

Policy on Privacy and Network Monitoring

0. Policy Particulars

Date of Approval by The Information Technology Steering Committee:	2000/09/28
Date of Approval by Senate:	2004/10/29
Date of Approval by Council:	?
Commencement Date:	2001/01/01
Revision History:	2000/09/28; 2004/10/29
Review Date:	Annually
Policy Level:	All users of the University's computing and communication facilities
Responsibility - Implementation & Monitoring:	Systems Manager, Information Technology Division
Responsibility - Review & Revision:	Director, Information Technology
Reporting Structure:	Director, Information Technology Division » Vice Principal » Senate » Council

1. Expectation of privacy

- 1.1 Privacy concerns in the Rhodes context revolve around the extent of the right to privacy in the workplace, given that computer and network facilities are for the most part provided by Rhodes — and Rhodes' right to control the working environment and duty to ensure the workplace is free from harassment.

This 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.

- 1.2 It should be understood that there are wider implications as regards privacy and monitoring, and some additional aspects are dealt with in the [Rhodes Acceptable Use Policy](#). Also, as the document describing [basic computer security principles](#) makes clear, users themselves are responsible for ensuring that sensitive files have the appropriate privileges set that would make them inaccessible to other users.
- 1.3 It should be noted that systems staff who have appropriate privileges have the ability to access all files, including electronic mail files, stored on the computer systems which they manage.
- 1.4 Staff and students should be aware that comprehensive logs are generated by the various internet services used on campus, including email and web access. While it is not the policy of the University to actively monitor activity on the network, it is sometimes necessary to examine such logs when a problem has occurred or when optimising traffic on both internal and external data links.

- 1.5 Facsimile transmissions and voice mail are technologies that may create an electronic record. Unlike a voice conversation, an electronic record is reproducible and is therefore not private. Such records may be subject to disclosure under public disclosure laws, or may be disclosed for audit or legitimate operational or management purposes.
- 1.6 In cases where reasonable grounds exist to support the belief that a communications or computer system is being used in a way that contravenes any of the relevant acceptable use policies, the Director of Information Technology may, at his/her discretion, authorise the interception of any electronic data or communication relating to the computer system or user in question. Information gathered in this way may be used in any subsequent disciplinary hearing or legal proceeding relating to the case.
- 1.7 Individuals may approach the relevant University authorities in order to report instances of harassment, threats or other abuse. These reports may result in investigations by the Information Technology Division of electronic audit trails to establish the identity of any perpetrator. Results of these investigations will be released to the relevant authority in order that due process may occur. In some instances, the investigation may best, or may only, be carried out by a remote service provider. In such cases it is very likely that a court order will be required.

2. Privacy on the web

Traffic logs are used as part of ongoing efforts to make the most effective use of our limited and expensive Internet access circuits. This includes the automated identification of inappropriate (ie. material which clearly bears no relation to any academic or research work) and excessive (ie. more than several megabytes of traffic in a few hours) use of web services. Traffic which falls into such categories is likely to be restricted to hours during which it has less of an adverse effect on other network users (eg. outside normal working hours).

3. Email privacy

- 3.1 Email is not a secure medium.
- 3.2 Note that there is a distinction between monitoring and disclosing information about emails, and monitoring and disclosing the content of emails. Divulgence of certain information is necessary to operate the network or to forward communications to an addressee, or even for the protection of Rhodes University's rights.
- 3.3 EMail logs contain information about the source and destination addresses, the length of the message, and the time of receipt and delivery. The contents of messages are not recorded. However, users should be aware that there is no guarantee that email contents will remain private between sender and recipient. Email is similar to sending a letter through the post in an unsealed envelope.
- 3.4 In some cases misdirected mail (ie. when an invalid addressee is entered) is redirected to site postmaster addresses. This process sometimes does not remove the original email contents. Users may also enter an incorrect but valid address so that their mail is delivered to the wrong destination user. While it is unlikely that email is intercepted and examined elsewhere, there is no guarantee of this as there is no control over messages once they have left the Rhodes network.
- 3.5 Users who are particularly concerned about email privacy and the integrity of

messages should investigate using one of the various forms of encryption and verification systems that are available.

- 3.6 There may be occasions where, for operational reasons such as SPAM control or virus checking, it is necessary to filter and reject network traffic — including email — which originates from particular sources.

4. Ownership of Information

- 4.1 Users do not own accounts on University computers, but are granted the privilege of exclusive use.
- 4.2 Access to staff or student files will not normally be given to another member of staff unless authorised by the Director of Information Technology, who will use his/her discretion in consultation with other senior officers of the University, if appropriate. In such circumstances the Head of Department or Section, or more senior line manager, will be informed, and will normally be consulted prior to action being taken. Such access will normally only be granted where a breach of the law or the Acceptable Use Policy is suspected.
- 4.3 Files which are left behind after a student or member of staff leaves the University will be considered to be the property of the University, and may be disposed of at its discretion.
- 4.4 In the case of persons who resign from the employ of Rhodes University, or of students ceasing to be registered, accounts and their associated files will be deleted during the course of the year following their departure. If no notification of departure is made, automated processes that detect inactive accounts will periodically be invoked to clear such accounts. Persons leaving Rhodes are expected to make timeous arrangements about providing themselves with an alternative computing environment.
- 4.5 In the case of the death of a user, supervisors and/or the next of kin should approach the Director of Information Technology to make arrangements as to the disposition of data files, including stored email. If no arrangements are made, the account will be considered to be inactive and thus subject to normal de-registration procedures.
- 4.6 In the case of an employee dismissed from Rhodes University or of a student being expelled, the privilege of access to the relevant user accounts will be immediately revoked. The associated files will be deleted during the course of the year following their dismissal or expulsion. Representations about retrieving data for which there are intellectual property claims will be considered