Technology Policies & Procedures

Employees and students are required to immediately notify campus security if they witness someone on campus with a weapon. In the event that campus security cannot be located, students must immediately report the incident to the nearest campus staff member.

Students or employees found in violation of this policy will be subject to the full range of disciplinary actions set forth in the **Student Code of Conduct** (applicable to students only) or the **Employee Handbook** (applicable to employees only).

In addition, students and employees are strongly urged to notify the Campus President about any restraining order in effect for themselves or any potentially violent situation outside of school or work that could result in violence on the campus.

CAMPUS SECURITY REPORT

A Campus Security Report is published annually for each ***SJVC*** campus. Information on the following is included in the report:

- Preparation, distribution and responsible parties of the CSR, including Campus Security Officers
- Access to Campus Facilities
- Campus policies on reporting criminal actions and other emergencies
- Security and Crime Prevention Awareness Prevention
- Timely Warning and Emergency Notification
- Drug and Alcohol Abuse Education
- Campus Sexual Violence Elimination Act
- Sexual Assault, Domestic Violence, Dating Violence, and Stalking Prevention and Response Procedures
- Sex Offender Registration
- 2014-2016 Crime Statistics

Copies of the report are distributed annually to all ***SJVC*** students and employees and may be requested from members of Campus Leadership.

TECHNOLOGY POLICIES

SJVC supports and encourages the use of technology in the educational process. The College recognizes the importance of equipping students with the necessary technological resources to achieve their educational goals and objectives. As such, students have access to various technology resources both on and off-campus. The technological resources available for student use include personal computers, computer equipment, and a network which allows access to the email system, internet, portal ("InfoZone") and Learning Management System. These resources are to be used for the primary purpose of facilitating and enhancing the educational experience. Any other use is limited and priority is given to individuals using the resources for educational purposes.

This section sets forth the College's policies pertaining to the use of its technological resources. This information is provided to give students an understanding of the various

technological resources available to them as well as the College's expectations of all students who utilize these resources. By using these resources, students agree to comply with all applicable policies and guidelines published herein.

Personal Technology Devices

Students may bring personal technology devices (PTD) on campus. PTDs include, but are not limited, to:

- Laptops
- Netbooks
- iPad/iPods
- Smartphones
- Tablets
- Kindles/Nooks/or other similar devices
- Web-enabled phones

Following are the guidelines for use of PTD's on campus:

- PTDs must be silenced during class time and may only be used with the express permission of the faculty member teaching the course.
- All audio/video functions must be disabled unless the student is given permission from the faculty member teaching the course to record all or a portion of the class session.
- PTDs may not be used to photograph ***SJVC*** employees, clinical sites, clinical patients, and clinical employees. Fellow ***SJVC*** students may only be photographed with their permission.
- ***SJVC*** does not provide any support or technology services for PTDs.
- ***SJVC*** assumes no responsibility for lost, stolen, or damaged PTDs.
- Students may not use their PTDs outside the classroom for non-educational purposes while on the ***SJVC*** wireless network.
- All terms and conditions of the Computer and Email Use policies apply to students' use of the ***SJVC*** wireless network on their PTDs. (See Catalog – Technology policies)

- Students are not to share the ID and password for the wireless network with non-***SJVC*** users.

Failure to adhere to these guidelines may result in disciplinary action. Any questions pertaining to appropriate use should be directed to by a member of the faculty.

Social Media

SJVC recognizes and supports the use of social media as a means of communication and fostering connectedness among users. To that end, ***SJVC*** maintains several social media sites (Facebook, Twitter, Instagram) that are updated regularly with news and information about college events, programs, and student accomplishments. Students are encouraged to fully leverage these resources for information-sharing purposes and to establish better communication across campuses.

Due to the capacity and reach of social medial, student posts have the potential to reach a much larger audience than intended. As such, the use of social medial requires a greater level of responsibility and accountability. ***SJVC*** students represent the College even when they are posting on non-***SJVC*** social media sites. Following are some general guidelines to ensure appropriate use of social media on both ***SJVC*** and non-***SJVC*** sponsored sites:

- Use good judgment when posting to social media sites. Once you post something to social media, you can never remove it – all of your posts are archived online; even those that you have deleted. Think about the image you want to project – does it align with your professional goals? Some employers use social media as a tool to screen applicants for employment – don't post something that may jeopardize your future employment opportunities.
- While the College recognizes that externship and clinical training generates anticipation and excitement, students may not post information, pictures, or personal statements of any form regarding their externship or clinical experience, patient conditions, and/or staff encounters (both positive and negative) on social medial sites (Facebook, Twitter, Instagram, Tumblr, Pinterest, Google+). Doing so may violate the Health Insurance Portability and Accountability Act (HIPAA). Potential and actual HIPAA violations put both the College and the student at risk of liability.

The only exception is when the College solicits student comments and/or photos ("selfies") for the ***SJVC*** blog. In these situations, an ***SJVC*** employee will provide explicit information and guidelines for submissions.

