Administrative Procedure
Chapter 3 – General Institution

AP 3720 COMPUTER AND NETWORK USE

References:

Government Code Section 3543.1 subdivision (b);
Penal Code Section 502;
Cal. Const., Art. 1 Section 1;
15 U.S. Code Sections 6801 et seq.;
17 U.S. Code Sections 101 et seq.;
16 Code of Federal Regulations Parts 314.1 et seq.;
Federal Rules of Civil Procedure, Rules 16, 26, 33, 34, 37, 45

The Executive Director, Information Systems and Technology shall administer this procedure. 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.

This procedure applies to all District students, faculty, and staff and to others granted use of District information resources (users). This procedure 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,

Legal Procedure

This procedure 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 procedures or the related policy will be subject to disciplinary action up to and including but not limited to loss of information resources privileges; disciplinary

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

Rights of Individuals

Email and Digital Communication

Electronic Civility - While the District encourages the free exchange of ideas, it is expected that this exchange will reflect the high ethical standards of the academic community and uphold standards

regarding discrimination or harassment, or which is defamatory or obscene, or which constitutes the unauthorized release of confidential information.

Disclosure

No Expectation of Privacy - 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 procedure and the integrity and security of the system.

Possibility of Disclosure - Users must be aware of the possibility of unintended disclosure of communications.

Retrieval - 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.

Public Records - 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.

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

Title IV Information Security Compliance
The District shall develop and maintain an information security program in compliance with the Gramm-Leach-Bliley Act which will include:

- A designated employee or employees to coordinate the entity's information security program.

- Identification of reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks. At a minimum, such a risk assessment should include consideration of risks in each relevant area of the entity's operations, including:

    (1) Employee training and management;

    (2) Information systems, including network and software design, as well as information processing, storage, transmission and disposal; and

(3) Detecting, preventing and responding to attacks, intrusions, or other systems failures.

- Design and implementation of information safeguards to control the risks the entity identifies through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.

- Oversee service providers, by:

  (1) Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue; and

  (2) Requiring the entity's service providers by contract to implement and maintain such safeguards.

- Evaluate and adjust the entity's information security program in light of the results of the testing and monitoring required; any material changes to the entity's operations or business arrangements; or any other circumstances that the entity knows or h ar

Approved: November 17, 1997
Revised: May 24, 2011; July 24, 2012; December 11, 2019; July 17, 2024

(Replaces former LBCC AR 6006)