SOUTH VERMILLION COMMUNITY SCHOOL CORPORATION
TECHNOLOGY ACCEPTABLE USE POLICY FOR STAFF

Philosophy

South Vermillion Community School Corporation (hereafter referred to as SVCS) is committed to the effective use of technology to enhance the quality of student learning, increase communication, and improve productivity. It also recognizes that safeguards must be established to ensure the protection of our staff. Safeguards protect the corporation's investment in hardware and software, ensure the benefits of technology and prevent negative side effects. This technology will allow SVCS staff to access and utilize global resources, communicate and collaborate with other individuals/groups, and significantly expand access to digital information.

The provisions of this policy and associated guidelines and agreements are subordinate to school, local, state and federal law. SVCS has the duty to investigate any suspected violations of this policy.

> The Acceptable Use Policy sets the standards to ensure that all users benefit from the technology in place in our school system. The policy encourages use of technology appropriate for a school environment, discourages harmful practices, and sets penalties for those who choose to violate the policy.

Definition of Technology

Technology resources are defined as any electronic tool, device, program, or system that aids the educational/work environment and enables the employee to be more productive. Technology includes, but is not limited to:

- computer hardware and software applications
- cell phones, handheld technologies and personal storage devices
- analog and digital networks (e.g., data, video, audio, voice, and multimedia)
- distance learning through multiple means and locations
- electronic (e-mail) mail systems, and communication technologies
- copiers, printers, and scanners
- televisions, projectors, telecommunications technology
- servers, routers, hubs, switches, and Internet gateways including wireless access
- information systems software, including online applications
- related and forthcoming systems and new technologies

Expectations and Acceptable Use

Personally-owned devices are included in this Acceptable Use Policy when connected to the SVCS network and must be authorized by building-level administration. SVCS is NOT responsible for any damage incurred while connected to the network. This includes, but is not limited, to power surges, viruses or malicious acts from other users.

Access to School-Provided Technology

SVCS personnel will be assigned access to school technologies as required by duties assigned to them. Upon employment, building administrators will request the necessary access and accounts will be created at that time. It is the responsibility of each staff member to maintain the security of login information, passwords, and any other security codes they are given. This confidential information will not be shared with any other individual, with the exception of the SVCS Technology Department.

It is also expected that all SVCS staff will change passwords at regularly scheduled intervals to ensure security of school data systems. If you feel your secure login information has been compromised, you are expected to contact the SVCS Technology Department immediately. Furthermore, sensitive login information and security codes should not be written or displayed where others may be able to retrieve the information.

Access to SVCS Technology may only be permitted by authorized users approved by building administration. Other non-authorized use is expressly forbidden.

The following uses of school-provided technology or personally-owned devices (used at school) are prohibited and may lead to disciplinary action:

a) remove or copy school-owned software from school computers
b) vandalize, damage, alter, or disable the property of SVCS
c) use technology to harass, bully, or threaten another individual
d) access, upload, download, create, distribute, use, or transmit pornographic, obscene, sexually explicit, abusive, slanderous, libelous, prejudicial, or otherwise inappropriate language or material at any time
e) attempt to circumvent SVCS policies or network restrictions. **It is a criminal offense to hack into a school system computer**.
f) plagiarize, violate copyright or use the intellectual property of an individual or organization without permission
g) introduce unauthorized information, computer viruses, or harmful programs into the computer system in public/private files or messages
h) participate in online gambling
i) send non-job related or unsolicited emails, or to engage in personal chat/instant messaging during work time
j) use the school network in a manner that would cause congestion of the network or otherwise interfere with the work of others
k) send personal ads or sell items using school e-mail
l) send fundraiser or electronic fliers using school e-mail without administrative approval
m) disclose personal email addresses of others through a group or chain email
n) utilize the school corporation technology for commercial purposes or financial gain
o) send non-school related digital communication to students
p) use social networks at school unless approved for curricular activities
q) use school technology for non-job related shopping or to use credit cards online during work time
r) share with any other individual user logins, passwords, or user codes at any time or to post login information so others may view.
s) leave the computer logged in and accessible when not present, unless directed by the SVCS

Technology Department

t) use technology hardware, software, information, and/or services of another individual without permission from administration
u) allow students to use technology without supervision
v) allow students to use teacher computers without direct teacher supervision

Inappropriate communication with staff or students during or outside of school time is a clear violation of this policy. If a staff member were to get an inappropriate communication from a student or another staff member, the communication should be ended and reported to their supervisor immediately. Inappropriate use of technology from outside the school corporation may result in disciplinary action if either of the following occurs:

a) The employee's actions violate a legitimate school policy or law
b) The school can show a substantial disruption or legitimate safety concern

Safety and Reliability

The school does not guarantee the reliability of the data connection and does not verify the accuracy of information found on the Internet.

Even though SVCS blocks access to certain sites, the faculty and staff are expected to diligently monitor students' computer and Internet usage. The school corporation will run filtering software as required by CIPA (Childhood Internet Protection Act). The staff is always responsible for the supervision of students whenever they are using technology.