- Students are highly discouraged from posting unprofessional or negative comments about classmates or the faculty on the ***SJVC*** and/or their personal social media accounts. As mentioned above, this type of behavior is viewed as unprofessional and may tarnish the student's reputation, and, ultimately, jeopardize future employment prospects. Students should use the established ***SJVC*** protocols for addressing complaints. (See ***SJVC*** Student Handbook, "Student Complaints & Grievances")
- Students may not use social media during class or clinical time – no exceptions!

Students who have questions or concerns about how these guidelines might apply to them or a specific situation should discuss the matter with a member of the faculty. Willful disregard of these guidelines may result in the full range of disciplinary action as set forth in the ***SJVC*** Student Code of Conduct. (See Student Handbook)

Recording

Students may not record any portion of a scheduled educational activity (e.g., class, lab, clinical/externship, or field trip) without the express permission of the faculty member teaching the course.

Computer Use

SJVC's computers, software, and any files stored on the computer or network are College property. All hardware and software are to be used primarily for educational purposes. Although students have passwords that restrict access to their computer accounts, ***SJVC*** may access personal e-mail accounts and any files stored or deleted from the computer system, at any time.

All software that resides on any of ***SJVC's*** computers must be licensed. ***SJVC*** prohibits the installation or removal of any software, unless directly related to a specific assignment approved and under the direction of the faculty member teaching the course. Users are also forbidden from altering or copying licensed software.

SJVC will not tolerate destruction or vandalism of any of its computer equipment. It also forbids the deliberate waste of computer resources. Disciplinary penalties, as outlined in the **Student Code of Conduct**, may be imposed upon any student who has been found in violation of this policy.

When leaving a computer terminal, students must either log off or shut the computer down in order to preserve and maintain the security of the network.

SJVC provides students with access to the internet for the purpose of enriching their educational experience. Although it is the College's intent that the internet will be used for achievement of educational goals and course objectives, every student should be aware that some material accessible via the internet could contain items that are illegal, defamatory, inaccurate, or potentially offensive. Each individual user is strongly cautioned to exercise prudent judgment in what materials are viewed, stored, or routed to others.

Students are solely responsible for using this resource in an educationally effective, efficient, ethical, non-discriminatory, and lawful manner. The following list, while not exhaustive, describes the acceptable and unacceptable usage of the internet through the ***SJVC*** network.

Acceptable Use

- Using the internet to conduct research related to the course(s) in which a student is enrolled.
- Using a current and valid ***SJVC*** user account.
- Using the internet to engage in electronic communication with the faculty, administration, staff, or fellow students through email and discussion boards.
- Any purpose that supports the educational mission of ***SJVC*** and is in keeping with the laws of the State and Federal government.

Prohibited Use

- Using the internet for commercial purposes and/or private enterprises that are not College related.
- Creating, displaying, or transmitting threatening, racist, sexist, discriminatory, pornographic, obscene or harassing language and/or material.
- Using the College's computer network to engage in illegal downloading and/or unauthorized distribution of copyrighted material, including peer-to-peer file sharing.
- Misrepresenting oneself as another user.
- Providing, assisting in, or attempting to modify or gain access to files, passwords, and data belonging to other users.
- Attempting to access restricted areas of the computer network belonging to ***SJVC***.
- Attempting to undermine or compromise the security of the College's computer network or any other computer network or workstation.
- Destruction of or damage to the equipment, software, or data belonging to the College or other users.
- Activities that interfere with the ability of others to use resources effectively.
- Activities that result in the loss of another user's work or unauthorized access to another user's work.
- Disclosure of user identification and/or password to another individual; using another individual's computer account for any purpose.
- Any other activity conducted through the College's computer network, including personal e-mail accounts, or use of the internet deemed by the College to be in violation of the **Student Code of Conduct**, College rules, and State or Federal laws.

Any misuse of the internet through the ***SJVC*** network constitutes a breach of the **Student Code of Conduct**. ***SJVC*** is the sole judge of what constitutes a breach. If the College determines that a student has engaged in unacceptable use of its technological resources, the student may be subject to the full range of disciplinary actions set forth in the **Student Code of Conduct**.

Copyright Infringement

Students, faculty and staff are prohibited from using the ***SJVC*** computer network to illegally download or share music, videos, or other copyrighted materials. ***SJVC*** supports the Higher Education Opportunity Act (HEOA) and Digital Millennium Copyright Act, including efforts to eliminate the illegal distribution of copyrighted material. Under the law, the College may be obligated to provide information to copyright holders and law enforcement officials about ***SJVC*** network users who have violated the law.

SJVC network users should be aware that illegal forms of downloading and file sharing as well as the unauthorized distribution of copyrighted materials are violations of the College's **Technology Policies** and may subject student offenders to the full range of disciplinary actions set forth in the **Student Code of Conduct**. In addition to violating College policy, offenders may also be subject to various penalties under civil and criminal copyright law, including monetary damages and prison time.

Network users are responsible to ensure that any file that they are downloading is not a copyrighted work, unless they have prior, written permission from the copyright holder.

