

General Policy Governing the Appropriate Use of Computer Resources

Table of Content

- [Introduction.](#)
- [Use of Resources.](#)
- [When Inappropriate Use of Computer Resources Occurs](#)
- [Information on Applicable Laws and Statutes](#)

(November 2002)

Introduction.

The University's computer and information network is a continually growing and changing resource that supports hundreds, soon to be thousands of users and systems. These resources are vital for the fulfillment of the academic, research and business needs of the University community. Their use is provided as a privilege. In order to ensure a reasonable and dependable level of service, it is essential that each individual faculty member, staff member, and student exercises responsible, ethical behavior when using these resources. Misuse by even a few individuals has the potential to disrupt University business, and, even worse, the legitimate academic and research work of faculty and students.

This policy outlines the application of the principles that govern our academic community in the appropriate use of University computer and information network resources. Because it is impossible to anticipate all the ways in which individuals may misuse these resources, this policy focuses on a few general rules and the principles behind them.

This policy applies to the entire user community (e.g., all faculty, staff, students, alumni and retirees) of the University and to the use of any and all University owned or managed computer-related equipment, computer systems, and interconnecting networks, as well as all information contained therein.

Use of Resources.

All users are expected to utilize University resources in a responsible manner consistent with University policies and the guidelines and operating policies that Academic Council may issue from time to time. You are expected to take reasonable measures to ensure that traffic entering the Jacobs University network from other networks conforms to this policy. Conversely, you are expected to take similar measures to avoid situations where traffic from the Jacobs University network violates the policies of connecting networks.

The unauthorized use of resources is prohibited and, in many cases, may be violations of the law. We are guided by the law in noting that unauthorized use includes, but is not limited to the following types of activities.

1. Harassment or threats to specific individuals, or a class of individuals:

- Transmitting unsolicited information that contains obscene, indecent, lewd or lascivious material or other material which explicitly or implicitly refers to sexual conduct;
- Using e-mail or newsgroups to threaten or stalk someone;
- Transmitting unsolicited information that contains profane language or panders to bigotry, sexism, or other forms of prohibited discrimination.

2. Interference or impairment to the activities of others:

- Creating, modifying, executing or retransmitting any computer program or instructions intended to: (1) obscure the true identity of the sender of electronic mail or electronic messages, such as the forgery of electronic mail or the alteration of system or user data used to identify the sender of electronic e-mail; (2) bypass, subvert, or otherwise render ineffective the security or access control measures on any network or computer system without the permission of the owner; or (3) examine or collect data from the network (e.g., a "network sniffer" program).
- Authorizing another person or organization to use your computer accounts or Jacobs University network resources. You are responsible for all use of your accounts. You must take all reasonable precautions, including password maintenance and file protection measures, to prevent use of your account by unauthorized persons. You must not share your password with anyone else or provide access to Jacobs University network resources to unauthorized persons.
- Communicating or using any password, personal identification number, credit card number or other personal or financial information without the permission of its owner.

3. Unauthorized access and use of the resources of others:

- Use of University resources to gain unauthorized access to resources of this or other institutions, organizations, or individuals.
- Use of false or misleading information for the purpose of obtaining access to unauthorized resources.
- Accessing, altering, copying, moving, or removing information, proprietary software or other files (including programs, libraries, data and electronic mail) from any network system or files of other users without prior authorization (e.g., use of a "network sniffer" program).
- Making unauthorized copies of copyrighted materials. You should assume all software, graphic images, music, and the like are copyrighted. Copying or downloading copyrighted materials without the authorization of the copyright owner is against the law, and may result in civil and criminal penalties, including fines and imprisonment.

4. Damage or impairment of University resources:

- Use of any resource irresponsibly or in a manner that adversely affects the work of others. This includes intentionally, recklessly or negligently (1) damaging any system (e.g., by the introduction of any so-called "virus", "worm", or "trojan-horse" program), (2) damaging or violating the privacy of information not belonging to you, or (3) misusing or allowing misuse of system resources.
- Use of University resources for non-University related activities that unduly increase network load (e.g., chain mail, network games and spamming).

5. Unauthorized commercial activities:

- Using University resources for one's own commercial gain, or for other commercial purposes not officially approved by the University, including web ads.
- Using University resources to operate or support a non-University related business.
- Use of University resources in a manner inconsistent with the University's contractual obligations to suppliers of those resources or with any published University policy.

6. Violation of the laws of the City of Bremen or of the Federal Republic of Germany:

- Pirating software, music and images.
- Effecting or receiving unauthorized electronic transfer of funds.
- Disseminating child pornography or other obscene material.
- Violating any laws or participating in the commission or furtherance of any crime or other unlawful or improper purpose.

When Inappropriate Use of Computer Resources Occurs

The use of University resources is a privilege. The resources have always been, and will remain, the property of the University.

It is your responsibility promptly to report any violation of this policy or other University policy or guideline. In addition, you must report any information relating to a flaw in or bypass of resource security to irc-director@jacobs-university.de.

Reports of unauthorized use or misuse of the resources will be investigated pursuant to standard University procedures. All illegal activities will be reported to local or national authorities, as appropriate, for investigation and prosecution.

While the University desires to maintain user privacy and to avoid the unnecessary interruption of user activities, the University reserves the right to investigate unauthorized or improper use of University resources, which may include, within the limits permitted by law, the inspection of data stored or transmitted on the network. In the event that use is determined to be contrary to University policy or applicable law, appropriate measures will be taken. These measures may include, but are not limited to, permanent or temporary suspension of user privileges, deletion of files, disconnection from the Jacobs University network, referral to student or administrative disciplinary processes, and cooperating with the appropriate law enforcement officials and government agencies.

The University is not responsible for information, including photographic or video images and musical recordings, published on or accessible through personal web pages, including personal home pages. The University does not monitor the contents of these personal web pages. The individual or group creating or maintaining personal web pages is solely responsible for the content of the web page and may be held civilly and criminally liable for the materials posted on the web site.

Information on Applicable Laws and Statutes

The examples of unauthorized use set forth above are not meant to be exhaustive. Whenever you are in doubt regarding an issue of questionable use, it is in your best interest to resolve the issue before pursuing any questionable use of University resources. All users of the University computer and information resources are expected to be familiar with and to abide by University codes and policies, as well as all laws relating to electronic media, copyrights, privacy, and security.

Responsible Parties: Academic Affairs, Information Resource Center