Policy Title	Acceptable Use	**Policy Number**	210
Section	Financial Affairs and Development	**Approval Date**	1/13/2004
Subsection	General Financial Policies	**Effective Date**	1/13/2004
Responsible Office	Information Technology	**Review Date**	3/4/2021

1.0 Purpose

1.1 The purpose of this policy is to establish basic guidelines for the appropriate use of computing resources (including but not limited to: computers, laptops, electronic mail, the Internet, mobile devices, and related electronic products) at Jamestown Community College (JCC). Jamestown Community College has created this policy to maximize the benefits of its computer resources and minimize potential liability.

2.0 Policy

2.1 It is the policy of JCC that all JCC employees, Foundation employees, FSA employees, students, and other computer users are obligated to use these resources responsibly, professionally, ethically, and lawfully. To ensure that all individuals granted access to the college computing resources are responsible productive users who protect the college's public image, the college has established guidelines for using the computing resources, electronic mail, the Internet, and related electronic products on its computers.

3.0 Procedures

3.1 Password Requirements. Jamestown Community College requires all JCC employees, Foundation, FSA personnel, students, and other computer users to use his or her own unique login username and password to access computing resources. This identity verification process is to protect the individual's privacy. Individuals are responsible for maintaining his or her own secure password on college owned equipment and on personal devices that are used to access college files and/or data. Passwords are not to be shared with others. Upon approval of the Executive Director of Technology, guests and consultants are issued a temporary password that expires upon completion of their visit.

3.2 Communications. All users are responsible for all content they place or send over the college network or Internet. Illegal activities and fraudulent, harassing, abusive, profane, obscene or offensive messages are prohibited. All messages communicated on the Internet should have the user's name attached. No messages will be transmitted under an assumed name. Users may not attempt to obscure the origin of any message. Information published on the Internet should not violate or infringe upon the rights of others. Users who wish to express personal opinions are encouraged to obtain their own usernames on other Internet systems.

3.3 Social Networking. Social media allows users to share information and resources over the Internet. Social media includes but is not limited to blogs, social networking, Internet forums, and photo/video sharing sites. For more information, refer to JCC's "Social Media Procedure."

Information posted on official college sites is information posted directly from the college. The college is not responsible for information posted to sites not officially affiliated with JCC. A list of officially affiliated SUNYJCC sites is found in the "Social Media Procedure."

3.4 Computers and Computer Networks. The following activities constitute a breach of ethics and are prohibited:

- Unauthorized access to and/or modification of files, programs, or system software;
- Unauthorized use of passwords and/or accounts to obtain access to information networks;
- Deliberate attempts to sabotage the normal operation of systems.

3.5 Copying Software. Copying software from any JCC computer system is illegal. Software is protected by the Federal Copyright Law as printed material and violation can result in criminal charges and college disciplinary action.

3.6 Copyright violations. The following activities are contrary to existing U.S. copyright legislation:

- Unauthorized duplication of copyrighted material;
- Distribution of illegally copied material;
- Unauthorized alteration of copyrighted material.

3.7 Peer-to-peer file sharing. JCC's "Peer-to-peer File Sharing" policy forbids illegal file sharing. Violation of copyright is a federal offense. Using a computer to copy or store any copyrighted material (text, images, music, movies, computer programs, etc.) in violation of state and federal law, and leaves the perpetrator liable, upon conviction, to heavy fines and possibly imprisonment.

3.8 Disclosure of confidential information. It is against college policy to seek out or use personal or confidential information relating to others for personal interest or advantage. Employees or agents of the college responsible for the collection, maintenance, use, and dissemination of information about individuals that relates to individuals' personal lives, including employment, medical history, financial transactions, marital status, and dependents, must hold this information in confidence.

3.9 Ethical Standards. Computing systems exist for the constructive manipulation of information. All JCC employees, Foundation, FSA personnel, students, and computer users should be guided by prevailing principles used to govern other processes and academic environments at Jamestown Community College. Conduct of users should take into account issues such as courtesy and good taste as well as those of pure legality. Users must not present false identification or misleading information to gain access to computing resources or use computing resources for which users are not authorized.

