

# (UPDATED) ACCEPTABLE USE POLICY FOR RHODES UNIVERSITY

---

## 1. The need for an Acceptable Use Policy

- 1.1 As part of its educational mission, Rhodes University acquires, develops, and maintains computers, computer systems and communication networks. These information technology resources are intended for University-related purposes, 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.
- 1.2 Rhodes University supports a campus and computing environment open to the free expression of ideas, including unpopular points of view. However, the use of University computing and communication resources, like the use of other University-provided resources and activities, is subject to the requirements of legal and ethical behavior.
- 1.3 Additionally, computing resources, in particular network bandwidth, are expensive and therefore finite. Once a resource is being utilized at a rate near its carrying capacity, additional use will degrade its value. Thus acceptable use of a computer, computer system or network does not extend to whatever is technically or legally possible, and implies that restrictions on access and usage must be imposed in order to constrain the demand for limited resources.
- 1.4 An Acceptable Use Policy is intended to provide the basis of a social contract, protecting both individual users and the University community, in which the expectation of what constitutes reasonable use of Rhodes University's computing/communication resources can be specified.

## 2. Scope of the Rhodes University Acceptable Use Policy

- 2.1 This Acceptable Use Policy applies to all users of all 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 should be interpreted such that it has the widest application. In particular, references to the Information Technology Division should, where appropriate, be taken to include departmental or other system managers responsible for the provision of a computing or communication service.
- 2.2 Only members of the teaching, research, administrative, technical, service and clerical staff, registered students of the University, or other persons specifically designated by the Director of Information Technology Division may use the IT facilities provided by Rhodes University. By definition, individuals dismissed or expelled from Rhodes University do not fall into this category and are not entitled to access.
- 2.3 This Acceptable Use Policy is taken to include the Acceptable Use Policies published by the Internet Service Providers used by Rhodes University, in particular those of [TENET \(the Tertiary Education Network\)](#). Members of the University and all other users of the University's facilities are bound by the provisions of these policies in addition to this Acceptable Use Policy.

### 3. Purposes for which IT facilities may be used

- 3.1 Rhodes University's computing resources are provided to facilitate a person's work as an employee or student of the University, specifically for educational, training, administrative or research purposes.

- 3.2 Use for other purposes, such as personal telephone calls, personal electronic mail or recreational use of the World Wide Web or Usenet News, is a withdrawable privilege and not a right. Any such use must not interfere with the user's duties or any other person's use of computer systems and must not, in any way, bring the University into disrepute. Priority must always be granted to those needing facilities for academic work.

- 3.3 Commercial work for outside bodies using centrally managed services requires explicit permission from the Director of Information Technology. Such use may be liable to charge.

### 4. Registration for use of IT facilities

- 4.1 In order to use the computing facilities of Rhodes University a person must first be authorised. All administratively registered students are automatically registered for the use of core IT facilities. Other members of the University should apply to the Information Technology Division for registration. Registration to use University services implies, and is conditional upon acceptance of this Acceptable Use Policy, for which a signature of acceptance is required on joining the University.

- 4.2 The registration process grants authorisation to use the core IT facilities of the University. Following registration, a username and password will be allocated. Registration for other services may be requested by application to the Information Technology Division. Users do not own accounts on University computers, but are granted the privilege of exclusive use.

- 4.3 Authorisation to use IT facilities shall normally be granted for as long as the individual continues to fall into the category for which initial application for use of the facilities was made, but this permission may be reviewed from time to time. This acceptable use policy is binding so long as such authorisation exists.

- 4.4 All individually allocated usernames and passwords are for the exclusive use of the individual to whom they are allocated. The user is personally responsible and accountable for all activities carried out under their username. The password associated with a particular personal username must not be divulged to another person. Attempts by any user to access or use any username which is not authorised to him/her, are prohibited.

- 4.5 All users must correctly identify themselves at all times. A user must not masquerade as another, withhold his/her identity or tamper with audit trails. A user should take all **reasonable precautions to protect and secure their resources**. In particular, passwords used must adhere to accepted **good password practice**. In cases where unauthorized use of accounts or resources is detected or suspected, the account owner should change the password and report the incident to the appropriate systems administrator. Forgotten passwords will be reset by system administrators only when the account owner presents, in person, proof of identity.

### 5. Privacy considerations

- 5.1 Users should be aware that their uses of Rhodes University computing

resources are not completely private. While the University does not routinely monitor individual usage of its computing or communications resources, the normal operation and maintenance of these resources require the backup and caching of data and communications, the logging of activity, the monitoring of general usage patterns and other such activities that are necessary for the rendition of service.

- 5.2 It should be noted that a "communication" — electronic or otherwise — by definition involves a sender and a recipient. While good assumptions may be made about the technology employed on the Rhodes campus and the legal framework in which it is used, these assumptions may not be valid at a remote site.
- 5.3 More details of privacy concerns may be found in the Rhodes [policy on Privacy and Network monitoring](#).

