San Ramon Valley Unified School District

Acceptable Use Guidelines for Technology

San Ramon Valley Unified School District makes a variety of communications and information technologies available to students through computer/network/Internet access. These technologies, when properly used, promote educational excellence in the District by facilitating resource sharing, innovation, and communication. Illegal, unethical or inappropriate use of these technologies can have dramatic consequences, harming the District, its students and its employees. These Acceptable Use Guidelines are intended to minimize the likelihood of such harm by educating District students and setting standards which will serve to protect the District. The District firmly believes that digital resources, information and interaction available on the computer/network/Internet far outweigh any disadvantages.

Mandatory Review

The District requires legal, ethical and appropriate computer/network/Internet use. To educate students on proper use and conduct, students and parents/legal guardians are required to review these guidelines at the beginning of each school year and acknowledge understanding of the guidelines. In addition, Responsible Use Guidelines for Technology are part of the Student Code of Conduct handbooks.

Student Access/Student Safety

Access to the District's electronic communications system, including the Internet, is made available to students for instructional purposes and to enhance learning consistent with the District's educational goals. Access to the District's computer/network/Internet is a privilege, not a right. The Network has filtering software that blocks access to inappropriate or harmful material and images as defined by the federal Children's Internet Protection Act (CIPA).

Student Email Accounts

Electronic communication is an important skill for 21st Century students. Email and other digital tools such as blogs and wikis are tools used to communicate within the District and beyond. SRVUSD students will be issued email accounts with access differentiated by grade level:

Grades 9-12: Email for open use on the Internet. This type of email account can be used to exchange email with any email account anywhere. District "inappropriate language" and spam filters are in place, but as with commercial email providers, these filters are not 100% preventative.

Grades 6-8: Email for District Internal Use Only. To ensure student safety and compliance with COPPA law these accounts can only be used to exchange email within our district @students.srvusd.net or @srvusd.net domains. In other words, email with district students and staff only.

Grades K-5: Email accounts for District Internal Use Only are issued on request by the students' teacher.

All student email accounts are set up with the student's user ID and are available while they are currently enrolled in the District.

San Ramon Valley Unified School District

Subject to Monitoring

Access and/or use of District Technology constitutes the User's acknowledgement and consent to this policy as well as his/her consent to the District's recording and monitoring of his/her use (whether for personal or business purposes) of District Technology, at any time and for any reason.

District computer/network/Internet usage shall not be considered confidential and is subject to monitoring by designated staff at any time to ensure appropriate use.

- Students should not use the District network to send, receive or store any information, including email messages, that they consider personal or confidential and wish to keep private.
- All electronic files, including email messages, transmitted through or stored in the District network system will be treated no differently than any other electronic file. The District reserves the right to access, review, copy, modify, delete or disclose such files for any purpose.
- District-owned electronic devices which are loaned to students for use on campus or at home are subject to search.

Student Code of Conduct and Computer/Network/Internet Responsibilities

District students are bound by all portions of the Acceptable Use Guidelines.

A student who knowingly violates any portion of the Acceptable Use Guidelines will be subject to suspension of access and/or revocation of privileges on the District's system and will be subject to disciplinary action in accordance with the Board-approved Discipline Management Plan and Student Code of Conduct.

Use of Social Networking/Digital Tools

Students may participate in District-approved social media learning environments related to curricular projects or school activities and use digital tools, such as, but not limited to blogs, discussion forums, RSS feeds, podcasts, wikis, and on-line meeting sessions. The use of blogs, wikis, podcasts, and other digital tools are considered an extension of the classroom. Verbal or written language that is considered inappropriate in the classroom is also inappropriate in all uses of blogs, wikis, podcasts, and other District-approved digital tools. Pictures, videos and photos should not be placed on Internet sites in an unrestricted manner. "Private" videos can be shared with specific family members and friends and should not be available to all Internet users.

Security

Students are required to maintain password confidentiality by not sharing their password with others. Students may not use another person's system account.

A student who gains access to any inappropriate or harmful material is expected to discontinue the access and to report the incident to the supervising staff member. The security problem should not be shared with others. Any student identified as a security risk or as having violated the Acceptable Use Guidelines may be denied access to the District's system and other consequences may also be assigned. A student who knowingly brings prohibited materials or network devices into the school's electronic environment will be subject to suspension of access and/or revocation of privileges on the District's system and will be subject to disciplinary action in accordance with the Board-approved policy.

Use of Personal Telecommunication Devices

The District's goal is to increase student access to digital tools and facilitate immediate access to technology-based information, much the way that students utilize pen and paper. To this end, some schools will allow students to connect privately-owned (personal) telecommunication devices to the District wireless network. Students using personal telecommunication devices must follow the guidelines stated in this document while on school property, attending any

school-sponsored activity, or using the SRVUSD network. Internet access is filtered by the District on personal telecommunication devices in the same manner as District-owned equipment. If network access is needed, connection to the filtered, wireless network provided by the District is required.

