

UND Student Acceptable Use of IT Resources Policy

Table of contents

- I. Reason for the Policy
- II. Applicability of the Policy
- III. Policy Statement
- IV. Policy Enforcement
- V. Definitions
- VI. Related Documents / Policies
- VII. Effective Dates
- VIII. Contacts

I. Reason for the Policy

The computing resources at the University of North Dakota support the academic, research and administrative activities of the University and the use of these resources is a privilege extended to members of the UND community. This policy outlines the responsible and appropriate use by students of these computing and network resources (IT resources). This policy is meant to complement the North Dakota University System (NDUS) 1901.2 Computer and Network Usage Procedure, and students should refer to 1901.2 as the definitive source for the appropriate use of computer and network resources on the UND campus.

II. Applicability of the Policy

This policy applies to all students, undergraduate and graduate, part-time and full-time, and distance degree students. This policy applies to the use of all IT Systems, including systems, networks, and facilities administered by ITSS, as well as those administered by individual colleges, departments, and other University-based entities. This policy governs the use of university IT resources, even when they are accessed on a privately owned computer that is not managed or maintained by the University.

III. Policy Statement

When using the IT resources at UND, students are expected to act in a responsible manner just as they would when using the physical resources at UND. This includes obeying the law, respecting others' rights to privacy, and respecting others' ability to make use of the resources. This policy sets forth the university's expectations regarding students' use of IT resources, outlines the responsibilities of all students, and provides some examples of inappropriate use. While there are specifics provided in this policy, it is not meant to be an exhaustive coverage of all acceptable use scenarios. Students should refer to NDUS Procedure 1901.2 and the UND Code of Student Life for further guidance.

Student Responsibilities

Comply with the law and University policy. A student's use of IT resources must not violate any federal, state, or local law, including, but not limited to, laws that prohibit threats, violence, obscenity, slander, and child pornography and those that protect copyrights, licenses, trademarks, and intellectual property rights. Student's use of IT resources must also be in compliance with all NDUS and UND policies, regulations, procedures, and rules.

Respect the rights and privacy of others. Students who use the University's IT resources are expected to respect the privacy and personal rights of others. Individuals are prohibited from looking at, copying, altering, or destroying another individual's electronic information without explicit permission. Students should also be respectful when using computing systems to communicate with others.

Recognize and honor the intellectual property rights of others. Users should not use, copy, store, or redistribute copyrighted material (i.e., digital music, movies, images, or electronic publications) or violate copyright or patent laws concerning computer software licenses or documentation. Generally, materials owned by others cannot be used without the owner's written permission. Students should also be careful of the unauthorized use of trademarks.

Refrain from unacceptable behavior. Students should refrain from any and all activities that are intended to damage IT resources or compromise the integrity of the network, computer systems, or data. This includes, but is not limited to, all items in the Inappropriate Use section of this policy.

Maintain the security of personal computers. Students are responsible for maintaining the security of their personal computers in order to ensure the integrity of the campus network. Anti-virus software should be installed and this and other installed software (especially the operating system) should be kept up to date with regard to security patches and signature files. Personal firewalls should be installed or enabled (such as Microsoft Windows's firewall) and configured to allow only the needed programs and services.

Inappropriate Use

Unlawful communications. Students may not use the UND computers or network to send illegal communications including, but not limited to, threats of violence, harassment, obscenity, and child pornography. Types of communications include emails, newsgroup postings, downloads, websites, etc.

Commercial or political use. Computing and network resources may not be used for private business, compensated outside work, commercial activities, advertising on behalf of non-UND organizations, or political purposes (except where such activities are permitted or authorized under applicable UND or NDUS policies). Students also are prohibited from reselling any UND IT resource.

Forging or concealing identity. Students must not attempt to conceal their identity when using IT resources, except when the option of anonymous access is explicitly authorized. Students are also prohibited from impersonating others or using a false identity.

Use of resources without authorization. Students must not attempt to access or acquire data on restricted portions of the network, network applications, databases or individual computer systems without appropriate authorization by the system owner or administrator. Students must not compromise the privacy or security of information by accessing or sharing data in which they are not authorized.

