Technology and Electronic Resources and Internet Safety

Acceptable Use Guidelines/Internet Safety Requirements
These procedures are written to support the Technology and Electronic Resources Policy of the board of directors and to promote positive and effective digital citizenship among students and staff. Digital citizenship represents more than technology literacy. Successful, technologically fluent digital citizens live safely and civilly in an increasingly digital world. They recognize that information posted on the Internet is public and permanent and can have a long-term impact on an individual's life and career. Expectations for student and staff behavior online are no different from face-to-face interactions.

Legal Requirements
The Stanwood-Camano School District is committed to complying with applicable information security requirements and relevant information security standards and protocols. These requirements include, but are not limited to the following:

1. The Family Educational Rights and Privacy Act (FERPA)
2. Children's Internet Protection Act (CIPA)
3. Individuals with Disabilities Education Act (IDEA)
4. Children's Online Privacy Protection Act (COPPA)
5. Health Insurance Portability and Accountability Act (HIPPA)

Use of Personal Electronic Devices
In accordance with all district policies and procedures, students and staff may use personal electronic devices (e.g. laptops, mobile devices and e-readers) to further the educational and research mission of the district. School staff will retain the final authority in deciding when and how students may use personal electronic devices on school grounds and during the school day.

Network
The district network includes wired and wireless devices and peripheral equipment, files and storage, e-mail and Internet content (blogs, websites, collaboration software, social networking sites, wikis, etc.). The district reserves the right to prioritize the use of, and access to, the network. All use of the network must support education and research and be consistent with the mission of the district.

Acceptable network use by district students and staff includes:

A. Creation of files, digital projects, videos, web pages and podcasts using network resources in support of education and research.
B. Participation in blogs, wikis, bulletin boards, social networking sites and groups and the creation of content for podcasts, e-mail and web pages that support education and research.
C. The online publication of original educational material, curriculum related materials and student work. Sources outside the classroom or school must be cited appropriately.
D. Staff use of the network for incidental personal use in accordance with all district policies and procedures.
E. Connection of personal electronic devices (wired or wireless) including portable devices with network capabilities to the district network understanding that the network policies and procedures for non-district hardware is followed which may include confirmation that the device is equipped with up-to-date virus software, compatible network card and is configured properly. Connection of any personal electronic device is subject to all procedures in this document.

Unacceptable network use by district students and staff includes but is not limited to:

A. Personal gain, commercial solicitation and compensation of any kind.
B. Actions that result in liability or cost incurred by the district.
C. Downloading, installing and use of games, audio files, video files, games or other applications

(including shareware or freeware) without permission or approval from the Technology Services Group.

D. Support for or opposition to ballot measures, candidates and any other political activity.
E. Hacking, cracking, vandalizing, the introduction of viruses, worms, Trojan horses, time bombs and changes to hardware, software and monitoring tools.
F. Unauthorized access to other district computers, networks and information systems.
G. Cyberbullying, hate mail, defamation, harassment of any kind, discriminatory jokes and remarks;
H. Information posted, sent or stored online that could endanger others (e.g., bomb construction, drug manufacturing).
I. Accessing, uploading, downloading, storage and distribution of obscene, pornographic or sexually explicit material.
J. Attaching unauthorized devices to the district network. Any such device will be confiscated and additional disciplinary action may be taken.
K. Accessing data, a server or an account for any purpose other than conducting official school business, even if you have authorized access, is prohibited.
L. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
M. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when staff is working at home or if a student is accessing classroom electronic resources outside of the school.
N. Using a school district technology or electronic resource asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or harassment, intimidation or bullying policies.
O. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the staff member or student is not an intended recipient or logging into a server or account that the staff member or student is not expressly authorized to access, unless these duties or activities are within the scope of regular duties or activities. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
P. Port scanning or security scanning is expressly prohibited unless prior notification to the Superintendent or Technology Director is made.
Q. Executing any form of network monitoring which will intercept data.
R. Circumventing user authentication or security of any host, network or account.
S. Interfering with or denying service to any user (for example, denial of service attack).
T. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
U. Providing information about, or lists of, Stanwood-Camano School District employees or students to parties outside the Stanwood-Camano School District.

