General Institution

COMPUTER AND NETWORK USE

References: *California Education Code Sections 32261, 32265, 32270, & 48900*
17 U.S. Code Sections 101, 107,110 et seq.;
18 U.S. Code Sections 110, 1462, 1465, 1466A, 1470, 2252B, 2252C
47 U.S. Code Section 230
Penal Code Section 502; Cal. Const., Art. 1 Section 1;
Government Code Sections 3543.1(b); and 12950.1;
Federal Rules of Civil Procedure, Rules 16, 26, 33, 34, 37, 45
Section 230 of the Communications Decency Act

SWC Policy 3050 BP - Institutional Code of Professional Ethics
SWC Policy 3430 BP - Prohibition of Harassment & Discrimination
SWC Procedure 5500 AP - Standards of Student Conduct
SWC Procedure 5530 AP - Student Rights and Grievances

Definitions

Academic Use: is defined to strictly cover use of College District computer and networks systems in the educational, teaching and learning environment for academic, artistic, scientific, literary, and research purposes.

Acceptable Use: is defined per College District Policy No. 3050 BP - Institutional Code of Professional Ethics, in particular as it relates to avoiding any conflict of interest appearance of impropriety between the obligations to the College District and private business or personal commitments and relationships; using College District time, supplies and equipment for non-business-related activities and refraining from using the goodwill or name of the College District for personal gain.

Copyright: (U.S. Copyright Office Definition) a form of protection provided by the laws of the United States for "original works of authorship", including literary, dramatic, musical, architectural, cartographic, choreographic, pantomimic, pictorial, graphic, sculptural, and audiovisual creations. "Copyright" literally means the right to copy but has come to mean that body of exclusive rights granted by law to copyright owners for protection of their work.

Cyber Bullying: California Education Code Sections 32261, 32265, 32270, and 48900 define bullying of students to include bullying committed by means of an electronic act, and authorizes school officials to suspend or recommend for expulsion students who engage in bullying. Violation of the standards (as set forth in Government Code Section 12950.1) and expectations of workplace conduct as set forth in the law or applicable policy. Workplace conduct by an employee, with malice, that a reasonable person would find hostile, offensive, and unrelated to an employer's legitimate business interests.

COMPUTER AND NETWORK USE

Personally Identifiable information (**PII**), or **Sensitive Personal Information** (**SPI**): as used in US privacy law and information security, is information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context. Computer users shall refrain from all acts of gathering/collecting and distribution with the intent of reselling PII or SPI.

Proper Authorization: is defined to entail the Governing Board approval of an employee for employment purposes or a consultant/contractor authorized to perform work under the terms of a designated contract/agreement/Memorandum of Understanding.

Proper authorization for purposes of releasing personal information is written authorization by the person whose information is being shared, whether that be a student or employee of the College District.

Proper Authorizations when relevant and as applicable shall also comprise authorization by the College District including authorization by College District's Human Resources Department or IT Department, whether it be verbal or written.

Personal profit/ Monetary gains: is defined to mean "individual profit" of which the College District receives no benefit from; provided, however, that this does not include faculty pursuing additional training/degrees, sabbatical work, research and writing for academic articles or books, from which the College District receives indirect benefit.

The College District Computer and Network systems are the sole property of Southwestern Community College District. They may not be used by any person without the proper authorization of the College District. The Computer and Network systems are for College District instructional and work related purposes only. The Network includes use of email with an @swccd.edu domain name, internet use through a school computer, school internet use through a guest computer, or use of any SWCCD electronic data systems such as but not limited to College District learning/educational systems, ERP system, commerce/accounting/finance systems, exchange mail, electronic filing systems and electronic communication systems.

This procedure applies to all College District students, employees and authorized users granted use of College District information resources, and govern desktop, network, email, telephone, internet, data security, and software uses of College District managed information technology equipment and resources. Pursuant to Policy 3050 BP, all employees of Southwestern Community College District are instrumental to the College District's mission of providing an environment in which students successfully achieve their educational goals and objectives. To support this mission, each employee is charged with personal responsibility to demonstrate a commitment to excellence in education without compromise

to the principles of ethical behavior, and to uphold the College District's Code of Professional Ethics.

Conditions of Use

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

Legal Process

This procedure exists within the framework of the College District policies, state and federal laws. The violations of this policy and procedure may subject the user to disciplinary action. Such disciplinary action must comply with relevant laws, policies and procedures and applicable collective bargaining agreements (including any progressive discipline provisions). Users may also be liable to the College District and/or third parties for violation of these policies, including misuse or misappropriation of personally identifiable information (PII), or Sensitive Personal Information (SPI), copyrights, trademarks and other intellectual property.

Copyrights and Licenses

Computer users shall follow all applicable protocols as it relates to laws governing 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 or licensor of the copyright, or as otherwise permitted by copyright law. Protected software may not be copied into, from, or by any College 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 any technology resources must be used in conformance with applicable copyright and other law. Copied material which has been lawfully copied must nonetheless be properly attributed. Plagiarism of computer information is prohibited but is not limited to the same way that plagiarism of any other protected work is prohibited.