## 6. Social considerations

- 6.1 Conventional norms of behaviour apply to computer based information technology just as they would apply to more traditional media. Within the University context this should also be taken to mean that the traditions of academic freedom will always be respected. The University, as expressed in its Equal Opportunities Policy, is committed to achieving an educational and working environment which provides equality of opportunity, and freedom from discrimination on the grounds of race, religion, sex, class, sexual orientation, age, disability or special need.

- 6.2 Storing, posting, publishing or otherwise distributing material, which is offensive, obscene or abusive, may be illegal and may also contravene University codes on harassment. Users of University computer systems must make themselves familiar with, and comply with, the [University codes and procedures concerning all forms of harassment](#).

- 6.3 No person shall wilfully jeopardise the integrity, performance or reliability of computer equipment, software, data or other stored information. Reasonable care should also be taken to ensure that resource use does not result in a denial of service to others.

- 6.4 No user shall interfere or attempt to interfere in any way with information belonging to, or material prepared by, another user. Similarly no user shall make unauthorised copies of information belonging to another user. The same conventions of privacy should apply to electronically held information as to that held on traditional media such as paper. The University [policy on plagiarism](#) should be taken into consideration when use is made of information obtained electronically.

- 6.5 Unauthorised extensions and modifications to the Rhodes network and telephone infrastructure by individuals or departments are prohibited. Such unauthorised extensions would include:

- 6.5.1 adding or removing wireless access points or bridges;
- 6.5.2 adding or removing hubs, switches or routers, or devices containing embedded switches or routers;
- 6.5.3 unplugging or removing fly leads or other cabling, or installing unshielded twisted pair fly leads not conforming to specifications;
- 6.5.4 plugging private computers into network points provided for

departmental or laboratory PCs.

6.6 For specific services the University may provide more detailed guidelines. In particular, users providing information on the World Wide Web must follow the [Web Unit's Code of Practice](#) in addition to the policies provided in this Acceptable Use Policy. Users of services external to the University are expected to abide by any rules and codes of conduct applying to such services.

6.7 **It is the responsibility of all users of Rhodes telecommunications facilities to:**

- 6.7.1 ensure that important files related to their work or research are backed up.
- 6.7.2 ensure that up to date and appropriate virus scanning software is installed and activated on the PCs for which they are responsible.
- 6.7.3 regularly check for, download, **INSTALL** and activate security patches from the vendors of the software on the PCs for which they are responsible.
- 6.7.4 ensure that permissions and other access controls are set appropriately on files that could be accessed by others.
- 6.7.5 periodically check that access restrictions on files that are being stored on a server that is not under the control of the user are functioning as intended, for example that files stored on a web or ftp server that should not be visible outside the Rhodes network are not in fact accessible to outsiders.

## 7. **Acceptable and unacceptable usage**

- 7.1 Unacceptable use of University computers, network and communications resources include the following:
  - 7.1.1 the retention or propagation of material that is offensive, obscene or abusive, except in the course of recognised research or teaching that is permitted under South African and international law; propagation will normally be considered to be a much more serious offence;
  - 7.1.2 causing annoyance, inconvenience or needless anxiety to others;
  - 7.1.3 defamation, with the understanding that genuine scholarly criticism is acceptable;
  - 7.1.4 intellectual property rights infringement, including copyright, trademark, patent, design and moral rights;
  - 7.1.5 inappropriate mass mailings to newsgroups, mailing lists, or individuals, e.g. "spamming," "flooding," or "bombing"
  - 7.1.6 breaking in, or attempting to break into or damaging computer systems or data held thereon;
  - 7.1.7 unauthorised resale of University computing services or information
  - 7.1.8 using institutional resources for personal benefit or gain or for the benefit or gain of other individuals or outside organizations, where personal benefit or gain may include a use solely to avoid personal expense.

