C2006/123

University of the Witwatersrand, Johannesburg

Information & Communication Technology
Policies and Standards

Acceptable Use Policy

1. POLICY STATEMENT

1.1. Policy Overview

This policy sets out the rules governing the use of the University's Information and Communication Technology (ICT) systems and services, including hardware, software, and transmissions going out from or entering into the computer network. Inappropriate use of ICT exposes the University to risks including virus attacks, the compromising of its systems and services, claims for damages and even criminal liability.

This policy must be read together with the University's other Rules, Regulations, Policies and Procedures. Without limiting the generality of the above, all Users of the University's ICT must comply with the University's codes of conduct for the use of Information and Communication Technology and its general codes of conduct for staff and students. In using the University's ICT, the conduct of any User should be such that it does not interfere with the governance and proper administration of the University, it does not interfere with the conditions necessary for teaching, learning, or research or bring the University into disrepute.

A staff member and any other person acting on behalf of the University has a fiduciary responsibility to the University.

1. When acting on behalf of the University a User must do so in good faith and in the best interest of the University. This duty is owed to the University and not to any individual. A User may not engage in conduct which results in another person's interests being in conflict with those of the University.
2. There must be no conflict between the User's private interests and that of the University. A User may not carry on business in competition with the University or use his or her relationship with the University to make a profit or earn a commission unless and until the University has duly authorised such conduct.
3. A User must act on behalf of the University with the care and skill that can reasonably be expected from a person with his or her knowledge and experience.

The University's resources including its Information & Communication Technology Resources may only be used for carrying on the business of the University except where the University has expressly provided otherwise in writing and for occasional, reasonable private use where this is necessary for meeting social or family responsibilities. (Users should bear in mind that there are limits to the right to privacy within the workplace. Not every expectation of privacy is legitimate or objectively reasonable and third parties may have a right to access information on the University's ICT systems).

The University strongly supports the right to academic freedom but this right must be balanced against the other rights enshrined in the Constitution. When conducting research using ICT the User must observe the same principles, policies, rules, regulations, and ethics that govern academic activity using any other research tool. Any research involving human or animal subjects must be referred to the relevant ethics committee.

1.2. Scope

This policy applies to all users including staff and students at the University and all personnel affiliated with third parties who make use of the University's ICT. This policy applies to all equipment that is owned or leased by the University, including any privately owned equipment but only when the latter is used for University business.

1.3. Definitions

Term	Definition
Director	Director of CNS or his or her nominee
VC	Vice Chancellor
DVC	Deputy Vice-Chancellor
IR	Industrial Relations
Spam	Unauthorized and/or unsolicited electronic mass mailings.
Systems	Includes but is not limited to: Desktops, Laptops, Tablet PCs, Servers (of any kind), and any node that is connected to the University network at any time and the software installed on such systems.
the University	The University of the Witwatersrand, Johannesburg
User	Any person using the University's ICT facilities and services
Personal information	It is defined in a similar manner in various acts. It is information about an identifiable, natural person and insofar as it is applicable, an identifiable juristic person, including but not limited to: a) information relating to the race, gender, sex, pregnancy, marital status, national ethnic or social origin, colour, sexual orientation, age, physical or mental health, well being, disability, religion, conscience, belief, culture, language and birth of the person; b) information relating to the education or the medical, criminal or employment history of the person or information relating to financial transactions in which the person has been involved; c) any identifying number, symbol or other particular assigned to the person; d) the address, fingerprints or blood type of a person; e) the personal opinions, views or preferences of the person except where they are about another individual or about a proposal for a grant, award or a prize to be made to another individual; f) correspondence sent by the person that is implicitly or explicitly of a private or confidential nature of further correspondence that would reveal the contents of the original correspondence; g) the views or opinions of another individual about the person; h) the views or opinions of another individual about a proposal for a grant, an award or a prize to be made to the person, but excluding the name of the other individual where it appears with the views or opinions of the other individual; i) the name of the person where it appears with other personal information relating to the person or where the disclosure of the name itself would reveal information about the person; j) but excludes information about a natural person who has been dead, or a juristic person who has ceased to exist for more than 20 years
Disruption	Includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

2. POLICY

2.1. General Use and Ownership

1. Users must exercise good judgement of sensitive or vulnerable information. For guidelines on information classification, see *Acceptable Use Policy - Information Sensitivity Standards & Guidelines.*
2. For security and network maintenance purposes the Director: and any other person authorised by the VC may monitor equipment, systems, and network traffic at any time. The University reserves the right to audit networks and systems on a periodic basis to ensure compliance with this Policy.
3. The University may impose bandwidth or computer resource related restrictions.
4. Users must not infringe the copyright of others. This means that other than for the purposes of fair dealing the owner of the copyright has exclusive rights to the work in which he or she holds copyright. A User may not infringe the copyright holder's exclusive right to reproduce the work, to perform it in public, broadcast the work, or adapt it. He or she may only reproduce, perform, broadcast, or adapt the work in accordance with the permission to do so granted by the copyright holder.

