6006. ADMINISTRATIVE REGULATIONS ON COMPUTER AND COMMUNICATIONS TECHNOLOGY USE

6006.1 The Executive Director of Academic Computing and Information Technology shall administer these regulations.

6006.2 All users of LBCCD computing systems must read, understand, and comply with the regulations outlined in this policy. BY USING ANY OF THESE SYSTEMS, USERS AGREE THAT THEY WILL COMPLY WITH THESE REGULATIONS.

6006.3 LBCCD reserves all rights, including termination of service without notice, to the computing resources which it owns and operates. These procedures shall not be construed as a waiver of any rights of LBCCD, nor shall they conflict with applicable acts of law. Users have rights that may be protected by Federal, State, and local laws. (See section 14 of this document.)

6006.4 Access and privileges on LBCCD computing systems are assigned and managed by the administrators of specific individual systems. Eligible individuals may become authorized users of a system and be granted appropriate access and privileges by following the approval steps prescribed for that system.

All access to LBCCD’s computer resources, including the issuing of passwords, must be approved by a designee of LBCCD.

Users may not, under any circumstances, transfer or confer these privileges to other individuals. Any account assigned to an individual shall not be used by others without written permission from the Executive Director of Academic Computing and Information Technology. The authorized user is responsible for the proper use of the system, including any password protection.

6006.5 Users are responsible for maintaining the following items:

A. An environment in which access to all LBCCD computing resources are shared equitably among users. The system administrator of each system sets minimum guidelines within which users must conduct their activities.

B. An environment conducive to learning:

1. A user who harasses, or makes defamatory remarks, shall bear full responsibility for his or her actions. Further, by using these systems, users agree that individuals who transmit such remarks shall bear sole responsibility for their actions. Users agree that LBCCD’s role in managing these systems is only as an information carrier, and that they will never consider transmission through these systems as an endorsement of said transmission by LBCCD.

2. Many of the LBCCD computing systems provide access to outside networks, both public and private, which furnish electronic mail, information services, bulletin boards, conferences, etc. Users are
advised that they may encounter material which may be considered offensive or objectionable in nature or content. Users are further advised that LBCCD does not assume responsibility for the contents of any of these outside networks.

3. The user agrees to comply with the acceptable use guidelines for whichever outside networks or services they may access through LBCCD systems.

4. Further, the user agrees to follow proper etiquette on outside networks. Documents regarding etiquette are available through system administrators and through specific individual networks.

5. The user agrees never to attempt to transmit, or cause to be transmitted, any message in which the origination is deliberately misleading (except for those outside services which may conceal identities as part of the service). The user agrees that, in the unlikely event that someone does transmit, or cause to be transmitted, a message that is inconsistent with an environment conducive to learning or with a misleading origination, the person who performed the transmission will be solely accountable for the message, not LBCCD, which is acting solely as the information carrier.

C. An environment free of illegal or malicious acts.

The user agrees never to use a system to perform an illegal or malicious act. Any attempt to increase the level of access to which (s)he is authorized, or any attempt to deprive other authorized users of resources or access to any LBCCD computer system shall be regarded as malicious, and may be treated as an illegal act.

D. A secure environment.

Any user who finds a possible security lapse on any system is obliged to report it to the system administrators. The system must not be used until the system administrator has investigated the problem.

E. Users are responsible for backup of their own data.

6006.6 An account assigned to an individual must not be used by others without written permission from the system administrator who assigned the account. The assigned individual is responsible for the proper use of the account, including proper password protection.

6006.7 Programs and files are confidential unless they have been made available, with written permission, to other authorized individuals. LBCCD reserves the right to access all information stored on LBCCD computers. File owners will be notified of file access and/or maintenance, in advance, if such notice is practical. When performing maintenance, every effort is made to ensure the privacy of a user’s files. However, if policy violations are discovered, they will be reported immediately to the violator’s supervisor.
6006.8 Electronic communications facilities (such as E-MAIL) are for college-related activities only. Fraudulent, harassing or obscene messages, and/or materials are not to be sent or stored.

6006.9 No one shall deliberately attempt to degrade the performance of a computer system or to deprive authorized personnel of resources or access to any college computer system.

6006.10 Loopholes in computer security systems or knowledge of a special password should not be used 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.

6006.11 Software Installation, Copies, Licenses and Ownership:

A. Computer software protected by copyright is not to be copied from, into, or by using college computing facilities, except as permitted by law or by the contract with the owner of the copyright. This means that such computer and microcomputer software may only be copied in order to make back-up copies, if permitted by the copyright owner. The number of copies and distribution of copies may not be done in such a way that the number of simultaneous users in a department exceeds the number of original copies purchased by that department.

B. Only legally purchased software may be used on LBCCD-purchased computers. Information Systems designated personnel will install LBCC-purchased software on computers provided for faculty or staff use.

C. Information Systems personnel will be available to assist in the installation of personally-owned software, which has been legally purchased by faculty or staff. To prove legal ownership and compliance with copyright restrictions, a copy of the license for faculty-owned or staff-owned software must be sent to Information Systems for retention by that department’s User Support/Network Coordinator.

D. Departments which have purchased software under a site license agreement must have the license agreement available on site to prove legal ownership and compliance with copyright restrictions or have sent a copy of the license agreement to Information Systems for retention by that department’s User Support/Network Coordinator.

6006.12 Any person detecting the apparent illegal use of software will report the suspected usage to the Executive Director of Academic Computing and Information Technology. The Executive Director of Academic Computing and Information Technology, after ascertaining the extent of such use, will meet with the appropriate dean or manager to discuss how any needed software can be legally purchased or licensed and the disposition of any illegal software.
An individual’s computer use privileges may be suspended immediately upon the discovery of a possible violation of these policies. Such suspected violation will be confidentially reported to the violator’s supervisors.

Violations of these policies will be dealt with in the same manner as violations of other college policies and may result in disciplinary review. In such a review, the full range of disciplinary sanctions available, including the loss of computer use privileges, dismissal from the college, and legal action, may be considered. Violations of some of the above policies may constitute a criminal offense.

6006.13 System administrators will establish more detailed guidelines, as needed, for specific computer systems and networks. These guidelines will cover such issues as allowable connect time and disk space, handling of unretrievable mail, responsibility for account approval, and other items related to administering the system.

6006.14 The following is a statement regarding this system that is mandated, or may soon be mandated, by Federal and State law. In some cases, local policy is also promulgated. This policy and procedure shall not be construed as a waiver of any rights of LBCCD:

The systems have the ability to read your mail: your own account, and the system administrator account. While reasonable attempts have been made to ensure the privacy of your accounts and your electronic mail, this is no guarantee that your accounts or your electronic mail is private. The systems are not secure, nor are they connected to a secure network.

6006.15 Appropriate regulations regarding student access to and use of computers and networks shall be developed, consistent with this policy and administrative regulations, approved by the appropriate vice president or designee and posted in prominent locations within all student-access computer areas and other appropriate locations throughout the college. These regulations shall be reviewed periodically and revised as needed.