

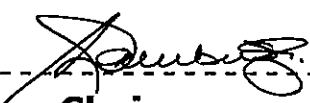


**WALTER SISULU UNIVERSITY  
ACCEPTABLE USE  
POLICY**

Policy library ID  
ICT: 01



## Acceptable Use Policy

<b>Sponsor division</b>	Operations and ICT Services
<b>Responsible Department</b>	ICT Services
<b>Related WSU policies</b>	
<b>Policy name</b>	<b>Policy Name</b>
Computing Passwords Policy	IT Service-desk Policy
IT Security Policy	
<b>Change History</b>	
<b>Approval authority</b>	<b>Council</b>
<b>Approval Date</b>	<b>01 July 2016</b>
<b>Latest revision date</b>	<b>01 July 2016</b>
<b>Effective date</b>	<b>Immediately</b>
 Chairperson of Council	

**Contents**

- 1. Preamble .....3**
- 2. Purpose .....3**
- 3. Scope .....3**
- 4. Definitions .....3 - 4**
- 5. Policy Implementation .....4 - 7**
- 6. Policy Review .....8**
- 7. Related Policies .....8**

## 1. PREAMBLE

- 1.1 Walter Sisulu University (WSU) acquires, develops, and maintains computers, computer systems and communication networks to support institutional activities. These include teaching and learning, research, administrative functions, student and campus life and the exchange of ideas within and among the University community and the local, national, and international communities.
- 1.2 As a user of these services and facilities, staff members and students will have access to valuable University resources, sensitive data, and internal and external networks. Consequently, it is important for staff members and students behave in a responsible, ethical, and legal manner.

## 2. PURPOSE

The purpose of this policy is to establish specific requirements for the use of all computing and network resources at WSU, including the use of computer laboratories and any personal equipment that may be registered for use on the University network.

## 3. SCOPE

This policy applies to all users of computing, networking, and telecommunications facilities provided by WSU, including privately owned or donated equipment connected to the University network and telecommunications infrastructure. It applies to staff, students, guests, visitors and outside individuals or organisations accessing network services via WSU computing facilities.

## 4. DEFINITIONS

Any definitions listed below apply to this document only with no implied or intended institution-wide use.

**"Acceptable Use"** - respecting the rights of other computer users, the integrity of the physical facilities and all pertinent license and contractual agreements.

**"Authorized User"** - any person granted express, implied or apparent authority to use a given resource.

**"Automated Processes"** – use of computers and other electronic communication devices that can gather, store, manipulate, prepare and distribute data with minimal human intervention.

**"Computing Resources"** – all university owned, licensed, or managed telephones, computer hardware and software, and university network accessed via a physical or wireless connection.

**"Data Owners"** - entity that can authorize or deny access to certain data, and is responsible for its accuracy, integrity, and timeliness.

**"Information Technology Steering Committee (ITSC)"** - a Sub-Committee of the Institutional Management Committee (IMC) with the strategic responsibility of prioritising IT investment programmes in line with university strategic plan, track status of projects and resolve resource conflicts as well as monitor service levels and service improvements.

**"Institutional Management Committee (IMC)"** - highest leadership organ of the university that reports to the Council.

**"Libel statement"** – defamation of character, calumny or misrepresentation.

**"Licence Agreement"** – an undertaking by the contractual owner of a resource giving permission to another to use that resource.

**"Quotas"** - a fixed share of usage that a user is entitled to receive or bound to contribute.

**"Slander"** – a false statement damaging to another person's reputation.

**"Third Party Resources"** – resources available to the university community through external service providers.

**"Time Limits"** - a limit of time within which an activity has to be accomplished.

**"Upstream Service Provider"** - a large Internet Service Provider that provides Internet access to a local Internet Service Provider.

## **5. POLICY IMPLEMENTATION**

### **5.1. Acceptable Use**

- a. Staff members / students may use only the computers, computer accounts, computer software and computer files for which they are officially authorised to use.
- b. Staff members / students may not use another individual's account, or attempt to capture or guess other users' passwords.
- c. Staff members / students individually responsible for appropriate use of all resources assigned to them, including the computer, the network access, software and hardware. Staff members / students are thus accountable to the University for the use of such resources. As an authorised WSU user of resources, staff members / students may not enable unauthorised users to access the network by using a university computer or other device that is connected to the network.

- d. The University is bound by its contractual and licence agreements respecting third party resources. Staff members / students are expected to comply with all such agreements when using these resources. Any staff member / student will be held liable for any transgression of any related contractual licences or legal agreements.
- e. Staff members / students should make a reasonable effort to protect their passwords and to secure resources against unauthorised use or access. Staff members / students must configure hardware and software in such a way that reasonably prevents unauthorised users from accessing university network and computing resources.
- f. Staff members / students must not attempt to access restricted portions of the network, an operating system, security software or other administrative applications without appropriate authorization by the system owner or administrator.
- g. Staff members / students must comply with the policies and guidelines for any specific set of resources to which they have been granted access. When other policies are more restrictive than this policy, the more restrictive policy takes precedence.
- h. Staff members / students must not use WSU computing and / or network resources in conjunction with the execution of programs, software, processes, or automated transaction-based commands that are intended to disrupt other computer or network users by damaging or degrading performance.
- i. Staff members / students must not use tools that are normally used to assess security or attack computer systems or networks unless they have been specifically authorised to do so.
- j. Staff members / students may make use of telephone facilities for making private calls provided this use is brief in duration, occurs infrequently, is the most effective use of time or resources, and does not interfere with the performance of one's official duties.
- k. Staff members / students may use personal equipment when a university issued device is not available. However users must then understand that their machines are acting as extensions of WSU network and are therefore subject to the same requirements that apply to WSU issued equipment.