To protect their intellectual property, companies have licensed hundreds of digital partners who offer a range of legal downloading options, including download and subscription services, legitimate peer-to-peer services, video-on-demand, podcasts and CD kiosks. For a list of sources that offer legal downloading sites, visit the RIAA website at https://www.riaa.com/ Questions pertaining to copyright issues should be directed to a member of the faculty.

Email Use

SJVC provides an email account for every student with a current network account and valid password. Students may use the email system for the primary purpose of communicating with members of the faculty, College administration and staff, and fellow students concerning their coursework or College-related business. The College reserves the right, if circumstances warrant, to access, inspect, and disclose the contents of messages created, sent, or received using the email system.

It is the responsibility of all email account holders to manage the use, message content, and size of their email accounts. Reading email daily, removing old messages, and deleting messages and attachments of unknown origin are among the most common practices that help ensure an efficient email system.

Unacceptable use of the email system puts both the user and the College at risk. Unacceptable use of the email system includes, but is not limited to:

- Unauthorized attempts to access another's email account.
- Sharing email account passwords.
- Violation of Federal, State or local laws or statutes pertaining to electronic communications.
- Sending harassing, threatening, abusive, or obscene messages.
- Broadcasting excessively large amounts of data (chain letters, graphic presentations, etc.) in such a way as to cause network congestion and failure

Any misuse of the College's email system may result in the imposition of disciplinary actions as outlined in the **Student Code of Conduct**.

Monitoring
In addition to College staff supervision during computer lab sessions, in the classroom, Student Center, or the LLRC, ***SJVC*** reserves the right to audit or randomly audit student computer user accounts. Upon discovery of a possible violation of the policies stated herein, a student's computer privileges may be suspended immediately. Such suspected violations will be reported to the appropriate member(s) of the Campus Leadership.

Violations of these policies will be addressed in a manner consistent with violations of other College policies or State and/or Federal law and may result in the College taking disciplinary action against the student, as well as possible legal action. In such review, the full range of disciplinary sanctions is available including the loss of computer privileges, termination from ***SJVC***, and legal action.

Reporting Suspected Violations
Any suspected violations of the **Computer**, **Internet**, or **Email Use Policies** should be immediately reported to Campus Leadership. Questions concerning this section should be directed to Campus Leadership.

STANDARDS FOR PROFESSIONAL DRESS

SJVC believes that it is important for each student to appear well groomed and professionally dressed while on campus or during situations in which students are representing the College. As such, ***SJVC*** has established standards for professional dress to which all students are expected to adhere. The standards include the requirement that students dress for class, including externships and clinical rotations, in the professional work-related ***SJVC*** uniform designated for their particular program of study.

Students are not permitted to wear their uniforms at events or functions that are not sponsored by the College. Any exception to the professional dress standards needed to comply with religious requirements must be discussed with the Dean of Student Services. For information on additional dress and grooming standards, please refer to the **Student Handbook**.

In addition to this policy, many ***SJVC*** programs have specific professional dress code requirements that students are expected to comply with. For information concerning specific programmatic dress codes, please see the respective Program Director or Division Manager.

STUDENT RIGHTS

Student rights are protected by State and Federal laws, and by the policies, procedures, and regulations established by ***SJVC.*** Specifically, we recognize these student rights:

- Freedom of access to higher education
- Freedom of classroom expression
- Confidentiality of educational records
- Participation in student affairs
- Procedural standards in disciplinary actions as outlined in the **Student Code of Conduct** and the **Academic Honesty Policy**
- An environment free from discrimination or harassment

ADDITIONAL POLICIES & PROCEDURES

The following publications contain additional information on student policies and procedures.

Student Handbook
Statement of Student Rights
Student Code of Conduct
Sexual Misconduct/Harassment
Student Complaints & Grievances
Academic Honesty
Dress Code & Grooming Requirements
Student Computer and Network Use
Eating and Drinking
Cell Phone Usage
Attendance
Academic Policies
Change of Student Information

Student Disability Accommodation Policy
Discrimination Prohibited
Admissions, Enrollments, and Recruitment
Academic Adjustments
Procedures for Determining Disability and Accommodations
Grievance Procedures Concerning Disputes and Accommodations

Substance Abuse Prevention Program Handbook
Substance Abuse
Medical Marijuana
California Drug and Alcohol Punishment
- Opiates and Depressants
- Marijuana
- Alcoholic Beverages

Federal Penalties
Federal Trafficking Penalties Marijuana
Drugs of Abuse/Uses and Effects
Federal Penalties
Federal Trafficking Penalties Marijuana
Drugs of Abuse/Uses and Effects

Campus Safety Procedures Manual
Medical Emergencies
Hazardous Material Spill or Release
Fire/Emergency Evacuation Protocol

SECTION 1
STUDENT SERVICES

SJVC offers a wide range of services that support students in their academic, professional, and personal endeavors. While the delivery of support services may vary based upon each campus' unique student population, the type and availability of services remains the same throughout the institution. For further information, please contact the Office of the Dean of Student Services.

NEW STUDENT ORIENTATION

On-Ground Campuses

All new students will participate in a group orientation prior to their first day of class. Orientation provides you with a valuable opportunity to meet the campus staff and faculty who will be providing support and instruction to you during your time at ***SJVC***. You will also be given the opportunity to meet other new students, receive valuable information and tips (e.g. study habits, note taking, carpool information) and available community resources. Orientation also provides the opportunity to ask any additional questions you may have prior to the first day of class.

