University Policy

Volume I1: Information Technology	**I1.01.1 Acceptable Use of Information Technology Resources**	**Responsible Office:** University Technology Services
Chapter 01: Acceptable Use	**Effective Date:** 01/01/2007 **Last Revised:** 07/29/2022 **Date of Next Review:** 07/01/2027	**Responsible Officer:** Chief Information Officer

POLICY STATEMENT

Northeastern Illinois University's (the "University") Information Technology Resources (ITR) exists to support the mission of the University and are to be used appropriately and in accordance with this policy, related policies, as well as local, state and federal laws.

PURPOSE OF THE POLICY

This Policy sets out the direction, expectation, and guidelines for use of the University's ITR including, its network and network resources, hardware and software (including applications), remote technology, communications facilities, and data.

WHO IS AFFECTED BY THIS POLICY

- All users of University Information Technology Resources (ITR)
- All users who conduct University business using its ITR either from the University's networks or external networks.

DEFINITIONS

Information Technology Resources (ITR) - all electronic and technology facilities, services, devices and data used for information processing, transfer, storage, display, printing, and communications by NEIU. These include, but are not limited to, networks, computer hardware and software, computer labs, classroom technologies such as computer-based instructional management systems, computing and electronic communications devices and services, modems, email, faxes, telephones, voicemail, video, multi-function printing devices, mobile devices, multimedia and instructional materials, and third-party hosted services used to conduct NEIU business.

User - An individual or entity authorized to use NEIU Information Technology Resources (ITR).

REGULATIONS

Illinois Criminal Code of 2012 (720 ILCS 5/16D-3, 720 ILCS 5/26.5-2)

University Information Technology Resources are to be used to advance the University's mission. Students, faculty and staff may use these resources only for purposes related to their studies, their responsibilities for providing instruction, the discharge of their duties as employees, their official business with the University, and other University-sanctioned or authorized activities.

The use of the University's ITR must be done responsibly, ethically and reflect academic honesty and reasonable consumption of these resources. Users must respect and adhere to policies that protect ownership and/or stewardship of data (including intellectual property information), system security, and individuals' rights to privacy and to freedom from intimidation and harassment. Users will be held accountable for their use of University ITR.

ACCEPTABLE USE

The University acknowledges that all employees and students occasionally use University ITR assigned to them or to which they are granted access for non-commercial, personal use. Such occasional non-commercial uses are permitted, provided they are not excessive, do not interfere with the University or its technology resources, and are not otherwise prohibited in any way. Decisions as to whether a particular use of information technology resources does not conform to the Acceptable Use of ITR policy shall be made by the Chief Information Officer, along with the Office of Academic Affairs if the use involves faculty or student academic matters, the Office of Student Affairs if the use involves non-academic student use, or the Office of Human Resources if the use involves non-academic administration.

ITR must only be used for legal purposes and must not be used for any of the following purposes or any other purpose which is illegal, unethical, or likely to subject the University to liability. Unauthorized uses (some of which may also constitute illegal uses) include, but are not limited to, the following:

- Political activities
- Commercial purposes outside the scope of academics or employment.
- Harassment
- Libel, slander
- Fraud, impersonation, or misrepresentation
- Destruction of or damage to equipment, software, or data belonging to the University or others
- Disruption or unauthorized monitoring of electronic communications
- Unauthorized scanning of NEIU networks
- Unauthorized use of the University's trademarks, logos, insignia, or copyrights
- Using unauthorized copyrighted materials in ways that fall outside of fair use
- Violation of software license agreements or installation of software that stores and processes University data without authorization by UTS (UTS has the authority to determine the software that is authorized for use)
- Violation or circumvention of computer system/network security
- Unauthorized use of computer accounts, access codes (including passwords), or network identification numbers (including e-mail addresses) assigned to others
- Accessing, without authorization, data stored within the ITR
- Use of University ITR in ways that unnecessarily interfere with work or studies, impede or disrupt the University's wider IT systems (*e.g.* spreading of any form of virus or malware), that cause excess streaming of unauthorized internet content sufficient to impede normal use of resources, or harm the University's reputation, bring it into disrepute, or incur liability on the part of the University
- Use of University IT resources to solicit charitable funds without an approved charitable solicitation agreement with Institutional Advancement.
- Development or use of unauthorized mailing lists for the use of solicitation or advertisement
- Use of computing facilities for private business purposes
- Academic dishonesty
- Student Conduct Code violations
- Violation of University policies and all federal, state, and applicable local laws.
- Violation of privacy

- Downloading, displaying, posting, sending, viewing, printing, distributing or otherwise communicating material (absent a legitimate academic or research purpose) that is contrary to the mission or values of the University including any content that is pornographic, illegal, obscene or defamatory, or in connection with activities (such as impersonation, bullying or harassing, malicious, discriminatory, offensive or abusive comments about ethnicity or nationality, gender, disability, age, sexual orientation, appearance, religious belief and practice, political belief or social background, to promote acts of violence, or to promote extremist ideologies and activities associated with terrorist groups) which could result in criminal or civil actions against an individual and/or the University.
- Child pornography. The downloading, displaying, posting, sending, viewing, printing, distributing or otherwise communicating any child pornography is a violation of federal and state law and must be immediately reported to University Police at (773) 442-4100
- Intentional or negligent distribution of malicious software
- Using ITR to violate any university policy, regulation or federal, state, or other applicable law
- Using ITR for profit or commercial purposes
- Using the resources to interfere with the normal operation of the University

ENFORCEMENT

The University considers any violation of the Acceptable Use of ITR policy to be a significant offense and reserves the right to disconnect and suspend violators' use of ITR. Violations of the Acceptable Use of ITR policy shall be subject to discipline in accordance with procedures outlined in the relevant collective bargaining agreements, handbooks, policies, Student Code of Conduct, procedures, practices, or contracts and may result in loss of their computing privileges and other measures, up to and including expulsion from the University, or loss of employment. Illegal acts involving University ITR may also subject violators to prosecution by local, state, and/or federal authorities.

