

## **NDSU PROCEDURE FOR INVESTIGATION OF POTENTIAL EMPLOYEE VIOLATIONS OF ACCEPTABLE USE OF ELECTRONIC COMMUNICATION DEVICES POLICIES**

Last revised: May 2004

### 1. INTRODUCTION AND PURPOSE.

Computers and other electronic communication devices (ECDs) have become vital tools in accomplishing the University's mission. Most employees and students depend on these devices daily to accomplish their work, and the University invests in and supports a variety of equipment and information technology (IT) related items.

These IT resources are not unlimited, however, and it is important to assure that they are used appropriately. In addition, the University has a responsibility to assure that they are used legally and in keeping with State Board of Higher Education and NDSU acceptable use policies (see Section 3 below).

Inappropriate use may range widely in seriousness and impact on the other users. Often misuse can be addressed by the supervisor or administrator in the unit where it occurs. On some occasions, however, the misuse may represent a major violation of acceptable use.

Major violations may include misuse that significantly impacts work performance, misuse that may affect the campus community (e.g., creates a potentially hostile environment) or the institutional image, and/or misuse that violates policy/law. When these potentially major violations are identified, the following procedures are used to provide fair and consistent treatment for employees, including student employees, and assure that evidence is protected.

### 2. PROCEDURAL GUIDELINES.

2.1. Initial discovery of a potential AUP violation can result from a number of triggering events which include but are not limited to: bandwidth and network monitoring; complaint by a supervisor, other employee or person; inadvertent discovery during routine service or maintenance; DMCA (federal copyright law) violation including pirated software; creation or distribution of SPAM or other network abuse; law enforcement query or subpoena; open records request; or other sources. The NDSU IT Security Officer will be notified if she/he is not already aware of the problem.

2.2. The appropriate Dean(s) or Director(s) will be notified as soon as possible so that there can be an initial decision or meeting established with the Appropriate Use Review Committee ("AURC") 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 when to notify the alleged violator has been made.

2.2.1. The AURC consists of the following or their designees:

Director of Human Resources  
Director of Equal Opportunity  
General Counsel  
Vice Provost and Chief Information Officer

2.2.2. The AURC may notify and involve other appropriate officials.

2.3: A course of action is determined that can include monitoring and/or seizure and examination of equipment and related IT items (for example: computers, communication devices, hardware, software, media). When items are seized, the ITS Equipment Seizure Form shall be used. Occasionally, emergency action might be necessary so that the NDSU IT Security Officer may not be able to contact all the above officials before an action is taken.

2.3.1. When equipment is seized, the appropriate supervisor(s) and the NDSU IT Security Officer will normally meet with the alleged violator. This seizure is an administrative process.

2.3.2. ITS will seize and examine equipment using the ITS Forensic Responsibility Chart as a guide.

2.4. If child pornography or other criminal violations are suspected, appropriate law enforcement will be notified. This notification will be coordinated with the General Counsel, NDSU IT Security Officer and Campus Police.

2.5. Outcomes of the investigation could include the following determinations: no violation, violation of law or policy, and/or possible criminal violations.

Sanctions, if a violation is found, 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; and termination of employment. Any criminal process is separate but can also be considered when deciding on appropriate sanctions.

2.6. The employee may use the normal employment appeals processes for any sanctions imposed.

### 3. POLICIES.

#### **State of North Dakota IT Policy S004-023: Acceptable Use of Electronic Communication Devices Policy**

##### **Scope and Purpose:**

The introduction of new and innovative methods of communication in the workplace adds challenges for the business entity to ensure that Electronic Communication Devices (ECDs) are used in an acceptable and appropriate manner. These devices include telephone, facsimile (fax) machines, all computer and network-related hardware, software, and/or peripheral devices (including e-mail and Internet). These devices are connected to the state's IT infrastructure and as such, public scrutiny and/or disclosure of usage must not damage the reputation of the state of North Dakota, nor jeopardize the systems' integrity.