- Personally-owned devices are the sole responsibility of the student owner. The campus or District assumes no responsibility for personal telecommunication devices if they are lost, loaned, damaged or stolen, and only limited time or resources will be spent trying to locate stolen or lost items.
- These devices have educational and monetary value. Students are prohibited from trading or selling these items to other students on District property, including school buses.
- Each student is responsible for his/her own device: set-up, maintenance, charging, and security. Staff members will not store student devices at any time, nor will any District staff diagnose, repair, or work on a student's personal telecommunication device.
- Telecommunication devices will not be used as a factor in grading or assessing student work. Students who do not have access to personal telecommunication devices will be provided with comparable District-owned equipment or given similar assignments that do not require access to electronic devices.
- Telecommunication devices are only to be used for educational purposes at the direction of a classroom teacher or as stated for specific age groups.
- Campus administrators and staff members have the right to prohibit use of devices at certain times or during designated activities (i.e. campus presentations, theatrical performances, or guest speakers) that occur during the school day.

Inappropriate Use

Inappropriate use includes, but is not limited to, those uses that violate the law, that are specifically named as violations in this document, that violate the rules of network etiquette, or that hamper the integrity or security of the SRVUSD computer/network/Internet system or any components that are connected to it. The following actions are considered inappropriate uses, are prohibited, and will result in revocation of the student's access to the computer/network/Internet.

- **Violations of Law.** Transmission of any material in violation of any federal or state law is prohibited. This includes, but is not limited to:
  - threatening, harassing, defamatory or obscene material;
  - copyrighted material;
  - plagiarized material;
  - material protected by trade secret; or
  - blog posts, Web posts, or discussion forum/replies posted to the Internet which violate federal or state law.
- Tampering with or theft of components from District systems may be regarded as criminal activity under applicable state and federal laws. Any attempt to break the law through the use of a District computer/network/Internet account may result in prosecution against the offender by the proper authorities.
- **Modification of computer or network**. Modifying or changing computer settings and/or internal or external configurations without appropriate permission is prohibited.
- **Transmitting Confidential Information.** Students may not redistribute or forward confidential information without proper authorization. Confidential information should never be transmitted, redistributed or forwarded to outside individuals who are not expressly authorized to receive the information. Revealing personal information about oneself such as, but not limited to, home addresses, phone numbers, email addresses, birthdates or of others is prohibited.
- **Commercial Use.** Use of the system for any type of income-generating activity is prohibited. Advertising the sale of products, whether commercial or personal is prohibited.
- **Marketing by Non-SRVUSD Organizations.** Use of the system for promoting activities or events for individuals or organizations not directly affiliated with or sanctioned by the District is prohibited.
- **Vandalism/Mischief**. Any malicious attempt to harm or destroy District equipment, materials or data;, or the malicious attempt to harm or destroy data of another user of the District's system, or any of the agencies or

other networks to which the District has access is prohibited. Deliberate attempts to degrade or disrupt system performance are violations of District policy and administrative regulations and may constitute criminal activity under applicable state and federal laws. Such prohibited activity includes, but is not limited to, the uploading or creating of computer viruses.

Vandalism as defined above is prohibited and will result in the cancellation of system use privileges. Students committing vandalism will be required to provide restitution for costs associated with system restoration and may be subject to other appropriate consequences.

- **Impersonation**. Attempts to log on to the computer/network/Internet impersonating a system administrator or District employee, student, or individual other than oneself, will result in revocation of the student's access to computer/network/Internet.
- I**llegally Accessing or Hacking Violations.** Intentional or unauthorized access or attempted access of any portion of the District's computer systems, networks, or private databases to view, obtain, manipulate, or transmit information, programs, or codes is prohibited.
- **File/Data Violations.** Deleting, examining, copying, or modifying files and/or data belonging to other users, without their permission is prohibited.
- **System Interference/Alteration.** Deliberate attempts to exceed, evade or change resource quotas are prohibited. The deliberate causing of network congestion through mass consumption of system resources is prohibited.

Consequences of Agreement Violation

Any attempt to violate the provisions of this agreement may result in revocation of the student's access to the computer/network/Internet, regardless of the success or failure of the attempt. In addition, school disciplinary and/or appropriate legal action may be taken.

Denial, Revocation, or Suspension of Access Privileges With just cause, the System Administrator and/or building principal, may deny, revoke, or suspend computer/network/Internet access as required, pending aninvestigation.

Student Safety/Internet Content/Third-Party Supplied Information.

Students and parents of students with access to the District's system should be aware that use of the system may provide access to other electronic communication systems in the global electronic network that may contain material that is illegal, defamatory, inaccurate or controversial. Each District computer with Internet access has filtering software that blocks access to visual depictions that are obscene, pornographic, inappropriate for students, or harmful to minors, as defined by the federal Children's Internet Protection Act (CIPA). The District makes every effort to limit access to objectionable material; however, controlling all such materials on the computer/network/Internet is impossible, even with filtering in place. With global access to computers and people, a risk exists that students may access material that may not be of educational value in the school setting.

Disclaimer

The District's system is provided on an "as is, as available" basis. The District does not make any warranties, whether expressed or implied, including, without limitation, those of merchantability and fitness for a particular purpose with respect to any services provided by the system and any information or software contained therein. The District does not guarantee that the functions or services performed by, or that the information or software contained on the system will meet the system user's requirements, or that the system will be uninterrupted or error free, or that defects will be corrected.

Opinions, advice, services, and all other information expressed by system users, information providers, service providers, or other third-party individuals in the system are those of the providers and not the District.

The District will cooperate fully with local, state, or federal officials in any investigation concerning or relating to misuse of the District's electronic communications system.