Elgin Community College

Acceptable Usage Guidelines for Electronic Student Services

These Acceptable Usage Guidelines describe activities that Elgin Community College considers violations in the usage of its electronic student services. The examples listed are not exhaustive and may change from time to time as technology and applications change. The examples are provided solely for guidance to users.

There are cases in which the use of electronic student services are deemed not acceptable; however, there are also cases in which these services may be used to conduct behaviors which violate local, state, or federal law. Though the use of electronic student services is the focus of this document, students and members of the Elgin Community College community are advised that use may be governed by other College guidelines including but not limited to those in the student handbook, College catalog, and other guidelines governing academic, student life, or personnel matters at the College or agreements between the College and affiliated organizations. Elgin Community College's electronic student services are not to be used for commercial purposes or non-College related activities. To ensure proper network performance, network security and appropriate usage, College staff may monitor and record user activity. No user shall have expectations of privacy in their use of electronic student services, including internet activity, e-mail messages and stored files.

Elgin Community College reserves the right to enforce applicable penalties and/or immediately terminate a student's or community member's access to College electronic student services when these services have been used in a manner that is disruptive or is otherwise believed to be in violation of acceptable use or other College guidelines or local, state, or federal law. As a recognized agent under the Digital Millennium Copyright Act, the College will act in accord with the provisions of this act in the event of notification of alleged copyright infringement by any user.

Instances of inappropriate use of electronic student services will be referred to the appropriate official for disciplinary action by the College and will be subject to these guidelines as well as to other applicable College guidelines. In addition, individuals may be subject to civil suit, and/or local, state, and federal prosecution depending on their actions. Among sanctions that can be imposed for violation of this or other applicable College guidelines, the College reserves the right to restrict an individual's access to electronic student services.

Student Responsibilities:

As a student of Elgin Community College, you have a shared responsibility with the College technologies staff to maintain the integrity of our systems, services, and information so that high quality services can be provided to everyone. Your responsibilities include:

1. To use the College's electronic student services responsibly and appropriately and to respect the rights of other students using these services.
2. To respect all contractual and license agreements, privacy of information, and the intellectual property of others.
3. To comply with College, federal, state, and local regulations regarding access and use of information resources (e.g., Federal Copyright Act, The Family Education Rights and Privacy Act, Gramm-Leach-Bliley Act, codes of professional responsibility, etc.).
4. To exercise due diligence in protecting computers from viruses, worms, and security vulnerabilities by regularly using anti-virus software (provided by the Information Technology Department for College issued computers or personally purchased anti-virus software for personally owned computers).

5. To keep your technology accounts (network, e-mail, accessECC, etc.) secure.
6. To not share your privileges with others. Your access to electronic student services is not transferable to other students or members of the Elgin Community College community, to family members, or to an outside individual or organization.
7. To comply with posted policies governing use of public computing facilities.
8. If enrolled in a College Web Design course, to present a web page that reflects the highest standards of quality and responsibility. As web page publisher, you are responsible both for the content of your web page and all links and references from your web page are consistent with this and other College guidelines, copyright laws, and applicable local, state, federal laws. Published web pages are not to be used for commercial purposes or for activities not related to the purposes of the College.
9. To understand the implications of sharing personal information or data via the Internet, WWW, e-mail, Instant Messaging or other services that either are open to access by others on and off-campus, or that can be forwarded to others.

Examples of Violations of "Acceptable Use"

Unauthorized Access & Account Violations

1. Attempting to obtain unauthorized access or circumventing user authentication or security of any host, network or account ("cracking"). This includes accessing data not intended for the user, logging into a server or account the user is not expressly authorized to access, or probing the security of systems or networks.
2. Supplying or attempting to supply false or misleading information or identification in order to access Elgin Community College's technology resources.
3. Sharing your network, e-mail, accessECC, etc. passwords with others
4. Using technology resources for unauthorized uses.
5. Logging onto an account other than your own and/or presenting yourself as somebody else such as by sending e-mail from an account other than your own.
6. Unauthorized use of the College's registered Internet domain name(s).

Service Violations

7. Attempting to interfere with service to any user, host, or network. This includes "denial of service" attacks, "flooding" of networks, deliberate attempts to overload a service, port scans and attempts to "crash" a host.
8. Use of any kind of program/script/command designed to interfere with a user's computer or network session.
9. Damaging a computer or part of a computer system.
10. Knowingly spreading computer viruses.
11. Modifying the software or hardware configuration of College technology resources, including dismantling computers in the lab for the purposes of connecting a notebook computer to the peripherals.
12. Excessive use of technology resources for "frivolous" purposes, such as game playing or downloading of files. This causes congestion of the network or may otherwise interfere with the work of others, especially those wanting to use public access PCs or network and Internet resources.
13. "Hacking" on computing and networking systems of the College or using the College's network to “hack” other networks.
14. Using College technology resources (networks, central computing systems, public access systems, voice and video systems) for new technologies research and development without College review and authorization.
15. Failure to follow the College's guidelines for use of wireless access points (WAPs).
16. Deploying wireless access points (WAPs) or wireless routers within the College environment.
17. Students and community members are prohibited from accessing, submitting, publishing, displaying, or posting any defamatory, inaccurate, abusive, obscene, profane, sexually oriented or explicit, threatening, racially offensive, harassing, or illegal material.

Violations Related to Software, Data & Information

18. Inspecting, modifying, distributing, or copying software or data without proper authorization, or attempting to do so.
19. Violating software licensing provisions.
20. Installing software on public access and other College machines without appropriate authorization from the Information Technology Department.
21. Installing any diagnostic, analyzer, "sniffer," keystroke/data capture software or devices on College technology resources.
22. Breaching confidentiality agreements for software and applications; breaching confidentiality provisions for institutional or individual information.

Email & Internet Messaging Violations

23. Harassing or annoying others, whether through language, frequency or size of messages, or number and frequency of telephone calls.
24. Sending e-mails or instant messages to any person who does not wish to receive it, or with whom you have no legitimate reason to communicate. If a recipient asks to stop receiving mail, the user must not send that person any further correspondence.
25. Sending unsolicited bulk mail messages ("junk mail" or "spam") which, in the College's judgment, is disruptive to system resources or generates a significant number of user complaints. This includes bulk mailing of commercial advertising, informational announcements, political tracts, or other inappropriate use of system e-mail distribution lists.
26. Forwarding or otherwise propagating chain e-mail and pyramid schemes, whether or not the recipients wish to receive such mailings. This includes chain e-mail for charitable or socially responsible causes.
27. Malicious e-mail, such as "mailbombing" or flooding a user or site with very large or numerous items of e-mail.
28. Forging of e-mail header information.
29. Sending malicious, harassing, or otherwise inappropriate e-mail from one’s own or another's account.

Web Page & Server Violations

30. Posting content on your web page that provides information on and encourages illegal activity, or is harassing and defaming to others.
31. Linking your web page to sites whose content violates College policies, local, state, and/or federal laws and regulations.
32. Running web sites that support commercial activities or running server systems under the College's registered domain name, ELGIN.EDU or variation thereof, without the College's authorization.