The district will not be responsible for any damages suffered by any user, including but not limited to, loss of data resulting from delays, non-deliveries, miss deliveries or service interruptions caused by his/her own negligence or any other errors or omissions. The district will not be responsible for unauthorized financial obligations resulting from the use of, or access to, the district’s computer network or the Internet.

Internet Safety

Personal Information and Inappropriate Content:

A. Students and staff should not reveal personal information, including a home address and phone number on websites, blogs, podcasts, videos, social networking sites, wikis, e-mail or as content on any other electronic medium.

B. Students and staff should not reveal personal information about another individual on any electronic medium without first obtaining permission.
C. No student pictures or names can be published on any public class, school or district website unless the appropriate permission has been obtained according to district policy.
D. If students encounter dangerous or inappropriate information or messages, they should notify the appropriate school authority.

Filtering and Monitoring

Filtering software is used to block or filter access to visual depictions that are obscene and all child pornography in accordance with the Children's Internet Protection Act (CIPA). Other objectionable material could be filtered. The determination of what constitutes "other objectionable" material is a local decision.

A. Filtering software is not 100 percent effective. While filters make it more difficult for objectionable material to be received or accessed, filters are not a solution in themselves. Every user must take responsibility for his/her use of the network and Internet and avoid objectionable sites.
B. Any attempts to defeat or bypass the district's Internet filter or conceal Internet activity are prohibited (e.g., proxies, https, special ports, modifications to district browser settings and any other techniques designed to evade filtering or enable the publication of inappropriate content).
C. E-mail inconsistent with the educational and research mission of the district will be considered SPAM and blocked from entering district e-mail boxes.
D. The district will provide appropriate adult supervision of Internet use. The first line of defense in controlling access by minors to inappropriate material on the Internet is deliberate and consistent monitoring of student access to district devices.
E. Staff members who supervise students, control electronic equipment or have occasion to observe student use of said equipment online, must make a reasonable effort to monitor the use of this equipment to assure that student use conforms to the mission and goals of the district.
F. Staff must make a reasonable effort to become familiar with the Internet and to monitor, instruct and assist effectively.
G. The district will provide a procedure for students and staff members to request access to internet websites blocked by the district's filtering software. A staff member or student may request access from the building principal who will contact the Technology Director. The requirements of the Children's Internet Protection Act (CIPA) will be considered in evaluation of the request.

Personal Telecommunication and Electronic Devices

Preserving a beneficial learning environment and assuring the safety and well being of all staff and students are primary concerns of the Board of Directors. To this end, inappropriate use of personal telecommunication and electronic devices shall be prohibited as described in this policy and its procedures.

The term "telecommunication and electronic devices" shall refer to, but not be limited to, devices which transmit a signal, receive a signal, create a sound or display visual media, capture photography digitally or conventionally, or capture sound digitally or conventionally, and which include, but are not limited to: computers, telephones (wired, cellular, wifi), fax machines, text messaging devices, digital cameras, video cameras, film cameras, portable gaming systems, or portable music players.

Students who engage in inappropriate use of personal telecommunication and electronic devices may be referred to law enforcement and shall be subject to disciplinary action including, but not limited to: losing the privilege to bring the device onto school property, confiscation of the device (which shall only be returned to the student's parent or guardian), and/or discipline/suspension/expulsion. The principal, his/her designee, and the classroom instructor will prohibit or limit the use of or confiscate electronic devices if used contrary to this policy and procedure.

