Policy for the Acceptable Use of Information and Communication Services (ICS) Resources.

Name of document:	Policy for the Acceptable Use of Information and Communication Services (ICS) Resources.	
Reference number: *(supplied by Office of the Registrar)*	CO/04/0312/12	
Originator/Author: *(name and position)*	Information and Communication Services (ICS) Division through the Office of the Registrar.	
Custodian: *(position/office)*	The Office of the Registrar.	
Approved by:	***Structure***: EMC Senate SSB Council	***Date***: 01/11/2012 07/11/2012 19/11/2012 03/12/2012
Effective date:	03/12/2012	
Document review date:	Subject to review and modification from time to time	
Implementation responsibility:	ICS Division, driven by Chief Information Officer (CIO)	

1. Purpose statement

The purpose of this Policy is to:

- Inform Users of the responsibilities and obligations borne by those who use the Information and Communication Services (ICS) resources (including all computing and communication equipment and network facilities) provided by the University of KwaZulu-Natal (UKZN);
- Create acceptable and appropriate rules for the responsible use of ICS resources;
- Provide for possible disciplinary action to be taken against Users who breach this Policy;
- Ensure and maintain the value and integrity of UKZN's equipment and network(s);
- Establish policy on privacy, confidentiality, and security in electronic communications and transactions;
- Ensure that ICS resources are used in compliance with the law and any UKZN rules, regulations and policies which may be applicable thereto;
- Prevent any disruption and/or misuse of ICS resources;
- Inform Users that indirect communications via ICS resources maybe intercepted as contemplated by section 6 of the Regulation of Interception of Communications and Provision of Communication-related Information Act No. 70 of 2002 ("RICA"); and
- Ensure that the safeguards of the University's rights and those of its employees as provided by RICA are upheld.

2. Introduction

The University of KwaZulu-Natal (UKZN) provides the University community with a modern electronic communications infrastructure, which is limited and needs to be shared equitably to serve the different needs and priorities of its Users.

Section 6 of RICA allows UKZN to intercept any indirect communication in the course of carrying on of its business activities provided that it has made all reasonable efforts to warn Users in advance that communications may, in accordance with the section, be intercepted.

UKZN has valuable information assets that must be managed carefully to ensure their confidentiality, integrity and availability for lawful business activities. In carrying out its business activities, UKZN provides ICS resources to its employees, contractors and students. The use of ICS resources has elements of cost and the potential to harm the reputation of UKZN, its students and its employees.

UKZN may be held vicariously liable for any action or conduct of Users utilising the ICS resources where such action or conduct is contrary to the law. This Policy aims to limit and/ or manage the associated risk; to provide protection to UKZN; and to educate UKZN students and employees on the concomitant duties for use of ICS resources and what constitutes unacceptable use of ICS resources. It is also important to understand that the purpose of this Policy is to facilitate and support authorised access to information.

This Policy and the rules that follow recognise the constitutional right to privacy and academic freedom and are intended to:

(i) manage and limit the risk to the University;

(ii) protect the University and its staff;

(iii) guide members of the University community and others who have access to the University's ICS resources as to what constitutes acceptable use of these resources; and

(iv) facilitate and support authorised access to information.

3. Definition of terms

3.1 **"Confidential Information"** means any information, product or process which by its nature or content is identifiable as confidential and/or proprietary to UKZN and/or any third party ("Disclosing Party") which the Disclosing Party or any person acting on its behalf may disclose or provide to the User(s) or which may come to the knowledge of the User(s) by whatsoever means. Confidential Information will include, without limitation, the following information that is not in the public domain:-

3.1.1 information relating to the Disclosing Party's business activities, business relationships, research, products, services and service providers;

3.1.2 information contained in or constituting the Disclosing Party's hardware or software including third party products, and associated material documentation;

3.1.3 the Disclosing Party's technical, scientific, commercial, financial and marketing information, intellectual property, know-how and trade secrets.

but excluding information or data which:

3.1.4 is lawfully in the public domain at the time of disclosure to the User(s); or

3.1.5 subsequently becomes lawfully part of the public domain by publication or otherwise; or

3.1.6 is disclosed pursuant to a requirement or request by operation of law, regulation or court order.

3.2 **"Electronic Communications Facilities"** include the following:-

3.2.1 Computing and communication equipment (such as laptop computers, desktop computers, external and internal hard disk drives, USB flash disks and any other peripheral device), servers and modems;

3.2.2 Electronic mail (e-mail) facilities and instant messaging systems;

3.2.3 Document management systems; and

3.2.4 Telephones, fax machines, cellular phones and videoconference units.

3.3 **"Electronic Communications Network"** includes the network and telecommunications infrastructure utilised by UKZN to transmit and receive information by electrical and electronic means.

