6006. ADMINISTRATIVE REGULATIONS ON COMPUTER AND NETWORK USE

6006.1 The Chief Information Systems Officer shall administer these regulations. The District Computer and Network systems are the sole property of Long Beach Community College District. They may not be used by any person without the proper authorization of the District. The Computer and Network systems are for District instructional and work related purposes only.

6006.2 This regulation applies to all District students, faculty, and staff and to others granted use of District information resources (users). This regulation refers to all District information resources whether individually controlled or shared, stand-alone or networked. It applies to all computer and computer communication facilities owned, leased, operated, or contracted by the District. This includes personal computers, workstations, mainframes, minicomputers, phones, tablets, and associated peripherals, software and information resources, regardless of whether used for administration, research, teaching, or other purposes.

6006.3 Individual units within the District may define additional conditions of use for information resources under their control. These statements must be consistent with this overall regulation but may provide additional detail, guidelines, or restrictions.

6006.4 This regulation exists within the framework of the District Board Policy and state and federal laws. A user of District information resources who is found to have violated any of these policies will be subject to disciplinary action up to and including but not limited to loss of information resources privileges; disciplinary suspension or termination from employment or expulsion; or civil or criminal legal action.

6006.5 Computer users must respect copyrights and licenses to software and other on-line information.

Software protected by copyright may not be copied except as expressly permitted by the owner of the copyright or otherwise permitted by copyright law. Protected software may not be copied into, from, or by any District facility or system, except pursuant to a valid license or as otherwise permitted by copyright law.

The number and distribution of copies must be handled in such a way that the number of simultaneous users in a department does not exceed the number of original copies purchased by that department, unless otherwise stipulated in the purchase contract.

In addition to software, all other copyrighted information (text, images, icons, programs, etc.) retrieved from computer or network resources must be used in conformance with applicable copyright and other law. Copied material must be properly attributed. Plagiarism of computer information is prohibited in the same way that plagiarism of any other protected work is prohibited.

6006.6 Computer users must respect the integrity of computer-based information resources.

Computer users must not attempt to modify, delete, or remove computer equipment, software, intellectual property, or peripherals that are owned by others without proper authorization from the Chief Information Systems Officer or designee.

Computer users must not interfere with others access and use of the District computers. This includes but is not limited to excessive messages, either locally or off-campus; printing excess copies of documents, files, data, or programs, running grossly inefficient programs when efficient alternatives are known by the user to be available; unauthorized modification of system facilities, operating systems, or disk partitions; attempting to crash or tie up a District computer or network; and damaging or vandalizing District computing facilities, equipment, software or computer files.

Computer users must not intentionally develop or use programs which disrupt other computer users or which access private or restricted portions of the system, or which damage the software or hardware components of the system. Computer users must ensure that they do not use programs or utilities that interfere with other computer users or that modify normally protected or restricted portions of the system or user accounts. The use of any unauthorized or destructive program will result in disciplinary action as provided in this regulation, and may further lead to civil or criminal legal proceedings.

6006.7 Computer users must not seek to gain unauthorized access to information resources and must not assist any other persons to gain unauthorized access.

Users of District information resources must not access computers, computer software, computer data, or information, or networks without proper authorization, or intentionally enable others to do so, regardless of whether the computer, software, data, information, or network in question is owned by the District. For example, abuse of the networks to which the District belongs or the computers at other sites connected to those networks will be treated as an abuse of District computing privileges.

Any defects discovered in system accounting or system security must be reported promptly to the Chief Information Systems Officer or designee so that steps can be taken to investigate and solve the problem.

A computer user who has been authorized to use a password-protected account must not share that password and may be subject to both civil and criminal liability if the user discloses the password or otherwise makes the account available to others.

6006.8 Computer users must respect the rights of other computer users. Attempts to circumvent these mechanisms in order to gain unauthorized access to the system or to another person's information are a violation of District regulation and may violate applicable law.

Users may not use electronic communication facilities to send defamatory, fraudulent, harassing, obscene, threatening, or other messages that violate applicable federal, state or other law or District policy, or which constitute the unauthorized release of confidential information.

Electronic communication facilities may not be used to transmit commercial or personal advertisements, solicitations or promotions (see Commercial Use, below).

Users shall not send communications or messages anonymously or without accurately identifying the originating network account or station.

6006.9 Users must not intentionally seek or provide information on, obtain copies of, or modify data files, or programs belonging to other users without the permission of the business owner or designee of that intellectual property.

6006.10 The District is a non-profit, tax-exempt organization and, as such, is subject to specific federal, state and local laws regarding sources of income, political activities, use of property and similar matters.

District information resources must not be used for partisan political activities where prohibited by federal, state, or other applicable laws.

District information resources should not be used for personal activities not related to District functions, except in an incidental manner.

District information resources should not be used for commercial purposes. Users also are reminded that the ".edu" domains on the Internet have rules restricting or prohibiting commercial use, and users may not conduct activities not authorized within those domains.

6006.11 All users have the right to be free from any conduct connected with the use of District network and computer resources which discriminates against

any person on the basis of ethnic group identification, national origin, religion, age, sex, gender, gender identification, gender expression, race, color, medical condition, genetic information, ancestry, sexual orientation, marital status, physical or mental disability, or military and veteran status or on the basis of these perceived characteristics (Board Policy 3001). No user shall use the District network and computer resources to transmit any message, create any communication of any kind, or store information which violates any District regulation regarding discrimination or harassment, or which is defamatory or obscene, or which constitutes the unauthorized release of confidential information.

6006.12 The District reserves the right to monitor all use of the District network and computer to assure compliance with these policies. Users should be aware that they have no expectation of privacy in the use of the District network and computer resources. The District will exercise this right only for legitimate District purposes, including but not limited to ensuring compliance with this regulation and the integrity and security of the system.

Users must be aware of the possibility of unintended disclosure of communications.

It is possible for information entered on or transmitted via computer and communications systems to be retrieved, even if a user has deleted such information.

6006.13 The California Public Records Act (Government Code Sections 6250 et seq.) includes computer transmissions in the definition of "public record" and nonexempt communications made on the District network or computers must be disclosed if requested by a member of the public.

6006.14 Computer transmissions and electronically stored information may be discoverable in litigation.

6006.15 All users shall be provided copies of these regulations and be directed to familiarize themselves with them.

Users shall sign and date the acknowledgment included in this regulation stating that they have read and understand the standards within this regulation. This acknowledgment shall be as follows:

Computer and Network Use Agreement

By signing this document, I am acknowledging I have received, read, and understand the Long Beach City College District ("District") Administrative Regulation 6006 on Computer and Network Use.

I agree to abide by the standards set in the Administrative Regulations for the duration of my employment. I agree I will not share or otherwise provide my District network password to any other individual under any circumstance.

I am aware that any violation of the Administrative Regulations may subject me to the full range of disciplinary sanctions available, including the revocation of my network account through termination and/or criminal prosecution for violation of State or Federal law.

Adopted: November 17, 1997
Revised: May 24, 2011; July 24, 2012; December 11, 2019