3.10 Internal email. Internet e-mail will be used for college related business only. Non-college related items such as the sale of personal items, discussion of non-college related issues, and the promotion of non-college related events is prohibited.

3.11 Network Code of Conduct. JCC's computing facilities are networked to provide for the most efficient use of limited resources. Access to college computer systems, software, networks, and the Internet is provided for the benefit of the college.

3.12 Software. Software purchased must be approved by the department and the Executive Director of Technology. Installation requests for software are made through the JCC Help Desk and approved by the technology department. If the software must be purchased, a departmental budget number and request should

be processed through the office of Information Technology Services.

3.13 Ownership. The computer systems and devices purchased by Jamestown Community College are owned by the college unless specifically indicated otherwise and should be used for college business or academic purposes only. Employees who are issued a college owned mobile device (i.e. laptops, iPads, and mobile phones, etc.) must sign an equipment checkout form. The systems are not intended for personal business. All software and files on Jamestown Community College's computer systems are the property of the college. The college reserves the right to inspect/delete/print files from all software and accounts. In addition, the college reserves the right to revoke computing privileges of any user. Users shall receive notification prior to any action taken unless extenuating circumstances prevent it.

3.14 Privacy: Users are given access to the college's computer network to assist in performing job duties or completing your academic tasks. Users should not have an expectation of privacy in anything users create, store, send, or receive on the computer system. Without prior notice, the college may review any material created, stored, sent, or received on its network or through the Internet or any other computer network.

3.15 Saving Work: Personal files and/or software should not be stored on the local computer hard drive.

3.16 Security: All messages created, sent, or retrieved over the Internet are the property of the college and should be considered public information. The college reserves the right to access and monitor all messages, files on the computer as deemed necessary, and appropriate. Internet messages are public communication and are not private. All communication, including text and images, can be disclosed to law enforcement or other third parties without prior consent of the sender or receiver.

3.17 Systems regulations: Individuals who receive computer login credentials (username and password) are liable for all activities on their accounts. Usernames and passwords are given the same significance as a handwritten signature; delegation of a username and password to another person, or use of another person's username or password, may be considered false representation.

3.18 All Users Prohibited Activities. Use of computer resources for the following activities is strictly prohibited, but not limited to:

- Monitoring, reading, or intercepting email, files, or electronic communications of other employees, or third parties, except in cases in which explicit authorization has been granted by the Vice President of Administration or designee;
- Knowingly sending, receiving, downloading, displaying, printing, or otherwise disseminating material that is sexually explicit, profane, obscene, harassing, fraudulent, racially offensive, defamatory, or otherwise unlawful;
- Disseminating or storing commercial or personal advertisements, solicitations, promotions, malicious software (i.e., viruses, self-replicating code, etc.) or political information;
- Computer resources should not be used for conducting private business affairs. Nor should computer resources be used for personal gain or advancement of individual views (i.e., commercial consulting or manuscript preparation for hire);
- Conducting business for political purposes;
- Wasting computer resources by, among other things, sending mass mailings or chain letters, spending excessive amounts of time on the Internet, social media, playing games, engaging in online chat groups, printing multiple copies of documents, printing excessively long Internet documents or otherwise creating unnecessary network traffic;
- Violating the privacy of others, including using other people's login credentials;
- Hacking or obtaining access to systems or accounts they are not authorized to use;
- Using programs (such as copying the password file or password cracking programs) that are designed to probe, describe, or to defeat computer security features of computer systems located

at the college or elsewhere, or the use of ordinary tools (e.g., ping) in a manner that may probe or describe network topology or computer security features without the express written consent of the Executive Director of Technology;

