# EMPLOYEE ACCEPTABLE USE GUIDELINES for Electronic Communication Resources

NDSU

## INTRODUCTION AND PURPOSE

Computers and electronic communication devices are vital tools in accomplishing the NDSU mission. The university invests in and supports a variety of information technology equipment and services. Most employees and students depend on these resources daily to accomplish their work.

NDSU faculty and staff need to be good stewards to ensure our limited IT resources are used effectively. In accordance with the policies of the State Board of Higher Education and NDSU acceptable use policies (see policies section), the university has a responsibility to ensure that IT resources are used appropriately and legally.

Please be aware that except where precluded by law, the university has the right to measure and monitor use of information technology resources. This includes, but is not limited to, storing, accessing and reviewing information received or sent through email or over the Internet. Although individual Internet usage is not routinely monitored, such monitoring is possible when requested by an appropriate official. The university will cooperate with law enforcement investigations. In addition, Internet sites deemed by the university to be unrelated or inconsistent with the university's mission may be blocked from NDSU's network.

If you have a question about appropriate use of information technology resources, be sure to discuss it with your supervisor. The Chief IT Security Officer also is available to answer questions and help supervisors facilitate a safe and productive work environment.

## APPROPRIATE USE OF NDSU ELECTRONIC COMMUNICATION RESOURCES

ACCEPTABLE USES INCLUDE

- Accessing material/information related to your job functions
- Conducting institutionally sanctioned research or outreach activities with internal or external constituencies
- Administering the business of the university
- Incidental personal use as determined by your college or department if it:
    - Does not interfere with your work performance
    - Is of nominal cost or value
    - Does not create the appearance of wrongdoing
    - Is not for political or personal commercial use
    - Is reasonable in time, duration and frequency
    - Makes minimal use of resources

EXAMPLES OF UNACCEPTABLE USE

- Engaging in any type of online harassment activity or similar inappropriate behavior
- Accessing or distributing sexually explicit, offensive or erotic material
- Probing or hacking
- Using peer-to-peer or streaming technologies for transfer of copyright-infringed materials and/or non-academic purposes
- Pirating software or data
- Knowingly distributing viruses or bypassing university virus protection
- Manipulating network addresses of electronic equipment

REMEMBER: Misuse can result in permanent loss of privileges and network access.

## POLICIES

NORTH DAKOTA STATE UNIVERSITY

NDSU Policy 158 - Acceptable Use of Electronic Communication Devices (www.ndsu.edu/policy)
NDSU Policy 158.1 - Email as an Official Communication Method for Employees (www.ndsu.edu/policy)
NDSU Procedural Guidelines (www.ndsu.edu/its/au)
NDSU Student Code of Behavior, section 4.7 (www.ndsu.edu/vpsa)

NORTH DAKOTA UNIVERSITY SYSTEM

NDUS policy 1901.2 - www.ndsu.edu/its/ndus-1901-2

- Section 1: Definitions - Authorized Use
- Section 3: Freedom From Harassment and Undesired Information
- Section 4.2: Imposition of Sanctions
- Section 4.3: System Administration Access
- Section 4.4: Monitoring of Usage, Inspection of Electronic Information

## PROCEDURAL GUIDELINES

NDSU has established procedural guidelines for investigating violations of acceptable use. The supervisor or administrator in the unit can often address misuse where it occurs. On some occasions, the misuse may represent a major violation of Acceptable Use Policies. For complete guidelines see: www.ndsu.edu/its/security

Initial discovery of a potential Acceptable Use Policy violation can result from a number of events, which include but are not limited to:

- Bandwidth and network monitoring
- Complaint by a supervisor or others
- Inadvertent discovery during routine service or maintenance
- Federal copyright law complaint (includes unauthorized distribution of music, movies and software)
- Creation or distribution of spam or other network abuse
- Law enforcement query or subpoena
- Open records request

## NOTIFICATION

The NDSU Chief IT Security Officer will be notified immediately to assist in the investigation of any impending or alleged violation. The appropriate dean and/or director(s) will be notified so that there can be an initial meeting established with the Appropriate Use Review Committee* to assess the situation and agree on an appropriate course of action. The alleged violator will not be notified until this discussion has taken place and a decision to notify the alleged violator has been made.

* Members of the Appropriate Use Review Committee include the director of human resources, vice president for equity and diversity, the university attorney, and the vice provost and Chief Information Officer or their designees.

## ACTION

A course of action will be determined that may include monitoring and/or seizure and examination of equipment and related IT items (e.g., computers, communication devices, hardware, software, portable media). Occasionally, emergency action might be necessary, and the NDSU Chief IT Security Officer may not have an opportunity to contact the appropriate officials before an action is taken. If child pornography or other criminal violations are suspected, appropriate law enforcement will be notified.

## OUTCOME

Outcomes of the investigation could include the following determinations:

- No violation
- Violation of law or policy and/or
- Possible criminal violations

If a violation is found, sanctions could include, but are not limited to:

- Verbal caution, letter of warning, loss of computer and/or network access
- Referral to the Employee Assistance Program
- Referral for training and education
- Letter of reprimand
- Suspension with or without pay
- Termination of employment

Any criminal process is separate, but also can be considered when deciding on appropriate sanctions. The employee may use the normal employment appeals processes for any sanctions imposed.

## FOR MORE INFORMATION

NDSU Chief IT Security Officer
Information Technology Division
(701) 231-5870
www.ndsu.edu/its/security

This publication will be made available in other formats upon request at (701) 231-5870.



Rev. 070114