of an interview and two additional professional outfits once they accept a job or internship offer. The Power Closet is supported by donations from faculty, staff, students and community members. If you would like more information on obtaining Power Closet services or donating, please contact us at power-closet@neiu.edu or Career Development at (773) 442-4680 or ocs@neiu.edu

# POLICIES

### Acceptable Use of Information Technology Resources

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. University information technology resources exist to support the mission of Northeastern Illinois 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.

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. Fundraising solicitation is limited to funds for University-related purposes only with the pre-approval from the Vice President of Institutional Advancement.

The Acceptable Use of Information Technology Resources document constitutes the University 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.

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, and by Human Resources if the use involves administrators or staff.

### 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 or 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 network nodes
- Unauthorized use of the University's trademarks, logos, insignia, or copyrights
- Using unauthorized copyrighted materials
- Installing unauthorized licensed 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 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 Code of Conduct 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 report 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

**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.

**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 Application 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.

**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.