Purpose

Ozarks Technical Community College provides students, faculty, staff, and members of the public access to campus and global information resources through networked computing technology to enhance our mission and in service to its many constituencies. The primary function of Information Technology resources at OTC is to support instruction and administration; other activities are secondary and may be subject to limitations. As a user of these services and facilities, access to valuable OTC resources, sensitive data, and internal/external networks is granted.

Scope

This policy applies to all members of the OTC community, which includes, but is not limited to employees, students, visitors, volunteers, third parties, contractors, consultants, and other users, who have been granted access to Information Technology resources.

IT resources include all college-owned, licensed, or managed hardware and software, and use of the college network via a physical or wireless connection, regardless of the ownership of the computer or device used.

These policies apply to technology administered in individual departments, the resources administered by central administrative departments, personally-owned computers and devices connected physically or wirelessly to the campus network, and to off-campus computers that connect remotely to the college network services.

User Responsibility

As a user of these services and facilities, access to valuable OTC resources, sensitive data, and internal/external networks is given. Consequently, it is important for you to behave in a responsible, ethical, and legal manner. All users must respect the rights of others, respect the integrity of the physical facilities and controls, and respect all pertinent license and contractual agreements.

Additionally, individual password security is the responsibility of each user. The user will be held responsible for all activity on their accounts, independent of authorization.

Privacy

Users have a lessened expectation of privacy when using Information Technology resources owned by public institutions. Issuance of a password or other means of access is not a guarantee of privacy, license for abuse, or improper use of OTC's resources and facilities. In the course of network administration, we may be required to open email and files. A forensic analysis may require the network staff to access, inspect, and copy Internet traffic, files, and portable media of users that have accessed OTC Information Technology resources without notice to the user.

Internet Use

OTC community members have been granted access to the Internet. However, users should be aware of the risks associated with accessing the Internet, including the lack of confidentiality or integrity of information accessed or sent via the Internet. Users should be aware that when browsing the Internet, each web server can obtain information relating to the individual, the computer they were using, and other locations visited during a browsing session. Therefore, discretion must be used in determining which web sites to visit from an OTC system. Users must use discretion when posting information on public Internet sites and may not disseminate any data classified as sensitive or confidential over the Internet that is not encrypted.

Content Filtering

It is the policy of OTC to filter some traffic passed through the college's network. This includes material that is defamatory, abusive, obscene, profane, sexually oriented, or illegal. The college may also block or filter other content deemed to be inappropriate, lacking educational or work-related content or that poses a threat to the network. If at any time in the course of completing college related or classroom projects you are unable to access a web site, you may contact the Information Technology Helpdesk and request access.

Commercial Use

Use of the college's Information Technology resources for unauthorized commercial activities, personal gain, private business, fundraising or business otherwise unrelated to the college is strictly prohibited. This includes soliciting, promoting, selling, marketing or advertising products or services, or reselling college resources.

Fraud

Use of college Information Technology resources for purposes of perpetrating fraud in any form is strictly prohibited. Fraudulent activities include but are not limited to sending any fraudulent electronic transmission, fraudulent requests for confidential information and fraudulent submission and/or authorization of electronic purchase requisitions. Further, impersonation, anonymity, spoofing, and any other methods of hiding one's true identity in order to mislead, harass, avoid detection, or generate financial gain is prohibited.

Political Activities

State law prohibits the use of state resources for political campaign activity. This provision does not apply to political activities related to on-campus student government, including the conduct of student elections, or student club activities and sponsored events conducted with prior approval of the college. It does not apply to individual student activities which constitute free speech. It does not apply to incidental and minimal use of state resources. Such activities must comply with all other provisions of this policy, including the section on electronic communications, when using college resources.

Harassment

OTC's Information Technology resources may not be used to harass, threaten, or otherwise cause harm to a specific individual(s), whether by direct or indirect reference. It may be a violation of this policy to use electronic means to harass or threaten groups of individuals by creating a hostile environment.

Copyright and Fair Use

Federal copyright law applies to all forms of information, including electronic communications, and violations are prohibited under this policy. Infringements of copyright laws include, but are not limited to, making unauthorized copies of any copyrighted material (including software, computer code, text, images, audio, and video), and displaying or distributing copyrighted materials over computer networks without the author's permission except as provided in limited form by copyright fair use restrictions. The "fair use" provision of the copyright law allows for limited reproduction and distribution of published works without permission for such purposes as criticism, news reporting, teaching (including multiple copies for classroom use), scholarship, or research. The college will not tolerate academic dishonesty or theft of intellectual property in any form.

Electronic Communications

College electronic communications are to be used to enhance and facilitate teaching, learning, scholarly research, support academic experiences, facilitate the effective business and administrative processes of the college, and foster effective communications within the academic community. Electronic mail, news posts, chat sessions or any other form of electronic communication must comply with State and Federal Law. The college reserves the right to review all electronic communications at its discretion.

Network and System Integrity

In accordance with state and federal law and OTC policy, activities and behaviors that threaten the integrity of computer networks or systems are prohibited on both college-owned and privately-owned equipment operated on or through college resources. These activities and behaviors include, but are not limited to:

- Intentional or careless interference with or disruption of computer systems and networks and related services, including but not limited to the propagation of malware and any other activities that could have a negative impact on the OTC computing environment in the judgment of the Chief Technology Officer or designee.
- Intentionally or carelessly performing an act that places an excessive load on a computer or network to the extent that other users may be denied service or the use of electronic networks or information systems.
- Failure to comply with authorized requests from designated college officials to discontinue activities that threaten the operation or integrity of computers, systems or networks

- Negligently or intentionally revealing passwords or otherwise permitting the use by others of college-assigned accounts for computer and network access.
- Altering or attempting to alter files or systems without authorization
- Unauthorized scanning of ports, computers and networks
- Unauthorized attempts to circumvent data protection schemes or uncover security vulnerabilities
- Connecting unauthorized equipment to the campus network or computers.
- Attempting to alter any college computing or network components, including but not limited to routers, switches, wiring, and connections, without authorization or beyond one's level of authorization as designated by the administrator responsible for that equipment, i.e. the Chief Technology Officer or designee.
- Providing services or accounts on College computers or via college networks to other users from a personal computer unless required to meet the normal activities of students working as individuals or in collaborative groups to fulfill current course requirements.

Consequences of Non-Compliance

Enforcement will be based upon one or more formal complaints received by the Information Technology department about a specific incident or thorough discovery of a possible violation in the normal course of administering Information Technology resources.

First offense and minor infractions of this policy, when accidental or unintentional, such as consuming excessive resources or overloading computer systems, are generally resolved informally by the unit administering the resource. This may be done through e-mail or in person, including discussion and education on the subject.

Repeated offenses and serious incidents of non-compliance may lead to college disciplinary action under section 3.32 and 5.16 of the college's policies and procedures for employees and students. Serious incidents of non-compliance include but are not limited to unauthorized use of computer resources, attempts to steal passwords or data, copyright violations, unauthorized use or copying of licensed software, repeated harassment, or threatening behavior.

In addition to the above, inappropriate use of Information Technology resources may result in personal criminal, civil and other administrative liability.

Appeals of college actions resulting from enforcement of this policy will be handled through existing disciplinary/grievance processes under sections 3.35 and 5.16 of the college's policies and procedures for employees and students.