University Policy

Volume I1: Information Technology	**I1.01.1** **Acceptable Use of Information Technology Resources** **Effective Date:** 01/02/07 **Last Revision:** 10/13/2015	**Responsible Office:** University Technology Services
Chapter 01: Acceptable Use		**Responsible Officer:** Chief Information Officer

POLICY STATEMENT

Responsible, acceptable use of information must be ethical, reflect academic honesty and show restraint in the consumption of shared resources. Users must respect intellectual property, ownership and/or stewardship of data, system security methods, and individuals' rights to privacy and to freedom from intimidation and harassment. Northeastern Illinois University's (the "University") information technology resources exist to support the mission of the University and must be used appropriately and in accordance with local, state and federal laws. Users will be held accountable for their use of University information technology resources.

PURPOSE OF THE POLICY

The Acceptable Use of Information Technology Resources document constitutes the University's statement on the management of computer networks, personal computers and the resources made available thereby. Computer networks, all computers and other devices connected to those networks, and the resources made available thereby comprise the University's Information Technology Resources (ITR). The statement reflects the ethical principles of the University community and outlines the privileges and responsibilities of those using University computing resources.

WHO IS AFFECTED BY THIS POLICY

- All users of University Information Technology Resources (ITR)
- All users who conduct University business using external networks

PROCEDURES

1. ACCEPTABLE USE

University information technology resources are to be used exclusively to advance the University's Mission. Faculty, staff, and students 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 University information technology resources for commercial purposes is prohibited. Fund raising solicitation is limited to funds for University events only with the pre-approval from the Vice President for Institutional Advancement.

The University acknowledges that faculty, staff, and students occasionally use University information technology resources assigned to them or to which they are granted access for non-commercial, personal use. Such occasional non-commercial uses are permitted, if 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 conforms to the Acceptable Use of ITR policy shall be made by the Office of Academic Affairs if the use involves faculty or student academic matters, by the Office of Student Affairs if the use involves non-academic student use, or by the Office of Human Resources if the use involves administrators or staff.

2. UNAUTHORIZED USE

Computing resources may only be used for legal purposes and may 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:

- Harassment
- Libel, slander
- Fraud 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 network nodes
- Unauthorized use of the University's trademarks, logos, insignia, or copyrights
- Using unauthorized copyrighted materials
- Installing unauthorized software
- 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 computer communications facilities in ways that unnecessarily impede the computing activities of others (such as random or unsolicited interactive electronic communications or e-mail exchanges, overuse of interactive network utilities or bandwidth)
- Use of University IT resources to solicit funds for or participation in non-University events.
- Development or use of unauthorized mailing lists
- Use of computing facilities for private business purposes unrelated to the mission of the university or to university life
- Academic dishonesty
- Student Conduct Code violations
- Violation of software license agreements
- Violation of Network Usage Policies and Regulations
- Violation of privacy
- Downloading, displaying, posting, sending, viewing, printing, distributing or otherwise communicating pornographic material, absent a legitimate academic or research purpose.
- Child pornography. The downloading, displaying, posting, sending, viewing, printing, distributing or otherwise communicating child pornography is a violation of federal and state law and must be immediately reported to University Police at 773-442-4100.
- Posting or sending material that is contrary to the mission or values of the University
- Intentional or negligent distribution of malicious software such as viruses or worms
- 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

3. 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 network resources. Violations of the Acceptable Use of ITR policy shall subject users to the regular disciplinary processes and procedures of the University for students, staff, administrators, and faculty and may result in loss of their computing privileges, and other measures up to and including discharge from the University, or loss of employment. Illegal acts involving University information technology resources may also subject violators to prosecution by local, state, and/or federal authorities.

4. USER RESPONSIBILITY

- User accounts, passwords, and other types of authorization are assigned to individual users and must not be shared
- Follow all IT-applicable policies, including but not limited to: Software Applications Security, Strong Password, Identity Protection and University E-Mail
- Any protective/defensive software (e.g. virus detection) provided by University Technology Services must be used in the manner specified
- Users have the responsibility to abide by existing regulations for the protection of sensitive institutional data (Refer to the Data Security Breach 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.

5. UNIVERSITY RESPONSIBILITY

5.1. 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 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 feasible. 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 device.

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

Users of electronic mail systems should be aware that electronic mail is not secure and is, therefore, extremely 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 email copies may sometimes be requested and obtained under the Illinois Freedom of Information Act (FOIA), and thereafter be made public.

5.2. DISCLAIMER

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.

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

RELATED POLICIES AND OTHER INFORMATIONAL MATERIAL

Data Security Breach
Identity Protection
Strong Password
Software Applications Security
University E-Mail

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.