MEMORANDUM

Date: September 27, 2012
To: NIU Faculty and Staff
From: Steve Cunningham
Vice President, Administration
Jim Fatz
Director, Information Security and Operations

RE: Acceptable Use and Electronic Mail Compliance Policy Updates

Significant updates have been made to university Acceptable Use and Electronic Email Policies in coordination with Information Security and Operations, Legal Counsel, and the President's Cabinet. These policy updates include important clarifications in terms of limitations and responsibilities related to employee utilization of E-mail and Information Technology resources. Given the close association with professional responsibilities, it is important that all faculty and staff be familiar with these policies. Attached are printed copies of both policies.

The policies are also available online. To view a full copy of the Acceptable Use Policy, please go to the Information Technology Services website at: http://its.niu.edu/its/policies_root/au.shtml and to view the Electronic Mail Policy, please go to: http://its.niu.edu/its/policies_root/email_pol.shtml

Inquiries can be directed to either of our offices or Celeste Latham at 753-6525.

Attachments

Via E-mail and Printed Copies
Northern Illinois University Acceptable Use Policy

Northern Illinois University information technology resources, including the electronic communications network (NIUnet) on the NIU campus and off-campus education and research centers, computers attached to this network, and any associated computational resource or service are for the use of persons affiliated with Northern Illinois University, including faculty, staff, emeritus personnel, and students in good standing. Information technology resources are provided by the university to further the university's mission of research, instruction, and public service. The use of these resources should be consistent with this mission, this policy, and the University’s other use, security policies, and other applicable regulations including the State Officials and Employees Ethics Act (SOEEA). Pursuant to the NIU Electronic Mail policy, the email system may be utilized for personal messages subject to the limitations set forth in these and other applicable policies and to the extent that personal usage does not interfere with assigned responsibilities. By using NIU services, all individuals, including, but not limited to, employees, students, customers, volunteers, and third parties, unconditionally accept the terms of this policy.

Acceptable use of NIU information technology resources is based on common sense, decency, ethical use, civility, and security applied to the computing environment. All authorized users may expect reasonable privacy with regard to all computer files and e-mail. The University may access university-owned or networked computers for maintenance and upgrades and to monitor or troubleshoot networks for related security, network audits, investigations, and/or legal requirements. Computers or systems may also be accessed through established procedures for reasonably suspected abuse of this policy and/or other University acceptable use policies. If illicit activity of any kind is suspected as a result of routine monitoring, an internal or external investigation may result. Users may be entitled to notification of such access, and, whenever possible, notification should precede access. Any actions that compromise the integrity of the University, data facilities, networks, services, or resources is strictly prohibited. Examples of unacceptable uses include, but are not limited to, the following:

- Using the resources for any purpose which violates federal or state laws.
- Using the resources for commercial, sales, and advertising purposes without university approval.
- Using excessive data storage or network bandwidth in activities such as the propagating of "chain letters" or "broadcasting" inappropriate messages to lists or individuals or generally transferring unusually large or numerous files or messages.
- Sending or storing for retrieval patently harassing, intimidating, or abusive material.
- Misrepresenting your identity or affiliation while using information technology resources.
- Use of the employment title or GroupWise signature in private communications. The public may potentially be misled by any individual's unauthorized use of an NIU employment title representing their status or position in private communications.
• Using someone else's identity and password for access to information technology resources, logging others into the network to access information technology resources, or using the network to make unauthorized entry to other computational, information, or communications devices or resources.
• Accessing material that, in NIU's evaluation, is obscene, defamatory, or constitutes a threat, including pornographic material.
• Attempting to evade, disable, or "crack" passwords or other security provisions of systems on the network.
• Reproducing and/or distributing material protected by copyright, trademark, trade secret, or other intellectual property without appropriate authorization.
• Copying or modifying files belonging to others or to the university without authorization, including altering data, introducing or propagating viruses or worms, or simply damaging files.
• Using the resources for political activities, including organizing or participating in any political meeting, rally, demonstration, soliciting contributions or votes, distributing material, surveying or polling for information connected to a political campaign, completing political surveys or polling information, and any other activities prohibited under the ethics act and/or other state/federal laws.
• Purposefully interfering with or disrupting another information technology user's work as well as the proper function of information processing and network services or equipment.
• Use of personal social media sites, following specific direction to cease or not utilize university equipment or time to an extent or during time periods that would interfere with professional responsibilities including, but not limited to, Facebook, Twitter, Flickr, Pinterest, LinkedIn, Foursquare, etc., unless associated with professional responsibilities.
• Intercepting or altering network packets.

These principles and guidelines are extended to networks and information technology resources outside the university accessed through NIUnet via the Internet. Networks or information technology resource providers outside the university may, in turn, impose additional conditions of appropriate use which the user is responsible to observe when using those resources. Certain violations of this acceptable use policy, which involve the potential for illegal conduct (including accessing certain pornographic sites or any activity which may constitute fraud or the misappropriation of university resources), may be reported to external agencies or law enforcement for investigation.

