XYZ Company

Effective: 08/01/2023

Computer and Network Use Policy

Background and Scope:

XYZ has developed the Computer and Network Use Policy to guide individuals in the acceptable use of computers, information systems, and networks owned, leased or used by XYZ. All such systems and networks are considered XYZ property for purposes of this policy. This policy is also intended to describe best practices to ensure availability, integrity, reliability, privacy, and confidentially of the Company's computers, information systems, data, and networks. XYZ makes computing and network resources available to faculty, staff, students, and, to some extent the general public, to support the educational, scholarship, research, and service mission of the College.

This policy supplements other XYZ policies and procedures, including, but not limited to, the E-Mail Policy, Peer-to-Peer File Sharing Policy, Social Medial Policy, and Connecting Devices to the XYZ Network Policy, should be read together with those policies.

The College reserves the right to amend this policy at its discretion with or without notice. In case of amendments to the policy, XYZ will make efforts to inform users of changes. The most current policy can be found on the XYZ Website: http://www.xyz.com/XYZ_employee_-_Computer_and_Network_Use_Policy.pdf

Policy and User Responsibilities:

XYZ's computing and network resources and services are limited and should be used wisely and carefully with consideration for the needs of others. By using the Company's computers, information systems, and networks, “you” – user of College computing resources, assume personal responsibility for acceptable use in conformity with this policy, other applicable XYZ policies, and with applicable federal, state, and local laws and regulations.

All communications and information transmitted by or through, received by or from, or stored in these systems are XYZ records and property of XYZ. You have no right of personal privacy in any matter stored in, created, received, or sent over XYZ computers, storage devices, email, internet, or voicemail system. This includes and is not limited to: Citrix, databases, employee Information System – SonisWeb, Blackboard, Simplicity, in-house software applications, all externally hosted software applications and the following site: www.xyz.com and any other www.xyz.* web domain name.

Be aware that even deleted or erased computer, e-mail and voicemail messages may remain stored in XYZ computer servers or telephone systems. By placing information on XYZ's computer systems or servers, or using any XYZ equipment, you have consented to XYZ's right to capture, edit, delete, copy, republish and distribute such information.

The XYZ Harassment and Bullying Policies and XYZ policy with respect to Confidential Information apply to all forms of communication including written, e-mail and voicemail.

XYZ provides access to Internet services such as web-browsing. Use of the Company's internet services are only for educational use. This restriction includes any Internet service which is accessed on or from XYZ's premises using XYZ's computer equipment or via XYZ-paid access methods and/or used in a manner that identifies you with XYZ. This also includes remote access such as Citrix and the MyLIM portal.

The following is a non-exclusive list of prohibited use of XYZ technology resources. In a constantly changing world of information technology, it is impossible to enumerate all non-acceptable uses of XYZ computers, information systems, and networks. XYZ reserves the right to prohibit any use of its computing facilities by any person(s) if and when such use appears to be inconsistent with this policy, other computer use policies, the mission of the College, or any applicable federal, state or local law.

Prohibited uses:

All users may not…

1. Attempt to use technology resources without proper authorization;
2. Attempt to obtain privileges or access for which you are not authorized;
3. Attempt to learn another user's password(s) or personal information;
4. Attempt to alter or obscure your identity or your computer's identity, including but not limited to IP Address and email address, while communicating on any network, system or application;
5. Attempt to access, modify and/or delete another user's files, configuration or application without the expressed agreement of the owner or by an XYZ Administrator;
6. Share confidential computer, system, application, or network password with any other person;
7. Attempt to interfere with or disrupt computer or network accounts, services or equipment of others including, but not limited to, consumption of excessive IT resources, (e.g. local area network or Internet bandwidth) through the propagation of worms, Trojans, or viruses;
8. Attempt to "crash" any College computing facilities, including any so-called "denial of service attack";
9. Attempt to monitor, intercept, analyze or modify network traffic or transactions;
10. Attempt to alter or reconfigure any XYZ IT resources, (e.g. network infrastructure, servers, wireless);
11. Attempt to use unauthorized devices when connecting to the XYZ network – view device policy on the XYZ Website - "Policy for Connecting Devices to the XYZ Network";
12. Attempt to remove, duplicate or export confidential / sensitive XYZ data in any digital format, outside of XYZ systems and network, without prior written consent by an XYZ administrator. This includes any/all data stored: on-premise and/or externally hosted third party provider.
    - Examples of confidential / sensitive information include, and are not limited to: social security numbers; financial account information; Family Education Rights and Privacy Act (FERPA) protected records, Health Insurance Portability and Accountability Act protected records; employee records; and accounting records.
    - Contact the IT Department or an XYZ Administrator for more information.
13. Attempt to use computing or network resources for profit or commercial gain outside of official XYZ business; {For students use?}
14. Download and/or share copyrighted material for which you do not have the proper authorization – view email policy on the XYZ Website - "XYZ - P2P Policy";
15. Attempt to copy software or any intellectual property in a manner that appears to violate copyright law, or otherwise infringing on any intellectual property rights of others;
16. Compose, transmit, or access data containing content that could be considered discriminatory, offensive, pornographic, obscene, threatening, harassing, intimidating, or disruptive to any other person. Examples of unacceptable content may include, but are not limited to, sexual comments or images, racial slurs, gender-specific comments, or any other comments or images that could reasonably offend someone on the basis of race, color, religion, creed, sex, gender, gender identification, sexual orientation, ethnicity, national origin, ancestry, age, disability (including HIV-AIDS status), marital status, military status, citizenship status, predisposing genetic characteristics, or any other characteristic protected by law.
17. Abuse email privileges – view email policy on the XYZ Website - "Electronic Mail (email) Policy and Procedure";
18. Consume any food or drink in any XYZ computer lab.

Federal, State and Local Laws:

All computer and network users are bound by applicable federal, state, and local laws relating to harassment, copyright, security, and privacy relating to digital media. The IT Department will cooperate fully with any local, state or federal law enforcement officials investigating any illegal use of XYZ information technology resources. View laws on the XYZ Website – "Technology – Federal, State, and Local Laws – XYZ"

IT Department Responsibilities:

Beyond controlling access and protecting against unauthorized access and computer or network threats, the IT Department plays a proactive role in developing, implementing and enforcing security or network procedures. Using hardware infrastructure and software tools, utilities and applications, the IT Department will maintain a network and computing environment enabling authorized campus users secure, reliable access to internal and external networking resources and applications.

The IT Department will respect and strive to ensure users' privacy and intellectual property while managing the computing and network infrastructure and information application transactions and data.

At times the IT Department may need to reconfigure network and/or computing resources. These actions include, but are not limited to, temporarily disabling access to an individual system, temporarily disabling access to/from a specific segment of the XYZ Local Area Network. Though rare and short in duration, these steps are necessary to isolate problems and threats, enable quick resolution, as well as for periodic system maintenance/upgrades.

Policy Enforcement:

XYZ at all times retains the right, without notice, to search all directories, indices, data storage devices of any type, files, databases, e-mail messages, voicemail messages, Internet access logs and any other electronic transmissions contained in or used in conjunction with XYZ's computer, e-mail, voicemail and Internet access systems and equipment.

IT Department senior staff and administrators will investigate alleged violations of this policy in order to ensure compliance. The IT Department may restrict individuals from the use of computers and networks where violations of this policy or federal, state, or local laws is suspected and/or found. Violations of this policy by a employee may result in disciplinary action.