

ACCEPTABLE USE POLICY INCLUDING NETWORK POLICY AND PASSWORD POLICY

1. POLICY PARTICULARS

DATE OF APPROVAL BY RELEVANT COMMITTEE STRUCTURE:
Information Technology Steering Committee:

DATE OF APPROVAL BY SENATE: 21st October 2016

DATE OF APPROVAL BY COUNCIL: 1st December 2016

COMMENCEMENT DATE: 1st January 2017

REVISION HISTORY: New Policy combining Password, Acceptable Use and Network Policy

REVIEW DATE: Every three years.

POLICY LEVEL: Council

RESPONSIBILITY

- IMPLEMENTATION & MONITORING: Manager: IT Operations, Manager: Service Delivery
- REVIEW AND REVISION: Director: Information & Technology Services

REPORTING STRUCTURE: Director : Information & Technology Services → Information Technology Steering Committee → Senate → Council

2.0 Policy Statement

2.1 Policy declaration

As part of its educational mission, Rhodes University acquires, develops, and maintains computers, computer systems and communication networks. These resources are intended to support University-related activities, including direct and indirect support of the University's

instruction, research and service missions; University administrative functions; student and campus life activities; and the free exchange of ideas within and among the University community and the wider local, national, and international communities.

As a user of these services and facilities, you have access to valuable University resources, to sensitive data, and to internal and external networks. Consequently, it is important for you to behave in a responsible, ethical, and legal manner.

In general, acceptable use means respecting the rights of other computer users, the integrity of the physical facilities and all pertinent license and contractual agreements. If an individual is found to be in violation of the Acceptable Use Policy, the University will take disciplinary action, including the restriction and possible loss of network privileges, up to and including suspension or termination from the University. Individuals are also subject to national laws and legislation governing many interactions that occur on the Internet. These policies and laws are subject to change as technologies evolve.

This document establishes specific requirements for the use of all computing and network resources at Rhodes University, including the use of computer laboratories and any personal equipment that may be registered for use on the Rhodes network.

2.2 Scope

This policy applies to all users of computing, networking, and communications facilities provided by any institute, department or section of Rhodes University wherever located, including privately owned or donated equipment connected to the University network and communications infrastructure. It applies to academic and support staff, students, guests, visitors and outside individuals or organisations accessing network services via Rhodes computing facilities.

Computing resources include all university owned, licensed, or managed telephones, computer hardware and software, and use of the university network via a physical or wireless connection, regardless of the ownership of the computer or device connected to the network.

In particular, references to the Information & Technology Services Division should, where appropriate, be taken to include departmental or other system managers responsible for the provision of a computing or communication service.

A separate, simplified acceptable use policy may be applied to services where users only receive limited Internet access, and are logically located outside of the University's network.

2.3 Your rights and responsibilities

As a member of the Rhodes community, the University provides you with the use of scholarly and/or work-related tools, including access to Library electronic resources, to certain computer systems, servers, software and databases, to the campus telephone and voicemail systems, and to the Internet. You have a reasonable expectation of unobstructed use of these tools, of certain

degrees of privacy (which may vary depending on whether you are a University employee or a registered student), and of protection from abuse and intrusion by others sharing these resources. You can expect your right to access information and to express your opinion to be protected as securely as it is for paper and other forms of non-electronic communication.

In turn, you are responsible for knowing the regulations and policies of the University that apply to appropriate use of the University's technologies and resources. You are responsible for exercising good judgment in the use of the University's technological and information resources. The acceptable use of a computer, computer system, telephone, or network does not extend to whatever is technically or legally possible.

As a representative of the Rhodes University community, you are expected to respect the University's good name in your electronic dealings with those outside the University.

3.0 Policy Implementation

3.1 Acceptable use (see Acceptable Use Examples)

- a. You may use only the computers, computer accounts, and computer files for which you are authorised.
- b. You may not use another individual's account, or attempt to capture or guess other users' passwords. These accounts, for example, range from email, Novell access, RUCConnected, ESS services and Protea access
- c. All passwords should meet the minimum standards as laid out in the Password Guideline, except where technically this is not feasible
- d. You should make a reasonable effort to protect your passwords and to secure resources against unauthorised use or access. You must configure hardware and software in a way that reasonably prevents unauthorised users from accessing Rhodes' network and computing resources.
- e. You are individually responsible for appropriate use of all resources assigned to you, including the computer, the network address or port, software and hardware. You are thus accountable to the University for all use of such resources. As an authorised Rhodes University user of resources, you may not enable unauthorised users to access the network by using a Rhodes computer or a personal computer or other device that is connected to the Rhodes network. You may only connect authorised equipment as per the technical specifications documented in the Network Connection Guideline
- f. The University is bound by its contractual and license agreements respecting certain third party resources; you are expected to comply with all such agreements when using such resources.
- g. You 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.
- h. You must comply with the policies and guidelines for any specific set of resources to which you have been granted access. When other policies are more restrictive than this policy, the more restrictive policy takes precedence.