Orientation for most programs is conducted on the Friday prior to a Monday start date. Campuses or programs with a different start schedule will conduct orientation at some point in the week preceding the program start date. The specific date, time, and location of the orientation will be communicated to you during the admissions process. If you know in advance that you will be unable to attend or are unexpectedly absent from orientation, please contact your Admissions Advisor immediately.

Online Division

Students who enroll in an online or hybrid program will complete the Online New Student Orientation; an online course covering a wide range of topics designed to prepare students for success in the online environment.

COMPUTER LOCATIONS

Every campus is equipped with computers and printers which are available for student use. Computers are located in designated classrooms, the Student Center, and the Library and Learning Resource Center (LLRC). The LLRC and Student Centers are the main locations for you to access computers outside of the classroom. The hours of operation vary by campus and are generally posted at each facility.

Computer Labs

The computer labs are available to all ***SJVC*** students, faculty, and staff. College staff supervise the labs to ensure that users abide by the rules of use.

Certain labs have restricted access but, in general, students may utilize the labs on a walk-in basis. If a class is being conducted in a computer lab, the lab is closed for general use until the class is over. You may request advance permission from instructors to work quietly in the lab while a class is in session.

Depending upon the size of the campus, you may be limited to a certain number of consecutive hours in the lab or you may be asked to relinquish the equipment per the priorities specified above.

In addition to the terms of use outlined in the **Computer**, **Internet**, and **Email Use policies,**[1] students must abide by the following rules:

- The labs will have a professional atmosphere at all times.
- Users are expected to conduct themselves in a quiet and respectful manner. Loud conversations and disruptive behavior will not be tolerated.
- Do not connect or disconnect lab equipment. If equipment needs to be connected, contact the SJVC Help Desk (help@sjvc.edu).
- Personal files should not be stored on lab computers. While ***SJVC*** does provide a limited amount of electronic storage space to each student user (see "**File Storage System**" below), any data or files saved to a lab computer will be periodically erased without warning.

If you use the computer labs, be aware that a violation of any of the College's technology policies may result in disciplinary action.[2] Further, any violation(s) which constitutes a criminal offense as defined by local, state, or federal laws may be referred to the appropriate agency for prosecution.

Questions concerning the use of the College's network, computers, or computer equipment should be directed to the Office of the Dean of Student Services.

File Storage System

Students will be assigned a personal folder on the ***SJVC*** servers to be used primarily for purposes related to your coursework. The data stored on your folder is password protected. Sharing your password could result in having your data compromised. You are ultimately responsible for the long-term retention of your data.

Privacy

Please be aware that there is no guarantee of privacy when using the ***SJVC*** network and computer system. While precautions are taken to protect student privacy and the integrity of their data, there is the possibility that others may inadvertently view email messages or data.

SJVC employees may find it necessary to view electronic data while troubleshooting problems in the system. They may also be required by law to provide computer files to third parties (e.g., in the case where electronically stored data is subpoenaed as evidence).

Further, ***SJVC*** reserves the right to review or monitor network traffic, e-mail messages, files, or other data for legitimate purposes, including, but not limited to: an emergency, investigation of suspected abuse or misconduct, or to remove material that may be illegal or that which violates College policies, rules, or regulations. ***SJVC*** will suspend a user's account if it is believed necessary to protect the integrity of the system, to curtail abuse, or during an investigation.

INFOZONE

Our website portal, known as ***InfoZone***, provides access to essential student information. ***InfoZone*** may be accessed at https://infozone.sjvc.edu.

Academic Information and Resources

The Academic Info section within ***InfoZone*** makes it possible for you to view your campus calendar, college publications and handbooks, access discussion boards and current event stories, and download your unofficial transcripts. ***InfoZone*** also gives you access to your course schedule, current courses and assignments, learning resources, grades,

[1] Published in Section 4 of the College Catalog.

[2] Computer, Internet, and Email Use policies (College Catalog, Section 4)

attendance, account statements, financial aid information, and more.

InfoZone also provides easy access to various educational resources including libraries, web sites, databases, museums, and repositories of research.

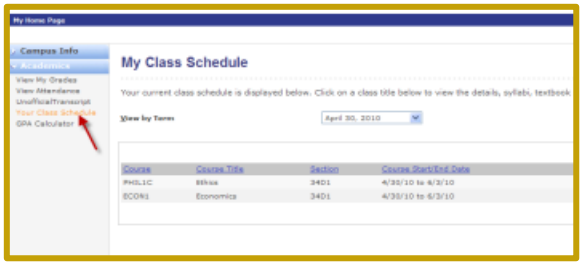
Tutorials
There are several tutorials available which provide step-by-step instructions on how to access various types of information. (InfoZone>Training & Help)

Email System
You may access and utilize the ***SJVC*** email system through ***InfoZone***. An email account will be created for all new students. Student email accounts are to be used primarily for communicating with your instructors, ***SJVC*** staff, and other students.