- 7.2 These restrictions should be taken to mean, for example, that the following activities will normally be considered to be a breach of this policy:
- 7.2.1 the distribution or storage by any means of pirated software or information
  - 7.2.2 the copying of unlicensed copyright software or information
  - 7.2.3 non-academic activities which generate heavy network traffic, especially those which interfere with others' legitimate use of IT services or which incur financial costs
  - 7.2.4 frivolous use of University owned computer laboratories, especially where such activities interfere with others' legitimate use of IT services
  - 7.2.5 storing, posting, publishing or otherwise displaying obscene or offensive data, even temporarily, in areas where they might be viewed passively or inadvertently
  - 7.2.6 originating or passing on electronic chain letters
  - 7.2.7 using electronic mail to harass or threaten others, including sending repeated, unwanted e-mail to another user
  - 7.2.8 using another site's mail server to relay mail without the express permission of the site
  - 7.2.9 the use of University or departmental mailing lists for non-academic purposes
  - 7.2.10 forging the identity of a user and/or machine or system in an electronic communication
  - 7.2.11 attempts to access, or actions intended to facilitate access to, computers for which the individual is not authorised
  - 7.2.12 probing, scanning or testing the vulnerability of a system or network without express authorization of the owner of the system or network
  - 7.2.13 the use of other people's web site material without the express permission of the copyright holder
  - 7.2.14 the use of peer to peer or other file sharing utilities and networks for the purposes of distributing material for which any license on that material may preclude distribution
  - 7.2.15 in the case of telephone systems: accepting or soliciting reverse charge calls
  - 7.2.16 spending excessive time on private calls
  - 7.2.17 harassing or threatening others telephonically;
- 7.3 Other uses may be unacceptable in certain circumstances. In particular, users of the Residence Network should take account of any particular conditions of use applying to that service.
- 7.4 Rhodes University can and does provide network connectivity to privately owned systems that belong to individuals associated with the University, such as members of staff or students. It also provides network connectivity to associated research institutes and other affiliated organisations. Individuals, or

organisations to whom the University has made such network access available, whether by direct access, remote access, or by any other means, are responsible for all the systems making use of this connectivity. These systems should not provide any services to others via remote access unless explicitly authorised.

7.5 Acceptable uses may include:

7.5.1 Personal email and recreational use of Internet services, as long as these are in keeping with the framework defined in this policy document and do not interfere with one's duties, studies or the work of others;

7.5.2 Advertising via electronic notice boards intended for this purpose, or via other University approved mechanisms. However such use must be regarded as a privilege and not as a right and may be withdrawn if abused or if the user is subject to a disciplinary procedure.

7.5.3 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 the persons official duties.

## 8. Legal implications

8.1 Any software and/or electronic or hard copy of data or information which is not generated by the user personally and which may become available through the use of University computing or communications resources shall not be copied or used without permission of the University or the copyright owner. In particular, it is up to the user to check the terms and conditions of any licence for the use of the software, data or information and to abide by them. Software, data and/or information provided by the University may only be used as part of the user's duties as an employee or student of the University or for educational purposes. The user agrees to abide by all the licensing agreements for software entered into by the University with other parties.

8.2 The user undertakes to comply with the provisions of the laws of South Africa as well as all other relevant legislation and legal precedent. See below for a summary of the main points of some of the relevant Acts. Copies of the applicable documents are available through the University Library or online at the [polity.org.za](http://polity.org.za) and other sites. Further advice should be obtained through the Director of Information Technology in the first instance.

## 9. Copyright Act no 98 of 1978

9.1 A copyright infringement occurs when the owner's exclusive rights to the work are infringed. Infringements are: to reproduce the work in any manner or form; to perform the work in public; to broadcast the work; and to make an adaptation of the work.

9.2 This Act, together with the statutes that have amended and extended it, defines and explains the voluminous fine print of copyright law. It makes it an offence to copy all, or a substantial part, which can be a quite small portion, of a copyright work. There are, however, certain limited use permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not

included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, sound, moving images, TV broadcasts and many other media.

- 9.3 Apart from the standard arguments associated with fair dealing, a person may claim that, by placing material on a web site, the proprietor has granted others an implicit non-exclusive licence to reproduce the material, for otherwise it would be impossible to view the material. It is contended that such a licence should cover transient copies only and that any additional rights should be granted in terms of an explicit licence on the web site. The process of caching is an example. A cache is made on a person's hard drive or on the service provider's network and acts as a temporary storage facility of electronic copies of material obtained from remote web sites. This form of reproduction is an essential procedure for efficient use of the Internet and should be regarded as authorised in terms of an implicit licence, or fair dealing. It could also amount to making a back-up copy, which is also authorised use.

- 9.4 When dealing with issues relating to intellectual property rights held in other countries, it should be noted that South Africa is a signatory to various [international treaties](#) aimed at protecting intellectual property, most notably the [Berne Convention for the Protection of Literary and Artistic Works](#).

## 10. Trade Marks Act no 194 of 1993

- 10.1 This Act provides protection for Registered Trade Marks, which can be any symbol (words or images) or even shapes of objects that are associated with a particular set of goods or services. Anyone who uses a Registered Trade Mark without permission can be sued. They can also be sued if they use a Mark that is confusingly similar to an existing Mark.
- 10.2 So called defensive registrations have applicability to Internet domain names and cybersquatting.

## 11. Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002

- 11.1 This provides that, unless authorised by a judge, one may not intentionally:
- 11.1.1 intercept a telephonic or telecommunications or postal communication without the dispatcher's knowledge; or
  - 11.1.2 monitor and/or record conversations or communications with a monitoring device so as to gather confidential information concerning any person, body or organisation.
- 11.2 The [Policy on Privacy and Network Monitoring](#) outlines the rights of both users and the University regarding access to information stored on or transmitted through University owned equipment.

