Appropriate Use Policy | UWCX Network and E-mail

Use of the Extension and Colleges computing systems are a privilege. Computer resources for these institutions are to be used for legal business and learning activity, and may not be used for purposes which are illegal, unethical or damaging to the reputation of the University or its members.

The following policy on acceptable use and e-mail use apply to users of the University of Wisconsin Extension and Colleges computing network known as UWCX and its resources. These rules do not override, but work in conjunction with other system and university policies.

Acceptable Use: Network Computer Systems

Impermissible activity includes but is 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
- Unauthorized access to the University network
- Deliberate misrepresentation of user identity
- Unauthorized copying of software and/or violating copyright protection laws and guidelines
- Violation of computer system security
- Use of unapproved mailing lists
- Use of computing facilities for private business purposes unrelated to the job duties of the University
- Downloading and / or running of destructive or disruptive programs
- Displaying or transmitting via the network material that is threatening, obscene or pornographic
- Intentional or negligent distribution of computer viruses
- Dissemination of personal information (i.e. Social Security Numbers)
- Any activity that derogates the UWCX network

E-mail Usage Policy

Users are responsible for conducting themselves in an ethical and lawful manner when using the University of Wisconsin Extension and Colleges Exchange e-mail system. When creating e-mail messages it is recommended users follow the basic standards required of written business communications. The following applies to the Exchange e-mail environment for Extension and Colleges employees, which is managed and maintained by the Central Information Technology Services department. Student e-mail is now hosted with Microsoft's Live@edu program which incorporates additional usage policies.

Prohibited Use of E-mail

Unless required by position or function, users shall not use the Extension and Colleges Exchange e-mail services to create, view, save, receive, or send material related to the following:

- Creating or exchanging obscene messages, including pornographic material
- Sending e-mail that promotes discrimination on the basis of race, gender, national origin, age, marital status, sexual orientation, religion, or disability
- Sending e-mail that contains a threatening or excessively violent message
- Exchanging proprietary information, trade secrets, or other confidential information to anyone not affiliated with the University
- Creating, forwarding, or exchanging SPAM, chain letters, solicitations, or advertising through global distribution lists
- Creating, storing, or exchanging e-mail that violates material protected under copyright laws
- Altering a message from another user without their permission
- Improperly using someone else's e-mail account without their permission

The above list of prohibited actions is by way of an example only and is not intended to be exhaustive.

Privacy

Confidentiality of e-mail may be compromised by the applicability of law or policy, including this policy, by unintended redistribution, or because of the inadequacy of current technologies to protect against unauthorized access. Users, therefore, should exercise extreme caution in using e-mail to communicate confidential or sensitive matters.

Users should be aware that system administrators need to, from time to time, observe certain e-mail transactional addressing information to ensure that the e-mail system is functioning properly. On these and other occasions, the contents of an e-mail message may be inadvertently displayed. Except as provided elsewhere in this policy, system administrators are not permitted to view the contents intentionally or disclose or otherwise use what they have seen.

The content of an e-mail message transmitted from or stored on UWCX computers, whether personal or business related is not necessarily protected from public disclosure and may be considered a public record under Wisconsin and Federal law. E-mail delivered to or sent from the UWCX e-mail system is considered to be an open record, much like a written or printed document, and can be requested. However, users should not assume that their information is

automatically subject to public inspection under the Wisconsin Open Records Law and should contact the appropriate authority if an Open Records Law request is received.

Mailbox Limits and Attachments

The UWCX e-mail system does not currently impose size limits on faculty or staff mailboxes. Student hosted mailboxes are limited to 10GB of storage. UWCX e-mail administrators may implement mailbox size limits for faculty and/or staff mailboxes should the size of the e-mail system grow beyond a cost justifiable size.

The UWCX e-mail system limits the size of incoming or outgoing e-mail messages to a maximum of 50MB for faculty and staff, and 20MB for students. If the total size of the e-mail message exceeds this limit it will not be sent or received. If there is a business need to send or receive larger e-mail messages, please contact the Central IT Service Center.

In addition, the central e-mail system blocks attachments that are known to cause damage to computer systems or install unwanted applications without the user's permission or knowledge (i.e. spyware).

Spam and Virus Protection

Incoming e-mail is scanned for viruses and for messages deemed to be “SPAM”, or unsolicited advertisements for products or services sent to a large distribution. Suspected messages are blocked from the user’s mailbox. Due to the complex nature of e-mail, it is impossible to guarantee protection against all SPAM and virus infected messages.

It is incumbent on each individual to use proper care and consideration to prevent the spread of viruses. In many cases viruses appear to be sent from a friend or coworker, and therefore attachments should only be opened when the users is sure of the nature of the message. If any doubt exists, the users should contact the Central IT Service Center.

Created: Monday, March 3, 2008
Modified: Thursday, February 22, 2012
Assistant Vice Chancellor of Information Technology