In addition to the terms of use outlined in the ***SJVC*** **Computer**, **Internet**, and **Email Use policies** published in the **College Catalog**, all users are expected to abide by the generally accepted rules of online etiquette when utilizing the College's email system. These include, but are not limited to, the following:

- Be polite and professional at all times. Do not use profanity or vulgar language. Abusive messages will not be tolerated.
- Do not reveal personal identification information such as a social security number, phone number, address, or personal information of others.
- Be aware that email is not considered private communication. System administrators have access to all electronic messages.
- Do not use the network in such a way as to disrupt the use of the network by others.

eCourses
eCourses is ***SJVC's*** virtual learning environment. eCourses allows you to access your courses in an online environment. This gives you the ability to stay connected to your instructors and course materials beyond the classroom setting.



For example, eCourses provides access to course syllabi, grades, and student learning outcomes. Many instructors use eCourses to provide important class updates, have students take exams, and generate course discussions. In addition, eCourses may be used to electronically submit coursework and access supplemental course materials. Lastly, eCourses is a resource you may use to voice your opinion on your course experience through an online course survey.

Technical Support Information
If you experience technical difficulties, you may request assistance from Technical Support Services. Technicians may be reached as indicated below:

Phone: (800) 530-7244
Email: help@sjvc.edu
Remote Control Support: https://remote.sjvc.edu

Hours of Availability
Monday – Thursday
7 a.m. to 6 p.m.
Friday
7 a.m. to 4 p.m.
Closed Weekends and Holidays

FINANCIAL AID

You may access your financial aid information through ***InfoZone*** as follows:

1. Login to https://infozone.sjvc.edu. **Remember to type ed\ before your username.**
2. Click on the **Academic Info** tab.

3. Login to **Academic Info**. **Do not type in ed\ before your username.**
4. Click on the **My Financial Aid** tab, then click on the item you would like to review (e.g., Award Letter).

All books, files, records, documents, appointment books and any other items relating to the College's business which have been or shall be prepared, possessed or controlled by employees during their employment and which either relate to the College's business or result from any work performed by the employee for the College are and shall forever remain the sole and exclusive property of the College. Accordingly, all employees shall surrender any and all such material to the College immediately upon request, or upon termination of their employment.

Upon employment, all employees are required to sign an agreement pertaining to non-disclosure of confidential information.

12. FERPA REQUIREMENTS

Family Educational Rights and Privacy Act (FERPA) is federal law designed to protect the privacy of education records, to establish the right of students to inspect and review their education records, and to provide guidelines for the correction of inaccurate and misleading data through informal and formal hearings.

It is the responsibility of every employee of the College to abide by these requirements and protect the privacy of education records. Violations of FERPA will result in disciplinary action up to and including discharge.

Employees are required to view the audio and visual PowerPoint presentation outlining FERPA requirements. To access this training go to:

InfoZone > Training & Help > Academic Info/CampusVue Library > FERPA Update

13. ELECTRONIC MEDIA USE

Purpose

This policy governs the use of electronic media by all *San Joaquin Valley College* employees, and applies to electronic media and all documents, recordings and other data contained in or recoverable from such media used by the College. This policy applies to all electronic media provided by the College as well as that used on College property for business purposes.

Online instructors working out of their homes and/or offices using their own electronic media must follow College policies and procedures that apply to conduct, behavior, responses, and teaching methods which represents the College and/or connects the online instructor to the College in any manner.

Scope

Electronic media include all types of electronic equipment, such as FAX machines, cell phones, voicemail systems, computers, computer peripherals, computer software, laptops, loose or removable media, electronic mail (e-mail), Internet access, World Wide Web access, social media access, online information services, Course Management System, televisions, VCRs/DVDs and any other equipment that the College deems as

electronic media.

Allowable Uses

Electronic media are provided to College employees to be used primarily for business related purposes. Allowable uses of College owned electronic media for College business purposes include:

- To facilitate performance of job functions
- To facilitate communication of information within the College
- To coordinate meetings of individuals, locations and resources of the College
- To communicate with outside organizations as required to perform an employee's job function.

Prohibited Uses

Electronic media provided by the College may not be used for personal purposes or any other purposes unrelated to College business. This prohibition applies at all times, whether the employee is on working time or not.

Prohibited uses of electronic media include, but are not limited to the following:

- Violating local, state and/or federal law
- Use in a way that may be disruptive, offensive to others, or harmful to morale
- Harassing or disparaging others in violation of applicable federal, state, or local law, which may include harassment or disparagement based on race/color, national origin/ancestry, sex, sexual orientation, gender identification, domestic partner status, age, disability, or religious or political beliefs. For example, the College prohibits the display or transmission of sexually explicit images, messages or cartoons, or any transmission or use of electronic communications that contain ethnic slurs, racial epithets, or anything that may be construed as harassment or disparagement of others.
- Threatening others
- Soliciting or proselytizing others for commercial ventures, religious or political causes, outside organizations, or other non-job related matters
- Intentionally disrupting network traffic or crashing the network and connected systems (for example, sabotaging and/or intentionally introducing a computer virus)
- Accessing others' files without authorization and with no substantial business purpose
- Vandalizing the data of another user
- Forging electronic and/or voicemail messages
- Wasting system resources
- Misrepresentation of the College
- Inappropriate and/or unauthorized website logging [blogging] or threaded discussions
- Personal social networking
- Sending personal messages such as chain letters
- Downloading music or video

- Internet gambling
- Online personals, dating or chat rooms
- Online pornography
- Using electronic media inappropriately, in a way deemed by the College to violate the intended purpose of any electronic media

Privacy

Employees shall have no expectation that the information they convey, create, receive, view, file, store or delete in such media will be confidential or private.

