system and is virus free.

© 2009 UNISA
All rights reserved

9.16 Sending, replying to or forwarding email messages or other electronic communications which hide the identity of the sender or represent the sender as someone else.

9.17 Using or accessing UNISA's equipment or communication facilities to commit fraud or any other criminal offence(s).

9.18 Initiating audio streaming of any kind. In cases where it is necessary and related to the work of a specific employee, written permission from the specific employee's head of department must be obtained.

10. LEAVING THE UNIVERSITY

On resignation, all electronic facilities will be terminated and equipment will be submitted on the last working day. It is the responsibility of the employee to timeously supply interested parties with his or her new email address and/or inform them that the current email address will no longer be valid.

11. SKYPE PHONES OR WEBCAMS

The use of skype phones or webcams is currently not allowed due to bandwidth limitations. The ICT Department will block the use thereof. The concept will be tested from time to time in a laboratory environment until such time as it proves to be viable for extensive use throughout UNISA.

12. DELETION OF E-COMMUNICATIONS

Users are responsible for knowing and adhering (managing and storing of electronic records / documents) to UNISA's Records Management Policy.

13. DUTY TO DISCLOSE AND REPORT

Users have the duty to disclose all true or suspected attempts that may reasonably breach any provision of this policy to the Executive Director: Legal Services.

14. CONSEQUENCES OF MISUSE

14.1 Users are bound by this policy. Any contravention of the policy will be treated as misconduct and will be dealt with within the framework of UNISA's disciplinary policy. The level of misconduct will be dependent upon the severity or persistence of the contravention. For the avoidance of doubt, any activities, which are identified in this code of conduct as prohibited, will be treated as misconduct. If users have a grievance associated with the use of the internet or email or other communication equipment, users should refer to UNISA's grievance policy for guidance on how to deal with such grievances.

14.2 If an employee has any questions about this code of conduct or does not understand any part of it, he or she should contact the ICT Department

© 2009 UNISA
All rights reserved

SECTION B

ELECTRONIC COMMUNICATION AND WEB MANAGEMENT (CCM)

15. WEB MANAGEMENT

15.1. The world wide web has provided the University with opportunities:

- to communicate and inform its stakeholders in new and innovative ways, and
- enables it to market its products and services in a cost-effective manner.

15.2 Managing the University's websites is the collective responsibility of CCM and every manager within the University.

15.3 The roles and responsibilities relating to the UNISA web are as follows:

- Heads of organisational units must assign responsibility for keeping their websites updated to web content managers in their respective departments.
- The content manager must liaise with CCM which, in turn, will provide training on how to use the Web Content Management System.
- CCM has the ultimate publishing rights to all corporate websites (public websites and the intranet) and coordinates the publication of all web pages.
- All websites must adhere to brand standards, and should be submitted for editorial and technical quality control by the EWCD.
- Information about formal and nonformal qualifications on the corporate websites will be coordinated by CCM through the colleges, the office of the Academic Planner and the Department of Student Admissions and Registrations.

16. EMAIL COMMUNICATION

16.1. Corporate email communication (Intcom)

16.1.1. Email has become one of the University's most important means of official communication.

16.1.2. The email address intcom@unisa.ac.za is the University's official internal electronic communication channel operated by the Electronic and Web Communication Directorate.

16.1.3. The facility is used to convey policy matters, general management decisions, media releases or news clips, University news, events and notices.

16.1.4. All public groups will be created and managed by CCM.

16.1.5. Intcom will publish the e-news, which is a weekly newsletter, and the e-notice, which is a daily notice to employees.

16.1.6. E-notice messages must reach intcom@unisa.ac.za at a time as indicated in the *Guidelines and Procedures for Electronic Communication and the Web*

© 2009 UNISA
All rights reserved

document on the day they are to be published. Only two repeats of notices are allowed; if more than two repeats are required, permission must be obtained from the Executive Director: Corporate Communication and Marketing.

16.1.7. Special e-notices may only be posted with the express permission of the Executive Director: Corporate Communication and Marketing.

16.1.8. The *Guidelines and Procedures for Electronic Communication and the Web* document will provide more information on publishing times and procedures.

16.1.9. All e-news and e-notice emails will be archived on the intranet.

16.2 Acceptable use of email

16.2.1 Users will use email, which includes applications such as Instant Messaging (Microsoft) and internet access, primarily for UNISA business purposes.

