3.a Information Technology Appropriate Use Policy

Responsible Office	Information Technology		
Effective	5/10/2016		
Revised	1/13/2021		
Last Reviewed	1/13/2021		
Compliance			
Classification	☒ Institutional	☐ Board of Directors	☐ Local unit(s):
Approving Body	☒ President's Council	☐ Board of Directors	☐ Unit VP

Policy

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. This policy applies to all who use Heritage University technology.

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. See Heritage University Copyright Policy.
- Engaging in conduct that interferes with others' use of shared IT resources.
- Using University IT resources for political or personal economic gain.
- 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;

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.

Related Documents

Records Management Policy
Data Security
Copyright Compliance