Western Dakota Tech Policy Number: 6018

AUTHORIZED USE OF WESTERN DAKOTA TECH NETWORK AND EMAIL

I. Purpose

The purpose of the policy is to ensure the proper use of the Western Dakota Tech (WDT) network and WDT email accounts.

II. General Statement of Policy

A. WDT has the responsibility to secure the WDT network and email systems against unauthorized access and/or abuse while making the systems accessible for faculty, staff, and students for educational and College-related purposes. All users of the WDT network and email systems must adhere to this policy, Policy 3010 – Use of Copyrighted Materials, and to local, state, federal, and international laws governing use of the Internet and governing copyright.

B. Users of WDT network resources and computers on that network are solely responsible for all actions taken. Wireless network and Internet access are available throughout the WDT campus. The use of any network on campus including Internet usage is restricted to College-related purposes.

1. Deletion, examination, copying, or modification of files and/or data belonging to other users without their prior consent is prohibited.
2. Deletion, copying, or modification of software or operating systems is prohibited.
3. File-sharing software that downloads and distributes songs, videos, games and software without permission of the owner is prohibited.
4. Use of WDT network and email systems for commercial purposes is prohibited.
5. Any unauthorized, deliberate action, which damages or disrupts a computing system, alters its normal performance, or causes it to malfunction, is a violation, regardless of the system location or time duration.
6. The copying of system files is prohibited.
7. Intentional attempts to “crash” the network system or programs are prohibited.
8. Any attempts to secure a higher level of privilege on the network are prohibited.
9. The willful introduction of a computer “virus” or other disruptive/destructive programs into the organization network or computers is prohibited.
10. Any attempt to knowingly enter sites that contain gambling or pornographic material is prohibited.

C. All employees and students are required to use their WDT issued email account when conducting College-related business. WDT email account holders are responsible for all electronic mail originating from their username. WDT email accounts are not for personal use.

1. Forgery or attempted forgery of electronic mail messages is prohibited.
2. Attempts to read, delete, copy, or modify the electronic mail of other users is prohibited.
3. Attempts at sending harassing, obscene, and/or other threatening email is prohibited.
4. All WDT policies concerning harassment and discrimination apply to email.
5. Attempts at sending unsolicited junk mail or chain letters is prohibited.

D. WDT reserves the right to monitor and track all network and Internet activity, and all interaction with WDT computers and software programs, which include, but are not limited to, the student learning management system, the student information system, email, and related servers. WDT network administrators and their authorized employees monitor the use of information technology resources to help ensure network and computer security as well as conformity with WDT policy and state and federal laws.

Administrators reserve the right to examine, use, and disclose any data found on WDT's information networks in order to further the health, safety, discipline, or security of any individual or property. WDT may also use this information in disciplinary actions and will furnish evidence of any crime to law enforcement.

E. Sanctions for Violation or Non-Compliance

Violations of this policy by employees will result in disciplinary actions that may include a warning, temporary suspension from duties with or without pay, or termination of employment. Disciplinary actions will be pursued consistent with existing policies and agreements. The nature and extent of these actions depend on a variety of factors, including the severity of any work rule violations, the pattern and frequency of observed violations, past work record, or any other consideration which may be considered relevant by the College. The need for disciplinary action and the appropriate penalty for employees will be handled accordingly by the Human Resources Director and others as appropriate. Evidence of a crime will be reported to law enforcement by the Information Systems Director or designee.

The Student Code of Conduct in the WDT Student Handbook addresses student violations of this policy. Violations of this policy by students will result in disciplinary actions that may include a warning; revocation of network, Internet usage, or email privileges; suspension; or other disciplinary actions consistent with the Student Code

of Conduct policy. Evidence of a crime will be reported to law enforcement by the Information Services Director or designee.

III. Definitions

A. Virus means any malicious software including malware, phishing, ransomware or any other software intended to cause harm to a computer or network.

IV. Reporting Procedures

A. Known or suspected violations of this policy by employees is to be reported to the employee's immediate supervisor and to the Information Systems Director.
B. Known or suspected violations of this policy by students is to be reported to the Student Success Director/Registrar and to the Information Systems Director.

V. Dissemination of Policy and Training

A. This policy shall appear on the WDT website on the policy page and in the WDT Student Handbook.
B. New employees receive a copy of the policy at the time of their new employee orientation.

Legal References: None

Board Approved 06/01/2020