Allegany College of Maryland

TECHNOLOGY RESOURCES POLICY

Adopted date 1/19/2008
Revised Date 6/17/2022
Approved by Board of Trustees 1/19/2008
Implementation 1/19/2008
Type of Policy: Operational

BACKGROUND AND PURPOSE

Allegany College of Maryland ("ACM" or "the College") makes every effort to provide students, faculty, and staff with the best technologies available. In this effort, the College has installed and maintains technology resources that support diverse and ever-growing learning and administrative functions. These technology resources include computer systems, information systems, telephone systems, network systems, access control and camera systems.

This policy has been constructed to advise on the acceptable uses of ACM technology resources, including but not limited to, computer equipment, the Internet, electronic mail ("email"), computer labs, voice mail, computer-based information systems, electronic access controls, cameras, and the College computer network including wireless Ethernet.

This policy also covers the subject of access to and disclosure of computer-stored information, voice mail messages and e-mail messages (created, sent, or received) by ACM's employees, and the College's rights and responsibilities in providing access to and control over its property.

POLICY

I. SCOPE OF THE POLICY

This policy and additional guidelines for using resources apply to the use of all technology resources at Allegany College of Maryland.

II. POLICY STATEMENT

Access to and use of the College's technology resources are privileges granted solely to Allegany College of Maryland faculty, staff, students, and those with special accounts. These privileges can be modified, limited, extended, or revoked at the discretion of the College with or without prior warning or consent.

All College technology resources are designed and intended for academic and administrative use. Alternate uses may be restricted or prohibited at the discretion of the college, especially when these uses conflict with or interfere with academic and administrative functions.

College technology resources are not to be used to create any threatening, abusive, or disruptive messages. Allegany College of Maryland does not discriminate on the basis of age, ancestry/national origin, color, disability, gender identity/expression, marital status, race, religion, sex, or sexual orientation in matters affecting employment or in providing access to programs and activities. Allegany College of Maryland also has "Principles of Conduct" for all employees; among these principles are prohibitions on immoral/unethical conduct, offensive/brutal treatment of students and colleagues, and disparagement of colleagues. Finally, the College has a Sexual Harassment policy that prohibits - among other things - conduct that has the purpose or effect of unreasonably interfering with an individual's work or academic performance or creating an intimidating, hostile, or offensive work environment. The College's computers, Internet, email, and voice mail systems may not be used to violate these standards.

III. User Provisions

An individual shale only use those technology resources assigned to them. This includes use of computer-based and network-based user accounts (including email mailboxes and voicemail mailboxes), assigned passwords, and computer/network identities.

Users may not attempt to obtain login credentials or passwords that are not specifically assigned to them. A user's attempt to disguise or otherwise obscure the identity of the credentials or resources he or she is using is prohibited. Attempts to gain unauthorized access to technology resources are prohibited.

All persons shall abide by the terms of all software licensing agreements and copyright laws. Unauthorized copying of copyrighted software is prohibited. The copying of site-licensed software for distribution to persons other than Allegany College of Maryland faculty, staff, and students, or the copying of site-licensed software for use at locations not covered under the terms of the license agreement is prohibited.

Any deliberate act which may impact the operation of technology resources is prohibited. Such acts include, but are not limited to, tampering with computer, network, and telephone systems, launching software attacks (viruses, denial of service, or other malicious software), and tampering with or otherwise modifying College software and systems.

Any action taken which may circumvent hardware and software security systems or data protection schemes is prohibited. Unauthorized attempts to uncover or exploit security loopholes are prohibited. If such a loophole is discovered, the user is required to report their findings to the Information Technology Department ("ITD").

Deliberate acts which are wasteful of computing/information network resources or which unfairly monopolize resources to the exclusion of others are prohibited. These acts include, but are not limited to, sending mass mailings or chain letters, creating unnecessary multiple jobs or processes, obtaining unnecessary output, or printing or creating unnecessary network traffic.

Use of the College's technology resources to monitor another user's data communications, or to read, copy, change, or delete another user's files or software without the user's permission is prohibited.

