

# LEWIS & CLARK COMMUNITY COLLEGE

## TECHNOLOGY RESOURCES POLICY

All College students, faculty, staff or other personnel who use or have access to the College's technology resources, including but not limited to computers (e.g. desktops and portable computers, servers, networks, printers, software and data storage media), e-mail, voicemail, facsimile machines, photocopiers and Internet access (collectively, technology resources) should be familiar with, and must comply with, these policies.

### A. CONFIDENTIALITY AND ACCESS POLICIES

The College's technology resources store confidential information. Access to this confidential information is granted to users only in connection with the College's function as an educational institution. Users may access and use the information only for proper purposes and must respect and maintain the confidentiality of that information. Users may not leak, place, post, transmit, or otherwise disclose confidential, sensitive, or proprietary College information, or any private information relating to any individual College employees, contractors, or students, to anyone outside of the College by any means, at any time, or for any reason.

A

### B. TYPES OF SOFTWARE USED AT COLLEGE AND SOFTWARE POLICIES

THIRD PARTY SOFTWARE. All third party software used by the College is proprietary to the third party vendor, is protected by copyright and/or trade secret law, and is subject to the terms of the specific software license agreement entered into by the College with the third party vendor with respect to that software. In general, these software license agreements expressly forbid copying of the software, forbid the use of unauthorized copies of the software, may restrict the use of software to particular hardware, and may limit the computers upon which the software may be used or the number of concurrent users of such software. In some cases, the College's licenses permit certain limited use by students, faculty or staff on home or portable computers. Violation of the provisions of software agreements and or copyright law can subject the College and individuals to substantial damage claims and possible criminal penalties.

COPYING OF SOFTWARE. The College prohibits any unauthorized duplication of all software owned or licensed by College. No user may, without proper authorization, duplicate the software that is loaded on his or her computer's hard disk for use on any other PC without consulting with and obtaining written authorization from the Academic Computing/Helpdesk staff.

INSTALLATION OF UNAUTHORIZED SOFTWARE. College computer users may install software on College hardware with prior written authorization from the Academic Computing/Helpdesk staff. Such approval will be granted unless there is a substantial danger of system or network conflicts, configuration changes, etc. Any maintenance required by a PC that was caused by the installation of unauthorized software will be placed at the bottom of the priority list for repair by the Academic Computing/Helpdesk Staff.

FILE-SHARING. Users may not post, upload, download, transmit, distribute, or engage in any "file-sharing" of any data or files (including software, music, audiovisual clips, movies, etc.) unless such activity is consistent with all applicable licenses and approved in advance by College's Academic Computing/Helpdesk Staff.

# LEWIS & CLARK COMMUNITY COLLEGE

## C. USE OF TECHNOLOGY RESOURCES

The College's technology resources are property of the College, or are licensed for use by the College and are intended to be used primarily for proper educational institutional purposes.

MONITORING. The College reserves the right to monitor, inspect, access, intercept, review, and when appropriate, disclose any and all information created, entered, received, stored, viewed, accessed or transmitted via College technology resources (including without limitation in databases, data file systems, data archives, Web/Internet/Intranet sites).

**Users should have no expectation of privacy in connection with the use of College technology resources, including the creation, entry, receipt, storage, accessing, viewing or transmission of data via such resources.**

PASSWORDS AND SECURITY. All passwords and security used in connection with College technology resources -- including voice mail access codes -- are College property and must be made available to the College. Users must understand that their use of passwords will not preclude access, monitoring, inspection, interception, review, or disclosure by authorized College personnel. The College also may unilaterally assign and/or change passwords and personal codes. The security of the College's technology resources is every user's responsibility.

Academic Computing Staff access each PC in the College periodically to perform system maintenance. Authorized and specifically designated College employees, agents, or representatives may also investigate and/or monitor the use of College systems to ensure that use is consistent with our Policies. They may also override all passwords or security codes when deemed necessary.

LAWFUL USE. College technology resources may not be used to intentionally or unintentionally violate any local, state, federal, or national civil or criminal laws, including copyright and patent laws of any jurisdiction. Unlawful activity includes but is not limited to lotteries, raffles, betting, gambling for anything of value, and participating or facilitating in the distribution of unlawful materials. Users likewise may not upload, post, e-mail, or otherwise transmit any data that is threatening, malicious, tortuous, defamatory, libelous, obscene, or invasive of another's privacy. Users also may not upload, download, post, e-mail, or otherwise transmit any material that contains software viruses or any other computer code, files, or programs designed to interrupt, destroy, or limit the functionality of any computer software, hardware, or telecommunications equipment.