- Attempting to gain access to any system for which the person is not an authorized user;
- Decrypting, or attempting to decrypt, scrambled files (e.g., the password file) that are not owned by the user;
- Using "network packet capture" or similar software programs so as to gain access to communications or data to which the user is not a party in a manner that degrades system or network performance (i.e., transmission of software containing a virus, Trojan horse, worm, or other malicious software);
- Altering systems configuration files (i.e., autoexec.bat or config.sys);
- Removing college-owned software, or alter files owned by another user;
- Downloading from the Internet any copyrighted material without explicit written permission from the author;
- Uploading to the Internet, posting, publishing, transmitting, or reproducing in any way, information, software or other material which is protected by copyright or other proprietary right;
- Uploading to the Internet, posting, publishing, electronically transmitting, or reproducing in any way college information that is confidential or legally protected according to the college's Information Security Program;
- Engaging in any form of harassment over the Internet, commonly referred to as cyberbullying. Cyberbullying includes, but is not limited to the following: transmitting unlawful messages to anyone that is threatening, abusive, libelous, obscene or pornographic, stalking, whether in text, audio, or graphic form; on the Internet such as through email, blogs or social networking sites.
- Sending unsolicited messages (such as chain letters or electronic junk mail) that may be perceived as harassing, annoying, or obscene; Interfering with or intercepting the electronic communications of another user;
- Obscuring or to attempting to obscure the identity and location of a remote connection;
- Physically abusing or misusing college computing equipment, and
- Engaging in activities prohibited by local, state, or federal law.

3.19 Rules & Regulations for Shared Computing Labs

3.19.1 Purpose of Computing Labs: The primary purpose of Jamestown Community College's computing facilities is for completion of class assignments requiring the use of college-owned software and hardware. Individuals who receive a computer login credentials (username and password) are liable for all activities on their accounts. Users should never sign anyone else in under their account.

3.19.2 Hours: Operating hours for computing labs are posted. The technology staff reserves the right to close the facilities with little or no notice for repair purposes. Hours may vary during vacation periods, summer sessions, and during mid-term recesses.

3.19.3 Internet Access: The technology staff makes every effort to provide Internet access to users searching academic resources in the computing facilities. Recreational use of the facilities may be limited during peak usage times.

3.19.4 Games: Games are not allowed in the computing facilities unless permission is granted by technology personnel.

3.19.5 Personal Equipment and Software: Users are not allowed to connect personal laptops into the network with a physical wire without special permission from the technology department. Personal software may not be loaded onto any networked computers in the computing facilities.

3.19.6 Saving Work: No one is allowed to store personal work and/or software on the hard drives in the computing facilities. All users should have a personal storage device for saving their work. Any files or software found on the hard drives will be deleted. The technology staff is not responsible in any way for unsaved data lost due to power failure, computer failure, or any other unplanned or unavoidable event or emergency.

3.19.7 Virus Protections: Technology staff reserves the right to refuse entry into a computing facility to any individual who has a non-removable virus on his/her storage device. In addition, technology staff reserves the right to remove any individual who refuses to scan their device.

3.19.8 Printing: There are a limited number of printers available in the student computing lab facilities. To avoid printing delays and backups, please print only necessary files.

3.20 Access to College Computing Facilities. The following individuals are provided with access to college computing facilities:

- **Students:** Registered students of Jamestown Community College have the privilege to access designated computing resources on campus.
- **Faculty/Staff:** All JCC employees, Foundation employees, FSA employees, students, and computer users have the privilege to access computing resources on campus unless otherwise specified by their supervisor. VPN connectivity must be utilized when remotely accessing college computing resources except publicly available web resources.
- **Authorized Guests:** Those individuals doing legitimate business with the college (i.e., Workforce Readiness customers, rentals, consultants, vendors).

3.21 Violations and Reporting.

3.21.1 Violations of this policy will be taken seriously and may result in disciplinary action according to the Student Conduct Code or the appropriate faculty or staff contract/procedure. Users not subject to the Student Conduct Code or the faculty or staff contract/procedure may face suspension of privileges, possible employment termination or college expulsion, and civil or criminal liability.

3.21.2 If users become aware of someone violating these policies, users are obligated to report the incident immediately to the Executive Director of Technology.

4.0 Definitions

VPN - A virtual private network is an encrypted connection over the Internet from a device to a network. The encrypted connection helps ensure that sensitive data is safely transmitted. It prevents unauthorized people from eavesdropping on the traffic and allows the user to conduct work remotely.

5.0 References