USER RESPONSIBILITY

- User accounts, passwords, and other authentication IDs are assigned to individual users and must not be shared
- Follow all University IT policies
- Any protective/defensive software and tools (e.g. anti-malware/virus software, Multifactor Authentication (MFA), VPN) provided through University Technology Services must be used in the manner specified by UTS
- Users have the responsibility to abide by existing regulations for the protection of sensitive institutional data (Refer to the I1.02.2 Information Incident Security Management policy for specific guidelines and information)

EXTERNAL NETWORKS

Members of the University community who use networks, facilities, or computers not owned by the University shall adhere to this Acceptable Use of ITR policy when conducting University business, and shall adhere to all policies and procedures established by the administrators of non-University networks, facilities, or computers they use. Whether or not an external policy exists for non-University information technologies, the Acceptable Use of ITR policy shall remain in effect and shall be adhered to by members of the University community at all times when doing Northeastern Illinois University-related work.

UNIVERSITY RESPONSIBILITY

1. Privacy and Confidentiality

The University reserves the right to inspect and examine any electronic content on any Northeastern Illinois University-owned or operated communications system, computing resource, or other mobile

or electronic device at any time. Any monitoring of a specific individual's voice mails, email exchanges, internet use, or personal computer files, shall be done only with reasonable suspicion of improper conduct and with written notice, when necessary. The Chief Information Officer or designee must approve any request to monitor, inspect or examine electronic content on any University-owned or operated communications system, computing resource or other electronic devices.

When sources outside the University request an inspection and/or examination of any Northeastern Illinois University-owned or operated communications system, computing resource, and/or files or information contained therein, the University will treat information as confidential unless any one or more of the following conditions exist:

- When approved by the Chief Information Officer or designee
- When authorized by the owner(s) of the information (Note: the University is the owner)
- When required by federal, state, or local law
- When required by a valid subpoena or court order

The University reserves the right to inspect and examine any electronic content on any Northeastern Illinois University owned or operated communications system, computing resource, cell phone, or other mobile or electronic device for work continuity purposes. For example, where an employee is away for a prolonged absence and it is necessary to retrieve such content.

Users of electronic mail systems should be aware that electronic mail is not one hundred percent secure and could therefore be vulnerable to unauthorized access and modification. Nothing should be written in an e-mail message that would not be put in a paper memo.

Users should also be aware that public records may be requested and obtained under the Illinois Freedom of Information Act (FOIA), and thereafter be made public. Subsection 2(c) of the Act defines the term "public records" to include all records, reports, forms, writings, letters, memoranda, books, papers, maps, photographs, microfilms, cards, tapes, recordings, electronic data processing records, recorded information and all other documentary information having been prepared, or having been or being used, received, possessed or under the control of any public body. It is the sole responsibility of the University's counsel to determine records that would be considered "exempt" from disclosure.

2. Reference and Links to External Content

As part of the services available through the Northeastern Illinois University ITR, the University provides access to a large number of conferences, lists, bulletins boards, and internet information sources. Information in the many World Wide Web pages that are linked to Northeastern Illinois University's web presence comes from a variety of sources. These materials are not affiliated with, endorsed by, edited by, or reviewed by Northeastern Illinois University. Northeastern Illinois University has no control over and is not responsible for the accuracy or completeness of the contents of any unofficial page. Moreover, some of these sources may contain materials that may be offensive or objectionable to some users.

PROCEDURES

All members of the University community are responsible for adhering to the procedural rules and directives outlined within the Regulations section of this policy.

GUIDELINES

Employees or students who receive emails with objectionable content (as described in the Acceptable Use list) from other employees or students of the University, or external parties, should report the matter to their line manager or academic supervisor.

HISTORY

10/20/2008 – Revised; edited various regulation information
06/30/2009 – Revised; edited responsible office
12/10/2009 – Revised; reformatted document
10/12/2015 – Revised; revisions to sections 2 and 5.1
06/24/2020 – Revised; edited procedures, unauthorized use
09/22/2021 – Revised; comprehensive 5-year review
07/29/2022 – Revised; updated policy links and refreshed content

RELATED POLICIES AND OTHER INFORMATIONAL MATERIAL

Information Incident Security Management
Identity Protection
Strong Password
Software Applications Security
University EMail
Student Code of Conduct

CONTACT INFORMATION

Please direct questions or concerns about this policy to:

Contact	Phone	E-Mail
Chief Information Officer	(773) 442-4357	helpdesk@neiu.edu

DISCLAIMER

The University reserves the right to modify or amend sections of this policy at any time at its sole discretion. This policy remains in effect until such time as the Responsible Officer calls for review. Requests for exception to any portion of this policy, but not to the policy statement, must be presented in writing to the Responsible Officer.