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.

3. Examples of **Electronic Communications Devices** (ECD) include NDSU provided computers, telephones, cell phones, facsimile (fax) machines, mobile devices, smart devices, network equipment and infrastructure, software, information services, peripherals, flash drives, storage 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: any activites that are prohibited by local, state, or federal laws, activities prohibited by NDSU or NDUS policy or procedures, activities prohibited by the student code of conduct, and 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 the NDSU IT Security Officer in turn will work with the AURC to assess the situation and recommend an appropriate course of action. The person(s) 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). Investigations will include relevant offices, such as, Human Resources, Equity, and/or Student Affairs. 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
Amended	November 25, 2019