16.2.2 Private and personal use, in moderation, will be tolerated, subject to the rules detailed in this policy. Common sense and good judgement should guide personal and private usage.

16.2.3 When forwarding or replying to email messages, the content of the original message should not be altered. If the content needs to be changed, then all changes must be clearly marked as such.

16.2.4 Email messages should be kept brief and should be formulated appropriately.

16.2.5 Email messages should be treated as formal business documents, written in accordance with UNISA's guidelines. Style, spelling, grammar and punctuation should be appropriate and accurate.

16.2.6 Front line departments must compile a list of frequently asked questions and answers, which must be edited by the Department: Language Services, to be consulted when replying to enquiries.

16.2.7 Users should check email recipient addresses prior to sending, forwarding or replying to messages.

16.2.8 When distribution lists are used, the sender should consider whether or not each group member really needs, or really should, receive the email.

16.2.9 The subject field of an email message should relate directly to the content or purpose of the message.

16.2.10 If users are out of the office for more than one day, they should activate the "Out of Office" function. This informs the sender of the email of the user’s absence. The "Out of Office" message should include both the period of absence and an alternative contact person.

16.3 Unacceptable use of email

16.3.1 Modifying an email message and forwarding or replying to it without noting the changes (ie deletions, removal of recipients, modification of content).

16.3.2 Fabricating a message and/or sender of a message.

16.3.3 Illegal content.

© 2009 UNISA
All rights reserved

16.3.4 Participating in email "chain letters" or similar activities; no employee may send emails to all employees, whatever the topic, or reply to such emails and include the entire list of recipients.

16.3.5 Using automatic forwarding of emails ("Auto Rules") to any person without such a person’s consent.

16.3.6 The creation, sending or forwarding of unsolicited mail (spam).

16.3.7 The creation, sending or forwarding of marketing information or advertising material unrelated to UNISA's official business, or advertising material without the consent of the Department of Corporate Communication and Marketing.

16.3.8 Using or accessing UNISA's equipment or communication facilities to commit fraud or any other criminal offence(s).

17. MULTIMEDIA AND POWERPOINT PUBLICATIONS

17.1. PowerPoint presentations used in the organisation for official use must adhere to the University's brand standards.[4]

17.2. EWCD will assist senior management with the preparation of PowerPoint presentations.

17.3. The request for PowerPoint presentations must reach the EWCD at least a week prior to the event, but preferably two weeks or even longer before, depending on the complexity of the presentation.

17.4. The request must include all the content, pictures and resources necessary to create the presentation, and should be sent to us via email or on CD/flash disk.

18. ONLINE ADVERTISING

18.1. Online advertising can be done in any of the following ways:

18.1.1 Search engine optimisation or improving rankings for relevant keywords in search results by rectifying the website structure. Content should be easy to read and understood by the search engine's software programmes.

18.1.2 Search engine advertising or paying the search engine company for a guaranteed high ranking, or an advertisement displayed with the results[5].

18.1.3 Paid inclusion or paying the search engine company for a guarantee that the website is included in their natural search index.

18.1.4 Affiliate marketing.

18.1.5 Banner advertisements.

18.1.6 Email advertisements.

18.2 Online advertising requests must be submitted to CCM and all requests will be evaluated individually. The following information must be included in the request, namely, the

- purpose of the advertisement,
- medium to be used (e.g. specific websites, portals and search engines),

[4] Templates for PowerPoint presentations can be downloaded from the intranet under the "resources" link.

[5] Commonly known as pay per click advertising

© 2009 UNISA
All rights reserved

- start and end date of the campaign, if this has been decided on,
- advertisement if it has already been designed (either via email or on CD/flash disc).

18.3 Advertising on the UNISA Website

- No advertising will be allowed on the Unisa Website unless it is approved by CCM.
- Online advertisements on UNISA website must relate to the University core business.
- Guidelines and procedures regarding online advertising on UNISA website can be found in the Electronic Communication and Web Guidelines.

19. IMPLEMENTATION OF POLICY

The Internet Policy is replaced with effect from the date on which Council approves this Policy.

☙ ☙ ☙ ☙

© 2009 UNISA
All rights reserved