University of Dubuque
Technology
Acceptable Use Policy

The Communications section of this policy applies to the University telephone and Voice Messaging System, as well as the computer network system.

ACCESS

1. Access to and use of the computer systems and networks is limited to the faculty, staff, and students of the University of Dubuque. Others may be granted access for good cause at the discretion of the University.

2. Acceptable use of hardware and software includes study, research, teaching, and administrative work. Incidental personal use is not permitted without express permission of a University Vice President or President.

3. All students will be granted full access to select software applications, the Internet and remote access capabilities.

4. All students, both full and part-time are provided with email accounts as long as registered at the University of Dubuque.

5. Attempts to gain access (log in) to another person's account, or attempts to read someone else's mail or files, unless the owner publishes the file on the Internet, is prohibited. Sharing an account with another person is prohibited. Passwords are to be confidential.

6. The University of Dubuque Computer System is capable of tracking "footprints" of all users. If a user disputes allegations of inappropriate use, the Office of Technology will make any relevant tracking documentation available as evidence to administrative and/or investigative authorities.

7. Students will be provided with an initial amount of 250 sheets of paper each semester for printing in the computer labs. Amounts used beyond that will be charged to the students at a rate that will cover the costs of paper and ink. Balance information is available anytime the student logs into the computer system.

8. Students living in University housing may connect to the Internet via the University network. Students must perform an initial system security certification before this access is granted. Students may obtain information about this procedure from the Office of Technology HelpDesk.

9. Network connections for students living in University housing will be deactivated if any other computer or device is plugged into that port, or if there is any unusual traffic or security issues. The student may need to bring in the desktop or laptop for recertification if a virus or other traffic generating activity is suspected.

10. Residential students may elect to use an alternative Internet Service Provider and bear the responsibility for the associated costs.

DATA

11. The University will take reasonable efforts to back up all data and files saved on the University servers. The University assumes no liability for data lost or destroyed.

12. The University of Dubuque does not guarantee computer systems to be safe from system errors or operator failures.

13. The Office of Technology will back up and protect all files and databases within the Administrative Software Application and Academic Servers. Files saved to the server by employees will also be backed up.

14. The Office of Technology may inspect or remove personal files as needed to diagnose problems and maintain the system in good working order. Reasonable effort will be taken to notify the owner prior to their removal.

15. Unauthorized use, duplication, or transmission of copyrighted material (including software) is prohibited.

COMMUNICATION

16. The University computer and telephone system may not be used for illegal activities, nor may it be used to threaten or harass others. The system may not be used to send chain letters, or to post solicitations or advertisements. The University is not liable for harassment, threats, or impositions resulting from unacceptable use of the computer network. Individuals who believe they are being harassed are to process the incident through the Human Resources Office or the Dean of Students.

17. Email should be used with the understanding that electronic communication is never really private. The UD email system is for UD related activities. Employees and students are encouraged to use external email accounts for personal or non-professional communication.

18. Mass email, or voice mail, (aka spamming) from any student or employee to the entire University of Dubuque community (students, employees, or both) must first be approved by the Vice President over the requesting Office. Periodic messages

may arrive via mass email, or voice mail, from the Office of Technology that relates to the functionality of the network.

19. The University of Dubuque Computer System is not a public forum and cannot be used for indiscriminate use. Use of the campus network (and all electronic components under the auspice of the Office of Technology, including voice mail) must be consistent with the Mission, Values, and Vision of the University. Any activity that does not reflect the University mission will be considered a violation of the *Acceptable Use Policy* and can result in restricted or eliminated access to the computer system. Examples of activities that are not permitted are:

    A. **Commercial Use** – No student or employee can use the University of Dubuque Computer System, or other equipment to offer or provide products or services unless approved by the University Administrative Cabinet. Purchasing products and services via the campus system is at risk of the user. The University of Dubuque is not responsible for financial obligations from unauthorized use of the system by anyone.

