TRI-COUNTY TECHNICAL COLLEGE
STATEMENT OF POLICY

POLICY NUMBER: 4-4-1031

PAGE: 1 of 4

TITLE: Acceptable Use of Information Technology Resources

RELATED POLICIES AND PROCEDURES:
1-8-1010, Reproduction of Copyrighted Print and Non-print Materials Policy
1-8-1010.1, Reproduction of Copyrighted Print Materials Procedure
1-8-1010.2, Reproduction of Copyrighted Non-print Materials Procedure
4-4-1031.1, Acceptable Use of Information Technology Resources Procedure
4-4-103, Internet Access (State Policy)

ADMINISTRATIVE RESPONSIBILITY: Vice President for Business Affairs

---

February 1, 2010	May 19, 2017	May 19, 2017
DATE APPROVED BY AREA COMMISSION	**DATE LAST REVIEW**	**DATE LAST REVISION**

The use of information technology (IT) resources at Tri-County Technical College is a privilege, not a right. Abuse of College IT resources or failure to adhere to the provisions of this policy by administrators, faculty, staff or students is subject to disciplinary action. Violation of federal or state legislation may also be subject to criminal or civil action.

1. Unacceptable use of College IT resources includes:

1.1. Violating any federal or state legislation, including the Federal Copyright Law, the Family Education Rights and Privacy Act (FERPA) and the Gramm-Leach-Bliley Act; or

1.2. Accessing, copying, modifying, damaging, removing or distributing restricted data and application software owned and licensed by the College

or any user data and application software without express permission from the manager of that data and application software; or

1.3. Removing, damaging or altering College IT resources, or any deliberate act affecting the operational readiness of these resources, disrupting normal computer usage or restricting network access; or

1.4. Exploiting College IT resources for activities not relevant to College business or academic pursuit, including solicitation, personal financial gain or commercial advertising; or

1.5. Circumventing, or attempting to circumvent, any protective software or device installed on any College computer system, fileserver or workstation; or

1.6. Initiating, accessing, or reproducing information that is offensive, harassing or libelous on any College computer system, fileserver or workstation; or

1.7. Intentionally wasting or monopolizing IT resources to the exclusion of others, including, but not limited to, sending mass mailings or chain letters, creating superfluous output, causing unnecessary network traffic, or generating excessive printing.

1.8 College IT resources are for college business use only. Resources are not to be used for personal activities such as personal e-mail, social networking, gaming, shopping or other activities that are not related to the official business of the College. This does not preclude occasional incidental use of resources provided that they are limited and do not interfere with business activities or IT resource availability.

1.9 Given the sensitive nature of information that may be contained in e-mails, employees are to only utilize the College provided e-mail for their business communications. This includes the receiving, storing and sending of e-mails. As such, redirecting e-mail from the College provided e-mail utility (Outlook) to a personal e-mail account is prohibited.

1.10 **Prohibited Use —** Use of the College's computers, network or electronic communication facilities (such as electronic mail or instant messaging, or systems with similar functions) to send, view or download fraudulent, harassing, obscene (i.e., pornographic), threatening, or other messages or material that are a violation of applicable law or College policy, or that might contribute to the creation of a hostile academic or work environment, is prohibited.

2. User IDs and Passwords:

2.1 **Personal User IDs and Passwords Responsibility** - Users must be responsible for all activity performed with their personal user IDs. They must not permit others to perform any activity with their user IDs or passwords of any form, and they must not perform any activity with IDs and passwords belonging to other users. Refer to procedure 4-4-1031.1.

3. Privacy related to IT resources:

3.1 **Privacy Legislation** — Information will be maintained and disclosed in accordance with all applicable state and federal laws to include the Family Educational Privacy Rights Act (FERPA), the Family Privacy Act and the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

3.2 In order to provide for the most efficient and effective use of our IT resources, the IT staff will monitor these resources to balance the network load and maintain adequate network security as they deem appropriate.

3.3 In addition to the above monitoring, and given that IT resources are only to be used for legitimate business purposes, the College reserves the right to monitor any and all information contained on any of the IT resources including individual personal computers, network drives, laptops and administrative systems. This includes the monitoring of e-mail and individual documents. Such monitoring will be conducted for investigative purposes and only in consultation with the Dean of Student Development for student-related offenses and with the Assistant VP for Human Resources for employee-related offenses.

3.4 Employees and students should not have any expectation of privacy of the data housed on their college issued e-mail or college-owned computers.

4. Security Incident Reporting

4.1 **Reporting Security Events** – Any suspected events that may compromise information security or are known to violate an existing security policy must be immediately reported to the IT department. Refer to procedure 4-4-1031.1.

5. Privileged Access to College Resources

5.1 **Training and Compliance Required –** Mandatory training and compliance must be completed prior to granting privileged access to a user's account. Refer to procedure 4-4-1031.1.