The College reserves the right to unrestricted access to electronically stored information stored electronically. This may include, but is not limited to retrieving business information, troubleshooting hardware and software problems, preventing system misuse, assuring compliance with software distribution policies and complying with legal and regulatory requests for information.

Supervisors, department managers, as well as the Information Systems staff of the College reserve the right to enter, search, monitor, copy and/or retrieve the computer files, voicemail, e-mail or any other type of electronic file of any employee, without notice, for business purposes including, but not limited to, investigating theft, disclosure of confidential business or proprietary information, use of the system for personal reasons or for any other purpose unrelated to College business, or for monitoring work flow or productivity.

Given these business requirements, the College cannot guarantee the privacy of documents and messages stored in company-owned files, desks, storage areas, and electronic media or produced by FAX machines. Information or files deleted from electronic media may not have been permanently deleted from the system. It is possible to recover deleted computer files, deleted e-mail and deleted voicemail messages at any time.

Although the College reserves the right to access such information, employees are strictly prohibited from accessing another employee's computer diskettes or files, voicemail or e-mail messages. In addition to the foregoing provisions, employees should note that data, files, messages and information on the College's computers, servers, and voicemail system might be subject to disclosure pursuant to discovery in litigation.

Computers, Computer Software, Laptops, PDA's, Phones and Computer Files

The College's computers, software and files stored on the computer or network are College property and are used primarily for its business purposes. Although employees have passwords that restrict access to their computers, the College may access any files stored on or deleted from the computer system. For security purposes, when leaving an office, employees should either lock or log off the computer even when locking their office.

All software that resides on any of the College's computers must be licensed; therefore, employees are prohibited from installing or removing software on College-owned equipment. Employees are prohibited from removing or down loading information to diskette, CD or thumb drive, etc., unless directly related to specific job assignments

approved by an immediate supervisor.

Use of Personal Electronic Media Equipment

An employee may choose to use his/her personal electronic media that includes, but is not limited to; computers, computer software, laptops, PDA's, and computer files for *business use only* on College property in lieu of equipment provided by the College. Use of personal electronic media is not required or requested by SJVC. However, if you choose to use personal electronic media on College property, you must comply with and agree to the following College policies, requirements and guidelines:

- Any electronic media shall be used for SJVC business purposes only.
- There should be no expectation of privacy when using personal electronic media on College property. SJVC reserves the right to monitor, review, and access or record any information, files or programs displayed, stored or transmitted through the use of any electronic media you choose to use on any College property. Although employees may have passwords that restrict access to their electronic media, be advised that if you choose to use your personal electronic media on College property, SJVC may access the electronic media and any files, information, programs or e-mail messages stored on or deleted from any electronic media irrespective of such passwords. Any electronic media used on College property shall be made immediately available for inspection upon request by SJVC.
- The employee is responsible for ensuring that all software on the electronic media was legally purchased, and is responsible for maintaining all license agreements for all such software. All such license agreements must be made available to SJVC for inspection and verification upon request.
- The employee is responsible for maintaining current antivirus software on his/her personal equipment. The employee is also responsible for ensuring that access to any student, course or any College or business-related information on his/her personal equipment (electronic media) is restricted and limited to their own use and that of SJVC.
- The employee is responsible for ensuring that any student, course or any College or business-related information on personal equipment (electronic media) is backed up on an appropriate medium to ensure that no information is lost or destroyed.
- SJVC is not responsible for lost, stolen or damaged personal equipment.
- Because of the nature of the Internet and wireless communications, no privacy or safeguards can be assumed. Therefore, employees shall not use their electronic media to send confidential information, including any student information, through the Internet or through any wireless transmission. Any Email accounts used on electronic media on College property are to be used strictly for business purposes.
- The following use of the laptops are expressly prohibited on College property:
  - The use of electronic media on College property for any non-business use;
  - Visitation to any WEB sites that are not business related;
  - Visitation to any and all sexually explicit internet sites;
  - Displaying, posting, transmitting, storing or downloading inappropriate material, such as sexually explicit images, messages, or cartoons, materials or information containing ethnic slurs, racial epithets, or anything that may be construed as harassment or disparagement of others based

on any protected category including, but not limited to, race, national origin, sex, sexual orientation, gender identity, age, disability, religion or political beliefs.

Online Information Service Use

Use of online information services, such as the Internet, Social Media and the World Wide Web and Course Management System, is restricted to approved plans and services provided by the College. Online information services may be used for College business related purposes and may not be used for personal reasons or any other purpose unrelated to College business. Access to online information services should be limited to a reasonable amount of time. The standard for a reasonable amount of time will be established at the discretion of the College.