3.4 **"ICS resources"** include the Information and Communication Services resources which include, without limitation, Electronic Communications Facilities, Electronic Communications Network, software, or data used in connection with information technology, which is owned, leased or used under license by UKZN.

3.5 **"ICS Division"** means UKZN's Information and Communication Services Division.

3.6 **"ICT Expert Desk"** refers to the published telephone number(s) and e-mail address(es) through which Users report any faults in ICS resources to the ICS Division.

3.7 **"Internet"** refers to a global system of interconnected computer networks that use the standard Internet Protocol Suite (TCP/IP) to serve users worldwide and shall in all cases include the institution's intranet.

3.8 **"Malicious Content"** means any virus(es), programme and any unauthorised software, material or data which threatens to overload, change, damage, corrupt or destroy any UKZN ICS resource(s).

3.9 **"Pornography"** refers to all the content and actions, simulated or real, graphic or written detailed in the Films and Publications Act 65 of 1996.

3.10 "**RICA**" refers to the Regulation of Interception of Communications and Provisions of Communication-related Information Act (No 70 of 2002).

3.11 **"Systems Controller"** means the Vice Chancellor of UKZN or his/her delegate.

3.12 **"Unacceptable Content"** means any e-mail, web site and stored content on the ICS resources that contains any material or data which is unlawful or in violation of any rule, regulation, policy or values of the UKZN including, without limitation, any discriminatory, pornographic, oppressive, racist, sexist or defamatory content; or material or data which infringes any copyright held by UKZN or a third party or constitutes a violation of any software licensing agreement. It includes any Malicious Content of which the downloading, storage or communication may bring UKZN into

disrepute. It shall not include material or data in the said form, which is used or required for demonstrable academic purpose.

3.13 **"User(s)"** means all employees employed by UKZN (including any post-graduate student currently registered and employed at UKZN), all students registered at UKZN and any other person with authorised access to ICS resources including, without limitation, visitors, freelance persons, independent contractors, consultants or registered juristic persons in terms of the Companies Act No.71 of 2008 engaged by UKZN.

4. Scope

This Policy applies to all Users who have access to ICS resources wherever located, including privately owned or donated Electronic Communications Facilities which are connected to UKZN's Electronic Communications Network and who:

- use the ICS resources to send and receive e-mail messages (including attachments); or
- access the Internet and the Internet's services including but not limited to Usenet newsgroups, the World Wide Web; Facebook and Internet chat rooms; or
- save, store, retrieve and/or print material, data, e-mail messages or other electronic documents through ICS resources.

5. Policy

5.1 UKZN provides extensive ICS resources to a wide range of Users for scholarly, teaching, learning, research, administrative and related business activities. All authorised Users are provided with login facilities and passwords. It is the responsibility of each User to safeguard their login username and password information and keep these confidential at all times.

5.2 UKZN has legal ownership of all material stored on its ICS resources, as well as all electronic communications material transmitted via its Electronic Communications Network and reserves the right to safeguard its information and interests against abuse and to maintain the integrity of the system and the information it contains. This right includes the right to intercept indirect communications in accordance with section 6 of RICA.

5.3 UKZN retains the right to monitor traffic on all lines owned or leased by the University.

5.4 The University reserves the right to restrict or otherwise control the use of any of the internet protocols. This right to restrict may include the right to set a limit on individual usage by volume for students and staff.

5.5 Users are responsible for ensuring that they have read and understood the provisions of this Policy which will be made available to them via UKZN's website: www.ukzn.ac.za.

6. Duties of Users of ICS resources

User(s) shall adhere to the following duties when making use of ICS resources, namely:-

6.1 A User must use his/her valid username and password that must remain confidential to the User and must not be disclosed to any third party;

6.2 A User is responsible for all activity that takes place under his/her username and password;

6.3 Users will lock work stations utilised by them when such work stations are left unattended;

6.4 Users must be courteous and considerate of others when using ICS resources;

6.5 Users shall use ICS resources primarily for scholarly, teaching, learning, research, administrative and related business activities;

6.6 Users will be permitted private and personal use of ICS resources, in moderation, subject to the provisions of clause 8 of this Policy;

6.7 When forwarding or replying to e-mail messages, the content of the original message should not be altered provided that where the content needs to be changed then all changes must be clearly marked as such.

