LHU Policy No – LHU-54
Original Date – 2010
Last Review Date – February 17,2021
Last Update Date – February 17, 2021
Next 5-Year Review Date – April, 2025

LOCK HAVEN UNIVERSITY
INFORMATION TECHNOLOGY ACCEPTABLE USE POLICY

1. Purpose

This policy addresses the use of information technology resources (IT resources) at Lock Haven University ("the university"). IT resources are intended to support the university's instructional, research, and administrative operations.

2. Scope

This policy applies to all users of IT resources owned or operated by Lock Haven University. Users include students, faculty, staff, contractors, and guest users of computer network resources, equipment or connecting resources. **Use of the university's IT resources signifies agreement to comply with this policy.**

3. Objective

The objective of this policy is to create a framework to ensure that IT resources are used in an appropriate fashion, and support the university's mission and institutional goals.

4. Policy

Use of the university's IT resources is a privilege and signifies agreement to comply with this policy. Users are expected to act responsibly, and follow the university's policies and any applicable laws related to the use of IT resources. This policy provides regulations to assure IT resources are allocated effectively.

While the university recognizes the role of privacy in an institution of higher learning, and will endeavor to honor that idea, there should be no expectation of privacy of information stored on or sent through university-owned IT resources, except as required by law. For example, the university may be required to provide information stored on IT resources to someone other than the user as a result of a court order, investigatory process, or in response to a request authorized under Pennsylvania's Right-to-Know statute (65 P.S. §67.101 et seq.). Information stored by the university may also be viewed by technical staff working to resolve technical issues.

5. Definitions

Information Technology (IT) resources include, but are not limited to, all university owned or operated hardware, software, computing equipment, systems, networks, programs, personal data assistants, cellular phones, fax machines, telephones, storage devices, cable television, security and surveillance systems, input/output, connecting devices via either a physical or wireless connection regardless of the ownership of the device connected to the network, and any electronic device issued by the university. IT resources include all electronic media, voice, video conferencing and video networks, electronic mail, and related mediums such as blogs, wikis, websites and electronic records stored on servers and systems. IT resources may be physically located on university premises, at a partner site, or within a cloud provider's infrastructure.

6. Responsibilities

A. Responsibilities of Users of IT Resources

1. Respect the intellectual property of authors, contributors, and publishers in all media.
2. Protect user account identification, password information, and all system(s) access from unauthorized use. Every user is accountable for all activities done via their account.
3. Report lost or stolen devices, especially devices that contain private or university information to the IT Department within 24 hours of discovery of the loss.
4. Adhere to the terms of software licenses and other contracts. Persons loading software on any university computer or device must adhere to all licensing requirements for the software. Except where allowed by university site licenses, the copying of university-licensed software for personal use is a violation of this policy.
5. Comply with federal, state and local laws, relevant university personal conduct regulations, and the terms and conditions of applicable collective bargaining agreements. Applicable laws include, but are not limited to, those regulating copyright infringement, copyright fair use, libel, slander and harassment.
6. Become acquainted with laws, licensing, contracts and university policies and regulations applicable to the appropriate use of IT resources. Users are expected to use good judgment and exercise civility at all times when utilizing IT resources, and respect the large, diverse community utilizing these resources in a shared manner.
7. Understand the appropriate use of assigned IT resources, including the computer or device, network address or port, software and hardware.
8. University business conducted by e-mail will be via the university's mail server accessed by the <username>@lockhaven.edu account assigned to the individual by the IT Department. Electronic mail should never be considered an appropriate tool for confidential communication and any content should adhere to the responsibilities put forth in this policy. Messages can be forwarded and printed, and some users permit others to review their e-mail accounts. Message content can be revealed as part of legal proceedings. Finally, messages are sometimes not successfully delivered due to technical issues requiring authorized IT personnel to review message content as part of the troubleshooting process.

B. Prohibited Uses of IT Resources

1. Providing false or misleading information to obtain or use a university computing account or other IT resources.
2. Unauthorized use of another user's account and/or attempting to capture or guess passwords of another user.
3. Attempting to gain or gaining unauthorized access to IT resources, files of another user, restricted portions of the network, an operating system, security software, or other administrative applications and databases without authorization by the system owner or administrator.
4. Operation of servers, switches, routers, hubs, wireless access points (including devices that act as wireless access points), or any other multi-host connection device by any user without express written permission of the IT Department.
5. Performing any act(s) that interfere with the normal operating, proper functioning, security mechanisms or integrity of IT resources.
6. Use of IT resources to transmit abusive, threatening, or harassing material, chain letters, spam, or other communications prohibited by law.
7. Copyright infringement, including illegal sharing of video, audio, software or data.
8. Use of unauthorized peer-to-peer file sharing applications for the purpose of illegally downloading or distributing copyrighted material.
9. Excessive use that overburdens or degrades the performance of IT resources to the exclusion of other users. This includes activities which unfairly deprive other users of access to IT resources or which impose a burden on the university. Users must be considerate when utilizing IT resources. The University reserves the right to set limits on a user through quotas, time limits, bandwidth shaping, and/or other mechanisms.
10. Intentionally or knowingly installing, executing, or providing to another, a program or file, on any of the IT resources that could result in the damage to any file, system, or network. This includes but is not limited to computer viruses, trojan horses, worms, spyware, or other malicious programs or files.
11. Excessive or prohibited personal use by employees.
12. Use of university IT resources for personal profit, commercial reasons, non-university fundraising, political campaigns, or any illegal purpose. The prohibition against using university IT resources for personal profit does not apply to:
    i. Scholarly activities, including the writing of textbooks or preparation of other teaching material by faculty members
    ii. Other activities that relate to the faculty member's professional development
    iii. Other activities as approved by the University President
13. Use of IT resources for non-authorized solicitations on behalf of individuals, groups, or organizations.

7. Procedures

A. Violations of this policy will be reported to appropriate levels of administrative oversight, depending on the statutes and policies violated. Suspected violations of federal and state statutes and local ordinances shall be reported to the Director of Public Safety (chief of campus police) for official action.

B. Non-statutory violations of this policy, such as “excessive use”, may be reported to the Chief Information Officer, the Director of Human Resources, the Dean of Student Affairs and/or the Director of Public Safety (chief of campus police).

C. A university employee or student who violates this policy risks a range of sanctions imposed by relevant university disciplinary processes, including denial of access to any or all IT resources. He or she also risks referral for prosecution under applicable local, state, or federal laws.

D. The University reserves the right to take immediate action in disabling accounts and/or blocking network access in the event the usage policy is violated and the offending action is detrimental to other users or IT resources.

E. The University President’s Senior Staff – via the Information Technology Department – is responsible for recommending the university’s Acceptable Use Policy. Questions regarding the applicability, violation of the policy, or appropriate access to information should be referred to the Chief Information Officer

8. Publications Statement

This policy should be published in the following publications:

A. Administrative Manual
B. Student Handbook
C. University Catalog
D. University Website

9. Distribution

A. All Employees
B. All Students
C. All affiliates with access to IT resources at the University

Revised February 2021