BOARD OF TRUSTEES, DISTRICT 504 **BUSINESS SERVICES**

APPROPRIATE USE OF INFORMATION TECHNOLOGY RESOURCES
Page 1 of 5

POLICY 3511
ADOPTED: 06/17/08
AMENDED: 12/20/16

PURPOSE

Triton College's computer and information network is a continually growing and changing resource supporting thousands of users and systems. These resources are vital for the fulfillment of the academic and business needs of the College community. In order to ensure the necessary services, it is essential that each member of the faculty, staff and student body exercise responsible and ethical behavior when using these resources. Any misuse has the potential to disrupt College business and the legitimate academic work of faculty and students.

This policy outlines the application of the principles governing the academic community's appropriate use of College computer and information network resources. This policy ensures the proper use of computing resources consistent with the College's governing principles. It demonstrates respect for intellectual property, ownership of data, system security mechanisms, and individuals' rights to privacy, and freedom from harassment. Computing and networking resources include: computers, computer networks, connections to external computer networks, telephones, mobile devices, laptops, identification cards, the Internet, email, all software applications and subscriptions to external computer services (collectively referred to as information technology or "IT" resources). Use of any College computing resource constitutes acceptance of this Policy.

SCOPE

This policy applies to all College staff, faculty, administrators, officers and students (collectively, "Users"), including those at remote campuses and extended learning sites.

POLICY

Triton College IT resources (the "Resources") are provided primarily for the use of students, faculty and staff. The Resources are intended to be used for administrative and educational purposes and to carry out the College's business. The Resources may also be available to alumni and members of the local community to facilitate communication with students and employees and to access College information resources and the Internet.

Appropriate use of the Resources includes conducting College business, instruction, study assignments, research, communications, and official work of campus organizations and agencies of the College. Access to the Resources is a privilege and requires all users to act responsibly, conserve computer resources, and consider the rights and privacy of others. The Resources are the sole property of Triton College. All users must use College resources in a responsible manner consistent with all College policies and guidelines.

Users are responsible for all of their accounts. Users must take all reasonable precautions, including password maintenance and file protection measures, to prevent use of their account by unauthorized persons. Users must not share their password or provide access to the Triton network resources to unauthorized persons.

Users should assume all software, graphic images, music, and other materials are copyrighted. Copying or downloading copyrighted materials without the express authorization of the copyright owner is a violation of this policy, against the law, and may result in civil and criminal penalties, including revocation of use privileges, fines and imprisonment.

PROHIBITED USE OF RESOURCES

Users should be aware that use of the Resources may result in being subjected to the laws of other states and countries. Users shall ascertain, understand, and comply with the laws, rules, policies, contracts, and licenses applicable to the particular uses of the Resources. The following uses of the Resources are prohibited:

1. Interfering or impairing others activities, including but not limited to the following:
    a. Creating, modifying, executing or retransmitting or otherwise using any computer program or instructions intended to obscure the true identity of the sender of electronic mail or electronic messages, such as the forgery of electronic mail or the alteration of system or user data used to identify the sender of electronic email.
    b. Bypassing, subverting, or otherwise rendering ineffective the security or access control measures on any network or computer system without the permission of the owner.
    c. Examining or collecting data from the network (e.g., a "network sniffer" program).
    d. Authorizing another person or organization to use College computer accounts or Triton network resources.

e. Communicating or using any password, personal identification number, credit card number or other personal or financial information without the permission of its owner.

2. Unauthorized access and use of the resources of others, including but not limited to the following:
   a. Use of College resources to gain unauthorized access to resources of any institution, organization, or individual.
   b. Use of false or misleading information for the purpose of obtaining access to unauthorized resources.
   c. Accessing, altering, copying, moving, or removing information, proprietary software or other files (including programs, libraries, data and electronic mail) from any network system or files of other users without prior authorization (e.g., use of a "network sniffer" program).
   d. Making unauthorized copies of copyrighted materials.