Important Notice: SVCS will take measures to filter and monitor resources and information accessed through its information and data systems. Although a conscious effort will be made to deter access to materials that are inappropriate for the educational setting, no safeguard is foolproof. The user is responsible for not seeking or initiating access to inappropriate or blocked material and for reporting incidents should they occur. In addition, if a staff member witnesses inappropriate activity, it is their responsibility to report this activity to building-level administration.

Furthermore, SVCS staff may have access to sensitive and confidential data. Staff members will only view data that is pertinent to the duties assigned to them, and will not violate Federal Laws such as FERPA and HIPAA.

No Expectation Of Privacy

Given valid reason, SVCS may at any time and without notice or consent from users, obtain access to all information, conveyed or stored anywhere on any of the school's electronic systems, including telephone calls and electronic mail messages, even if the information has been password protected or encrypted. SVCS may use the information obtained for any legal purpose, including disclosure to third parties, subject only to applicable law, but otherwise is the sole discretion of SVCS. SVCS may exercise an investigation triggered by any indication of impropriety (school or personal technologies) or as necessary to locate substantive information that is not readily available by other less intrusive means.

a) Personal information (from either school-owned or personal technology devices) sent to

school-owned equipment or accounts should not be considered private.

b) Personal equipment brought to school is subject to the SVCS Technology Acceptable Use Policy and may be detained and searched by administration with valid cause.

Hardware/Software

SVCS has the right to regulate hardware/software technologies that are on its network or used within the school and workplace environment. This includes personally-owned devices and/or media used on SVCS property.

Documents/Files

The school corporation has final editorial authority over online content (which includes but is not limited to websites, wiki's, blogs, and Moodle) that is stored on SVCS servers.

All data stored on SVCS networks is archived and is subject to EDiscovery laws and is part of public record. This includes email, Internet activity, documents, files, and voicemail messages that do not violate FERPA and HIPPA laws. The storage of personal data files on the SVCS network servers is expressly forbidden.

Each individual is responsible for any and all data stored on the device whether personal or school-owned. If non-AUP compliant material is found, disciplinary action may be taken.

Corporation-Provided Mobile Technology

1. Overview

SVCS may provide mobile technology (laptops, tablets, iPods, iPads) to staff members to be used at school and off SVCS property. The purpose of such mobile technology is to provide opportunities for collaboration within the school corporation and to provide tools to work at home on school-related materials. The corporation-provided mobile technology is not to be considered as personal property. It is corporation-owned property and should be treated accordingly. The following guidelines have been established for use.

2. Purpose

a) Mobility for moving from room to room, within the building or around SVCS schools using the wireless network
b) Professional development/collaboration purposes
c) Use at home for educational productivity

3. Educational Use

a) While at school, staff will ensure that the laptop is always kept secure when not in use. Classrooms will be locked while they are unattended.
b) Laptops can print to the assigned network copier/printer, but are not able to print to any others in the building or district.
c) Periodically, the laptop must remain at school for necessary updates. Advanced notice will be given along with an approximate timeframe for such work. Updates/maintenance may occur during the school year or during summer months as needed.

4. Home Use

a) Laptops are to be used only by staff; other family members may not use the school-owned laptop.
b) If a laptop has performance issues, then it will be reformatted. Any information one may have saved to the laptop could be retried and replaced if part of external backup performed by individual (Email, Harmony, and documents on the server are safe).
c) Personal files (pictures, videos, music, documents, etc) may be saved to the laptop, but should be backed up to an external hard drive.
d) If accessing the Internet from home on your laptop, access would be filtered as it is at school (via content filtering software).
e) The Technology Staff does not support home or personal use, including but not limited to: troubleshooting home internet service provider issues, installing personal software, printers, or providing access to non-educational websites.

5. Liability

a) SVCS Staff are responsible for maintaining and securing confidential files that may be stored on the local computer.
b) SVCS Staff are financially responsible for the replacement cost of the laptop or its accessories if damaged or stolen while outside the SVCS community. If concerned about liability, then the laptop should remain on SVCS grounds at all times. Staff may consider purchasing an insurance policy for take-home use at their discretion.
c) If damage occurs while on SVCS property, disciplinary action may be taken.
d) SVCS is not responsible for damages resulting from the use of the laptop, which includes, but not limited to: home service interruption, spread of viruses to other personal computers and loss of personal data.

Policy Exceptions

The Acceptable Use Policy will be followed by all SVCS technology users. Exceptions will be made for SVCS employees or agents, designated by the Superintendent of Schools, conducting an investigation of student or employee use which potentially violates the law, SVCS policy, rules or procedures. Exceptions will also be made for computer system administrators and designated staff who need access to the school's technology resources in order to maintain the integrity of the SVCS network.

Any violation of SVCS policy and rules may result in disciplinary action up to and including dismissal. When applicable, law enforcement agencies may be involved.

Staff Agreement – Staff Signature Required

Rules and regulations are necessary in order to offer technology opportunities in the workplace. I agree to abide by the above Acceptable Use Policy Guidelines as stated in this document.

_____ _____

Staff Signature Date