Appropriate Use of Clark's Information Technology System Policy

Section 1. PURPOSE AND SCOPE

This policy sets forth standards for responsible and acceptable use of Clark University's Information Technology Systems (ITS) resources. These resources include computer systems, computer labs, applications, networks, software, electronic communications and information sources, web pages, and related services.

The policy is based on the principle that the electronic information environment is provided to support University business and its mission of education, research and service. All other uses are secondary. These resources are made available for the sole use of university faculty, staff, students, and other authorized guests to accomplish tasks related to and consistent with the university's mission. Information technology resources are limited, and should be used wisely and with consideration for the rights and needs of others. Prohibited are activities that jeopardize the integrity of the system; consume an unfair share of resources; infringe upon the privacy of other users; or threaten the actual or perceived safety of others; or that are illegal.

All members of the Clark University community, including faculty, staff and students should be familiar with this policy. This policy applies to all university-owned content and devices as well as all privately-owned devices that connect to our network.

Section 2. PROCEDURES AND ENFORCEMENT

Users who violate this policy may be denied access to University computing resources and may be subject to disciplinary actions and/or criminal and civil penalties. Violations will normally be handled through the University disciplinary procedures applicable to the relevant user and may include referring suspected violations of applicable law to appropriate law enforcement agencies. However, the University may immediately suspend or block access to an account, prior to the initiation or completion of such procedures, when it appears necessary to do so in order to protect the integrity, security or functionality of University or other computing resources, or to protect the University from liability.

In addition, with appropriate authorization, the University will investigate complaints received from both internal and external sources about alleged violations of Clark's computing facilities and/or computer network. Requests to access or disclose the content of electronic files and/or communications will be handled within the following guidelines:

If the alleged violation involves a:	Then permission must be obtained from:
Faculty Member, Student	Provost
Staff Member (including student employees)	Director of Human Resources
Alumni or Alumnae	Vice President for University Advancement

Permission may also be granted by the Title IX Coordinator, the Executive Vice President, and the Vice President for Information Technology and CIO. All requests to access or disclose the content of electronic files, including detailed information on why the request is being made, should be sent from the appropriate person authorized above to the Assistant Vice President for Information Technology for processing.

Section 3. BASIC PRINCIPLES

As a user of Clark University's IT resources, you have a reasonable expectation of privacy and fair access to those resources within the limits described below. You are responsible for respecting the privacy of other users and for protecting access to your account. You also are responsible for properly utilizing resources and avoiding any activity that would have a detrimental effect on the work of others. You should take appropriate precautions to ensure the security of passwords and prevent others from obtaining access to your computer resources.

Section 4. PRIVACY AND MONITORING

While the University respects the privacy of electronic communications and makes every attempt to keep electronic information secure, privacy is not guaranteed. The maintenance, operation, and security of ITS resources require responsible university personnel to monitor and access systems and networks. The content of electronic communications will not be accessed during the routine execution of systems support, network performance, and related security functions; but system administrators may access and disclose such contents when access and disclosure are necessary to protect the integrity of information technology resources, to ensure that these resources are equitably shared, to respond to health and safety emergencies, or to respond to subpoenas, court orders, or other valid forms of legal process. Where there is evidence of a criminal offense, the matter will be reported to Clark's judicial systems and/or law enforcement. The University will cooperate with the justice system in the investigation of the alleged offense.

Section 5. SECURITY

Although it is the University's intention to provide and preserve the security of files, account numbers, authorization codes and passwords, security can be breached through actions or causes beyond its reasonable control. The University cannot guarantee the absolute security, confidentiality and privacy of electronic content. It is the user's responsibility to safeguard data, personal information, passwords, and authorization

codes; to take full advantage of security mechanisms built into systems; to choose passwords wisely and change them periodically; and to follow any security policies and procedures related to the access and use of data. For secure remote access to computing resources at Clark, the University provides a Virtual Private Network (VPN) for use by students, employees and authorized third parties. Users of the Clark VPN are a de facto extension of Clark University's network and subject to the requirements of this policy. For more information on the requirements for using the VPN for access to Clark University's computing resources see Clark University's Remote Access Policy.

Section 6. FAIR ACCESS

Information Technology Services, and other University departments which operate and maintain computers, network systems and servers, expect to maintain an acceptable level of performance and must assure that frivolous, excessive, or inappropriate use of the resources by one person or a few people does not degrade performance for others. The University may choose to set limits on an individual's use of a resource through quotas, time limits, and other mechanisms to ensure that these resources can be used by anyone who needs them.