3. Damage or impairment of The Resources, including but not limited to the following:
   a. Use of the Resources irresponsibly or in a manner adversely affecting the work of others, such as:
      (1) Hacking - attempting to obtain or use passwords, IP addresses or other network codes that have not been assigned to you or authorized for use as College employees, attempting to obtain unauthorized access to computer accounts, software, files, or any other College IT resources.
      (2) Malicious Activity - intentionally, recklessly or negligently damaging any system (e.g., by the introduction of any so-called "virus", "worm", or "trojan-horse" program); damaging or violating the privacy of information not belonging to the user; or misusing or allowing misuse of system resources.
   b. Use of College resources for non-College related activities that unduly increase network load (e.g., network games, spamming, and video streaming).
   c. Any other activity not specifically cited above that may be illegal, harmful, destructive, damaging, or constitute an inappropriate use of the Resources.
4. Unauthorized commercial activities, including but not limited to the following:
   a. Using the Resources for one's own commercial gain, or for other commercial purposes not officially approved by the College, including web ads.
   b. Using the Resources to operate or support a non-College related business.
   c. Using the Resources in a manner inconsistent with the College's contractual obligations to suppliers of those resources or with any published College Policy.

5. Violation of city, state or federal laws, including but not limited to the following:
   a. Pirating software, music and images.
   b. Effecting or receiving unauthorized electronic transfer of funds.
   c. Disseminating or viewing child pornography or other illegal material.
   d. Violating any laws or participating in the commission or furtherance of any crime or other unlawful or improper purpose.

MONITORING

- Methods of monitoring may include, but are not limited to the following;
  - Reviewing a list of internet sites visited by employees
  - Reviewing email messages sent or received by employees
  - Reviewing employees keystrokes while using the College network

SECURITY OBLIGATION

- System Security: Access to information stored on the College's computers and network equipment is controlled by assignment of accounts and passwords. These accounts and passwords are controlled by Triton Information Systems. This security information is the property of Triton.

- All College employees have an obligation to report security breach information to Triton Information Systems. Failure to do so may result in disciplinary action, up to and including termination. Any attempt to access, copy or modify this security information or to obtain system privileges to which employees are not entitled or any action which interferes with the supervisory or accounting functions of the systems or that is likely to have such effects will result in appropriate disciplinary action.

DE MINIMIS USAGE

In the interest of making the use of the Resources part of the day-to-day learning and work of all members of the College community, incidental personal use is tolerated. However, College email, Internet access, and other IT services should not be used for unrelated activities of an extensive nature. Excessive use of systems for recreational Internet browsing, email, or game playing is to be avoided and may subject College employees to disciplinary action, up to and including termination.

ENFORCEMENT

The College reserves the right to monitor computer and network use. The College considers any violation of this policy to be a serious offense and reserves the right to copy and examine any files or information contained on College systems or equipment.

The Associate Vice President of Information Systems reserves the right to authorize disconnecting a user's account if the user represents a serious threat to system or email integrity. Violators are subject to disciplinary action as dictated by College policy. Users should be aware that offenders may be subject to prosecution under laws including, but not limited to, the

> Privacy Act of 1974, The Computer Fraud and Abuse Act of 1986, National Stolen Property Act, and the Electronic Communications Privacy Act.

Suspected violations of this policy or related statute should be reported to the Office of the Associate VP of Information Systems in an email message addressed to: the Associate VP of Information Systems or by calling extension 3684. In reporting a violation, complainants should cite the specific violation of this policy.

If any provision of this policy is ruled invalid under law, it shall be deemed modified or omitted solely to the extent necessary to comply with said law, and the remainder of the policy shall continue in full force and effect.

QUESTIONS OR PROBLEMS

Questions, concerns or additional information about this and any IT policy shall be directed to the Associate VP of Information Systems.

RESPONSIBILITY

The Associate VP of Information Technology shall administer this policy and will ensure the maintenance of all necessary processes. All administrators shall be responsible for compliance with College policy within their respective administrative areas.