NORTH DAKOTA
STATE BOARD OF HIGHER EDUCATION
Policy Manual

Policy: 1202.1 Acceptable Use of Information Technology Resources Policy
Effective: May 23, 2018

---

1. Policy

Computing and networking resources are provided to support the academic, research, instructional, outreach, and administrative objectives of the North Dakota University System (NDUS) and its Institutions. These resources are extended to accomplish tasks related to the individual's status with the NDUS or its Institutions.

When using NDUS Information Technology (IT) resources, individuals are expected to act in a responsible manner just as they would when using the physical resources of the NDUS. This includes adhering to all laws and regulations, respecting others' rights to privacy, and respecting others' ability to make use of the resources. This policy sets forth NDUS' expectations regarding use of IT resources, outlines the user's responsibilities, and provides some examples of inappropriate use. While there are specifics provided in this policy, it is not meant to be an exhaustive outline of all acceptable use scenarios.

This policy applies to (1) current faculty, staff, and students of the NDUS ; (2) individuals connecting to a public information service provided by the NDUS; and (3) other individuals or organizations specifically authorized by the NDUS or an NDUS Institution to access or use NDUS IT resources.

2. Purpose of Policy

The IT resources of the NDUS support the academic, research, instructional, outreach, and administrative activities of the University System and the use of these resources is a privilege extended to members of the NDUS community. This policy outlines the responsible and appropriate use of these IT resources.

3. Definitions

a. Data - Information collected, created, maintained, transmitted, or stored by or for the NDUS and its Institutions to conduct business. It includes, but is not limited to, information in electronic, paper, video, and audio formats.

b. Institution - Any of the eleven colleges or universities within the NDUS.

c. Confidentiality - Access to information is limited to those persons authorized to use the information.

d. Integrity - Maintaining and assuring the accuracy and consistency of data over its entire life-cycle.

e. Availability - The systems used to store information, the controls used to protect information, and the communications channels used to access information must be functioning correctly.

f. Information Technology (IT) Resources - All NDUS or Institution owned, operated, leased, or contracted systems and services including, but not limited to, computers, databases, storage, servers, networks, input/output connecting devices, telecommunications infrastructure and equipment, software, and applications.

4. Policy Details

a. Responsibilities

i. **Comply with the law and NDUS policy.** An individual'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. An individual's use of IT resources must also be in compliance with all NDUS policies, regulations, procedures, and standards.

ii. **Respect the rights and privacy of others**. Individuals must be respectful of others within the NDUS and campus communities; value the right of privacy of other members; recognize and respect the diversity of the campus community; and, comply with NDUS and Institution policies, state and federal laws, industry regulations, and contracts regarding the use of information that is the property of others.

iii. **Abide by all applicable copyright laws and observe intellectual property rights.** Individuals are prohibited from using, copying, storing, or redistributing copyrighted material (i.e., digital music, movies, images, or electronic publications) or otherwise violating copyright or patent laws concerning computer software licenses or documentation. Generally, materials owned by others cannot be used without the owner's written permission. Individuals should also be careful of the unauthorized use of trademarks. Certain uses of such marks on websites or in domain names can constitute trademark infringement. Unauthorized use of an Institution's name in these situations can also constitute trademark infringement.

iv. **Refrain from unacceptable behavior.** Individuals should refrain from any and all activities that damage IT resources or compromise the integrity of the network, computer systems, or data. This includes, but is not limited to, all items outlined in Section 2: Inappropriate Use.

b. Inappropriate Use

i. **Unlawful or inappropriate communications.** Individuals shall not:

1. Impersonate another individual with intent to deceive or cause harm; or
2. Send illegal or inappropriate communications including, but not limited to, threats of violence, harassment, obscenity, or child pornography.

ii. **Commercial or political use.** Use of IT resources for political purposes, private gain, private business purposes, or other personal use not related to job duties or academic pursuits is prohibited, unless such use is expressly authorized under NDUS or Institutional procedures, or, when not expressly authorized, such use is incidental to job duties or limited in time and scope, and such use does not: (1) interfere with NDUS or Institutional operation of IT resources ; (2) create additional costs; or (3) interfere with the user's obligations to the NDUS or Institution. Refer to N.D.C.C 16.1-10-02.

iii. **Use of resources without authorization.** Individuals must not attempt to access or acquire data without appropriate authorization by the system owner or administrator. Individuals must not compromise the privacy or security of information by accessing or sharing data that they are not authorized to access or share.

iv. **Interference with the operation of computer systems or networks.** Deliberate attempts to degrade or interfere with the performance or integrity of any IT resource are prohibited. Users also cannot prevent authorized individuals from accessing any resource.

v. **Sharing of credentials.** Accounts, passwords, and other types of authorization assigned to individuals must not be shared with others. Users are responsible for any use or misuse of their authentication information and authorized services.

vi. **Use of tools to assess security or attack computer systems or networks.** Unless authorized by the NDUS or Institution CIO, or NDUS or Institution IT Security personnel, individuals must not download and/or use tools that are used to assess the security of IT resources, or that are used to monitor communications (e.g., vulnerability scanners, network sniffers, port scanners, etc.). Individuals may not attempt to circumvent or subvert any system's security measures or data protection schemes, or exploit vulnerabilities to gain access to IT resources.

vii. **Attempting to alter an NDUS IT resource.** Individuals who do not have the appropriate authorization must not alter or attempt to alter the hardware or software configuration of any NDUS or Institution IT resource. Individuals are prohibited from physically damaging any IT resource, whether intentionally or through negligence, unless specified to do so through appropriate data management standards and device de-commissioning.

viii. **Harassment.** Individuals may not use NDUS or Institution IT resources to harass any other person or group. Prohibited activities include: (1) harassing, terrifying, terrorizing, intimidating, threatening, or offending another individual by conveying obscene language, pictures, or other inappropriate materials or threats of bodily harm, injury, or death to the recipient or the recipient's immediate family; (2) using an IT resource to contact another person repeatedly regarding a matter when an individual does not have a legal right or Institutional purpose to communicate, once the recipient has provided reasonable notice that he or she desires such communication to cease; (3) using an IT resource to disrupt or damage the academic, research, administrative, or related pursuits of another individual or group; or (4) using an IT resource to invade or threaten the privacy, academic or otherwise, of another.

ix. **Export Control.** Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate Institutional contact should be consulted prior to export of any material that is in question.

x. **Encryption of Data.** No data protection schemes may be used to intentionally deprive a unit or Institution from access to data or computing equipment to which they are entitled.

xi. **Academic Dishonesty.** Use of NDUS or Institution IT resources to commit acts of academic dishonesty will be handled through the appropriate Institutional procedures.

xii. **Respect the policies of NDUS member Institutions.** Individuals shall follow the policies and procedures of the NDUS institutions to which they are a student, faculty, staff or affiliate.

c. Policy Compliance and Sanctions

i. Individuals who use IT resources to violate NDUS or Institution policy, law, or contractual agreement, may be subject to limitation or termination of user privileges as well as appropriate disciplinary action, legal action, or both. Alleged violations will be referred to the appropriate NDUS or Institution office or law enforcement agency, according to NDUS or Institutional procedures.

ii. The NDUS or Institution may deny access to information technology resources if it appears necessary to protect the confidentiality, integrity, or availability of these resources or to protect itself from liability.

iii. Notice of violations and appeals of decisions will follow NDUS or Institutional procedures.