University of Fort Hare
Electronic Communications Policy

University of Fort Hare
Together in Excellence

Policy number	**ICT006**			
Policy Version Number	Version 1.1			
Policy originator / owner	Information, Communications and Technology			
	Date	**Minute ref**	**Name**	**Signature**
Approved by EMT				
Approved by Senate				
Approved by JBF				
Approved by Council				
Next review date	2018			

1 APPLICATIONS AND DEFINITIONS

The University of Fort Hare ("the institution") may be held liable for the actions of students and staff using the institution's e-mail and Internet access services. This policy creates rules that aim to limit or manage the risk associated with unlimited e-mail use and Internet access.

Definitions:

"User(s)" means all employees employed by the institution and all students actually registered at the institution and includes part-time, visiting and freelance students, contract workers and/or academics with access to the institution's e-mail, Internet access and IT network.

"Illegal Content" means e-mail and web site content that contains material that is pornographic, oppressive, racist, sexist, defamatory against any User or third party, offensive to any group, a violation of a User's or a third party's privacy, identity or personality, copyright infringement, malicious codes such as viruses and Trojan Horses, and content containing any Personal Information of User's or third parties without their consent;

"Personal Information" means Personal Information as defined in the Promotion of Access to Information Act (click here to download the Act: http://www.polity.org.za/html/govdocs/legislation/2000/act2.pdf)

"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 (to download the Act click here: http://www.polity.org.za/html/govdocs/legislation/1996/act96-065.html); and

"Internet" shall in all cases include the institution's intranet.

Application:

This Policy applies to all Users as well as third parties that have access to the institution's e-mail, Internet access or network and who:

- use the institution's facilities to send and receive e-mail messages (including attachments thereto);
- access the Internet and the Internet's services including but not limited to usenet newsgroups, the World Wide Web and Internet chat rooms; and
- save, retrieve or print files, e-mail messages or other electronic documents to and/or from the institution's network or a computer, hard drive or disk.

2 PURPOSE

The **purpose** of this electronic communications policy is to:

- inform Users on the use of e-mail and the Internet;
- create rules for the use of e-mail and the Internet;
- provide for disciplinary action against Users who fail to comply with this policy; and
- ensure and maintain the value and integrity of the institution's equipment and network(s).

3. OWNERSHIP, RESPONSIBLE PERSONS AND RIGHT TO MONITOR

3.1 RESPONSIBLE PERSONS AND DUTIES

3.1.1 Users are personally responsible to abide by the rules created in this policy. and must delete all incoming e-mail messages that contain content or links to content that are not allowed in terms of this policy;

3.1.2 The institution's ICT department is responsible for:

- the technical issues related to e-mail use and Internet access;
- assisting the institution's management to conduct searches / monitoring of User's incoming and outgoing e-mail messages, stored messages, stored files and browsing habits;
- causing all outgoing e-mail messages to contain the institution's official e-mail disclaimer;
- scanning all incoming message and file downloads for malicious codes such as viruses or Trojan Horses;
- sustaining Users' awareness of this and other Institutional polices related to the use of the Institution's electronic facilities; and
- offering training for Users in the proper use of the Institution's electronic facilities.

3.1.3 The institution's management is responsible for taking any necessary action against Users who fail and/or refuse to abide by this policy.

3.2. RIGHT TO MONITOR

With due regard to the South African Constitution and the Regulation of Interception of Communications Act, each and every User, when he or she registers as a student, commences a visit or starts employment, is deemed to have given his or her consent that the ICT department and management of the institution may, without prior warning:

3.2.1. Intercept, monitor, block, delete, read and act upon any incoming or outgoing e-mail message addressed to or originating from the User;

3.2.2. Intercept, monitor, read and act upon the User's Internet browsing habits, including the User's history files, web sites visited, files downloaded and stored by the User; and

3.2.3. Intercept, monitor, block, delete, read and act upon any file, in whatever

format, stored by a User on any computer or other facilities of the institution.

