Computer Usage

Definition of "computer": Programmable, usually electronic, device that can store, retrieve, and process data (Webster's Dictionary).

The district computer-and-network systems are the sole property of MiraCosta 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. 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, servers, and associated peripherals (not restricted to but including printers, copiers, telephones, and projectors), software and information resources, regardless of whether 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 and Disciplinary Process

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 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, and/or civil or criminal legal action.

Copyrights and Licenses

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

Effective Date:	2/15/11, 5/20/16, 12/16/21
References:	17 United States Code §101 et seq. Penal Code §502 California Constitution, Article 1, Section 1 Government Code §3543.1(b) Federal Rules of Civil Procedure, Rules 16, 26, 33, 34, 37, 45
CCLC Update:	#9, 9/05; #11, 8/06; #12, 2/07; #24, 4/14; #25, 11/14; #27, 10/15, #31, 10/17
Steering:	VPAS/VPHR/VPIS/VPSS / N/A

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 computer equipment, software, or peripherals that are owned by the District and other service providers without proper authorization.

Unauthorized Use: Computer users must not interfere with others' access and use of the district computers. This includes but is not limited to the following: sending chain letters or 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.

Unauthorized Programs: Computer users must not intentionally develop or use programs that disrupt other computer users or access private or restricted portions of the system, or that damage the software or hardware components of the system. Computer users must ensure 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 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, 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.

Reporting Problems: Any defects discovered in system accounting or system security must be reported promptly to Academic Information Services (AIS) so that steps can be taken to investigate and solve the problem.

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.

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 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 that 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.

Political, Personal and Commercial Use: The district is a nonprofit, 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.

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

B. Personal Use: District information resources should not be used for personal activities not related to appropriate district functions, except in a purely incidental manner. The following are guidelines for this type of usage:

    1. Incidental personal use of computing resources is an *exception* to the general prohibition against the use of district equipment for anything other than official district business.

    2. Incidental computer use must meet these stipulations:

        a. Occasional use for personal purposes

b. Minimal time and duration

c. No additional cost to the district

d. No financial gain for the user

e. Not for business purposes where the business is owned by the employee or the work is done for another business

3. Incidental computer use must not interfere with assigned job responsibilities or be in violation of existing security access policies and procedures.

C. Commercial Use: Electronic-communication facilities may not be used to transmit commercial or personal advertisements, solicitations, or promotions. Some authorized college groups have been approved by the superintendent/president or designee to sell items and may be used appropriately, according to the stated purpose of the group(s). Users also are reminded that the ".cc" and ".edu" domains on the Internet have rules restricting or prohibiting commercial use, and users may not conduct activities not appropriate within those domains.

D. Contractors or subcontractors that require access to district data or information systems are required to read, sign, and comply with the compliance statement regarding contractor access to district data and information systems, which is available from and filed with Academic Information Services.

Acceptable Use of District Data and Information Systems

Different types of data have unique requirements as follows:

A. Student Data

1. Employee access to data is based upon job function. Security will be determined by the appropriate manager and granted accordingly by AIS staff.

2. Within the scope of an employee's job function, student data may be used in aggregate (not individually identifiable) form without prior permission, as long as the use is in compliance with federal and state privacy laws.

3. Outside the scope of an employee's job function, individually identifiable data may only be used with permission of the dean of Admissions, Assessment, and Student Aid or their designee. These uses might include contacting a student by telephone, mail, or e-mail.

4. Only the registrar is authorized to release student data. Any request for student data from law enforcement or other federal, state, or local authority or other agency must be cleared by the registrar or their designee.

B. Employee Data

1. Employee access to data is based upon job function. Security will be determined by the appropriate manager and granted accordingly by AIS staff.

2. Within the scope of an employee's job function, use of college personnel-directory information does not require prior permission.

3. Within the scope of an employee's job function, employee data may be used in aggregate (not individually identifiable) form without prior permission, as long as the use is in compliance with federal and state privacy laws.

4. Outside the scope of an employee's job function, individually identifiable employee data may only be used with permission of the director of Human Resources or their designee. These uses might include contacting an employee by telephone, mail, or e-mail.

5. Only the vice president of Human Resources is authorized to release employee data. Any request for employee data from law enforcement or other federal, state, or local authority or other agency must be cleared by the vice president of Human Resources or their designee.

C. Business Data

1. Employee access to data is based upon job function. Security will be determined by the appropriate manager and granted accordingly by AIS staff.

2. Within the scope of an employee's job function, business data may be used in aggregate form without prior permission as long as the use is in compliance with federal and state privacy laws.

3. Outside the scope of an employee's job function, specific business data may only be used with permission of the Director of Fiscal Services or their designee. These uses might include reporting on the status of a purchase requisition, disclosing the amount of payment to an employee or vendor, or reporting on the total amount spent by the district for particular goods or services.

4. Only the vice president, Administrative Services, is authorized to release business data. Any request for business data from law enforcement or other federal, state, or local authority or other agency must be cleared by the vice president, Administrative Services, or their designee.

D. Vendor Data

1. Employee access to data is based upon job function. Security will be determined by the appropriate manager and granted accordingly by AIS staff.

2. Within the scope of an employee's job function, vendor data, such as vendor proposals, bid specifications, or assessment test data may be used in aggregate (not individually identifiable) form without prior permission, as long as the use is in compliance with federal and state privacy laws.

3. Outside the scope of an employee's job function, individually identifiable vendor data may only be used with permission of the director of Purchasing and Material Management or their designee. These uses might include a bid amount submitted by a vendor in response to a district request for proposal or the legal owner of a particular business concern.

4. Only the director of Purchasing and Material Management is authorized to release vendor data. Any request for vendor data from law enforcement or other federal, state, or local authority or other agency must be cleared by the director of Purchasing and Material Management or their designee.

Nondiscrimination

All users have the right to be free from any conduct connected with the use of MiraCosta Community College District network and computer resources that discriminates against any person on the basis of accent, age, ancestry, citizenship, status, color, disability, economic status, ethnic-group identification, gender, marital, status, medical condition, national origin, parental status, race, religion, sexual orientation, or veteran status (as listed in Board Policy 3410). No user shall use the district network and computer resources to transmit any message, create any communication of any kind, or store information that violates any district procedure regarding discrimination or harassment, or is defamatory or obscene, or that 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 §§6250 et seq.) includes computer transmissions in the definition of "public record" 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.

Dissemination and User Acknowledgment

All users shall have access to these procedures and be directed to familiarize themselves with them.

Users shall sign and date the acknowledgment and waiver included in this procedure stating that they have read and understand this procedure and will comply with it. This acknowledgment and waiver shall be in the form as follows: