TECHNOLOGY USAGE POLICY

University of Northwestern and Northwestern Media

IMPORTANT - By connecting to a Northwestern network, the user agrees to the terms and conditions of this policy.

Philosophy

University of Northwestern and Northwestern Media (Northwestern) recognize that technology can be a great resource in the personal, professional and academic environments. University of Northwestern and Northwestern Media provide technology resources (computers, telecommunication, network and Internet connections, e-mail, and other resources) to accomplish their respective missions.

University of Northwestern Mission Statement: University of Northwestern exists to provide Christ-centered higher education, equipping students to grow intellectually and spiritually, to serve effectively in their professions, and to give God-honoring leadership in the home, church, community, and world.

Northwestern Media Mission Statement: The purpose of Northwestern Radio is to lead people to Christ and to nurture them in their spiritual growth through Christ-centered media.

Responsible use of these resources requires the exercise of discernment and the implementation of usage guidelines.

It is the responsibility of every Northwestern community member to use these resources in accordance with community standards and in compliance with all Northwestern policies and all local, state, and federal laws and regulations. To ensure access to these resources is maintained, all Northwestern community members must comply with this technology usage policy.

Rights and Responsibilities

Northwestern provides network and Internet connections which allow access to local, national, and international sources of information and collaboration vital to organizational operations and intellectual inquiry. In return for this access, each user has the responsibility to respect and protect the access, privacy, values, feelings and property of every other user in our community and on the Internet. Internet communication through websites, including social networking websites, is to be conducted in a positive, wise and discerning manner, recognizing that each individual is responsible for all information authorized, posted, or permitted on his or her site. Northwestern community members are expected to act in a responsible, ethical, and legal manner when accessing and using these forms of technology in keeping with our shared framework of values.

Technology Access

Access to Northwestern technology is a privilege provided to its community members. All technology services, software, hardware, network and other equipment provided by Northwestern are considered the property of Northwestern and are provided to enable the missions of the organization. There is no guarantee of user privacy on messaging systems such as e-mail or voicemail. Northwestern reserves the right to monitor, restrict or remove access to technology resources to anyone using these resources in an inappropriate manner at any time without notice.

Residential Network Access

The Northwestern residential network provides students who live in the campus residence halls the ability to further their educational experience with direct access to the services provided via the campus network. Each student is provided a wired or wireless network connection in the room as well as additional wired and wireless network connections located around common areas in each residential facility.

Usage Guidelines

Community members are responsible for their use of technology and must abide by the usage guidelines below.

1. Computers, computer files, the e-mail system, Northwestern networks, and software provided for employee or student use are Northwestern property intended for business or educational use. Employees and students should not, without proper authorization, use a username or password, access a file, access a computer belonging to Northwestern or to another user, or retrieve any stored communication.

2. Northwestern strives to maintain a workplace and community free of harassment and sensitive to the diversity of its community members. Therefore, Northwestern prohibits the use of telephone, computer, e-mail, the Internet, and other electronic devices in ways that are disruptive, defamatory, abusive, unlawful, unethical, or harmful to morale.

3. The creation, display, transmission, willful receipt, or storage of sexually explicit or pornographic images, messages, cartoons, documents, programs, chats, or files is strictly prohibited.

4. Any action taken for the purpose of harassing, threatening, or disparaging others is prohibited. This includes but is not limited to ethnic slurs, racial epithets, or anything else based on race, national origin, sex, sexual orientation, age, disability, religion, political beliefs, or any other protected class status. Cyberbullying will not be tolerated and is considered a severe violation of this policy.

5. Northwestern purchases and licenses a variety of computer software programs for business or educational purposes and do not own the copyright to this software or its related documentation. Unless authorized by the software developer, Northwestern does not have the right to reproduce such software for use on more than one computer. Therefore, Northwestern prohibits the illegal duplication of software and its related documentation.

6. Employees and students should not attach to a network any computer which represents a security risk. Therefore, computers connecting to the network must have operating systems that have up-to-date security patches, updated and operational antivirus programs, and must be free of worms, viruses, and other malware. Computers that are infected with viruses or worms, or that open unnecessary security risks to the network due to non-compliance with this requirement, may have their network connection disabled upon detection.

7. An employee or student should not use or install personal software on any computer other than his or her personally-owned without permission of the owner. Permission from Information Technology must be obtained prior to installing personal software on a Northwestern computer.

8. Employees and students are prohibited, except under copyright fair use statutes, from disseminating, copying, or printing any copyrighted materials, including, but not limited to, music and software. For information relating to fair use guidelines see http://fairuse.stanford.edu/ or other available resources. If questions arise relating to copyright or fair use, please contact University of Northwestern library or academic personnel or Northwestern's technology personnel.

9. The Internet and e-mail may not be used for private business purposes, to solicit interest in non-Northwestern events, to utilize Northwestern network resources to generate monetary or equivalent compensation, or to solicit others for commercial ventures or financial gain. Web sites are not allowed to be used for commerce, personal gain, or political campaigning.

10. Students must receive prior approval before sending out e-mail communications to a large number (50+ people receiving the same message content) of University of Northwestern and/or Northwestern Media e-mail addresses, even for academic purposes. The Office of Marketing & Communications maintains guidelines to assist with effective distribution of mass e-mail communications. Employees who need to send campus-wide communication are encouraged to review the Editorial Policy for the Northwestern Daily Journal and other electronic messages for mass distribution, located in the General and Misc Northwestern Information section of the Employee Handbook. Employee-generated communication to students group for course-related or administrative messages should be governed by communication and technology best practices.

