

North Dakota State University

Policy Manual

SECTION 158

ACCEPTABLE USE OF ELECTRONIC COMMUNICATIONS DEVICES

SOURCE: SBHE Policy Manual, Section 1200 (Information Technology)

1. All employees, students, and other users of North Dakota University System computing and networking resources shall comply with applicable laws, policies, and procedures. The chancellor shall adopt procedures establishing rules governing access to and use of computing and networking resources.
2. NDUS Policy 1202.1, "Acceptable Use of Information Technology Resources Policy," contains specific policies, procedures, rights, and responsibilities which also apply to NDSU. See: [NDUS Policy 1202.1](#).

Of central importance in this document are the definitions of "Authorized Use" and "Authorized Users" from section 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."

"Authorized user(s): Computing and networking resources are provided to support the academic research, instructional, outreach and administrative objectives of the NDUS and its institutions. These resources are extended to accomplish tasks related to the individual's status with NDUS or its institutions. Authorized users are (1) current faculty, staff and students of the North Dakota University System; (2) individuals connecting to a public information service (see section 5.3); and (3) other individuals or organizations specifically authorized by the NDUS or an NDUS institution. For the purposes of this policy, no attempt is made to differentiate among users by the user's group. These policies treat all users similarly, whether student, faculty, staff or other authorized user, in terms of expectations of the user's conduct."

3. Examples of **Electronic Communications Devices** (ECD) include NDSU provided computers, telephones, cell phones, facsimile (fax) machines, personal digital assistants (PDA's), network equipment and infrastructure, software, information services, peripherals, flash drives, data media, etc. Use of some of these devices may also be affected by other policies or procedures and local, state, and federal laws. In particular, NDSU Policy Section 710 contains further administrative policy on Computer and Electronic Communications Facilities.
4. Examples of uses which NDSU considers to be **unauthorized and unacceptable uses** of NDSU provided electronic communications devices include but are not limited to: intentionally viewing, listening to, or sharing obscene or pornographic materials including child pornography; political use; personal commercial gain; copyright (DMCA) violations; hacking or other disruption of operations for

other ECD's; attempting to conceal one's identity (such as anonymous emails) for an unlawful or improper purpose or use of a false identity; threatening communications; harassment; use contributing to a hostile, intimidating, or offensive work environment; fraud; stalking; luring of minors; and invasion of privacy.

5. The **Acceptable Use Review Committee** (AURC) is charged with establishing recommended procedures and working with NDSU administrators and the NDSU Information Technology Security Officer to ensure consistent responses to alleged violations of this policy.
6. **Alleged violations** of this policy by employees should be reported to the NDSU Information Technology Security Officer and the responsible administrator at the Dean or Director level or higher. The administrator and NDSU IT Security Officer in turn will work with the AURC to assess the situation and recommend an appropriate course of action. The person accused of the violation should not be notified until this discussion has taken place. Allegations concerning students who are not employed by NDSU are guided by the Code of Student Conduct (See Policy Section 601). The outcome of an investigation might include a finding of no violation, a violation of policy or law, and/or referral to law enforcement for criminal investigation.
7. **Sanctions** for violations of policy or law include but are not limited to one or more of the following actions: verbal caution; letter of warning; loss of computer and/or network access; referral to the Employee Assistance Program, training, or education; letter of reprimand; suspension with or without pay; and termination of employment.
8. Employee **questions** about acceptable use should be directed to their supervisors. Supervisors and administrators may contact AURC members or the NDSU IT Security Officer in Information Technology Services (231-8685 option 1) if they have questions.

HISTORY:

| | |
|--------------|--------------------|
| New | April 15, 1988 |
| Amended | October 2004 |
| Amended | March 2006 |
| Amended | October 2007 |
| Housekeeping | July 2010 |
| Housekeeping | December 2010 |
| Housekeeping | April 01, 2011 |
| Housekeeping | September 2015 |
| Housekeeping | September 29, 2015 |
| Housekeeping | June 15, 2018 |