Passwords

Passwords are an important aspect of computer security and they are the front line for network user accounts. A poorly chosen password may result in the compromise of SJVC's entire corporate network. As such, all SJVC employees and contractors or vendors with access to SJVC systems are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

- All network passwords (e.g., user account, CampusVue, Evolution, etc.) must be changed at least every six months.
- When away from a computer it should be locked or logged off even if your office is secured.
- All passwords must conform to the guidelines described below.

Passwords must meet the following guidelines:

- Must be a minimum of eight characters long
- Contains at least one number
- May not be based on personal information, names of family, etc.

Do not share SJVC passwords with anyone; all passwords are to be treated as sensitive, confidential SJVC information.

If an account or password is suspected to have been compromised, report the incident to the SJVC Information Services Department and change all passwords.

Password cracking or guessing may be performed on a periodic or random basis by SJVC or its delegates. If a password is guessed or cracked during one of these audits, the user will be required to change it immediately.

Any employee found to have violated this policy may be subject to disciplinary action, up to and including discharge.

Voicemail

Although employees have passwords that restrict access to voicemail messages left for

them on the system, employees should be aware that the College can access any messages stored in the voicemail system and may do so for any reason at any time. Therefore, employees may not assume that such messages are confidential.

E-mail / Threaded Discussions / Instant Messaging

Electronic mail, threaded discussions and instant messaging addressed to, generated by, or received by employees on the College's computers, servers, cell phones, etc. is the property of the College and should be used primarily for business related purposes. As with voicemail, although employees have passwords that restrict access to their computers, the College may access any files, e-mail messages, threaded discussion and/or instant messaging stored on or deleted from the computer system. The College reserves the right to access such information for any purpose at any time. Therefore, employees may not assume that such email, discussions and messaging are confidential.

Employees are to use only their SJVC address/email when corresponding and/or conducting business with College contacts, accrediting entities, agencies, etc.

When an employee separates from the College their email access is disabled and emails are forwarded to the supervisor for thirty days after employment ends. At the end of that period, the account is deleted.

Checking Email on a Regular Basis

The College uses email to communicate and distribute important and/or required information, including electronic Employee Status Updates (ESUs), acknowledgements of receipt, etc., to its employees. To assure that everyone is well informed of important matters and or respond in a timely manner employees are required to check their email on a regular basis. At a minimum an employee should check his/her email once daily [on scheduled work days].

Social Media

Business Use

The College uses social media in limited circumstances for defined business purposes. Social media is a set of Internet tools that aid in the facilitation of interaction between people online. Use of Internet based programs such as Facebook, LinkedIn, Instagram and Twitter (this is not meant to be an exhaustive list – if you are unsure or have specific questions about which programs the College deems to be social media, consult with your supervisor or Human Resources) may be used in furtherance of College goals. The College's public relations department will develop approved sites for authorized employees to use. Your Campus Director will authorize you in writing if you can use these tools to perform your job duties. Your authorization is limited to business purposes and personal use of these tools during work hours is prohibited and can result in discipline up to and including discharge.

Personal Use

San Joaquin Valley College understands that its employees and students participate in

social networks on a personal level on their own time outside of SJVC, and in acknowledging this the college expects that employees will do so in a responsible manner. The absence of explicit reference to specific sites does not limit the extent of the application of this policy. Where no policy or guidelines exist, employees should use their professional judgment and take the most prudent action possible. Employees should consult with his or her Campus or Corporate Director when uncertain.

- Employee published comments, information, videos and/or images should comply with the college's confidentiality and disclosure of proprietary information policies. This would apply to employee comments posted on other blogs, forums, v-logs and/or social networking sites.
- Employee personal blogs, v-logs, and/or postings on social networking sites shall not violate College policies against inappropriate usage, including the College's no tolerance for discrimination, harassment or retaliation in the workplace.
- Employee personal blogs or v-logs should include disclaimers that clearly establish that the views the employee as expressed are solely his or her views and do not represent the views of the college. Personal blogs or v-logs should be written / stated in a first person format so that it is clear that the employee is speaking for him/herself and not on behalf of the college.
- Employee participation in social media activities should not interfere with work commitments.
- Employee actions captured by images/videos, posts and/or comments should not be negatively and/or unprofessionally associated to the college.
- Employee references and/or citations may not be of a college employee, student, and/or associate.
- Employee should respect copyright laws, and reference or cite sources within these laws.
- Employee may not use the college logo and/or program emblems.

San Joaquin Valley College will not request or required employees or applicants to:

- Disclose their user name or password to gain access to personal social media content;
- Access their personal social media in the presence of a College representative; or
- Divulge any personal social media content.

Unless there is reasonable belief that the employee's personal social media content is related to an investigation of misconduct or a violation of the law, or the College is requesting or requiring an employee to disclose his or her user name, password, or other method for the purpose of accessing an employer-issued electronic device.

Violations of Policy

Violations within the college's media electronic use policy will be reviewed on a case-by-case basis and may result in disciplinary action, up to and including discharge.

