RHODES UNIVERSITY
Grahamstown • 6140 • South Africa

Policy on Access to ICT Accounts and Information

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	5 December 2013
Policy Approval Pathways (e.g. committee, Senex, Senate, Council)	Director : Information & Technology Services → Information Technology Steering Committee → Senate → ARC → Council
Revision History: Approved Reviews	2016, 2019, 2023
Review Cycle (e.g. every 2/5/7 years etc)	Every 3 Years
Next Review Date	2026

1. POLICY PARTICULARS

1.1. Policy Title	Policy on Access to ICT Accounts and Information
1.2. Policy Statement	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.
1.3. Reason for Policy	This policy is intended to cover all ICT systems — irrespective of where they are housed and who administers them — or whether users may store or transmit personal (i.e. not related to the business of the University) information or communications in the system. This policy is intended to cover access to information stored on a device protected by an ICT authenticated password as well as information held within emails under the @ru.ac.za domain and the University's Google G Suite for Education services. 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 associated with the University's business processes.
1.4. Policy Objective/s	All users of Rhodes University ICT facilities are granted exclusive use of an ICT account. In addition, they are afforded the privilege of limited personal use of email and other ICT facilities. Users who use the Rhodes University account for personal matters do so with an understanding that the mailbox and storage spaces as well as the contents thereof, may from time to time be accessed under certain conditions. Whilst it is not the Rhodes University's intention to do away with these benefits, the 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 and access to information. The policy seeks to ensure that the Protection of Personal Information Act[1] and the Regulation of Interception of Communication Act[2] are adhered to, whilst acknowledging that there are also institutional imperatives that need support.
1.5. People affected by this Policy	All University staff, students and guests
1.5. Who should read this Policy	All University staff, students and guests
1.6. Implementers of this Policy	Information and Technology Services
1.7 Website address/link for this Policy	https://www.ru.ac.za/institutionalplanningunit/qualitypromotion/rhodesuniversitypolicies/policiesa-z/

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

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

2. RELATED DOCUMENTS FORMS AND TOOLS

Relevant Legislation
Rhodes University Statute The Constitution of South Africa Higher Education Act, 1997 South African Protection of Personal Information Act Regulation of Interception of Communication Act
Related Policies
Acceptable Use Policy Web Policy
Related Protocols
Acceptable Use Guidelines Public Acceptable Use Policy (AUP) Network Connection Guidelines Email Guidelines Password Guidelines Copyright and Take-Down at Rhodes University Identity Framework
Forms and Tools
Policy template Access to ICT Accounts & Information Application Form

3. POLICY DEFINITIONS

No	TERM	DEFINITION
3.1	**Email Address**	**Rhodes University email address associated with individual @ru.ac.za**
3.2	**User Account**	**ICT account ie. Log in to 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**

4. PRINCIPLES GOVERNING THIS POLICY

OVERVIEW
Rhodes University strives to carry out the following, as far as is reasonably practicable:
4.1. Only access email and files when absolutely necessary and under strict guidelines
4.2. Ascertain the reason why the access is requested before granting access
4.3. Record and document the access that was authorised as well as files/emails that were accessed during the process
4.4 Limit the use of the policy to reasons that pertain only to business continuity, legal investigations, death or illness of an employee

5. DIRECTIVES FOR IMPLEMENTING THIS POLICY

5.1. Effective date

All users who continue to make use of Rhodes University 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[3]

5.2. Requirement for Access to Information provisioning

The Information & Technology Services Division shall only grant access once approval has been received in writing from the relevant authority.

Approval from the authority may be granted under the following conditions:

- 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) and business processes are being affected or delayed without access to the information;
- 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.

5.3. Detail of circumstances in which access may be granted

Information in mailboxes and Google space is usually only available within 1 month of termination of employment. Under certain circumstances and provided that I&TS is made aware, a mailbox/google space can be retained for as long as required, either for investigation or winding up of a deceased estate. Information on local PC's/laptops is usually only available if the PC/laptop has not been re-issued to another member of staff. In the event that there is a pending disciplinary process the onus is on HR to seize the PC/laptop and secure it with the Director I&TS.