11. Any action which degrades or disrupts technology equipment, software, or system performance, accesses the account of another user, vandalizes the data of another user, misuses network resources, invades the privacy of individuals, or wastefully uses finite resources is not acceptable. Examples include but are not limited to:
    a. Alteration of any kind to assigned IP address or related settings
    b. Using an unauthorized IP address or masking your true IP address
    c. Printing directly to a printer by use of IP address to circumvent print page accounting
    d. Use of any domain name other than those authorized by Northwestern
    e. The use of network monitors/sniffers or network scanners
    f. MAC address spoofing
    g. Any action that impairs and/or alters network services, equipment, wiring, or jacks
    h. Connecting a network appliance (hub, switch, router, etc.), a wireless device, or private network to the NWC network, without prior written approval from Information Technology
    i. Setting up a server (i.e. a computer that provides files or services to others) and/or Network Operating System on the network without prior written approval from Information Technology. In those cases where network users have obtained written permission to setup personal computers as servers, they are responsible for the security of those servers and must accept full responsibility for any inappropriate setup or activities on that server or approved private network attached to them

j. Performing any action that denies another user access to network and/or computing resources

k. Any action that compromises the integrity of the network

l. Actions, programs, or services that put unusually high demands on the network

m. The storage of personal music, videos, pictures, or files on the network storage system

n. Attempts to circumvent system security, such as allowing another to use your account or guessing another's password, or in any way gaining unauthorized access to local or network resources

12. Northwestern’s technology resources are designed for use by those within the Northwestern community: employees and students. Access to Northwestern technology resources may also be permitted as appropriate to those associated with Northwestern (vendors, parents, prospective students, groups renting campus facilities, others) assuming a reasonable need and assuming appropriate levels of authorization and supervision.

13. File storage is a limited commodity which should not be abused. Employees and students are required to keep their usage below quota and review space usage periodically to remove any files that are no longer needed.

14. Employees are to use technology for work tasks during work time. Personal use of technology should be limited to breaks or non-work times and should not compromise resources. The storage of illegally-obtained copyrighted material such as commercial music or videos on any Northwestern computer or network storage device is not allowed.

Additional Statements

1. E-mail, voicemail, and other messaging solutions may be monitored to the extent necessary to ensure compliance with Northwestern policies. Community members have no legitimate expectation of privacy in Northwestern messaging systems. The use of personal identification numbers (PIN numbers) or passwords by a student or employee to access a messaging system does not preclude Northwestern from accessing messages contained in and saved in Northwestern messaging systems. Unauthorized use of encryption technology to block access to any message is strictly prohibited.

2. Internet access at Northwestern is filtered. Northwestern has implemented software to block access to obscene or objectionable content for moral, legal, and network security reasons. This software blocks obscene content while maintaining the ability to access legitimate sites.

3. Northwestern makes no warranty with respect to Internet service or content. Northwestern does not have control of the information on the Internet, nor can comprehensive barriers be provided to account holders accessing the full range of information available. Other sites accessible via the Internet may contain material that is illegal, defamatory, inaccurate or potentially offensive to some people.

4. Northwestern believes that the benefits to employees, educators, and students from access to the Internet, in the form of information, resources and opportunities for collaboration, far exceed any disadvantages of access.

5. The Information Technology department reserves the right to monitor network traffic as defined by Northwestern policies as well as by local, state and federal laws and regulations.

Violations

Upon learning of violations of this policy, employees should notify their immediate supervisor or Human Resources, students should notify Student Development, or employees and students may contact Information Technology.

FOR STUDENTS:

Violations of these policies will result in the student being referred to the appropriate disciplinary organization. Sanctions imposed as a result of such violations may include but are not limited to:

- Suspension/termination of technology and/or network privileges and resources
- Disciplinary action as defined in the current Student Handbook
- Suspension or expulsion from the University
- Monetary reimbursement to the University or other appropriate sources
- Legal action under applicable civil and/or criminal laws

Documentation of the incident will be placed in the student's file.

In addition, the student may (1) be required to submit to Student Development a response paper (contract) indicating the student's ownership of the incident, and/or (2) be required to send written apologies to those, if any, who have been negatively impacted by the incident.

FOR EMPLOYEES:

Employees who violate this policy will be subject to disciplinary action up to and including termination of employment as well as possible legal action under applicable civil and/or criminal laws.

Liability

Northwestern maintains a data backup schedule as well as virus protection for all data on its servers. Northwestern disclaims any and all liability in which data is lost and unrecoverable for reasons such as, but not limited to, server failure, network equipment failure, human error, or technical failure of any type. Users are responsible for safely storing relevant business or academic data. Northwestern assumes no liability for personal data or the loss of data in any and all areas.

Disclaimer

Northwestern reserves the right to change all matters contained in this Policy, to interpret the provisions of this Policy, and to vary from any provision of this Policy in any instance where Northwestern determines that such variance is appropriate.

Last Updated: August 2014
Responsible University Officer: David Richert
Policy Owner: Information Technology
Policy Contact: David Richert, CIO