Students are responsible for the safety and security of their personal telecommunication and electronic devices. The District assumes no responsibility in any circumstance for the loss/destruction/damage or theft of telecommunication and electronic devices. Inappropriate use of telecommunication and electronic devices includes, but is not limited to the following:

A. Using telecommunication and electronic devices for texting, instant messaging, or conversation during class time unless expressly authorized by a school administrator or staff member.
B. Using telecommunication and electronic devices in classrooms, locker rooms, restrooms, or other non-public areas of the building unless expressly authorized by a school administrator or staff member.
C. Using telecommunication and electronic devices to take or produce photographs or recordings without the knowledge of the person or persons being photographed or recorded and without express authorization of a school administrator or staff member.
D. Using telecommunication and electronic devices in a manner, which interferes with the educational environment, or to annoy or offend others.
E. Using telecommunication and electronic devices to commit (or conspire to commit) or aid or abet an act of harassment, intimidation or bullying regardless of where initiated (i.e. at a residence, public place, or on school property) and when initiated (i.e. during school hours or outside school hours) provided such use causes substantial disruption to the educational process or environment.
F. Using telecommunication and electronic devices during any type of assessment unless expressly authorized by a certificated staff member.
G. Using telecommunication and electronic devices in a way that violates other Board Policy.

Internet Safety Instruction
All students will be educated about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, and cyber bullying awareness and response:

A. Age appropriate materials will be made available for use across grade levels; and
B. Training on online safety issues and materials implementation will be made available for administration, staff and families.

Copyright
Downloading, copying, duplicating and distributing software, music, sound files, movies, images or other copyrighted materials without the specific written permission of the copyright owner is generally prohibited. However, the duplication and distribution of materials for educational purposes is permitted when such duplication and distribution falls within the Fair Use Doctrine of the United States Copyright Law (Title 17, USC) and content is cited appropriately.

Ownership of Work
All work completed by employees as part of their employment will be considered property of the district. The District will own any and all rights to such work including any and all derivative works, unless there is a written agreement to the contrary.

All work completed by students as part of the regular instructional program is owned by the student as soon as it is created, unless such work is created while the student is acting as an employee of the school system or unless such work has been paid for under a written agreement with the school system. If under an agreement with the district, the work will be considered the property of the District. Staff members must obtain a student's permission prior to distributing his/her work to parties outside the school.

Network Security and Privacy
Passwords are the first level of security for a user account. System logins and accounts are to be used only by the authorized owner of the account for authorized district purposes. Students and staff are

responsible for all activity on their account and must not share their account password. The following procedures are designed to safeguard network user accounts:

A. Passwords
   a. Change passwords according to district guidelines.
   b. Do not share passwords with anyone.
   c. All passwords are to be treated as sensitive, confidential information.
   d. Passwords should never be written down or stored on-line without encryption.
   e. Do not reveal a password in email, chat, or other electronic communication.
   f. Do not speak about a password in front of others.
   g. Do not hint at the format of a password (e.g., "my family name").
   h. Do not reveal a password on questionnaires or security forms.
   i. If someone demands a password, refer them to this document and direct them to the Technology Services Group.
   j. Always decline the use of the "Remember Password" feature of applications or Internet browsers (e.g., Safari, Chrome, Firefox).

B. Email Security
   a. All use of email must be consistent with Stanwood-Camano School District policies and procedures of ethical conduct, safety, compliance with applicable laws and proper business practices.
   b. School email accounts should be used primarily for school and educationally related purposes; personal communication is permitted on a limited basis, but non-related school district commercial uses are prohibited.
   c. Email that is identified as a record shall be retained according to the school district's Record Retention Schedule.
   d. The Stanwood-Camano School District's email system shall not be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about age, creed, religion, race, color, national origin, sex, marital status, sexual orientation including gender expression or identity, honorably discharged veteran or military status, or the presence of any sensory, mental or physical disability. Students or staff who receive any emails with this content, should report the matter to their teacher or supervisor immediately.
   e. Users are prohibited from automatically forwarding email to a third party email system unless written permission is given by the Superintendent or Technology Director.
   f. Users are prohibited from using third-party email systems and storage servers such as Google, Yahoo, and MSN Hotmail, Live, iCloud,l etc. to conduct school business, to create or memorialize any binding transactions, or to store or retain email on behalf of the school district. Such communications and transactions should be conducted through proper channels using Stanwood-Camano School District approved documentation.
   g. Using a reasonable amount of Stanwood-Camano School District resources for personal emails is acceptable, but non-work related email shall be saved in a separate folder from work related email. Sending chain letters or joke emails from a school district email account is prohibited.
   h. There is no expectation of privacy in anything that a staff or student stores, sends or receives on the company's email system.
   i. Stanwood-Camano School District may monitor messages without prior notice. Stanwood-Camano School District is not obliged to monitor email messages.
   j. Extreme caution must be used when opening email attachments received from unknown senders, which may contain malware, viruses etc.