Interference with the operation of computer systems or network. Deliberate attempts to degrade or interfere with the performance or integrity of any IT resource or to deprive authorized individuals access to any resource are prohibited. Some examples include

propagating worms or viruses, denial of service attacks, or broadcasting, spamming, or mass mailing messages to large numbers of individuals.

Use by others of personal accounts. Students are given individual user accounts and passwords to provide access to computer and networking resources. These accounts and passwords must not be shared with others. Likewise, students should never use the account or password of another individual to access a computer or network resource.

Use of tools to assess security or attack computer systems or networks. Students must not download and/or use tools that are used to assess the security or attack computer systems or networks, or used to monitor communications (i.e., password crackers, vulnerability scanners, network sniffers, port scanners, etc.). Students should not attempt to circumvent or subvert any system's security measures or data protection schemes, or exploit loopholes to gain access to systems or data.

Attempting to alter a UND IT resource. Students must not alter or attempt to alter the hardware or software configuration of any UND IT resource without the explicit permission from the system or network owner or administrator. Students are also prohibited from physically damaging an IT resource, whether intentionally or through negligence.

Academic Dishonesty. Use of UND IT resources to commit acts of academic dishonesty will be handled through existing campus procedures as outlined in the UND Code of Student Life.

Respecting the policies of individual departments and colleges. Students must respect and follow the policies and procedures regarding the use of IT resources as required by the student's home college or department, when not in conflict with University or N D U S policies and procedures.

IV. Policy Enforcement

Violations of this policy should be reported to abuse@und.edu or reported to the UND Information Technology Security Officer (ITSO) (see the Contacts section of this policy).

Disciplinary Sanctions

Students who violate this policy will be subject to sanctions administered by the appropriate college, department, system owner, or network owner in conjunction with the UND ITSO. This may include warnings, immediate loss of network or system access privileges, or the temporary or permanent modification of those privileges.

Repeated or severe violations of this policy will result in the student being referred to the Dean of Students Office to hear the case as outlined in [Section 2-5 of the Code of Student Life](#). If warranted, the Dean of Students Office may administer disciplinary sanctions as outlined in [Section 2-4 of the Code of Student Life](#). The basic sanctions are Written Reprimand, Warning Probation, Conduct Probation, Suspension, and Indefinite Suspension.

Any offense which violates local, state, or federal laws may result in the immediate loss of all computing and networking resource privileges and will be referred to appropriate law enforcement authorities.

Appeals

Notice of violations and appeals of decisions will follow the appeals process of the college or department administering the sanction, and for those violators referred to the Dean of Students Office, the Basic Appeal Procedures will be followed as outlined in [Section 2-8 of the Code of Student Life](#).

V. Definitions

IT Resource	A computing asset provided by the University to further its mission. Examples include, but are not limited to, network bandwidth, networking equipment, workstations, computer systems, data, databases, servers, and printers.
Intellectual Property	Property that derives from the work of the mind or intellect, specifically, an idea, invention, trade secret, process, program, data, formula, patent, copyright, or trademark. As it relates to this policy, it typically refers to digital music, movies, video, images, electronic publications, and software.
Denial of Service Attack	An attack on a computer system or network that causes a loss of service to users. Typically, this type of attack causes the loss of network connectivity and services by consuming the bandwidth of the victim network or overloading the computational resources of the victim system.
Spamming	Sending nearly identical and unsolicited bulk and/or commercial messages to hundreds, thousands, or even millions of users.

VI. Related Documents / Policies

NDUS Procedure 1901.2 Computer and Network Usage
<http://www.ndus.edu/policies/ndus-policies/subpolicy.asp?ref=2551>
UND Code of Student Life
<http://sos.und.edu/csl/>
ResNET Acceptable Use Policy
<http://www.resnet.und.edu/use.html>

VII. Effective Dates

Last Edited: Aug 10, 2006
Approved: Jan 7, 2007
Next Review Date: Jan 7, 2009

VIII. Contacts

Subject	Contact	Phone
Information Security	UND IT Security Officer (ITSO)	777-3587
Information Technology Services	UND Chief Information Officer (CIO)	777-3171
Reporting a violation	abuse@und.edu	777-2222