RHODES UNIVERSITY
Grahamstown • 6140 • South Africa

# ACCEPTABLE USE POLICY INCLUDING NETWORK POLICY AND PASSWORD POLICY

| | |
|---|---|
| **Policy Volume** | Support Services |
| **Policy Chapter** | Information & Technology Services |
| **Responsible Committee/Unit/Division/Faculty** | Information Technology Steering Committee |
| **Responsible Chairperson/Director/Manager** | Director: Information & Technology Services |
| **Dates of First and Subsequent Council Approvals** | 1 December 2016 |
| **Policy Approval Pathways (e.g. committee, Senex, Senate, Council)** | Director : Information & Technology Services → Information Technology Steering Committee → Senate → Council |
| **Revision History: Approved Reviews** | 27 November 2020 |
| **Review Cycle (e.g. every 2/5/7 years etc)** | Every 3 Years |
| **Next Review Date** | 2023 |

## 1. POLICY PARTICULARS

| | |
|---|---|
| **1.1. Policy Title** | Policy on Acceptable Use including Network Policy and Password Policy |
| **1.2. Policy Statement**<br>(State in a single paragraph the policy mandate and how this relates to the University Mission and Vision) | This policy establishes specific acceptable behaviours 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.<br><br>A separate acceptable use policy exists for users who receive limited internet access and are logically located outside of the Rhodes Network<br><br>https://www.ru.ac.za/media/rhodesuniversity/content/informationtechnology/AUP_for_the_Public_Network.pdf |
| **1.3. Reason for Policy**<br>(What this policy aims to achieve) | 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 Policy is intended to inform basic principles and acceptable behavior of all users of the Rhodes Network and resources. |
| **1.4. Policy Objective/s**<br>(What are the measurable objectives of this policy) | This Policy informs and guides acceptable use on all computing resources including University owned, licensed, or managed telephones, computer hardware and software, University owned routers 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 and regardless of method of connectivity.<br><br>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 within divisions and departments.<br><br>This Policy documents in one document acceptable behaviour across all platforms. |
| **1.5. People affected by this Policy**<br>(e.g. All units of the University) | All University staff, students and guests with access to the University network and resources |
| **1.5. Who should read this Policy**<br>(People who need to heed this policy to fulfil their duties) | All University staff, students and guests with access to the University network and resources |
| **1.6. Implementers of this Policy**<br>(Who will manage the implementation of this policy) | Information and Technology Services |
| **1.7 Website address/link for this Policy** | https://www.ru.ac.za/media/rhodesuniversity/content/informationtechnology/AUP_Pass_Net_Final.pdf |

## 2. RELATED DOCUMENTS FORMS AND TOOLS

(University Policies, Protocols and Documents (such as rules/policies/protocols/guidelines related to this policy)

| **Relevant Legislation** (Legislation/Regulatory requirements/Organisational Reports – name these) |
|---|
| Regulation of Interception of Communication Act<br>TENET SLA |

| Related Policies |
|---|
| |
| **Related Protocols** |
| Public AUP<br>Network Connection Guidelines<br>Email Guidelines<br>Password Guidelines<br>Copyright & Take-Down at Rhodes University<br>Identity Framework |
| **Forms and Tools** (documents to be completed in support of this policy implementation) |
| Policy template |

## 3. POLICY DEFINITIONS

(Technical or Conceptual terms used in the policy)

| No | TERM | DEFINITION |
|---|---|---|
| **3.1** | **Email Address** | **Rhodes email address associated with @ru.ac.za** |
| **3.2** | **User Account** | **ICT account ie. log into systems and internet** |
| **3.3** | **PC Profile** | **Local log in to the PC on which the individual works day to day** |
| **3.4** | **Server Directory** | **Storage space linked to the user ICT account** |
| **3.5** | **Shared space** | **Server space accessible to a number of users in a team/division/department** |
| | | |

## 4. PRINCIPLES GOVERNING THIS POLICY

| OVERVIEW |
|---|
| Rhodes University strives to carry out the following, as far as is reasonably practicable: |
| 4.1. **Adjust the policy as and when technology requirements require a significant change in behaviours** |
| 4.2. Adjust the guidelines associated with the Policy as regularly as possible |
| 4.3. Fairly assess breaches of the AUP and levels of seriousness of the impact |
| 4.4. **Communicate via appropriate channels changes to the AUP** |

## 5. DIRECTIVES FOR IMPLEMENTING THIS POLICY

(Actions and processes by which the objectives of the policy will be achieved.)

**5.1. Effective date**

**As soon as a user accesses and makes use of the network the Policy is applied**

## 5.2. Acceptable use (See Acceptable Use Guidelines)

You may use only the computers, computer accounts, and computer files for which you are authorised.