## 12. Electronic Communications and Transactions Act 25 of 2002

- 12.1 This comprehensive act regulates the activities of an information service provider, and gives a legal framework for the protection of both consumers and service providers in an increasingly online world. It also defines, for the first time, offences related to hacking and/or cracking.
- 12.2 For example, section 86(4) dealing with "Unauthorised access to, interception of or interference with data", says:

"A person who commits any act described in this section with the intent to interfere with access to an information system so as to constitute a denial, including a partial denial, of service to legitimate users is guilty of an offence."

The penalty for this offence is specified in Section 89(2):

- 12.3 "A person convicted of an offence referred to in section 86(4) or (5) or section 87 is liable to a fine or imprisonment for a period not exceeding five years."

### **13. The Promotion of Access to Information Act No. 2 of 2000**

13.1 This Act gives effect to section 32 of the Constitution, which provides that everyone has the right to access any information held by the State or any information that is held by another person, where such information is required for the exercise or the protection of any rights.

13.2 The Act creates mechanisms to facilitate access to records held by public and private bodies irrespective of their size and the nature of their business.

13.3 To facilitate this access, the Act sets out various procedures to be followed by persons requesting information (called requesters) and the "head"/delegated Information Officer of private bodies (referred to for convenience as "Information Officer" — which in the case of Rhodes is the Registrar). Any person may request access, including an employee, the public, government or competitors.

13.4 Each institution must have a "PROATIA Manual" available explaining these procedures as they apply to the institution.

### **14. The Films and Publication Act no 65 of 1996 and its Amendment Act no 34 of 1999**

14.1 The amendment was to bring Internet material relating to online pornography within its ambit. One of the expressed objects of the Act is to punish exploitative use of children on the Internet. Anyone who knowingly distributes, creates, produces, imports or possesses visual presentations of child pornography commits an offence. Offences under the Act are not restricted to child pornography. Subject to some exceptions, knowingly to distribute material which contains depictions of extreme violence, explicit violent or degrading sexual conduct and bestiality is also prohibited.

14.2 For a discussion of this Act as it applies to Internet use, see [ISPA Advisory No 3, 22 May 2000](#).

### **15. Criminal Procedures Act No 51 of 1977**

15.1 This Act contains provisions which would render searches of persons or premises and seizure of goods lawful in certain circumstances.

### **16. Common Law**

16.1 Finally, aspects of South African Common Law applies, especially that of *crimen injuria* which defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, s/he:-

- 16.1.1 uses threatening, abusive or insulting words or behaviour, or disorderly behaviour; or  
displays any writing, sign or other visible representation which is
- 16.1.2 threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

16.2 Common Law would also apply to:

- 16.2.1 malicious injury to property as in the case of hacking or cracking.

16.3 These particular aspects would also contravene the student disciplinary code.

## 17. Disciplinary processes and procedures

- 17.1 Minor infractions of this policy, when accidental, such as consuming excessive resources or overloading computer systems, are generally resolved informally by the unit administering the systems or network. This may be done through electronic mail or in-person discussion and education.
- 17.2 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.
- 17.3 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.
- 17.4 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.

## 18. Implementation and supervision of policy

- 18.1 The responsibility for the supervision of this Acceptable Use Policy is delegated to the Information Technology Division. A senior member of the Information Technology Division, normally the Support Manager or their nominee, will be designated as the person responsible for the day to day management of the policy's enforcement. He/she will liaise with the Director of Information Technology, the University Librarian, the Manager of the Campus Protection Unit, the Dean of Students, the Dean of the Faculty of Law, the Registrar and Heads of Department as required. Procedural guidelines will be published from time to time as a separate document.

- 18.2 Any suspected breach of this policy should be reported to a member of the Information Technology Division staff. The responsible senior member will then take the appropriate action within the University's disciplinary framework, in conjunction with other relevant branches of the University. Information Technology Division staff will also take action when infringements are detected in the course of their normal duties. Actions will include, where relevant, immediate removal from online information systems of material that is believed to infringe the law. The University reserves the right to audit and/or suspend without notice any account pending an enquiry.

- 18.3 This policy cannot be exhaustive and inevitably **new social and technical developments** will lead to further uses which are not fully covered. In the first instance students should address questions concerning what is acceptable to their supervisor; staff should initially contact their supervisor or Head of Department/Section. Where there is any doubt the matter should be raised

with the Information Technology Division, whose staff will ensure that all such questions are dealt with at the appropriate level within the University.

*Copyright ©2004 Rhodes University - Version 2.6 - Approved by Senate, 2004/xx/yy*