2.2. Security and Proprietary Information

1. The User interface for information contained on ICT-related systems must be classified as either confidential or not confidential, as defined by the University's confidentiality guidelines. Users must take all necessary steps to prevent unauthorized access to this information particularly personal information.

2. Users may not:
    a. Leave PC's, laptops and workstations unattended and unsecured. All PCs, laptops, and workstations (excluding student PC Labs) must be secured with an automatic password-protected screensaver or the system must be locked, when the host will be unattended. See *"Acceptable Use - Technical Standards & Guidelines"* for further information.
    b. Play games in PC Labs using the University's ICT resources.
    c. Allow any external parties unauthorized usage or access to the University's ICT resources
    d. Share computer accounts and passwords. Users are responsible for the security of their passwords and accounts.
    e. Be in violation of the Intellectual Property policy

3. Users must:
    a. Protect laptops in accordance with the *"Laptop Security Guidelines" S*
    b. Continually execute virus-scanning software with a current virus database approved by the Director, on any system connected to the University Network, whether or not the University owns it. (Certain operating systems are not as vulnerable to viruses and exploits, nonetheless systems that act as servers (i.e. email & fileservers) must run antivirus software, to protect the rest of the University community) See *"Acceptable Use - Technical Standards & Guidelines"* for further information.
    c. Immediately delete an email:
        i. If it has been sent from a source unknown to the receiver
        ii. If it has unknown e-mail attachments. These attachments may contain viruses, e-mail bombs, or Trojan Horse code.

4. All email communications and postings to news groups must contain a disclaimer stating that the opinions expressed therein are those of the author and not necessarily those of the University. The following email disclaimer is the standard as per document A2003/101:

Standard disclaimer:

> *This communication is intended for the addressee only. It is confidential. If you have received this communication in error, please notify us immediately and destroy the original message. You may not copy or disseminate this communication without the permission of the University. Only authorized signatories are competent to enter into agreements on behalf of the University and recipients are thus advised that the content of this message may not be legally binding on the University and may contain the personal views and opinions of the author, which are not necessarily the views and opinions of The University of the Witwatersrand, Johannesburg. All agreements between the University and outsiders are subject to South African Law unless the University agrees in writing to the contrary.*

This disclaimer will be added to all outgoing email at the central email gateways.

2.3. Unacceptable Use

Certain activities are unacceptable and may not be engaged by any User

System and Network Activities

The following activities are strictly prohibited, with no exceptions.

1. Infringement of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to:
    a. The installation or distribution of "pirated" or other software products and the installation of any copyrighted software for which the University or the end user does not have an active license.
    b. Digitization and distribution of photographs from magazines, books or other copyrighted sources, music, movies, video clips.
2. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to:
    a. Executing any form of network monitoring which will intercept data not intended for the user's host.
    b. Circumventing user authentication or security of any host, network, or account.
    c. Port scanning or security scanning.
    d. Accessing data of which the user is not an intended recipient.
    e. Logging into a server or account that the user is not expressly authorized to access, unless these duties are within the scope of regular duties.
    f. Interfering with or denying service to any user other than the user's host (for example, denial of service attack).
    g. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the network.
    h. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
3. Providing personal information including information about, or lists of, members of staff or students at the University to parties outside the University.

Email and Communications Activities

The following activities are strictly forbidden without exception.

1. Sending email that hides the true identity of the sender, or sending to a recipient that is not known by the sender as accepting of such email, including the sending of:
    a. "Junk mail" or other advertising material (email spam).
    b. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
    c. Email originating from within The University's networks advertising services that are not related to the University's business or are sent on behalf of any third party without consent.
2. The transmission, storage, or distribution of any material or content where such action is intended to defame, abuse, stalk, harass, or physically threaten any individual.
3. Unauthorized use, or forging, of email header information.
4. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).
5. Posting to distribution lists unless sent via the approved channel. Users may not use distribution lists unless there is a direct relationship to a specific committee/school or any other bodies that requires contact via email.

3. Enforcement

Any suspicion of violation of this policy and related policies must be reported to the Director and to Legal Advisor, IR Advisor, or the Registrar.

The User should note the following:

1. The Electronic Communications Transaction Act No.25 of 2002 provides for inter alia "the facilitation and regulation of electronic communications and communications ...," the development of an e-strategy, the promotion of access to electronic communications and to prevent abuse of information systems. Various offences are defined in the Act including in sections 37 (3), 40 (2), 58 (2), 80 (5), 82(2) and in Chapter XII CYBER CRIME. This chapter specifically provides for various offences relating to unauthorised access to, or interception of or interference with data. The penalties for these offences range from a fine or imprisonment not exceeding 12 months, to a fine or imprisonment for a period not exceeding 5 years.