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, RUConnected, ESS services, Protea access and any other access account running on a Rhodes platform.

All passwords should meet the minimum standards as laid out in the Password Guideline, except where technically this is not feasible

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.

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

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.

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.

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.

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.

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.

Forwarding "spam", chain letters, or any other type of unauthorized widespread distribution of unsolicited mail should be carefully considered.

Use of Rhodes email for any or all of the following is prohibited (See Use of Email Guideline)

i. Commercial activities or personal gain.
ii. 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.
iii. Creation and use of a false or alias email address in order to impersonate another or send fraudulent communications.
iv. 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.

## 5.3. 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, are 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 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 Guidelines for further clarification. Changes in the management of the resources occur without necessarily any prior notification. You are expected to update yourself with the AUP on an ongoing basis.

## 5.4. Adherence with national laws

As a member of the Rhodes University community, you are expected to uphold local ordinances and South African legislation. These ordinances change and you are expected to keep yourself updated with these changes that will usually be communicated via a change in the AUP. 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:

a. Abide by all local and national laws.

b. 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.

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.

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

## 5.5. 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:

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

## 5.6. Privacy and personal rights

a. All users of the university's network and computing resources are expected to respect the privacy and personal rights of others. Storage of any material that may cause offense to another who may stumble across the material is inappropriate behaviour.

b. Storage of personal material on a departmental shared space is prohibited.

c. 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.

d. 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. Refer to the guidelines on how to use email appropriately. Do not copy individuals in unnecessarily and only respond where appropriate.

e. 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.

.

## 5.7 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.

### 5.8 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.

### 5.9 Email Use

All Rhodes business and research related emails will be sent and received using the ru.ac.za email address assigned to you or where appropriate using a shared mailbox.

Use of a private email address for Rhodes activities is not allowed.

Use of the Rhodes email address for private emails is allowed provided that the user understands the implications of Rhodes accessing the Rhodes mail box under certain conditions as detailed in the Emergency Access to Information and ICT Policy.

https://www.ru.ac.za/media/rhodesuniversity/content/informationtechnology/ICT_Emergency_Access_Policy.pdf

## 6. ROLES AND RESPONSIBILITIES

(Roles and responsibilities of Key personal/Divisions/Faculties/Departments)

| ROLE | RESPONSIBILITY |
|---|---|
| **ROLE 1**<br>HoD's and Divisional Heads | Advise new staff about the Acceptable Use Policy |

| | |
|---|---|
| **ROLE 2**<br>**I&TS Staff** | Report breaches of the AUP to Line Managers and Director I&TS |
| **ROLE 3**<br>**Director I&TS** | Report serious staff breaches to HR for processing via the Staff Disciplinary Code<br>Report serious student breaches to the Student Higher Disciplinary proctors |
| **ROLE 4**<br>**HR Division** | **Processing staff disciplinary processes** |
| **ROLE 5**<br>**Proctors** | Processing of student disciplinary processes |

## 7. CONTACTS

| Area of Concern | Division/Faculty/Department | Telephone | Email |
|---|---|---|---|
| Change in ICT laws and regulations | Director I&TS | 7456 | N.Ripley@ru.ac.za |
| Breach by a user of ICT | Relevant Line Managers I&TS | 8288 | L.Angus@ru.ac.za<br>T.Chambers@ru.ac.za<br>D.Sieborger@ru.ac.za<br>N.Ripley@ru.ac.za |
| | | | |
| | | | |
| | | | |

## 8. POLICY REVIEW PROCEDURE

(Actions and processes by which the policy will be reviewed)

| |
|---|
| **This Policy should be reviewed every 3 years or when changes in circumstances or legislation dictate** |
| |
| **Communication of the review process**<br>**Via Toplist once approved by Council** |

## 9. POLICY CONTEXT: RELEVANT DOCUMENTS CITED/CONSULTED/ADOPTED

| | |
|---|---|
| 1 | http://www.justice.gov.za/legislation/acts/2013-004.pdf |
| 2 | http://www.justice.gov.za/legislation/acts/2002-070.pdf |
| 3 | https://www.ru.ac.za/media/rhodesuniversity/content/informationtechnology/ICT_Emergency_Access_Policy.pdf |
| 4 | Acceptable Use Guidelines |
| 5 | Copyright & Take-down procedures |
| 6 | Password Guidelines |
| 7 | Email Guidelines |
| 8 | Network Connection Guidelines |

| | |
|---|---|
| 9 | https://www.ru.ac.za/media/rhodesuniversity/content/informationtechnology/AUP_for_the_Public_Network.pdf |

## LIST OF APPENDICES