

Internet Use Policy

Most employees and students will be provided with access to the Internet to assist them in performing their jobs and instruction. The Internet can be a valuable source of information and research. In addition, e-mail can provide excellent means of communicating with other employees, our students, our customers and clients, outside vendors, and other businesses. Use of the Internet, however, must be tempered with common sense and good judgment.

If you abuse your right to use the Internet, it will be taken away from you. In addition, you may be subject to disciplinary action, including possible termination, and civil and criminal liability.

Your use of the Internet is governed by this policy:

Disclaimer of liability for use of Internet. Eastern Iowa Community Colleges is not responsible for material viewed or downloaded by users from the Internet. The Internet is a worldwide network of computers that contains millions of pages of information. Users are cautioned that many of these pages include offensive, sexually explicit, and inappropriate material. In general, it is difficult to avoid at least some contact with this material while using the Internet. Even innocuous search requests may lead to sites with highly offensive content. In addition, having an e-mail address on the Internet may lead to receipt of unsolicited e-mail containing offensive content. Users accessing the Internet do so at their own risk.

Employee's duty of care. Employees should endeavor to make each electronic communication truthful and accurate. You should use the same care in drafting e-mail and other electronic documents as you would for any other written communication. Please keep in mind that anything created or stored on the computer system may, and likely will, be reviewed by others.

Duties not to waste computer resources. Users must not deliberately perform acts that waste computer resources or unfairly monopolize resources to the exclusion of others. These acts include, but are not limited to, sending mass mailings or chain letters, spending excessive amounts of time on the Internet, playing games, listening to Internet radio stations, non-job/schoolwork related audio/video streaming, engaging in online chat groups, printing multiple copies of documents, or otherwise creating unnecessary network traffic. Because audio, video, and picture files require significant storage space, files of this sort may not be downloaded unless they are business-related.

No expectation of privacy. The computers and computer accounts given to employees are to assist them in performance of their jobs. Employees should not have an expectation of privacy in anything they create, store, send, or receive on the computer system. The computer system belongs to the district and may only be used for business purposes.

No privacy in communications. Employees should never consider electronic communications to be either private or secure. E-mail may be stored indefinitely on any number of computers, including that of the recipient. Copies of your messages may be forwarded to others either electronically or on paper. In addition, e-mail sent to nonexistent or incorrect usernames may be delivered to persons that you never intended.

Monitoring of computer usage. The Colleges have the right, but not the duty, to monitor any and all aspects of its computer systems, including, but not limited to, monitoring sites visited by employees on the Internet, monitoring chat groups and newsgroups, reviewing material downloaded or uploaded by users of the Internet, and reviewing e-mail sent and received by users.

Blocking of inappropriate content. The Colleges may use software to identify inappropriate or sexually explicit Internet sites. Such sites may be blocked from access by district networks. In the event you nonetheless encounter inappropriate or sexually explicit material while browsing on the Internet, immediately disconnect from the site, regardless of whether the site was subject to district blocking software.

Prohibited activities. Material that is fraudulent, harassing, embarrassing, sexually explicit, profane, obscene, intimidating, defamatory, or otherwise unlawful or inappropriate may not be sent by e-mail or other form of electronic communication (bulletin board systems, newsgroups, chat groups), downloaded from the Internet, or displayed on or stored in Eastern Iowa Community Colleges' computers. Employees encountering or receiving this kind of material should immediately report the incident to their supervisors.

Games and entertainment software. Employees may not use the Colleges' Internet connection to download games or other entertainment software, including screen savers, or to play games over the Internet.

Illegal copying. Employees may not illegally copy material protected under copyright law or make that material available to others for copying. You are responsible for complying with copyright law and applicable licenses that may apply to software, files, graphics, documents, messages, and other material you wish to download or copy. You may not agree to a license or download any material for which a registration fee is charged without first obtaining the express written permission of the Director of Computing and Telecommunications.

Accessing the Internet. To ensure security and avoid the spread of viruses, employees accessing the Internet through a computer attached to Eastern Iowa Community Colleges' network must do so through an approved Internet firewall. Accessing the Internet directly, by modem, is strictly prohibited unless the computer you are using is not connected to the district's network.

