Electronic Communications Code of Conduct

SVA's computer services and facilities are an important aspect of its educational mission, which includes a commitment to the pursuit of academic excellence and the highest level of artistic expression. To achieve these goals, all users of computing resources are expected to behave in a responsible, ethical, and legal manner, in accordance with the following guidelines which apply to internal and external electronic communications, Internet usage, SVA owned or licensed hardware and software, voicemail communications, and the content of all electronic data created and stored. Students, faculty, staff, vendors, temporary workers, and alumni should have no expectation of personal privacy with respect to matter stored in, created by, received by, or sent via SVA's computer systems and facilities.

Authorized SVA staff members monitor and record computing access in order to maintain security and the highest level of operation of the administrative computing resources. Internal communication systems, electronic messages, files and data, and all hardware and software are, and remain the property of, SVA at all times. Subject to the provisions of applicable law, SVA has the right to retrieve, review, and monitor any message or file composed, sent, received, or rendered accessible through SVA equipment or technologies, including any message or file deleted from the SVA computer system or voicemail system. Although access to SVA networks and email accounts allow for the use of passwords for security, be advised that confidentiality should not be assumed and ultimate privacy should not be expected, subject to the provisions of applicable law. SVA reserves the right to monitor access and usage of SVA's communication facilities for any reason, and without warning, prior consent, or notification to the individual.

All accounts are issued for the sole use of students, faculty, staff, vendors, temporary workers, or alumni. Users are responsible for all actions on the account issued to them and should take the proper precautions to safeguard its usage. Users are not permitted to share login credentials for SVA networks, systems, or applications. Users will be required to follow the password creation guidelines as listed in SVA's Password Policy document.

Users are not permitted to use SVA computing facilities in any manner that violates institutional policies or procedures, or any federal, state, or local law, including the provisions of the Family Educational Rights and Privacy Act designed to protect the confidentiality of data and the privacy of individuals. Unauthorized downloading, copying, or distribution of copyrighted materials in SVA facilities or using SVA networks or technologies, is strictly prohibited. Duplicating and downloading copyrighted software, music, movies, and other data is illegal and expressly forbidden by SVA policy, and can lead to termination of access, and disciplinary or legal action.

Users cannot delete, examine, copy, or modify files and/or any other data belonging to other students, faculty, staff, vendors, temporary workers, or alumni without prior consent. Users will not attempt to spread computer viruses, Trojan horses, worms, or any program designed to violate security, interfere with the proper operation of any computer system or technology, or destroy another person's data. Users are not permitted to install any unauthorized software on any SVA-owned computer system or device.

All shared computer stations are configured to delete locally stored data every 24 hours through a re-imaging process. Users must ensure their work is backed-up while using any SVA computer systems. SVA is not responsible for backing up or recovering student data to/from SVA-owned computer stations. User data can be backed-up using a locally attached hard drive, USB thumb drive, or cloud storage services, such as Google Drive. Google Drive is available for all students, faculty, staff, and alumni at no charge, and offers unlimited cloud-based storage.

Users should not expect confidentiality on the SVA network. Subject to the provisions of applicable law, systems and network administrators have the legal right to read/access files and email being transmitted over SVA networks. This includes all accessed information for any purpose whatsoever, as well as possible monitoring by SVA of websites visited, chat rooms, instant messages, news groups, social networking activities, email (including personal password-protected email accounts accessed using SVA's systems), and blogs, as well as review of deleted files, temporary files, cached files, browsing history, metadata, and other electronic information stored on SVA's central back-up system or otherwise available as part of its data management. Whenever electronic mail is sent, your name and user ID are included with the message. Users are responsible for all electronic mail originating from their user ID.

Internet access should not be used for personal gain, advancement of personal views, or for solicitation of business unrelated to SVA. In addition, users should not send or upload SVA copyrighted materials or proprietary information to unauthorized parties outside of SVA. Electronic communications or any websites (regardless if owned or operated by SVA) accessed by students, faculty, staff, vendors, temporary workers, or alumni should not contain anything that would reasonably be considered offensive or disruptive to another employee. Offensive content includes, but is not limited to, sexual comments or images, racial slurs, comments that would offend someone on the basis of gender (including gender identity), race, color, religious or political beliefs, creed, pregnancy, disability, age, sexual orientation, marital status, national origin, genetic predisposition or carrier status, alienage or citizenship status, military or veteran status, domestic violence status, or other legally protected status. At all times, individuals remain subject to the College's Harassment Policy. Users that discover that they have inadvertently accessed an inappropriate website or system, must immediately disconnect from that website or system.

Access to any and all SVA systems, regardless of the technology that they fall under or employ, including, but not limited to hardware, software, and infrastructure (including wiring) is restricted to the authorized personnel assigned to maintain and manage that technology and infrastructure. Unauthorized access and/or alterations to any hardware, software, infrastructure component, or technology is strictly prohibited.

Any violation of the SVA Electronic Communications Code of Conduct may result in disciplinary action up to and including expulsion from the College, termination of employment, and legal action. In addition, activities believed to be illegal in nature may be referred to the proper authorities.

The technological resources (i.e. computer and networks resources) provided by the College reflect the computing and networking environment at large. Since this environment is dynamic and constantly evolving, these guidelines may change accordingly. It is the responsibility of each user in the SVA community to stay informed of current policy. The intent of the Electronic Communications Code of Conduct policy is equally applicable.

The College reserves the right to use software/hardware filters and other techniques/technologies whenever possible to restrict access to inappropriate information on the Internet by students, faculty, staff, vendors, temporary workers, and alumni at all areas on campus including, but not limited to, labs, classrooms, libraries, offices, and residence halls. Additionally, domain names,

Internet website categories, or individual websites that consume excessive amounts of network resources, or pose a security risk to SVA, will be subject to review and possible temporary or even permanent blocking. Requests to unblock legal/valid domain names can be sent to the SVA Help Desk, and are usually addressed in 1-2 business days.

DISCLAIMER

SVA assumes no liability for any direct or indirect damages arising from the user's connection to the Internet. SVA is not responsible for the accuracy of information found on the Internet, and only facilitates the accessing and dissemination of information through its systems. Users are solely responsible for any material that they access and disseminate through the Internet.