5.3.1 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.

When employees leave employment of the University they are expected to hand over documents and emails relevant to the business continuity to HoDs, either by sharing documents stored in the Google space or forwarding mailbox information to the HoD or delegated colleague. HoDs are responsible for ensuring that all relevant and necessary business continuity information is made available at exit. Access to information via this policy is not intended to be granted for every employee exiting employment of the University.

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. This does not require permission from an Authority and is deemed to be an operational matter.

The "out of office" message should inform new correspondents of the correct alternative contact details for University business and, where possible, indicate the time frame 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. While setting up 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 it may be implemented immediately. As such this should be the default method by which continuity of communication is maintained.

Business continuity is maintained further by use of shared mail boxes that are monitored by more than one individual. Where appropriate, HoDs and Directors may request a shared mailbox is set up to manage communications.

5.3.2 Access to email or other electronic information

Where business requirements dictate, Heads of Departments may apply to the authority for access to information. Upon receipt of authorisation, Information & Technology Services will release relevant and approved information in one or more of the following ways:

- Full access to individual's email in order to search for relevant emails underpinning the business process

[3] https://www.ru.ac.za/aup/

- Full access to a PC or laptop profile, files, server home directory or Google space in order to search for relevant documents underpinning the business process
- Limited controlled release of emails forwarded by I&TS to approved recipient
- Limited controlled release of documents forwarded by I&TS to approved recipient

Authorisation must include but is not restricted to include:

- The name of the person whose information needs to be accessed (the affected user);
- The name of the person to whom access should be granted (the authorised recipient); and
- The specifics of the information that is approved/required (for instance, particular files stored on a file server, email messages matching given filter criteria etc.).
- The specifics around how the mailbox and files can be shared ie. view access only, forwarded access only, full access to mailbox or profile without I&TS intervention

On receipt of a valid authorisation , the Information & Technology Services Division will provision access in one of the following ways, relevant to the request and determined by the Authority

- by making a copy of the requested information available to the authorised recipient,
- by forwarding relevant emails and documents to the approved recipient,
- by allowing full access to the recipient

Where the information is not controlled centrally and 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 authorisation in writing from the relevant Authority.**

5.3.3 Access to personal correspondence or information

Where practical, and except where full access has been approved, the Information & Technology Services Division will endeavour to avoid releasing any correspondence or information that is clearly personal. However, all users must be aware that any personal correspondence or information stored on University servers is not private, and may be 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 or 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. Authorisation for release to the next-of-kin will be in writing from the Authority.

5.3.4 Access due to disciplinary proceedings

Where a user is subject to formal disciplinary proceedings in terms of an established University disciplinary policy for either student higher discipline or 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.

5.3.5 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 Registrar. The Information & Technology Services Division will act in terms of written advice and in accordance with South African law. In certain circumstances, where the Registrar is unavailable, the VC or acting VC may grant approval.

5.4. Processing of requests

Requests for access shall be processed by a senior member of the appropriate I&TS section. They are empowered to release all information approved in writing by the Authority 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.

5.5. 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 Authority in the event of a dispute arising.

6. ROLES AND RESPONSIBILITIES

ROLE	RESPONSIBILITY
ROLE 1 **Authority**	Grants approval for Access as per Appendix
ROLE 2 **I&TS Staff**	Provide approved access and keep record of what is accessed and/or provided
ROLE 3 **Director I&TS**	Ensure the approval form and policy is relevant and up to date, modifying it as circumstances and trends require

7. CONTACTS

Area of Concern	Division/Faculty/Department	Telephone	Email
Breach by I&TS staff	Director I&TS	7456	N.Ripley@ru.ac.za
Breach by applicant	Registrar	8101	A.Moodly@ru.ac.za

8. POLICY REVIEW PROCEDURE

This policy should be reviewed every three years, or when changes in circumstances or legislation dictate. The approval form and list of Authorities should be reviewed as and when new processes and Authority changes are required. Usually this would be on an annual basis
Communication of the review process will be via Toplist

LIST OF APPENDICES

Authority to Approve Access to Information