Section 7. OPEN EXPRESSION

The University cherishes the diversity of values and perspectives that are part an academic institution and so is respectful of freedom of thought, inquiry and expression. Users are free from censorship in expressing their views through electronic communications facilities (including, but not limited to, e-mail and "chat" programs) as long as their views are not represented as the views of Clark University. Within this framework of free expression, however, users are not to use University information technologies to originate, disseminate, or store material that intimidates, threatens, or harasses individuals or groups in violation of law or University policy, endangers the security of University information technologies resources, or violates other state law, federal law or University policy.

Computers and networks provide access to resources on and off campus, as well as the ability to communicate with other users worldwide. It is important that users recognize that such open access carries some risk of access to information that might be considered offensive or unorthodox. Users are advised to take responsibility for their own use and navigation of these resources.

Section 8. COPYRIGHT AND LICENSED MATERIAL

Copyright is a form of intellectual property protection provided by the laws of the United States to the authors of original works of authorship including literary, dramatic, musical, artistic, and certain other intellectual works. You should assume materials you find on the Internet, or software you use on campus, are copyrighted unless a disclaimer or waiver is expressly stated. If you do not abide by these legal and contractual restrictions, you may be subject to civil or criminal prosecution.

There are many misconceptions regarding copyright, fair use, and the academic use of copyrighted materials. Although this is not an exhaustive list, you are likely to violate copyright by:

- Displaying pictures or graphics you have not created in a course or within a PowerPoint presentation.
- Offering/sharing sound recordings you have not recorded yourself. Even if you have recorded them, you must have permission from the copyright holder.
- Placing any materials owned by others, (i.e. copyrighted works) on your Web page, course web site (even if it is password-protected), or in any other publicly accessible location, without the expressed permission of the copyright owner (i.e., cartoons, photographs, songs, movies, software, graphics scanned in from published works or other web pages).
- Reselling, copying or giving away licensed programs or data.
- Using educational-licensed programs/data for non-educational or unintended purposes.
- Using programs/data without being among the individuals/groups licensed to do so.
- Making Clark license keys publicly available without authorization.

Read the full Copyright Compliance Policy for more specific information.

Section 9. ADHERENCE TO OTHER FEDERAL STATE AND LOCAL LAWS

As a member of the Clark community, you are expected to abide by this policy as well as other relevant University policies, local ordinances, state law, and federal law. The University reserves the right to limit or refuse access to its information resources and networks when applicable University policies, contractual obligations, or state or federal laws are violated.

Section 10. PROHIBITED ACTIVITIES

The following list describes prohibited conduct that is based on the principles above. The list is not comprehensive but serves to illustrate and help interpret this policy.

- Revealing passwords or otherwise permitting the use by others (by intent or negligence) of personal accounts for computer and network access.
- Using or accessing restricted University computer resources or electronic information without or beyond one's level of authorization.
- Attempting to access, or accessing another user's accounts, private files, e-mail messages, or intercepting network communication without the owner's permission except as appropriate to your job duties and in accordance with legitimate university purposes.
- Knowingly performing an act which will interfere with the normal operation of computers, systems, peripherals, or networks.

- Knowingly running or installing on any computer system or network, or giving to another user, a program intended to disrupt, damage, or place excessive load on a computer system, service or network (e.g., the propagation of computer "worms" and "viruses", the sending of electronic chain mail, etc.).
- Misrepresenting oneself as another individual in electronic communication.
- Installing, copying, distributing, or using electronic content (including software, music, text, images, and video) without the consent of the publisher, author or copyright holder.
- Engaging in conduct that interferes with others' use of shared IT resources.
- Using University IT resources for political or personal economic gain (except as covered by the university's Intellectual Property Policy.
- Unauthorized access, possession, or distribution, by electronic or any other means, of electronic information or data that is confidential under the University's policies regarding privacy or the confidentiality of student, administrative, personnel, archival, or other records.
- Using IT resources for illegal activities. Criminal or illegal use may include obscenity, child pornography, threats, harassment, copyright infringement, university trademark infringement, defamation, theft, identity theft, and unauthorized access.
- Making available any materials, the possession or distribution of which is illegal.
- Unauthorized scanning of networks for security vulnerabilities.
- Unauthorized wiring, including attempts to create unauthorized network connections, or any unauthorized extension or re-transmission of any computer or network services;

Related Policies and Regulations

Remote Access Policy

Copyright Compliance Policy

University's Intellectual Property Policy

History/Revision Information

Responsible Office/ Division: ITS

Effective Date: February 2, 2008
Last Amended Date: September 20, 2018
Next Review Date: September 20, 2023