INFRINGEMENT OF PROPRIETARY RIGHTS. College computer, electronic, e-mail, and Internet resources may not be used to violate proprietary rights, including copyright, trademark, trade secret, patent, rights of publicity, or any other intellectual property rights.

NO HARASSMENT. Users are absolutely forbidden from using College technology resources in any way that may be construed to violate the College's harassment-free workplace policy or otherwise harass fellow students or other individuals. This prohibition includes sexually explicit or offensive images, messages, cartoons, jokes, ethnic or religious slurs, racial epithets or any other statement or image that might be construed as harassment or disparagement on the basis of race, color, religion, sex, national origin, age, disability, sexual orientation, or any other status protected by law. Users are required to take all reasonable steps to avoid and eliminate receipt of any potentially offensive

# LEWIS & CLARK COMMUNITY COLLEGE

material; claiming to be a passive recipient of prohibited material is unacceptable. Prohibited conduct includes sending e-mail messages to someone who has requested that the user not do so.

MISREPRESENTATION OF IDENTITY. College computer, electronic, e-mail, and Internet resources may not be used to misrepresent, obscure, suppress, or replace one's identity or the origin of data or communications. For example, "spoofing" and "phishing" (e.g. constructing electronic communications to appear to be from someone else, including to solicit personally identifiable information from recipients) is prohibited. Each user's name, e-mail address, organizational affiliation, time and date of transmission, and related information included with electronic communications (including postings) must always reflect the true originator, time, date, and place of origination, as well as the original message's true content.

## D. INTERNET GUIDELINES

In addition to the above terms of use, the following guidelines specifically apply to Internet usage. Members of the Lewis and Clark campus community must remember that access to the Internet is a privilege. All College Students, Faculty, Staff or other personnel who use or have access to the Internet through the College must use the Internet resources in an effective, ethical and lawful manner. The following guidelines must be adhered to by all persons whether using systems on-campus or dialing in from off-campus. Failure to do so may result in removal of your account. The account is to be closed if you are no longer associated with the College. Because of limited disk space, it is expected that you check e-mail daily and delete unnecessary messages immediately. Keep messages remaining in your electronic mailbox to a minimum. Subscribers to news and messaging groups/services have an additional responsibility to monitor their electronic mailbox.

COMMUNICATIONS OVER THE INTERNET. Electronic communications facilities (such as e-mail, talk, network news and Internet Relay Chat) are primarily for College activities. Each individual is responsible for his/her image on the Internet as well as the image of the College. Fraudulent, harassing, or obscene messages and/or other materials must not be transmitted over the Internet or any other network on- or off-campus. Inappropriate messages include but are not limited to the following:

FRAUDULENT MESSAGES. Messages sent under an assumed name or modified address or with the intent to obscure the origin of the message.

HARASSING MESSAGES. Messages that harass an individual or group because of their sex, race, age, religious beliefs, national origin, physical attributes or sexual preference.

OBSCENE MESSAGES. Messages that contain obscene or inflammatory remarks directed toward an individual or group.

INAPPROPRIATE USE OF RESOURCES No one may deliberately attempt to degrade the performance of a computer system on the Internet or to deprive authorized personnel of resources or access to any computer system.

NETWORK CONFIGURATION. No one may establish a TCP/IP resource on campus without the explicit consent of Academic Computing/Helpdesk. All

## LEWIS & CLARK COMMUNITY COLLEGE

addresses are administered by Academic Computing/Helpdesk and all users must adhere to the addressing conventions established by that department.

SECURITY. No one may use loopholes in computer security systems or knowledge of a special password to damage computer systems, obtain extra resources, take resources from another user, gain access to systems or use systems for which proper authorization has not been given.

SYSTEM ACCOUNTS. Accounts are assigned to individuals and no one may use another person's account. Use of another user's account may result in automatic suspension of the account.

FINANCIAL GAIN. No one may use resources of the Internet for personal financial gain by posting messages that promote the products or services of a local business or their own product or services.