Access to the information technology environment at Northern Illinois University is a privilege and must be treated as such by all users of these systems. Like any other campus facility, abuse of these privileges can be a matter of legal action or official campus disciplinary procedures, up to and including termination. Depending on the seriousness of an offense, violation of the policy can result in penalties ranging from reprimand, loss of access, or referral to university authorities for disciplinary or legal action. In a case where unacceptable use severely impacts performance or security, in order to sustain reasonable performance and security, Information Technology Services will immediately suspend an individual's access privileges.

Policy last reviewed: 09.13.12
Northern Illinois University Electronic Mail (E-Mail) Policy

Northern Illinois University (NIU) participates in a range of computing networks. Many members of the university community, including faculty, staff, volunteers, and students, use electronic mail (e-mail) in their day-to-day activities. E-mail services are provided on university-owned computing and networking systems to further the university's mission of research, instruction, and public service. E-mail services are also considered a conditional employee benefit and may be utilized for personal messages subject to the limitations set forth in these and other applicable policies and to the extent that personal usage does not interfere with assigned responsibilities. Use of e-mail should be consistent with this mission and this policy.

The university utilizes GroupWise as its official email communication mechanism. Official university correspondence, including, but not limited to, messages from the President, policy information, employment, and benefit notifications, are electronically distributed through the GroupWise system. Employees whose departments utilize other email systems are responsible for checking their GroupWise accounts or forwarding such messages to their alternative email system for official university correspondence. Employees who choose to forward NIU email content to third-party email providers have the responsibility to ensure that appropriate security is maintained whenever such content is classified as "restricted" or "sensitive" information (see the NIU Information Security Policy for definitions and requirements).

Mass mailings are permitted but need to follow these guidelines:

Mass Mailing Requirements (for more than 100 users):

- Provost (or designee) approval for distribution to students (only required if students are outside of the sender's academic area of responsibility).
- Vice President for Administration (or designee) approval for distribution to employees (only required if the distribution is to include employees outside of the sender's area of responsibility).
- Whenever possible, include the content within the message itself as opposed to utilizing attachments.
- Utilize a web-based link to the source for any high-resolution graphics, streaming content, or any material that would substantially increase the message size.
- Distribution lists are not released by the approval areas. Therefore, coordination is necessary between the approval area and the individual requesting the distribution. The message will be sent out from the primary approval area when authorized.
- University Relations general distribution measures may be utilized after approval by the primary approval area when most appropriate.

Unacceptable uses include, but are not limited to, the following:

- Using e-mail for any purpose that violates federal law, state law, or university policy.
- Use of electronic mail inconsistent with university Acceptable Use policies.
- Using e-mail for commercial purposes.
- Misrepresenting your identity or affiliation in e-mail communications.
- Sending patently harassing, intimidating, abusive, or offensive material to or about others.
- Intercepting, disrupting, or altering electronic communications packets.
- Using someone else's identity and password.
Communications in this medium are protected by the same laws and policies, and are subject to the same limitations, as communications in other media. However, users should exercise caution when committing confidential information to electronic media because the confidentiality of such material cannot be guaranteed. For example, e-mail messages can be saved indefinitely on the receiving computer. Copies can easily be made and forwarded to others either electronically or on paper. Messages sent to nonexistent or incorrect user names are delivered to a person designated as Postmaster for either the remote or local site. Routine maintenance or system administration of a computer may result in the contents of files and communications being seen (network and system administrators are, however, expected to treat the contents of electronic files as private and confidential).

Under the Illinois Freedom of Information Act (FOIA) and e-Discovery laws, electronic files are considered the same as paper files. Any official university documents (as defined by law) in the files of employees of the State of Illinois are considered public documents and may be subject to inspection through FOIA or e-Discovery unless exempted by law. In such cases, the campus Freedom of Information Officer, or other applicable official, should inspect files to determine which portions may be exempt from disclosure. Any inspection of electronic files and any action based upon such inspection will be governed by all applicable U.S. and Illinois laws and by university policies.

Acceptable use of NIU information technology resources is based on common sense, decency, ethical use, civility, and security applied to the computing environment. All authorized users may expect reasonable privacy with regard to all computer files and e-mail. The University may access university-owned or networked computers for maintenance and upgrades and to monitor or troubleshoot networks for related security, network audits, investigations, and/or legal requirements. Computers or systems may also be accessed through established procedures for reasonably suspected abuse of this policy and/or other University acceptable use policies. If illicit activity of any kind is suspected as a result of routine monitoring, an internal or external investigation may result. The university reserves the right to access university property with or without notice. Thus, users may or may not receive notification of such access. Certain violations of this electronic mail policy, which involve the potential for illegal conduct (including accessing certain pornographic sites or any activity which may constitute fraud or the misappropriation of university resources) may be reported to external agencies or law enforcement for investigation.

Access to the information technology environment in general, and electronic mail in particular, at Northern Illinois University is a privilege and must be treated as such by all users of these systems. Like any other campus facility, abuse of these privileges can be a matter of legal action or official campus disciplinary procedures. Depending on the seriousness of an offense, violation of the policy can result in penalties ranging from written warning (i.e., don't do this anymore), to loss of access, to referral to university authorities for disciplinary action. In a case where unacceptable use severely impacts performance or security, in order to sustain reasonable performance and secure services for the rest of the user community, Information Technology Services (ITS) will immediately suspend an individual's access privileges.

Policy modified: 09/14/12