    B. **Political Lobbying** – Although everyone is allowed to express opinions and analyze measures regarding legislative matters, using the University of Dubuque Computer System, or other equipment to engage in fund raising or other political lobbying must first be approved by a Vice President, or the University Administrative Cabinet. It is acceptable to use the Computer System to communicate opinions to elected officials via the Internet.

    C. **Inappropriate Use**
        1. Criminal speech and/or speech or use, in the course of committing a crime—e.g., threats to persons, instructions on breaking into computer systems; child pornography; drug dealing; gang activity, etc.
        2. Speech, or use, that is inappropriate:
            a. Inappropriate language, video, or graphics – obscene, profane, lewd, vulgar, disrespectful, threatening, or inflammatory language; harassment; personal attacks, including prejudicial or discriminatory attacks; or false or defamatory material about a person or organization.
            b. Dangerous information – information that if acted upon, could cause damage or present a danger of educational or business operation disruption.
            c. Violations of privacy – revealing personal information about others.
            d. Abuse of resources – chain letters, "spamming," jokes or other such mail. (Spamming is sending an annoying or unnecessary message to a large number of people)

e. Sending messages for the purpose of selling goods or soliciting responses for goods or services. (This excludes sales announcements by administrative/academic departments and University related groups.)
f. Copyright infringement or plagiarism.
g. Pornographic material – electronic and print material which, by their design, are salacious, lascivious, lecherous, lustful, or demeaning to humans in their portrayal of aberrant sexual behavior.
h. It is unacceptable to distribute a computer virus or engage in any procedure that interferes with the normal operation and delivery of services over the network.

HARDWARE & SOFTWARE

20. Users of the UD network should conserve network resources. Activities that result in excessive use of network bandwidth, server storage, or system time are restricted (this specifically includes the downloading and storing of video or music files along with the storage of personal pictures).
21. Only legal, licensed software applications may reside on or be transferred over the UD network. Reproduction of such software or its related documentation is forbidden unless explicitly authorized by the software developer. All University faculty, students and employees shall use computer software only in accordance with license agreements and Mission, regardless of the ownership of the license. All shareware programs must be registered in accordance with their license and use provision.
22. Hacking--unauthorized modification of operating systems, application software, or network software on any system attached to the UD network is strictly forbidden. This includes any activities that result in a denial of service.
23. Tampering with terminals, microcomputers, printers or any other associated University-owned equipment is strictly forbidden. Removal of computer equipment, disks, paper or documentation from a computing facility is also unacceptable.

CONSEQUENCES

24. Violation of the above policy and any other inappropriate use of the computer system, Internet, telephone system, or any systems under the purview of the Office of Technology will result in the suspension of the privilege of use. Suspension of use will be immediate, with the duration of the suspension then determined by the University judicial processes. The System Administrator may close a suspect account at any time, as required, and will, in the case of a University student, then notify the Dean of Student Life and the Vice President of Academic Affairs; and in the case of a seminary student, then notify the Dean of the Seminary. The administration, faculty, and staff may request the Office of Technology to deny, revoke or suspend specific user accounts. Any person

identified as a security risk may also be denied access. If an employee of the University is in violation of the policy as previously described, they will be subject to discipline in accordance with University Policy.

25. Any person, or persons, altering or attempting to alter without authorization, the cabling or component of any computer system, will be restricted from access and/or subject to criminal prosecution, if appropriate.

26. The Office of Technology will investigate complaints it receives from computer users at this and other institutions when those complaints pertain to inappropriate use, including messages that are sent by University of Dubuque students.

27. A student suspected of violating the *Acceptable Use Policy* will be notified via campus email, mail, telephone, or appointment with the Office of Technology. An office of a Vice President or President will notify University employees suspected of violation. It should be understood that the above policies do not preclude prosecution in cases of criminal misconduct under current laws and regulations of the city, the state, and Federal Government.