Information Technology Appropriate Use Policy (AUP)

Policy Statement
This policy sets forth standards for responsible and acceptable use of Heritage University’s Information Technology (IT) resources. These resources include computer systems, computer labs, applications, networks, software, electronic communications and information sources, telecommunication devices and equipment, web pages, and related services.

Reason for Policy/Purpose
The Heritage information technology 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; threaten the actual or perceived safety of others; or are illegal.

Who Needs to Know This Policy
All members of the Heritage University community, including faculty, staff, students and authorized guests and contractors 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.

Website Address for this Policy
TBD

Contacts
Additional information, questions and comments may be directed to the Director of Information Technology, James Bush, Bush_J@Heritage.edu
Definitions

N/A

Policy Standard/Procedures

Guiding Principles

• Privilege of Use: Access to and use of the Heritage University computing resources is a privilege. All equipment and the software, applications, data, and scripts residing on this equipment or in transit to or from it are the property of the University.

• Privacy: Users of Heritage University’s IT resources have a reasonable expectation of privacy and fair access to those resources. 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 IT resources require responsible university personnel to monitor and access systems and networks. Heritage University does not routinely monitor or access the content of electronic files or messages whether stored on University equipment or in transit on the University network. System administrators may, however, 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.

• Security: Heritage University will take all available means to provide and preserve the security and integrity of data, files, account numbers, authorization codes and passwords through secure servers, system backups, virus control software, firewalls and other mechanisms. It is the user's responsibility to safeguard their 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 or as required; to prevent others from obtaining access to assigned computer resources and to follow security policies and procedures related to the access and use of data.

• Fair Use: Users are responsible for properly utilizing resources and avoiding any activity that would have a detrimental effect on the work of others. It is the responsibility of the University to ensure 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.

• The University reserves the right to limit or refuse access to its information resources and networks in order to protect the confidentiality, integrity, availability or functionality of technology resources or when applicable University policies or codes, contractual obligations, or state or federal laws are violated.
Prohibited Activities

- Revealing passwords or otherwise permitting the use by others (by intent or negligence) of personal accounts for computer and network access.
- 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.
- Copying software, applications, databases, program code or scripts of any sort to or from University computers unless authorized by the University IT Department.
- 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.
- Attaching and/or installing equipment, devices, software or applications not owned by or licensed to the University unless authorized by the University IT Department.
- Unauthorized moving or removing of equipment or devices.
- Installing, copying, distributing, or using electronic content (including software, music, text, images, and video) without the consent of the publisher, author or copyright holder.
- Misrepresenting oneself as another individual in electronic communication.
- Attaching and/or installing equipment, devices, software or applications not owned by or licensed to the University unless authorized by the University IT Department.
- Unauthorized moving or removing of equipment or devices.
- Installing, copying, distributing, or using electronic content (including software, music, text, images, and video) without the consent of the publisher, author or copyright holder.
- Misrepresenting oneself as another individual in electronic communication.

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.

Forms/Instructions
N/A
Related Policies and Resources

- Data Security Policy
- Handheld and Portable Device Access Policy
- Copyright Policy
- 1.3.4 Records Management Policy