## **5.2. Fair Share of Resources**

5.2.1 The WSU Information & Communication Technology (ICT) Services Department which operates and maintains computers, network systems and servers, is expected to maintain an acceptable level of performance and must ensure that frivolous, excessive, or inappropriate use of the resources by one person or a few people does not degrade performance for others. The network, computer clusters, mail servers and other central computing resources are shared widely and have limited capacity, requiring that resources be utilized with consideration for others who also use them.

Therefore, the use of any automated processes to gain technical advantage over others in the WSU community is explicitly forbidden.

5.2.2 The University may choose to set limits on an individual's use of a resource through quotas, time limits, and other mechanisms to ensure that these resources can be used by anyone who needs them.

### **5.3. Adherence with National Laws**

5.3.1 As a member of the WSU community, you are expected to uphold local ordinances and South African legislation. Some WSU guidelines related to use of technologies derive from that concern, including laws regarding license and copyright, and the protection of intellectual property.

5.3.2 As a user of WSU computing and network resources you must:

- a. Abide by all local and national laws.
- b. Abide by all applicable copyright laws and licences. WSU has entered into legal agreements or contracts for many of our software and network resources which require each individual using them to comply with those agreements.
- c. Observe the copyright law as it applies to music, videos, games, images, texts and other media in both personal use and in production of electronic information. The ease with which electronic materials can be copied, modified and sent over the Internet makes electronic materials extremely vulnerable to unauthorised access, invasion of privacy and copyright infringement.

### **5.4. Inappropriate Activities**

You are expected to use WSU computing facilities and services for those activities that are consistent with the educational, research and community engagement mission of the University. Prohibited activities include:

- a. Use of WSU computing services and facilities for political purposes.
- b. Activities that would jeopardize the University's tax-exempt status
- c. Use of WSU computing services and facilities for any other personal and or economic gain.

### **5.5. Privacy and Personal Rights**

5.5.1 General;

- a. All users are expected to respect the privacy and personal rights of others.
- b. Do not access or copy another user's email, data, programs, or other files.
- c. Be professional and respectful when using computing systems to communicate with others; the use of computing resources to libel, slander, or harass any other person is not allowed and could lead to university discipline as well as legal action by those who are the recipient of these actions.

5.5.2 While the University does not monitor or limit content of information transmitted on the campus network, it reserves the right to access and review such information under certain conditions. These may include but is not limited to the following: investigating performance deviations and system problems, determining if an individual is in violation of this policy, forensic investigations, as may be necessary, to ensure that WSU is not subject to claims of institutional misconduct.

5.5.3 User access to enterprise data will be approved by respective data owners on application through line managers.

## **5.6. Privacy in Email Communication**

While every effort is made to ensure the privacy of WSU email users, this may not always be possible. In addition, since employees are granted use of electronic information systems and network services to conduct University business, there may be instances when the University, based on approval from authorised officers, reserves and retains the right to access and inspect stored information without the consent of the user.

## **5.7. User Compliance**

When using University computing services, and accept any University issued computing accounts, you agree to comply with this and all other computing related policies. You have the responsibility to keep up-to-date on changes in the computing environment, as published, using University electronic and print publication mechanisms, and to adapt to those changes as necessary.

## **5.8. Consequences and Sanctions**

5.8.1 Minor infringements of this policy, when accidental, are generally resolved informally by the unit administering the systems or network. This may be done through email or in-person discussion and education.



5.8.2 Repeated minor infractions or misconduct which is more serious may result in staff or students finding themselves subject to the University's disciplinary procedures and may be subject to criminal proceedings.

5.8.3 The University reserves its right to take legal action against individuals who cause it to be involved in legal proceedings as a result of their violation of licensing agreements and/or other contraventions of this policy. This may include the recovery of any costs associated with claims for legal damages.

5.8.4 The University may also, at its discretion, pass on the details of an individual who has contravened the acceptable use policies of an upstream service provider to the appropriate individuals representing that service provider.

## **6. POLICY REVIEW**

6.1 This policy should be reviewed every three years, or as changes in legislation or technology dictate. Changes to the policy should be referred to the ITSC, who will refer any substantive changes to the IMC and Council.

6.2 This policy refers to a number of related guidelines and policies. Unless otherwise specified in a specific document, revisions to those documents may happen more frequently, and major changes need only be approved by the ITSC. However, the ITSC, at its discretion, may refer these to the university Council.

## **7. RELATED POLICIES**

- a. Computing Passwords Policy
- b. IT Security Policy
- c. IT Service-desk Policy