COMPUTER AND NETWORK USE

Integrity of Information Resources

Acceptable Use of Information resources include:

- Use resources only for purposes authorized by this procedure;
- Protect user ID, password, and resources from unauthorized use;
- Access only information that is publicly available, or to which authorized access has been granted;
- Be aware of copyright laws as they apply to computer software and other materials that may be accessed with College District information technology resources.
- Be aware of Federal Laws, Privacy laws, and other applicable Penal, Civil, Government Codes and regulations that apply to College District computer and information technology use.

Unacceptable use of information resources include, but is not limited to:

- Modification or removal, or attempted modification or removal, of equipment without permission from Institutional Technology;
- Unauthorized use, or attempted unauthorized use, of another person's system access, user ID, password, files, or data, or giving one's system, user ID, password to another individual or organization;
- Disguising or attempting to disguise the identity of the account or computer being used;
- Gaining unauthorized access or attempting to gain unauthorized access to resources and data, including the passwords of other users;
- Circumventing, subverting, or disabling, or attempting to circumvent, subvert, or disable system or network security measures;
- Engaging, or attempting to engage, in activities that may lead to disruption of services, or which interfere with the normal operation of computing resources, including activities that place an excessive load on the system;
- Engaging, or attempting to engage, in cyber bullying activities;
- Intentionally damaging files or making unauthorized modifications to College District data;
- Downloading, making or using, or attempting to download, make or use copyrighted materials: (1) without the proper license, or (2) by means of illegal copies of copyrighted materials, software, or music, store such copies on College District resources, or transmitting them over College District networks;
- Creation, display, distribution, or attempted creation, display or distribution of threatening, racist, sexist, defamatory, or harassing material which is in violation of existing law or College District policy;
- Other than for Academic Use, creation, production, distribution, receiving, display (visual representation) transferring of obscene matter (obscene matter as established

by the U.S. Supreme Court), which is in violation of all applicable Federal laws or College District policy and procedures;

- Use or attempted use of the College District's resources or networks for personal profits/ monetary gains;
- Installation, or attempted installation, of unauthorized hardware or software onto any College District owned computer/network (the Institutional Technology Department or appropriate College District authorized personnel are responsible for all installations, requests for exceptions should be sent to the Chief Information Systems Officer);
- Connecting or attempting to connect a personal computer to the College District's network that does not meet technical and security standards established by the College District;
- Using or attempting to use College District information resources for commercial purposes for personal profits/monetary gain in the open marketplace.;
- Intentionally seeking or providing information regarding obtaining copies of, or modifying data files, programs, or passwords belonging to other users, without the permission of those other users;
- Releasing or attempting to release any individual's (student, faculty, and staff) PII or SPI to any third party without Proper Authorization;
- Releasing or attempting to release any individual's (student, faculty, and staff) PII or SPI to any third party for personal profits/monetary gain in the open marketplace;
- Sending mass advertisements or solicitations for personal profits/monetary gain;
- Using or attempting to use College District information resources for partisan activities where prohibited by local, state, federal, or other applicable laws;
- Using computing and information resources in a manner that violates federal laws, privacy laws, and other applicable penal, civil, government codes and regulations that apply to College District computer and information technology use.

Reporting Problems - Any defects discovered in system accounting or system security must be reported promptly to the appropriate system administrator or IT so that steps can be taken to investigate and solve the problem. For cases of Cyber Bullying, reporting should take place with Student Affairs for student issues and with Human Resources for faculty and staff issues.

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 system administrator. Users are required to change passwords as mandated by the College District. User passwords at Southwestern must meet specific complexity requirements which include; at least 8 characters in length, an English uppercase letter, an English lowercase letter, or a number. A non-alphabetic character may be substituted for one of the last three

listed criteria. A password must be changed at least once every 6 months and history of the last 30 passwords is enforced. Additionally, account lockout features are set where 10 invalid attempts are allowed with a time out of 10 minutes.

Personal Use - College District information resources should not be used for personal activities not related to College District functions, except in a limited capacity and/or a purely incidental manner.

Nondiscrimination

All users have the right to be free from any conduct connected with the use of the College District network and computer resources which discriminate against any person on the basis of race, color, religion, national origin, gender, sexual orientation, disability, age, marital status or any other protected classification. No user shall use the College District network and computer resources to transmit any message, create any communication of any kind, or store information which violates any College District procedure 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 College District reserves the right to monitor all use of the College District network and computer to assure compliance with the law and these policies and procedures. Users must be aware there is no expectation of privacy in the use of the College District network and computer resources. The College District will exercise this right for legitimate College District purposes, including, but not limited to, data that is discoverable in litigation, ensuring compliance with this procedure, and the integrity and security of the system. Permission from the Superintendent/President, or his/her designee, is required to access electronic data beyond standard and routine operations.

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 College District network or computers must be disclosed if requested by a member of the public. A user’s documents and other computer information created and/or stored on College District computers and networks may be considered public records and subject to disclosure under the Public Records Act or other laws, or subject to discovery as part of litigation.

COMPUTER AND NETWORK USE

Dissemination and User Acknowledgment

All users shall be provided copies of this procedure 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.