Allan Hancock Joint Community College District
Board Policy
Chapter 3 – General Institution

BP 3720 COMPUTER AND NETWORK USE

Electronic communications and data systems of the District are provided to facilitate staff performance of District business and student participation in educational activities. Such systems include the devices used (for example: phones, printers, computers), the infrastructure (for example: data communication network, network storage, computer appliances), and the enterprise systems used (for example: email, Banner, ONESolution). Incidental personal use is secondary and must not interfere or conflict with business use.

The District holds that privacy, freedom of speech, academic freedom, and shared governance inform our use of electronic communications. This policy reflects the District's firm commitment to these principles within the context of the District's legal obligations.

Employees and students who use District computers and networks and the information they contain and related resources have a responsibility not to abuse those resources and to respect the rights of others. The Superintendent/President shall establish procedures that provide guidelines to students and staff for the appropriate use of information technologies. The procedures shall include that users must respect software copyrights and licenses, respect the integrity of computer-based information resources, refrain from seeking to gain unauthorized access, and respect the rights of other computer users.

Reference: Board Policies 6520 titled Use of Facilities and Services by College Employees & 4030 titled Academic Freedom and Responsibility Policy

Adopted: 1980
Revised: 4/17/01
Revised: 8/19/03
Revised: 5/10/16

(Replaces Board Policy 8990)

Allan Hancock Joint Community College District
Administrative Procedure
Chapter 3 – General Institution

AP 3720 COMPUTER AND NETWORK USE

The District computer and network systems are the sole property of the Allan Hancock Joint 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.

This procedure applies to all District students, faculty, and staff and to others granted use of District information resources. 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 computers and associated peripherals, as well as software and information resources, used for administration, research, teaching, or other purposes.

Conditions of Use

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 procedure but may provide additional detail, guidelines and/or restrictions.

Legal Process

This procedure exists within the framework of the District Board Policy 3720, state laws, and federal laws. A user of District information resources who is found to have violated any of these policies will be subject to action pursuant to the applicable collective bargaining agreement, Education Code, and/or other laws or regulations.

Copyrights and Licenses

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

- Copying - 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.

- Number of Simultaneous Users - 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.
- Copyrights - 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.

Integrity of Information Resources

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

- Modification or Removal of Equipment - Computer users must not attempt to modify or remove District computer equipment, software, or peripherals without proper authorization.
- Unauthorized Use - Computer users must not interfere with others' access and use of District computers. This includes but is not limited to unauthorized modification of system infrastructure, operating systems, or disk partitions; attempting to crash or tie up a District computer or network; damaging or vandalizing District computing facilities, equipment, software or computer files.
- Unauthorized Programs - Computer users must not intentionally develop or use programs (including all forms of malware such as spam, viruses, and worms) that disrupt other computer users or that access private or restricted portions of the system, or that damage the software or hardware components of the system. The use of any unauthorized or destructive program will result in disciplinary action as provided in this procedure, and may further lead to civil or criminal legal proceedings.

Unauthorized Access

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

- Abuse of Computing Privileges - Users of District information resources must not access computers, software, data or information, or networks without proper authorization, or intentionally enable others to do so.
- Password Protection - A computer user who has been authorized to use a password-protected account may be subject to both civil and criminal liability if the user discloses the password or otherwise makes the account available to others without permission of the Information Technology Services department.
- Responsibility to Report Problems - Any defects discovered in system security must be reported promptly to the Information Technology Services department so that steps can be taken to investigate and solve the problem.

Usage

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 procedure and may violate applicable law.

- Unlawful Messages - Users may not use District information resources to send defamatory, fraudulent, harassing, obscene, threatening, or other messages that violate applicable federal, state or other law or Board policy, or which constitute the unauthorized release of confidential information.
- Information Belonging to Others - Users must not intentionally seek or provide information on, obtain copies of, or modify data files, programs, or passwords belonging to other users, without the permission of those other users.
- Rights of Individuals - Users must not release any individual's (student, faculty, and staff) personal information to anyone without proper authorization.
- User identification - Users shall not send communications or messages anonymously or without accurately identifying the originating account, unless input is sought in an anonymous manner. Examples of permissible anonymous communications are student evaluations and responses to accreditation surveys.
- Political, Personal, and Commercial Use - The District is a public entity, 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.
    - Political Use - District information resources must not be used for partisan political activities where prohibited by federal, state, or other applicable laws.
    - Personal Use - District information resources should not be used for personal activities that interfere with District functions, except in a purely incidental manner.
    - Commercial Use - District information resources may not be used to transmit commercial or personal advertisements, solicitations, or promotions. Individual personal advertisements in authorized internal newsletters and bulletin boards will not be considered a commercial purpose.
    - Contractor or Subcontractor Use – Contractors or Subcontractors who require access to District information resources must formally request such access on their company letterhead specifying purpose, duration and a list of authorized persons. The request will be directed to and managed by Information Technology Services.

Disclosure

Privacy

Although the district holds that privacy, freedom of speech, and academic freedom, inform our use of electronic communication, users should also be aware that the District reserves

the right to monitor use of the District's network and computers to assure compliance with AP 3720.

- The District will only exercise this right for legitimate District purposes, for example: ensuring the integrity and security of the system or responding to a subpoena or court order.
- In addition, users should also be aware that Information Technology Services, contractor or external agency personnel may have incidental access to data contained in or transported by network, email, voice mail, telephone and other systems in the course of routine system operation, problem resolution and support.
- Every effort will be made to avoid such disclosure.

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 and computer must be disclosed if requested by a member of the public.
- Litigation - Computer transmissions and electronically stored information may be discoverable in litigation.

Limits to the District's Disclosure Responsibility

Users must be aware that all electronic communications and electronic documents may be subject to disclosure by the District in response to law enforcement investigations, judicial orders, California Public Records Act requests and other requests/demands that are outside of the District's control to limit or deny. Additionally, the District will notify the user of the disclosure demand and/or the response to that demand unless legally prohibited from doing so.

Dissemination

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

Board Policy 4030 titled Academic Freedom and Responsibility Policy and Board Policy 3730 titled Privacy Protection

---

Approved: 1980
Revised: 4/17/01
Revised: 8/19/03
Revised: 4/12/16
(Replaces Administrative Procedure 8990.01)