IV. Data Provisions

The College observes all federal, state, and local laws pertaining to the protection of user data, including those specified by FERPA, GLBA, PCI DSS and HIPAA regulations. To the best of its ability, the College maintains the privacy of stored data including, but not limited to, user-created files, log entries, and electronic communications utilizing multiple levels of security and data protection schemes.

The College maintains multiple levels of data backup and data loss prevention systems. At no time should a user expect that a deleted file has been completely destroyed, but the College does not guarantee the ability to recover any specific file or files in the event of accidental or unwanted deletion.

The College maintains the right to, but does not regularly monitor voice mail or electronic mail messages. The College will, however, inspect the contents of computers, voice mail or electronic mail in the course of an investigation triggered by indications of unacceptable behavior or as necessary to locate needed information that is not more readily available by some other less intrusive means. The contents of computers, voice mail, and electronic mail, properly obtained for some legitimate business purpose, may be disclosed by authorized College employees. Allegany College of Maryland's President, Vice Presidents, Deans, Directors or designees will grant or deny any request for access to the contents of an individual's computer, voice mail, or electronic mail prior to access being made without the individual's consent. With exception to the College's right to retrieve and read electronic mail messages, such messages should be treated as confidential and should only be accessed by intended recipients.

The College can restrict through compliance rules the use of employee personal devices used to access systems and data resources if the device operating system is out of date and the device is not setup with necessary virus protections. As a rule, College restricted or protected data can never be saved to or stored on an employee's personal device. Any employee granted the right by a supervisor to use paper files at home must take precautions to protect that information from loss or accidental exposure to unauthorized individuals. Such loss or exposure

must be reported to one's supervisor who will document the incident and submit it to the Information Technology Department for review.

The following types of information cannot be created or stored on any College technology resource:

a. Information that infringes upon the rights of any other individual or group of individuals.

b. Information that infringes on the copyright of any other individual or group of individuals including, but not limited to, copied or "pirated" software, music, videos, et al.

c. Information that may injure someone else and/or lead to a lawsuit or criminal charges including, but not limited to, viruses, malware. pornographic materials, or libelous statements.

Any data or network traffic exiting the College is subject to the acceptable use policies of the network through which it flows, as well as to the policies listed herein.

V. Resource Provisions

Use of College technology resources for personal or financial gain is prohibited. The College reserves the right to offer systems and services that allow for the promotion of personal goods and services, but does not sponsor, endorse, or support said goods and services. The College reserves the right to offer systems and services that allow for the promotion of charitable goods and services, and to solicit for charitable contributions, but does not sponsor, endorse, or support said goods, services, and solicitations. Use of the College's technology resources to operate any unauthorized network server is prohibited. This includes, but is not limited to chat, file, print, web, and application servers.

VI. Responsibilities and Notification

The user community is expected to cooperate with the College in its operation of technology resources as well as in the investigation of misuse or abuse. Existing College policies including Technology Security Policy, Breach Notification policy, Wireless Network Security Policy, Employee Email Use Policy, Use of Electronic Signatures Policy, Sexual Harassment policies, policies on Student Conduct, Academic Integrity, Facilities Use, etc. will be enforced as they relate to a violation of the Allegany College of Maryland Technology Resources Policy.

The Information Technology Department Dean or designee should be notified about violations of laws and policies governing information use, intellectual property rights, or copyrights, as well as about potential loopholes in the security of the College's technology resources. The ITD Dean will report these violations to the President, Vice Presidents, Deans and Department heads of the College as required.

VII. Enforcement

Technology resources and their uses are governed by college policy as well as federal, state and local laws. Individuals who inappropriately or illegally use college technology services and resources may suffer all applicable college and legal penalties for such misuse.

VIII. Administration of Policy

The office of the Dean of Information Technology, in consultation with The Vice President of Finance and Administration, shall be responsible for maintaining this policy.

IX. Changes

Substantive changes to this policy require approval by the Board of Trustees; editorial changes, title/position changes, and/or changes to its implementation procedures may be made as required by federal or state mandate and/or institutional need with timely notice to students and employees.