RHODES UNIVERSITY

POLICY ON EMERGENCY ACCESS TO ICT ACCOUNTS AND INFORMATION

1. POLICY PARTICULARS

DATE OF APPROVAL BY RELEVANT COMMITTEE STRUCTURE:

Information Technology Steering Committee: 7 October 2013

DATE OF APPROVAL BY SENATE: 25 October 2013

DATE OF APPROVAL BY COUNCIL: 5 December 2013

COMMENCEMENT DATE: Per 3.1, effective for all users on 1 July 2014

REVISION HISTORY: New Policy, 2016

REVIEW DATE: Every three years, Next review 2019

POLICY LEVEL: Council

RESPONSIBILITY

- IMPLEMENTATION & MONITORING: Manager: IT Operations
- 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

This policy limits individual users' right to privacy and establishes a mechanism by which the University may obtain emergency access to an individual account or other electronic information to ensure business continuity.

2.2. Policy objectives

All users of Rhodes' ICT facilities are granted exclusive use of an account. In addition, they are afforded the privilege of limited personal use of email and other ICT facilities. As such they have a reasonable expectation that their personal electronic communications and other information will remain private.

Whilst it is not the University's intention to do away with these benefits, this expectation of privacy sometimes presents an obstacle to business continuity and good governance.

This policy seeks to balance individual users' right to privacy and the institutional need for business continuity. The policy seeks to ensure that the Protection of Personal Information Act as well as RICA are adhered to, whilst acknowledging that there are also institutional imperatives that need support.

http://www.justice.gov.za/legislation/acts/2013-004.pdf

http://www.justice.gov.za/legislation/acts/2002-070.pdf

2.3. Policy scope

This policy is intended to cover all ICT systems — irrespective of where they are housed and who administers them — where users may store or transmit personal (i.e. not related to the business of the University) information or communications.

Systems that exist solely in support of the University's business operations (such as the student records system) do not normally contain such information, and are therefore excluded from the scope of this policy. Users should not store unnecessary personal information within their accounts on such systems. Those systems falling outside the scope of this policy may be subject to different procedures, as recommended by the department or division responsible for the system and as approved by the Information Officer.

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.

3. Policy implementation

3.1. Effective date

All users who continue to make use of the University's ICT facilities for personal correspondence or to store personal information will be deemed to have granted consent to the provisions of this policy by accepting this policy as part of the Acceptable Use Policy https:\\www.ru.ac.za\aup.

3.2. Requirement for consent

The Information & Technology Services Division shall seek an individual user's consent, unless this is not practically possible, before granting access or making any change that might result in a loss of personal privacy. Such consent may be granted in person, telephonically, or via email or other electronic communications channel.

It is recognised that at times it may not be possible for a user to timeously provide such consent. Examples of such circumstances include, but are not limited to:

- A user is on leave or otherwise away from the University and cannot be reached within a reasonable timeframe (which may vary according to the business requirements);
- A user is temporarily or permanently unable to make use of a computer or other communications device (incapacitated) for a known reason;
- A user is subject to disciplinary proceedings or sanction; or
- A user is deceased.

In such circumstances, the requirement for consent may be waived but not before every attempt has been made to reach the individual user's consent.

3.3. Circumstances in which access may be granted without consent

3.3.1. Continuity of communication

When users are away from the University and are unable to respond to email or other electronic communication, they are expected to create an "out of office" message informing correspondents of alternative arrangements during their absence.

Should an individual user neglect or be unable to do this, and where business requirements dictate that an "out of office" or vacation notification is needed, their immediate supervisor, line manager, or department head can request the Information & Technology Services Division to create such a message on their behalf.

The "out of office" message should inform new correspondents of the correct alternative contact details for University business and, where possible, indicate the timeframe of the

change. For privacy reasons, it should not state the reason for absence unless the affected user has given consent for this information to be released. In processing this out of office message I&TS staff are not granted permission to access any information within the mailbox.

There are no privacy implications to creating an "out of office" message, and may be implemented immediately and without attempting to obtain consent. As such this should be the default method by which continuity of communication is maintained.

3.3.2. Emergency access to email or other electronic information

Where urgent business requirements dictate, reasonable steps must be taken to acquire an individual user's consent, prior to the relevant head of an academic department or director (or deputy director) of an administrative division requesting access to business related information stored under a user's profile.

Such a request must include but is not restricted to include:

- The name of the person who's information needs to be accessed (the affected user);
- The name of the person to whom access should be granted (the authorised recipient);
- The specifics of the information that is required (for instance, particular files stored on a file server, email messages matching given filter criteria, etc);
- An indication as to why the requirement for consent should be waived; and
- If the user is contactable but timeframes dictate that the information is required before a response might reasonably be expected, an indication of the business requirement for expedient access to this information and/or risk associated with not having such access.
- Details of the steps taken to obtain the consent of the individual user

In addition to the above requirements, the University Information Officer may require that further steps be taken to obtain the necessary consent

On receipt of a valid request for emergency access and with approval from the University Information Officer (Vice Chancellor or his/her nominee), the Information & Technology Services Division will make a copy of the requested information available to the authorised recipient. Where the information is not accessible to the Information Technology Services staff, they will liaise with departmental support staff to obtain the requested information and then convey it to the authorised recipient. **No information will be provided to anyone without formal consent in writing from the University Information Officer.**

Under no circumstances will direct and unrestricted access to an individual user account be provided; only copies of specific information may be provided.

3.3.3. Access to personal correspondence or information

Where practical, the Information & Technology Services Division will endeavour to avoid releasing any correspondence or information that is clearly personal in response to a request for emergency access on business grounds. However, all users must be aware that any personal correspondence or information stored on University servers is not private, and may be unavoidably or unintentionally released in some circumstances. If individuals wish to retain the privacy of their personal communications, they should make arrangements with another provider and should not make use of University ICT facilities for those communications.

In the event of a user's death or prolonged incapacitation, the person recorded in employee or student records as next-of-kin, alternatively the duly appointed Executor of the deceased, may request copies of personal correspondence and other personal information stored on University systems. Should these sources contradict each other, the information in an employee or a student record shall prevail.

3.3.4. Access due to disciplinary proceedings

Where a user is subject to formal disciplinary proceedings in terms of an established University disciplinary policy for both student higher discipline and staff discipline, the presiding officer/proctor, the disciplinary board, the prosecutor/presenter and the accused/accused's representative of those proceedings may request access to information via the University Information Officer or his/her nominee.

3.3.5. Access in response to a court order or other legal process

All third-party requests for access to an individual user's account or information shall be referred to the University's Information Officer or his/her nominee, and the Information Technology Services Division will act in terms of their written advice and in accordance with South African law.

3.4. Processing of requests

Requests for access shall be processed by a senior member of the appropriate I&TS section and they are empowered to release all information approved in writing by the Information Officer and will not be held liable for damages relating to negligence for provision of information but will be held accountable for ensuring confidentiality of any enquiry.

3.5. Record keeping and notification

The Information & Technology Services Division shall keep records of all requests made in terms of this policy in their normal request tracking system. Such records will be made available to the affected user in the event of a dispute arising.

Unless specifically requested and authorised by the Information Officer not to do so, the affected user must be notified when a change is made to their account or emergency access to their information has been granted. Such notification will normally be sent via email and should include the name of the authorised recipient and details of the information that was provided or the change that was made.

3.6. Review procedure

This policy should be reviewed every three years, or when changes in circumstances or legislation dictate.