2. *The Regulation of Interception of Communications and Provision of Communication-related Information Act No 70 of 2002*
   This regulates the interception of certain communications and the monitoring of certain signals and frequencies. It establishes certain offences and prescribes the penalties for these offences. Section 49(1), for instance, provides that any person who intentionally intercepts or attempts to intercept…….. any communication in the course of its occurrence or transmission is guilty of an offence and section 54, for instance, provides that any person who intentionally and unlawfully and in any manner a) modifies, tampers with alters, reconfigures or interferes with any telecommunication equipment including a cellular phone and a SIM card or any part thereof b) reverse engineers, decompiles, disassembles or interferes with software installed on any telecommunication equipment including a cellular phone and a SIM card by the manufacturer thereof……" is guilty of an offence. Any such person, if convicted, is liable to a fine not exceeding R2 000 000 or to imprisonment for a period not exceeding 10 years

3. *The Promotion of Access to Information Act.*
   The University has a policy dealing with this Act and has published a manual as required by this Act.
4. The proposed act to promote the protection of personal information processed by public and private bodies.

POLICY IMPLEMENTATION

Definitions

Clickwrap	Of or relating to a legal agreement, such as a software license, to which one indicates acceptance by clicking on a button or hyperlink http://www.thefreedictionary.com/clickwrap

4.1. What will be used to gauge the success of the policy

4.1.1. What needs to be tracked

System and Network Activities

1. The maximum use of bandwidth
2. This includes but is not limited to:
   2.1. Bandwidth usage (Internal and External)
   2.2. Bandwidth shaping and prioritising (Internal and External)

Email and Communication Activities

1. This includes but is not limited to:
   1.1. Decrease in internal and external generated “spam”, “chain letter”, etc
   1.2. Reduction in risk of email virus outbreaks

4.1.2. What are the success measurements

Tracking the success of the Acceptable Use Policy, will be no easy task, although in certain areas this can be achieved more will be explained below.

General Use

1. Preventing and decreasing the current rising trend in legal litigation
2. Mitigation of Risk
3. Elimination of illegal activities on the Wits infrastructure
4. Decreased incidents and events related all IT resources caused my misuse.

System and Network Activities

1. Monitoring of the network with regards to Network Bandwidth (internal and external)
2. Increased business use of bandwidth
3. Elimination of illegal activities on the Wits infrastructure

Email and Communication Activities

1. This will be a combination of human feedback (legal, complaints) and monitoring of usage
2. Elimination of illegal activities on the Wits infrastructure
3. Reduction in risk of email virus outbreaks

4.1.3. Who is responsible for monitoring what is tracked against the success measures

General Use

1. Each individual user
2. Line Management
3. Local Area Network Administrators
4. CNS

System and Network Activities

1. Each individual user
2. Line Management
3. Local Area Network Administrators
4. CNS – statistical monitoring

Email and Communication Activities

1. Each individual user
2. Line Management
3. Local Area Network Administrators
4. CNS – statistical monitoring

4.2. Senate standing orders (if applicable)

4.3. Communicating the policy

This policy will be communicated and distributed to all the University organs to ensure acceptance.

This policy will be made available in electronic format and hard copy in the following areas to all parties defined in the scope:

1. On the Intranet pages of the Registrar's office and CNS, it will be available for download and printing.
2. First logon into email; account will provide a copy of the policy.
3. Printed copies available at HR, CNS or SEnC
   3.1. A copy will also be given to any person that starts employment with Wits.
4. On logon to area domain, click wrap acceptance of The University's Policies, i.e. Acceptable Use Policy, IP Policy, etc., with a link to these policies must be displayed.

   Legal Notice:

   By logging on to this system and any other IT Resource of the University of the Witwatersrand, JHB you agree to the policies set forth by the University of the Witwatersrand, JHB. These policies can be found on the Registrar's Helpdesk website (http://intranet.wits.ac.za/Academic/RegistrarsHelpdesk/helphome.html).

4.4. Resource consequences of the policy

There will be no noticeable effect on resources.

5. POLICY REVIEW

5.1. Review procedure

Feedback on progress to be presented to Senate IT and the Risk Committee.

6. POLICY RECORD

6.1. Date of approval

6.1.1. by relevant committee
IT Senate; 27 February 2006

6.1.2. by appropriate statutory governing body (usually Senate or Council)
Council

6.1.3. by Council (if applicable)
9 May 2006

6.2. Commencement date

10 May 2006

6.3. Revision history

C2006/123

6.4. Review date

Annual – 9 May 2007

6.5. Policy implementation level

The implementation level of this policy affects the whole University as it is described in Section 1.

6.6. Responsibility

6.6.1. Implementation

6.6.1.1. Each individual user
6.6.1.2. Line Management
6.6.1.3. Local Area Network Administrators
6.6.1.4. CNS

6.6.2. Monitoring

6.6.2.1. Each individual user
6.6.2.2. Line Management
6.6.2.3. Local Area Network Administrators
6.6.2.4. CNS

6.6.3. Review and revision

Senate IT as per instruction

6.7. Reporting structure

6.8. Associated documentation

6.8.1. Electronic Communications and Transactions Act (No 25 of 2002) - Implications of the Act for the way we conduct business *A2003/101*
6.8.2. Delegation of Authority Document
6.8.3. Acceptable Use – Information Sensitivity Standards & Guidelines
6.8.4. Acceptable Use - Laptop Security Guidelines
6.8.5. Acceptable Use - Technical Standards & Guidelines

6.9. Other pertinent matters