



**UNIVERSITY OF THE FREE STATE
POLICY**

Document number	IS 1007
Document name	Policy for Acceptable Use of Computer Resources
Document type	Enterprise Policy
Co-ordinating UMC member	Senior Director: ICT Services
Contact	Manager: Information Security and Compliance
Status	v1
Approved by	UMC
Date approved	19 September 2011
Date last amended	8 September 2011
Date for next review	Annually
Related policies/legislation	<ul style="list-style-type: none">• Information Security Policy for Users of Information• Software Licensing and Preservation Policy• Electronic Communications and Transactions Act, 2002

TABLE OF CONTENTS

1. Purpose	3
2. Scope	3
3. Explanatory Terms	3
4. Acceptable Use Policy Compliance	4
5. Procedures, Standards and Guidelines	4
6. Exceptions	4
7. Policy Statements	4

1. Purpose

The University of the Free State (“UFS”) acknowledges the need for employees, students, contractors and authorised guests to have access to the computer network and other electronic resources, specifically to promote educational purposes by increasing accessibility to information, information technology, infrastructure and the common knowledge base of similar institutions, and by improving communication and distance education both within the UFS and globally.

This document will explain the need to regulate the utilisation of the UFS electronic resources. Furthermore, the computer and telecommunications systems belonging to the University and access to this equipment are provided as a tool to support the University with regard to business purposes. University equipment may be used for business, business-related, and employee personal use if the personal use is of an incidental nature and does not interfere with business activities or infringe any of the terms set out in the policy. Usage of and access to corporate resources will be granted as needed. Only management-approved technologies shall be used.

2. Scope

All information users are responsible for meeting the relevant policies and procedures.

3. Explanatory Terms

3.1. “Must”, “will”, “shall”

These terms denote a mandatory requirement that must be adhered to by everyone. The only allowable deviation is through a formal exception waiver.

3.2. “Should”

This term denotes a highly suggested, but not mandatory, recommendation.

3.3. “May”, “can”

These terms denote non-mandatory recommendations.

3.4. “UFS”

Refers to the “University of the Free State”.

3.5. “University”

Refers to the “University of the Free State”.

3.6. “Users”

Refers to any person or entity requiring access to the UFS computer network or information.

3.7. “Information”

Refers to any information whether in written/printed, verbal or electronic form.

3.8. “warez”

Refers primarily to copyrighted works distributed without fees or royalties, and may be traded, in general violation of copyright law.

4. Acceptable Use Policy Compliance

- 4.1. Failure to comply with this policy or other relevant policies may result in the termination of a user's privileges with regard to the use of systems or services and/or disciplinary action. Utilisation of the UFS computer network constitutes a privilege of the user, and not an established right.
- 4.2. All information users are required to indicate their understanding and acceptance of this policy when accessing the system. By accepting this policy the users also accept the following ICT Services Policies:
 - a. Information Security Policy for Users of Information
 - b. Software Licensing and Preservation Policy

5. Procedures, Standards and Guidelines

- 5.1. Procedures, standards and guidelines will be published as attachments to this policy to assist the relevant users to meet their requirements.

6. Exceptions

- 6.1. Exceptions to any policy statement must be approved by the Senior Director: ICT Services which may require higher-level management authorisation. All exceptions to policies shall be formally recorded, tracked and reviewed by ICT Services.

7. Policy Statements

- 7.1.1. Unless stated otherwise, any new features, augmentations, enhancements or services to the computer network, shall be subject to the provisions of this document.
- 7.1.2. The user understands that facilities are provided by the computer network on an "as is" and "as available" basis. The UFS therefore does not accept responsibility for the availability or timeliness, due to defectiveness or otherwise, of the computer network or any other service provided in this regard.
- 7.1.3. The University reserves the right to monitor and analyse any information that is created, stored, sent or received on University computers and through the University's network if it has reasonable grounds to believe that such creation, storage or transmission of information may be harmful to the interests of the University.
- 7.1.4. All information, data, communication and files on the computer network can be accessed by the UFS, which access the user consents to.
- 7.1.5. Only registered staff, students and authorised third parties are allowed to use the computer network.
- 7.1.6. Users may not use the computer network for any illegal activities of any nature, or activities that do not comply with the policies, rules and regulations of the UFS.
- 7.1.7. Users must not upload, download, email or use any content that is fraudulent, illegal, harmful, defamatory, sexually explicit, abusive or invasive of privacy. Illegal sites include, but are not limited to, warez and hacker sites, and media repositories hosting copyright material.

- 7.1.8. Users shall not violate the rights of any person or company protected by copyright, trade secret rights, patent rights or other intellectual property rights, or similar laws or regulations.
- 7.1.9. Users shall not transmit any information that is damaging to the University or other users.
- 7.1.10. The user should always abide by generally accepted rules of computer network etiquette. For example always be polite.
- 7.1.11. Users must not reveal any personal or confidential information of staff or students to the public e.g. personal addresses, identity numbers, personal telephone numbers, etc. unless authorised to do so.
- 7.1.12. The user must not remove any computer hardware from the premises where it is installed without permission.
- 7.1.13. Users must refrain from any conduct that could result in disruptions, negative influence, obstructions or alterations of the computer network, system, hardware or software.
- 7.1.14. The UFS will make reasonable efforts to maintain the integrity and effective operation of its email systems. Based on the nature and technology of email communication, the UFS cannot assure privacy with regard to individual use of the UFS's email resources nor the confidentiality of particular messages that may be created, transmitted, received or stored thereby.
- 7.1.15. The UFS cannot guarantee the delivery of email messages to systems which are not under the UFS control.
- 7.1.16. All users should regularly check their email.
- 7.1.17. All users should, on a frequent basis, delete email that is no longer required in order to avoid taking up large amounts of data storage capacity.
- 7.1.18. Users must take care to verify the accuracy of the addressee's name and other recipient information.
- 7.1.19. Users must not send offensive email messages.
- 7.1.20. Users must not commit any form of harassment via email, whether through language, frequency or the size of messages.
- 7.1.21. Users may not pass on electronic chain letters or send unsolicited email messages, including junk mail or other advertising material, to individuals who did not specifically request such material.
- 7.1.22. Users are responsible for the backup of data on the UFS computers under their control.
- 7.1.23. By accepting this policy, the user waives all claims against the University resulting from any damage or loss of data or information resulting from computer viruses or any other computer code, files, programmes or defects, obtained from or transmitted via the computer network.