4. ACCEPTABLE USE AND GENERAL GUIDELINES

The following actions and content will be considered acceptable use of e-mail and Internet facilities by Users:

4.1 Users shall use e-mail and Internet access primarily for academic purposes. Private and personal use, in moderation, will be tolerated, subject to the rules detailed in this policy;

4.2. Equipment, systems, services and software on the Institute's networks are to be used primarily for academic purposes. Common sense and good judgement should guide personal and private usage;

4.3. When forwarding or replying to e-mail messages, the contents of the original message should not be altered. If the contents need to be changed, then all changes must be clearly marked as such;

4.4. The institution has the right to limit the size of incoming and outgoing e-mail messages and attachments, downloads and other files and may block and delete e-mail 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 the electronic mail system resources;

4.5. E-mail messages should be kept brief and formulated appropriately;

4.6. Virus warnings or pop-ups that result from incoming e-mail or file downloads must be reported to the ICT department immediately at the following number: [Extension 887 on all campuses];

4.7. All outgoing e-mails must have the institution's standard e-mail disclaimer at the end of the message. This e-mail disclaimer may not be removed or tampered with by Users;

4.8. Users must check e-mail recipients prior to sending, forwarding or replying to messages. When distribution lists are used the sender should consider whether or not each group member really needs, or really should, receive the e-mail;

4.9. The subject field of an email message should relate directly to the contents or purpose of the message;

4.10. Users must log-off or use screen savers with passwords in times of absence from a computer terminal to avoid improper and/or illegal use;

4.11. Notebook and/or offline Users should load and update the "address book", if any, regularly; and

4.12. If Users (non-students) are out of the office for more than one day, they should activate the "Out of Office" function. This informs the sender of an e-mail of a recipient's absence. The "Out of Office" message should include both the period of absence and an alternative contact person.

5. NON – ACCEPTABLE AND PUNISHABLE USE

The following actions and content are not allowed and will lead to investigation and disciplinary action:

5.1 Sharing logon usernames with or disclosing passwords to any third person(s);

5.2 Modifying an e-mail message and forwarding or replying therewith without noting the changes (i.e. deletions, removal of recipients, modification of content, etc.);

5.3 Fabricating a message and/or sender of a message;

5.4 Intentionally bypassing the security mechanisms of the mail system or any other secure web site or network (e.g. creating bogus accounts);

5.5 Modifying the internal mail transport mechanism to forge a routing path that a message takes through the Internet;

5.6 Receiving, storing, downloading, printing, distributing, sending or accessing Illegal Content (as defined above);

5.7 Participating in e-mail "chain letters" or similar activities;

5.8 Downloading, receiving and/or installing software applications not approved by the IT department;

5.9 Knowingly burdening the institution's network with non-academic data (e.g. forwarding, downloading or accessing large video clips or graphics to or from a distribution list or file-sharing server);

5.10 Using automatic forwarding of e-mails ("Auto Rules") to any person without such person's consent;

5.11 The creation, sending or forwarding of unsolicited mail (spam);

5.12 The creation, sending or forwarding of marketing information about commercial and/or non-academic issues;

5.13 Sending or forwarding messages and attachments that are infected with malicious codes such as viruses;

5.14 Using discs that may be infected with malicious code;

5.15 Accessing and using internet relay chat if such actions burden the institution's systems or prevent other Users from using them;

5.16 Any non-academic actions that knowingly prevent other Users from using e-mail or Internet access;

5.17 Taking any of those 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 (click here to download the ECT Act:

http://www.polity.org.za/pdf/ElectronicCommunications.pdf see sections 85, 86, 87, 88 and 89);

5.18 Any destructive and disruptive practices either via e-mail or the Internet;

5.19 Indiscriminate storage and/or forwarding of e-mail, files, web sites and attachments for which permission has not been obtained from the originator or copyright holder;

5.20 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;

5.21 Sending, replying to or forwarding e-mail messages or other electronic communications which hides the identity of the sender or represents the sender as someone else;

5.22 Users of the institution's electronic mail systems who obtain access to materials of other organisations may not copy, modify or forward copyrighted materials, except under the specific copyright terms and conditions; and

5.23 Using information, e-mail, files, downloads or data to commit fraud or any other criminal offence(s).

7. CONSEQUENCES OF MIS-USE

Failure and/or refusal to abide by the rules detailed in this policy shall be deemed as misconduct and the institution may initiate the appropriate investigation and disciplinary action against Users. Such steps may include dismissal or expulsion, as the case may be.

Contact details for TENET: ceo@tenet.ac.za, 021 686 6010.