7. Unacceptable Use of ICS resources

Specific activities or conduct that constitute unacceptable use of ICS resources include but are not limited to:-

7.1 deliberate unauthorised corruption or destruction of ICS resources through the introduction, propagation or use of any Malicious Content;

7.2 deliberate unauthorised attempts to gain access to ICS resources;

7.3 deliberate unauthorised attempts to make the ICS resources unavailable to other Users;

7.4 unauthorised use of data and/or information obtained from the use of ICS resources for purposes unrelated to UKZN business;

7.5 use of ICS resources to access, view, copy, store, transmit or solicit any Unacceptable Content;

7.6 deliberate impersonation of another User by the use of that person's username and password, email address or other means;

7.7 violation of privacy protecting the personal information of other Users;

7.8 unauthorised disclosure of Confidential Information;

7.9 use of ICS resources to harass or threaten Users or third parties;

7.10 use of ICS resources to gain unauthorised access to any third party information technology network or facilities;

7.11 use which deliberately and significantly degrades the performance of ICS resources for other Users save and except for where such use is specifically required to be carried out by the User(s) in the course and scope of their employment with UKZN;

7.12 connection of any non-approved computer or computing equipment without the express permission of the ICS Division;

7.13 connection of any privately owned or donated Electronic Communications Facilities without the express permission of the ICS Division; and

7.14 viewing, storing, downloading or forwarding images, moving images, sound files, texts or recordings that are sexually explicit or sexually suggestive, racist, harassing, intimidating or defamatory, except where there is demonstrable academic need to access or distribute such content.

.

8. Private and Personal Use of ICS resources

8.1 UKZN allows Users to make reasonable personal use of its ICS resources.

8.2 Users must ensure that personal use of ICS resources is occasional, reasonable and compatible with the primary purpose for which such ICS resources are provided.

8.3 UKZN provides access to its Electronic Communications Network as a privilege not a right that must be exercised with discretion and in compliance with this Policy.

8.4 ICS resources may be utilised for the purposes of private remunerative or personal monetary gain only where it is performed on the Electronic Communications Facilities provided by UKZN to the User and such private remunerative work or work for personal monetary gain is approved in writing by the applicable Line Manager.

8.5 ICS resources may not be removed from UKZN premises save and except where ICS resources, which by virtue of their design, are normally used by staff offsite (for example, laptops, cellular phones and certain audio visual equipment). All other ICS resources may only be removed from UKZN premises if approved in writing by the Finance Division of UKZN.

8.6 User(s) are cautioned that where any non-approved computer or computing equipment, or privately owned or donated Electronic Communications Facilities are connected to the ICS resources, whether or not in compliance with clauses 7.1.12 and 7.1.13, such non-approved computer or computing equipment, or privately owned or donated Electronic Communications Facilities will, upon instructions of the Systems Controller, be impounded by UKZN for the purposes of conducting any investigation, forensic or otherwise.

9. Management of ICS resources and the right to monitor

9.1 UKZN reserves the right to limit the size of incoming and outgoing e-mail messages and attachments, downloads and other files and may electronically block and delete e-mail messages, downloads, attachments or other files at any time and without notice.

9.2 UKZN is obliged to manage and protect its ICS resources, and may therefore intercept and/ or refuse any indirect communication in the exercise of its responsibility for the operation of its ICS resources.

10. Consequences for Non-Compliance

10.1 Where a legitimate reason exists, UKZN reserves the right, subject to 10.2 below, to do the following:

- monitor User activity;
- search and seize any material;
- amend User privileges and access rights; or
- access and examine the Electronic Communications Facilities including archived e-mail, Internet browsing history, personal file directories and any other material, at any time without prior notice.

10.2 The prior written permission of the University's System Controller shall be obtained where the University wishes to undertake any of the activities listed in paragraph 10.1 above.

10.3 This Policy compels Users to ensure that they comply with South African and International law.

10.4 Where it is suspected on reasonable grounds that there has been a violation of any of the provisions of this Policy by a User, an investigation may be initiated and disciplinary proceedings conducted in accordance with the appropriate UKZN disciplinary procedure.

10.5 The sanctions applicable where violation of this Policy has been determined through the appropriate UKZN disciplinary procedure may include either one or more of the following:-

10.5.1 immediate withdrawal of access to ICS resources, with or without prior notice;

10.5.2 disconnection and seizure of Electronic Communications Facilities which are used in the contravention of this Policy;

10.5.4 criminal prosecution where violation contravenes any law of the Republic of South Africa; and

10.5.5 legal action by UKZN which may include the recovery of any costs associated with any claim or legal proceedings instituted against or by UKZN.

11. Policy Review

This Policy shall be subject to review and modification from time to time, as circumstances require.