Virus detection. Files obtained from sources outside the district, including disks brought from home; files downloaded from the Internet, newsgroups, bulletin boards, or other online services; files attached to e-mail; and files provided by customers or vendors, may contain dangerous computer viruses that may damage the district's computer network. Employees should never download files from the Internet, accept e-mail attachments from outsiders, or use disks from nondistrict sources without first scanning the material with district-approved virus checking software. If you suspect that a virus has been introduced into the district's network, notify the Help Desk, at extension 3456, immediately.

Sending unsolicited e-mail (spamming). Without the express permission of their supervisors, employees may not send unsolicited e-mail to persons with whom they do not have a prior relationship.

Altering attribution information. Employees must not alter the "From:" line or other attribution-of-origin information in e-mail, messages, or postings. Anonymous or pseudonymous electronic communication is forbidden. Employees must identify themselves honestly and accurately when participating in chat groups, making postings to newsgroups, sending e-mail, or otherwise communicating online.

Standard footers for e-mail. This footer should be appended to all e-mail sent outside the district:

This e-mail and any files transmitted with it are confidential and are intended solely for the use of the individual or entity to whom they are addressed. This communication may contain material protected by the attorney-client privilege. If you are not the intended recipient or the person responsible for delivering the e-mail to the intended recipient, be advised that you have received this e-mail in error and that any use, dissemination, forwarding, printing, or copying of this e-mail is strictly prohibited. If you have received this e-mail in error, please immediately notify the Help Desk by telephone at 3456.

Attorney-client communications. E-mail sent from or to an attorney representing the Colleges should include this warning header on each page: "ATTORNEY-CLIENT PRIVILEGED; DO NOT FORWARD WITHOUT PERMISSION." Communication from attorneys may not be forwarded without the sender's express permission.

Use of encryption software. Employees may not install or use encryption software on any of Eastern Iowa Community Colleges' computer without first obtaining written permission from their supervisors. You must not use passwords or encryption keys that are unknown to your supervisor.

Export restrictions. The federal government has imposed restriction on export of programs or files containing encryption technology (such as e-mail programs that permit encryption of messages and electronic commerce software that encodes transactions). Software containing encryption technology is not to be placed on the Internet or transmitted in any way outside the United States without prior written authorization from the Director of Computing and Telecommunications.

Other policies applicable. In their use of the Internet, users must observe and comply with all other policies and guidelines of the Eastern Iowa Community Colleges.

Amendments and revisions. This policy may be amended or revised from time to time as the need arises. Users will be provided with copies of all amendments and revisions.

Violation of this policy will be taken seriously and may result in disciplinary action, including possible termination, and civil and criminal liability.

I have read and agree to comply with the terms of this policy.

Date _____

Signature

Printed name

Short Form E-mail and Computer Use Policy

To maximize the benefits of its computer resources and minimize potential liability, Eastern Iowa Community Colleges has created this policy. All computer users are obligated to use these resources responsibly, professionally, ethically, and lawfully.

You are given access to our computer network to assist you in performing your job. You should not have an expectation of privacy in anything you create, store, send, or receive on the computer system. The computer system belongs to the district and may only be used for business purposes. Without prior notice, the district may review any material created, stored, sent, or received on its network or through the Internet or any other computer network.

Use of computer resources for any of these activities is strictly prohibited:

- Sending, receiving, downloading, displaying, printing, or otherwise disseminating material that is sexually explicit, profane, obscene, harassing, fraudulent, racially offensive, defamatory, or otherwise unlawful.
- Disseminating or storing commercial or personal advertisements, solicitations, promotions, destructive programs (that is, viruses or self-replicating code), political information, or any other unauthorized material.
- Wasting computer resources by, among other things, sending mass mailings or chain letters, spending excessive amounts of time on the Internet, playing games, engaging in online chat groups, printing multiple copies of documents, or otherwise creating unnecessary network traffic.
- Using or copying software in violation of a license agreement or copyright.
- Violating any state, federal, or international law.

If you become aware of someone using computer resources for any of these activities, you are obligated to report the incident immediately to your supervisor.

Violation of this policy will be taken seriously and may result in disciplinary action, including possible termination, and civil and criminal liability.

I have read and agree to comply with terms of this policy.

Date _____

Signature _____

Printed name _____