- i. You must not use Rhodes computing and/or network resources in conjunction with the execution of programs, software, processes, or automated transaction-based commands that are intended to disrupt (or that could reasonably be expected to disrupt) other computer or network users, or damage or degrade performance, software or hardware components of a system. This includes attempts to set up wireless connectivity within research laboratories in order to avoid process of requesting and budgeting for network points.
- j. On Rhodes' network and/or computing systems, do not use tools that are normally used to assess security or to attack computer systems or networks (e.g., password "crackers", vulnerability scanners, network sniffers, etc.) unless you have been specifically authorised to do so by the Director: Information & Technology Services.
- k. Forwarding "spam", chain letters, or any other type of unauthorized widespread distribution of unsolicited mail should be carefully considered.
- l. Use of Rhodes email for any or all of the following is prohibited (See Use of Email Guideline)
 - Commercial activities or personal gain.
 - For partisan political or lobbying activities. sending messages that constitute violations of Rhodes's student disciplinary code, harassment policy, or any other policy of the University.
 - Creation and use of a false or alias email address in order to impersonate another or send fraudulent communications.
 - Use of email to transmit materials in a manner which violates copyright laws.

Abuses of Rhodes's email services should be reported to abuse@ru.ac.za.

3.2 Fair share of resources

The Rhodes Information & Technology Services (I&TS) Division, and other University departments which operate and maintain computers, network systems and servers, expect 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 campus 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 Rhodes community is explicitly forbidden.

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. Please see the Fair Share of Resources section of the [Acceptable Use Examples](#) for further clarification.

3.3 Adherence with national laws

As a member of the Rhodes University community, you are expected to uphold local ordinances and South African legislation. Some Rhodes guidelines related to use of technologies derive

from that concern, including laws regarding license and copyright, and the protection of intellectual property.

As a user of Rhodes computing and network resources you must:

- Abide by all local and national laws.
- Abide by all applicable copyright laws and licenses. Rhodes University 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.
- 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.

Please visit Rhodes University's [Copyright & Take-down procedures](#) Rhodes University follows in responding to notifications of alleged copyright infringements on the University network.

3.4 Inappropriate activities

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

- Use of Rhodes's computing services and facilities for political purposes.
- Activities that would jeopardize the University's tax-exempt status
- Use of Rhodes's computing services and facilities for personal economic gain.

3.5 Privacy and personal rights

- All users of the university's network and computing resources are expected to respect the privacy and personal rights of others.
- No individual may access or copy another user's email, data, programs, or other files except as provided for in the [Policy on Emergency Access to ICT Accounts and Information](#).
- 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.
- While the University does not generally monitor or limit content of information transmitted on the campus network, it reserves the right to access and review such information under certain conditions, see [Policy on Emergency Access to ICT Accounts and Information](#).

3.6 User compliance

When you use 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. Important ICT-related announcements can be received by subscribing to ict-announce@lists.ru.ac.za Information is also made available on the noticeboard on the Information & Technology Services web site when necessary.

3.7 Consequences and sanctions

Minor infractions of this policy, when accidental, such as using more than one's fair share, are generally resolved informally by the unit administering the systems or network. This may be done through email or in-person discussion and education.

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. The University will follow the approved disciplinary procedure to determine the severity as well as the sanction for both students and staff.

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.

The University may also, within the framework of the Protection of Personal Information Act, 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.

4.0 Review procedure

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 Information Technology Steering Committee, who will refer any substantive changes to Senate and Council. Changes to the guidelines that accompany this policy must also undergo an annual review at the Information Technology Steering Committee and will be done so at the second meeting of the ITSC each year. ITSC may at its discretion refer these reviews to Senate and Council.

5.0 Related Policies and Links

[Acceptable Use Examples](#)

[Password Guideline](#)

[Email Guideline](#)

[Network Connection Guideline](#)

[Emergency Access to ICT Accounts and Information Policy](#)

[Copyright & Take-down procedures](#)