PERSONNEL POLICY & PROCEDURES — SECTION 300
NUMBER: **309**
SUBJECT: EMPLOYEE INFORMATION TECHNOLOGY ACCEPTABLE USE POLICY & PROCEDURE
LAST REVIEWED: 7/20/2020
EXECUTIVE STAFF APPROVAL: 9/14/2020
BOARD APPROVAL: 10/21/2020

(PRINTED COPIES ARE FOR REFERENCE ONLY. PLEASE REFER TO THE ELECTRONIC COPY FOR THE LATEST VERSION.)

309.1 PURPOSE

The purpose of this policy is to establish guidelines for the acceptable use of the information technology resources of Mountainland Technical College, and to ensure that all employees consistently use those resources to support the mission and purpose of the College.

It is important to recognize that with increased access to computerized information, access to controversial material may increase, which may contradict the mission and purpose of the College. While some internet sites and information accessed through College Campus network resources may contain material that is illegal, defamatory, offensive or inaccurate, Mountainland Technical College has no control of such information.

By accessing the College's computer resources, all users agree to comply with, and will be subject to this Acceptable Use policy. Users are responsible for maintaining a current understanding of its terms, which the College reserves the right to change without prior notice.

309.2 REFERENCES

2.1 Mountainland Technical College Policy 300.317 Social Media policy
2.2 Mountainland Technical College Policy 300.318 Telecommuting policy & procedure

309.3 DEFINITIONS

3.1 **Financial Gain-** Gain derived from any activity recognized under current U.S. Tax Code as qualifying as a business.

3.2 **Illegal Activities**- A violation of local, state, and/or federal laws.

3.3 **Inappropriate Use**- A violation of the intended use of MTECH network resources.

3.4 **Political Lobbying**- Activities on behalf of a particular party or candidate.

3.5 **Network Resource**- any computing device connected or has the potential to connect to College Campus wiring infrastructure.

3.6 **Malware or Malicious Software**- software designed to infiltrate or damage a computer system without the owner's informed consent.

309.4 POLICY

This policy is not intended to be considered exhaustive, but to provide general guidelines regarding activities that are considered unacceptable.

4.1 System and Network Activities

The following activities are strictly prohibited uses of the MTECH information systems:

1. Allowing others access to your accounts and passwords associated with your employment at Mountainland Technical College. This includes household members when work is being done at home.

2. Using an MTECH computer or other asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws.

3. Any use for personal financial gain.

4. Any use for the advertisement of products or partisan political activities, such as campaigning for or against candidates for elected office or measures on a ballot.

5. Any use, download, copying, or installation that violates the copyright protections of any materials, software, photographs, music, etc.

6. Introduction of any malicious programs into the MTECH network or servers. This includes, but is not limited to viruses, worms, email bombs, Trojan horses, etc.

7. Security breaches, or network disruptions of any kind. These include but are not limited to, accessing data that the employee is not the intended recipient, and logging into a server or account that the employee has not been strictly granted access.

8. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is part of the performance of the normal job duties of the employee.

9. Circumventing user authentication or security of any host, network or account.

10. Interfering with or denying service to any users other than the employee's host (for example, denial of service attack). Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's network

resource or computing device, by any means, locally or via the Internet/Intranet/Extranet.

11. Any use for illegal activities of any kind.

4.2 Email and Communication Activities

The following activities are strictly prohibited uses of the MTECH email and communication systems:

1. Any form of harassment via telephone, messaging, email, etc. This includes through language, length of messages, images or frequency.

2. Unauthorized use, or forging of email header information.

3. Requesting an email for any other email address, other than that of the poster's account, with the intent to harass, or collect replies.

4. Sending unsolicited email messages, including advertising to individuals who did not specifically request the material (email spam). This includes creating/forwarding email of chain letters, and pyramid schemes of any kind.

5. Other activities not mentioned specifically herein but which violate the general guidelines above.

4.3 Privacy of Information

4.3.1 The Technology Department takes considerable care to ensure the confidentiality of information, and to protect the right of privacy of the users of the Mountainland Technical College networks and systems.

4.3.2 All communications, logs, and information accessible via the College network should be assumed College property and are subject to review and inspection by the College network administrators aligned with applicable federal and state laws, as well as College policy.

4.3.3 It is important to note that College property includes employee emails. Employees should understand and expect that nothing delivered or received via email is private. It should also be understood that MTECH is obligated to disclose email messages to law enforcement or other authorized personnel without prior notice to the employee. Caution should be taken by employees not to engage in prohibited e-mail activity including illegal messaging, electronic chain letters, and mailbox contents which consume inordinate amounts of system resources.

309.5 PROCEDURE

5.1 Use of Computer Equipment and Telecommunication Systems

5.1.1 The intended use of College telecommunication equipment is for official College business. Personal use of the resources should be kept to a minimum.

5.1.2 Employees are expected to use College-owned equipment primarily for College business in connection with their jobs. College policy also allows College-owned equipment to be used for incidental personal use. However, the use or possession of College-owned equipment must substantially outweigh the personal benefit derived by the employee from the incidental use. Additionally, network users are required to exercise reasonable precautions in caring for any equipment authorized for use off-premises, and are personally responsible for any damage resulting from use by unauthorized persons.

5.1.3 Mountainland Technical College recognizes that a reasonable amount of wear is to be expected, any damage which is deemed to be the result of intentional misuse, abuse, or gross negligence will be the financial responsibility of the employee. Additionally, employees will be held accountable for any wear or damage caused by use of the equipment for non-approved or inappropriate purposes.

5.2 Authorization and Installation of Software

5.2.1 The Technology Department is responsible for ensuring the compatibility of software applications used at the College. It is recommended that employees both notify, and receive consent from the Technology Department when installing software applications in order to minimize potential issues.

5.2.2 Installation of personal copies of software by College employees is discouraged due to possible licensing infringements. This procedure is intended to ensure compliance with software licensing obligations and also to safeguard against avoidable introduction of computer viruses, as well as to avoid unnecessary potential overloading of storage capacity of College owned equipment.

5.2.3 College owned software should not be installed on personal devices or any other equipment. Any deviation from this procedure for any reason should be specifically authorized through the Technology department.

5.3 Internet Access and Use

College employees are expected to exercise sound judgment in limiting internet use primarily to official College-related purposes. Incidental and off-duty personal uses should be appropriate to standards of ethical behavior. College employees with off-premises access to the Internet are required to safeguard against its use by unauthorized persons. Technology staff will monitor and periodically check the sites addressed using College Internet access.

5.4 Policy Violations

In the event that the Technology Department suspects or detects a violation of this policy and procedure, they will report findings to Human Resources for further investigation. The Vice President of Administration, the Director of Technology, and the Director of Human

Resources will determine what sanctions will be applied to the individual, up to and including termination.

5.5 Employee Authorization and Consent

Every employee of the College is required to sign an agreement relating to this policy before being given access to equipment, email or network resources.