Workstation and Hardware Security
To ensure that all sensitive/confidential materials are secure within the technology and electronic resources, staff and students must secure the technology or electronic resources they are using or assigned to.

A. All workstations should be shut down and secure before leaving at the end of the school or workday.
B. Laptops are to be locked away when not in use.
C. If a staff member or student leaves his/her area, one should lock the screen or log off if leaving the computer. This is one of the top strategies to utilize when trying to reduce the risk of security breaches.
C. Computer workstations must be locked when the workspace is unoccupied.
D. Staff who are assigned laptops are responsible for the security of that hardware. The laptop must be either locked with a locking cable or locked away in a drawer.
E. Lock away portable computing devices such as laptops and tablets when these devices are traveling outside of school district property.
F. Do not leave portable computing devices in a school or personal vehicle.
G. Printouts containing sensitive information should be immediately removed from the printer.
H. Treat mass storage devices such as CD ROM, DVD or USB "flash" drives as sensitive and secure them in a locked drawer.
I. Staff have the responsibility to promptly report the theft, loss or unauthorized disclosure of hardware or secure information.
J. Passwords must not be left on sticky notes posted on or under a computer, nor may they be left written down in an accessible location.

Student Data is Confidential
District staff must maintain the confidentiality of student data in accordance with the Family Educational Rights and Privacy Act (FERPA).

No Expectation of Privacy
The district provides the network system, e-mail and Internet access as a tool for education and research in support of the district's mission. The district reserves the right to monitor, inspect, copy, review and store without prior notice information about the content and usage of:

A. The network,
B. user files and disk space utilization,
C. user applications and bandwidth utilization,
D. user document files, folders and electronic communications,
E. E-mail,
F. internet access, and
G. any and all information transmitted or received in connection with network and e-mail use.

For security and network maintenance purposes, authorized individuals within Stanwood-Camano School District may monitor equipment, systems and network traffic at any time. The school district reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

No student or staff user should have any expectation of privacy when using the district's network. The district reserves the right to disclose any electronic messages to law enforcement officials or third parties as appropriate. All documents are subject to the public records disclosure laws of the State of Washington.

Archive and Backup
Backups are made of all district e-mail correspondence for purposes of public disclosure and disaster recovery. Barring power outage or intermittent technical issues, staff and student files are backed up on district servers regularly. Refer to the district retention policy for specific records retention requirements.

Disciplinary Action
All users of the district's technology and electronic resources are required to comply with the district's

policy and procedures and agree to abide by the provisions set forth in the Informed Consent Agreement Form for Students. Violation of any of the conditions of use explained in the district's user agreement, Technology and Electronic Resources policy or in these procedures could be cause for disciplinary action, including suspension or expulsion from school and suspension or revocation of network and computer access privileges.

For school district staff, violation of the Stanwood-Camano School District's expectations for use of technology and electronic resources may be cause for disciplinary action up to, and including, termination and reporting to the Office of Superintendent of Public Instruction's Office of Professional Practices.

Adopted: 08.05.03
Stanwood-Camano School District
Revised: 03.03.06; 01.05.09; 09.18.12; 06.07.16