North Dakota state government branches and agencies are responsible for developing and administering policies to prevent or detect abuse and reduce legal exposure related to the use of ECDs. The purpose of this policy is to require all who use the state's IT infrastructure to develop a policy that ensures the appropriate use of ECDs.

##### **Criteria:**

The following criteria should be considered when developing an Acceptable Use (AU) policy:

##### **Usage of Electronic Communication Devices:**

- An AU policy should inform the reader what is acceptable use to the agency or entity. For those areas covered by it, a reminder that North Dakota's Open Records Law may apply is important. The policy should limit the use of ECDs to official business. However, it may also allow people to utilize ECDs for personal use, off-duty, and if in compliance with items such as the ones noted below:
- Does not interfere with the performance of the person's public duties;
- Is of nominal cost or value;
- Does not create the appearance of impropriety;
- Is not for a political or personal commercial purpose;
- Is reasonable in time, duration, and frequency; and
- Makes minimal use of hardware and software resources.

##### **Standards of Conduct:**

An AU policy should also contain standards of conduct. These should hold the individual responsible for the misuse of ECDs. While some of these items may seem obvious, or may be included in other policies, repeating them in an acceptable use policy helps to clarify expectations and create an awareness in employees and their supervisors.

Agencies should include a definition of terms like "inappropriate" or "offensive" or include examples if necessary to create a clear message to the employee.

- ECDs should not be used for harassment or similar inappropriate behavior;
- ECDs should not be used for accessing sexually explicit, offensive, or erotic material;

- Remind the reader that copyright rules applies to most information found on the Internet. Approval for the use and distribution of such information must be obtained from the owner/author;
- ECDs should not be used for the purposes of probing or hacking;
- The use of non-business related “streaming” audio & video (including Internet radio, stock/news tickers, and software such as WeatherBug, etc.) that use significant amounts of the state’s bandwidth should be limited;
- ECDs should not be used for any type of illegal activity;
- The use of pirated software or data should be prohibited;
- Individuals should not knowingly distribute viruses or bypass any state virus detection system in place; and
- The AU policy should also contain a notice that all business related purchases made via an ECD must conform to state procurement policies.

**Training:**

Individual training on computer security and appropriate usage is strongly encouraged. An AU policy should note where and how training can be obtained.

**Measuring & Monitoring:**

It is important to inform everyone about the rights the state/agency has to measure and monitor ECD usage. Some items that should be included are as follows:

- Except where precluded by law, the state has the right to monitor the usage of ECDs, including but not limited to storing, accessing, and reviewing information received or sent through e-mail or over the Internet.
- The tools available to the Information Technology Department (by request of a agency/entity) allow for monitoring of an individual’s Internet site access. A request for such monitoring must be made by the agency/entity.
- The state reserves the right to block out any Internet sites deemed by the State to be unrelated to the State’s responsibilities.
- The state will cooperate with any law enforcement investigation.

**Non-compliance:**

A statement should be included in the agency/entity’s AU policy addressing the disciplinary action for violation of the policy.

Copyright violation complaints from external sources are handled through the Digital Millennium Copyright Act Policy. See <http://www.nodak.edu/hecn/dmca.html>.

Other relevant policies may include, but are not limited to: NDSU 162: Sexual Harassment; NDSU 163: Anti-Harassment; NDSU 163: Code of Student Behavior

=====

**NDUS PROCEDURE 1901.2.1 Authorized use:** Use of computing and networking resources shall be limited to those resources and purposes for which access is granted. Use for political purposes is prohibited. Use for private gain or other personal use not related to job duties or academic pursuits is prohibited, unless such use is expressly authorized under governing institution or system 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 operation of information technologies or electronic mail services; (2) burden the NDUS with incremental costs; or (3) interfere with the user's obligations to the institution or NDUS.

**1901.2.3 Freedom from harassment and undesired information:** All members of the campus community have the right not to be harassed by computer or network usage of others (see 3.1.3.).

**1901.4.2 Imposition of sanctions:** The Institution may impose sanctions on anyone who violates the Computer and Network Usage Policy.

