Acceptable Use Policy for University Computer Labs DRAFT

Policy Title:
Acceptable Use Policy for University Computer Labs

Responsible Executive(s):
Jim Pardonek, Director and Chief Information Security Officer

Responsible Office(s):
University Information Security Office

Contact(s):
If you have questions about this policy, please contact the University Information Security Office.

I. Policy Statement

The Acceptable Use Policy for University Computer Labs ensures a safe, secure, and productive environment for academic and research activities. The policy prioritizes lab use for educational purposes and mandates respectful behavior to maintain a conducive environment. It strictly prohibits unauthorized access, malicious activities, inappropriate content, commercial use, and misuse of resources. Users must comply with software licensing agreements and are prohibited from tampering with hardware. The policy emphasizes the importance of data privacy and security, both personal and university related. Compliance is enforced through monitoring, and violations may result in disciplinary action.

II. Definitions

Not applicable.

III. Policy

Introduction

This Acceptable Use Policy (AUP) outlines the expectations and responsibilities of all users of the computer labs at Loyola University Chicago. These guidelines are designed to ensure a safe, secure, and productive environment for academic and research activities.

Purpose

The purpose of this policy is to ensure that the computer labs are used in a manner that is ethical, legal, and conducive to the university's academic mission.

Scope

This policy applies to all students, faculty, staff, and authorized visitors using the university computer labs.

General Guidelines

- *Priority Use: Computer labs are primarily for academic use. Priority is given to users engaged in educational, research, and university-related activities.*
- *Respect for Others: Users must be considerate of others and avoid activities that may disrupt the lab environment. This includes keeping noise levels low and not monopolizing shared resources.*
- *Access Control: Users must use their own university credentials to access lab computers. Sharing login information is prohibited.*

Prohibited Activities

- *Unauthorized Access: Attempting to gain unauthorized access to any network, system, or data is strictly prohibited.*
- *Malicious Activities: The use of lab resources to engage in activities such as hacking, spreading malware, or conducting denial-of-service attacks is forbidden.*
- *Inappropriate Content: Accessing, creating, or distributing material that is obscene, harassing, or otherwise inappropriate is not allowed.*
- *Commercial Use: Using lab resources for commercial purposes or personal financial gain is prohibited.*
- *Resource Misuse: Excessive use of resources, including bandwidth, storage, or computational power, for non-academic purposes is not allowed.*
- *Software and Hardware Use*
- *Licensed Software: Users must adhere to all software licensing agreements and may not install, copy, or distribute software without proper authorization.*
- *Hardware Tampering: Modifying or tampering with lab hardware or network configurations is prohibited.*

Data Privacy and Security

- *Personal Data: Users are responsible for the security of their own data. It is recommended to save work frequently and back up important files.*
- *University Data: Unauthorized access, use, or disclosure of university data is prohibited.*

Compliance and Enforcement

- *Monitoring: The University reserves the right to monitor the use of lab resources to ensure compliance with this policy.*
- *Violations: Violations of this policy may result in disciplinary action, including loss of lab access privileges, university disciplinary measures, and legal action.*

Reporting Issues

Technical Support: For technical assistance, users should contact the university's ITS Service Desk.

Policy Violations: Suspected policy violations should be reported to the lab supervisor or Information Technology Services.

IV. Related Documents and Forms

Not applicable.

V. Roles and Responsibilities

Jim Pardonek, Associate Director and Chief Information Security Officer	Enforcing the Policy at the University by setting the necessary requirements.

VI. Related Policies

Please see below for additional related policies:

- Acceptable Use Policy

Approval Authority:	ITESC	**Approval Date:**	
Review Authority:	Jim Pardonek	**Review Date:**	
Responsible Office:	UISO	**Contact:**	datasecurity@luc.edu