14. PROHIBITING USE OF A CELL PHONE WHILE DRIVING

The College is concerned about the safety of its employees and emphasize that

employees should not feel obligated to conduct work related calls or text messages while driving; therefore, San Joaquin Valley College employees are prohibited from using cell phones while driving on College business and/or College time. Personal and/or company provided cell phones are to be turned off any time you are driving on College business or College time.

If your job requires that you keep your cell phone turned on while you are driving, you must use a hands-free device and safely pull off the road before conducting College business. Under no circumstances should employees place phone calls or text messages while operating a motor vehicle while driving on College business and/or College time.

Persons under the age of 18 years are prohibited from driving a motor vehicle while using a wireless telephone, even if equipped with a hands-free device, or while using a mobile service device. The prohibition would not apply to such a person using a wireless telephone or a mobile service device for emergency purposes. Violating this policy is a violation of law and a violation of College policy that may result in disciplinary action up to and including discharge.

15. USING CAMERA PHONES OR OTHER RECORDING/PICTURE-TAKING DEVICES

Employees are not permitted to use any camera or any other recording / picture-taking device in any area without expressed permission and never in areas that the College has designated as secure.

Employees must also respect the privacy of fellow employees. Camera phones and/or any other recording/picture-taking devices are prohibited in restrooms, changing rooms, break rooms, lunchrooms and areas designated to provide and/or solely used by women to express breast milk.

Violations of this policy will be reviewed on a case-by-case basis and may result in disciplinary action, up to and including discharge.

16. PUBLIC REQUESTS FOR INFORMATION

The integrity of any business is dependent upon its presentation in the community. It is important that we give out only accurate and factual information that can be substantiated by the College.

The College has disclosure statements regarding the completion, placement, graduate salary and licensure exam pass rates as well as catalogs and handbooks available upon request.

The provisions of the Family Education Rights and Privacy Act of 1974 limits disclosure of certain types of information pertaining to students, including student records. Before releasing student information to anyone other than the student himself or herself, we ask that you consult with the Vice President of Administration.
All requests for verification of employment should be forwarded to the Human Resources Department.

SJVC Email Retention Policy

Overview

In order to maintain an efficient and reliable email system, SJVC has implemented an Email Retention Policy that is applied to all folders on all SJVC email accounts. Emails will be stored in one of three locations within a user's account for a period of up to but not to exceed 5 years from date of receipt for received mail or date of creation for sent items.

Terms and Concepts

Primary Mailbox

A user's primary mailbox contains all folders such as inbox (including subfolders), sent items, and deleted items, etc, for a user's account on the main Exchange server storage level. It is accessible via Outlook and Outlook Web Access.

Online Archive

A second Exchange server storage area where items from any folder in a user's account are moved to after a period of one year. The Online Archive appears as a second set of folders in the account and is accessible via Outlook and Outlook Web Access.

eDiscovery (Legal Department Access Only)

A third storage area where all mail is housed for legal retention. These emails are inaccessible to users and can be retrieved only via request by the Legal Department. This is a third Exchange server storage area where items from any folder in a user's account are moved to after a period of three years. Items remain in eDiscovery for a period of 2 years.

Permanently Deleted

Items are removed from SJVC servers and are unrecoverable.

Active Employee Policy

All sent and received mail is stored upon creation or receipt in a user's Primary Mailbox. After a period of 1 year from the date of receipt or creation, items are moved to the Online Archive. Items remain in the Online Archive until they have reached 3 years from date of creation or receipt at which time they are no longer accessible to users.

Items older than 3 years are moved to the eDiscovery storage area for legal retention purposes and are no longer accessible to the end user.

Emails are permanently deleted when 5 years from the date of receipt or the date of creation has been reached.

Table 1 summarizes this policy.

Table 1 : Active Employee Policy

Dates	**Action**	**Storage Area**
Receipt date		Primary mailbox
Receipt date + 1 year	Move to	Online Archive
Receipt date + 3 years	No longer accessible to user	
	Move to	eDiscovery for legal retention
Receipt date + 5 years	Permanently delete	

Separated Employee Policy

Upon separation of employment with SJVC an employee's mailbox will have their direct supervisor granted access to all mail. Access to the separated employee's Primary Mailbox and Online Archive will be granted to the direct supervisor. The employee's email address will remain active and able to receive mail for a period of 30 days following separation. Upon the 31st day following separation all mail in the separated employee's Primary Mailbox and Online Archive will be moved to eDiscovery. The direct supervisor will no longer have access to any email from the separated employee's account. The separated employee's email address will be disabled and unable to receive mail. All email in the eDiscovery storage area will be deleted at 5 years beyond the date of receipt or date of creation. Table 2 summarizes this policy.

Table 2 :Separated Employee Policy

Dates	**Action**	**Storage Area**
Receipt date		Primary mailbox
Termination date + 30 Days	Forwarded to supervisor – still receiving email	Primary mailbox
> 30 Days from termination date	Move mailbox to eDiscovery – account disabled	eDiscovery
Receipt date + 5 years	Permanently delete	