**1901.4.3 System administration access:** A system administrator (i.e., the person responsible for the technical operation of a particular machine) may access electronic information as required for the maintenance of networks and computer and storage systems, such as to create backup copies of media. However, in all cases, all rights to privacy of information are to be preserved to the greatest extent possible.

**1901.4.4 Monitoring of usage, inspection of electronic information:** The Electronic Communications Privacy Act allows system administrators or other authorized campus and NDUS employees to access a person's electronic information in the normal course of employment, when necessary, to protect the integrity of computing and networking resources or the rights or property of the Institution or NDUS. Additionally, other laws, including the PATRIOT ACT of 2001, may expand the rights and responsibilities of campus administrators. Electronic information may be subject to search by law enforcement agencies under court order.

The NDUS and Institution may also specifically monitor the activity, systems and accounts of individual users of the Institutions' computing and networking resources without notice. This includes individual login sessions, electronic information and communications. This monitoring may occur in the following instances:

1. The user has voluntarily made them accessible to the public.
2. It reasonably appears necessary to do so to protect the integrity, security, or functionality of the Institution or to protect the Institution or NDUS from liability.
3. There is reasonable cause to believe that the user has violated, or is violating, Institution or NDUS policies or any applicable laws.

- 4. An account appears to be engaged in unusual or unusually excessive activity, as indicated by the monitoring of general activity and usage patterns.
- 5. Upon receipt of a legally served directive of appropriate law enforcement agencies.
- 6. Upon receipt of a specific complaint of suspected or alleged violation of policy or law regarding a specific system or activity.

Any such monitoring must be accomplished in such manner that all privileges and right to privacy are preserved to the greatest extent possible.

For further information, please see 2.1 for information on privacy.

=====

**NDSU Policy 158(3)**: No obscene or offensive material shall be entered into the computer or sent through external networks or electronic mail systems.

**NDSU Policy 158(4)**: Unauthorized copies of copyrighted material shall not be created, distributed, or knowingly utilized.

**NDSU Policy 710(4)**: Users shall not use computing facilities for any illegal purpose or to enter or send any material that is obscene or defamatory, or to enter or send material that is intended to annoy, harass or alarm another person which serves no legitimate purpose.

=====

**2003 North Dakota Century Code: Title 12.1 Criminal Code**

**NDCC § 12.1-20-05.1: Luring Minors by Computer**

Makes it a crime for an adult to lure a minor to engage in sexual acts. Is a felony if the adult is over 22+ and the minor is under 15.

**NDCC § 12.1-06.1-08: Computer Fraud – Computer Crime**

Whoever gains or attempts to gain unauthorized access to alter, damage, copy disclose, take possession of any part of a computer, computer system, computer network, with the intent to defraud, control, or prevent authorized use, is guilty of a computer fraud, a class C felony.

**NDCC § 12.1-27.1-01. Obscenity - Definitions - Dissemination - Classification of offenses.** A person is guilty of a class C felony if, knowing of its character, the person disseminates obscene material or if the person produces, transports, or sends obscene material with intent that it be disseminated.

**NDCC § 12.1-27.2-04.1. Possession of certain materials prohibited.** A person is guilty of a class A misdemeanor following a first offense or a class C felony following a second or subsequent offense if, knowing of its character and content, that person knowingly possesses any motion picture, photograph, or other visual representation that includes sexual conduct by a minor.

=====

## **Federal Laws**

### **18 USC § 1462: Importation or Transportation of Obscene Matters**

Whoever uses an interactive computer service through interstate commerce to transmit obscene material is guilty of a felony.

### **18 USC § 2252: Certain Activities Relating to Material Involving the Sexual Exploitation of Minors**

Whoever transports, receives or distributes any visual depiction of a minor engaging in sexual activity by means of computer or mail deliveries can be fined and or imprisoned up to 15 years. If a prior offense has occurred under this law, imprisonment can be up to than 30 years.

### **18 USC 2422(b): Coercion and Enticement**

Whoever uses a computer in interstate commerce that persuades, induces, entices or coerces any individual under the age of 18 to engage in prostitution or sexual activity can be fined and or imprisonment up to 15 years.