Suring Public School District Acceptable Use of Electronic Networks and Technology Resources for Student

Purpose of Technology Use

The Suring Public School District provides technology resources to its students solely for educational purposes. Through technology, the District provides access for students and staff to resources from around the world. Expanding technologies take students and staff beyond the confines of the classroom, and provide tremendous opportunities for enhancing, extending, and rethinking the learning process. The goal in providing these resources is to promote educational excellence in the District by facilitating resource sharing, innovation, and communication with the support and supervision of parents, teachers, and support staff.

The Opportunities and Risks of Technology Use

With access to computers/Chromebooks and unlimited, worldwide access comes the potential availability of material that may not be considered of educational value in the context of the school setting, or that may be harmful or disruptive. Because information on networks is transitory and diverse, the District cannot completely predict or control what users may or may not locate. The Board of Education believes that the educational value of limited access to the information, interaction, and research capabilities that technology offers outweighs the possibility that users may obtain or encounter material that is not consistent with the educational goals of the District.

In accordance with the Children's Internet Protection Act, the District installs and operates filtering software to limit users' Internet access to materials that are obscene, pornographic, harmful to children, or otherwise inappropriate, or disruptive to the educational process, notwithstanding that such software may in certain cases block access to other materials as well. At the same time, the District cannot guarantee that filtering software will in all instances successfully block access to materials deemed harmful, indecent, offensive, pornographic, or otherwise inappropriate. The use of filtering software, as explained in the Internet Safety Policy 7540.3, does not negate or otherwise affect the obligations of users to abide by the terms of this policy and to refrain from accessing such inappropriate materials.

No technology is guaranteed to be error-free or totally dependable, nor is it safe when used irresponsibly. Among other matters, the District is not liable or responsible for:

- Any information that may be lost, damaged, or unavailable due to technical, or other, difficulties;
- The accuracy or suitability of any information that is retrieved through technology;
- Breaches of confidentiality;
- Defamatory material; or
- The consequences that may come from failure to follow procedures governing the use of technology.

Privileges and Responsibilities

The District's electronic network is part of the curriculum and is not a public forum for general use. Student users may access technology for only educational purposes. The actions of student users accessing networks through the District reflect on the District; therefore, student users must conduct themselves accordingly by exercising good judgment and complying with this policy and any accompanying guidelines. Students are responsible for their behavior and communications using the Districts computers/Chromebooks and networks.

Student users of technology shall

- Use or access District technology only for educational purposes
- Comply with copyright laws and software licensing agreements

- Understand that email and network files are not private. Network administrators may review files and communications to maintain system integrity and monitor responsible student use.
- Respect the privacy rights of others.
- Be responsible at all times for the proper use of technology, including proper use of access privileges, complying with all required system security identification codes, and not sharing any codes or passwords.
- Maintain the integrity of technological resources from potentially damaging messages, physical abuse, or viruses.
- Abide by the policies and procedures of networks and systems linked by technology.

Students may not use District technology including property issued under the 1:1 program for improper uses. These uses include, but are not limited to:

- Any and all illegal purposes;
- Any and all obscene or pornographic purposes, including, but not limited to, retrieving, viewing or sharing sexually explicit material;
- Any and all discriminatory purposes, including harassment and bullying of individuals based on race, gender, religion, sexual orientation, disability, or for other reasons;
- Any and all purposes that would violate state, federal or international law, including
    - Copyright laws;
    - Cyberbullying laws; and
    - Sexting laws.
- Any use of profanity, obscenity, or language that is offensive or threatening;
- Reposting or forwarding personal communications without the author's prior consent;
- Reposting or forwarding of junk mail, chain letters, or inappropriate or offensive jokes;
- Destruction, alteration, disfigurement or unauthorized access of hardware, software, or firmware;
- Obtaining financial gain or Transacting any business or commercial activities;
- Plagiarizing (claiming another person's writings as your own);
- Political advocacy;
- Disrupting the use of others to any process, program or tool, including downloading or otherwise spreading computer viruses;
- Engaging in hacking of any kind, including, but not limited to, the illegal or unauthorized access;
- Allowing others to use property issued under the program without authorization, including students whose access privileges have been suspended or revoked;
- Soliciting or distributing information with the intent to incite violence, cause personal harm, damage a person's character, or to harass another individual.
- Any and all other purposes that would violate the Suring School District Student Code of Conduct.

Internet Safety:
Students must take steps to ensure their safety on the internet, including, but not limited to, the following rules:

- Students should never give out identifying information such as home address, school name, or telephone number to others on the Internet or by email, including in a public message made via social media, blogs, personal webpages, etc. If a person asks for such personal information, students must have approval of their parent or guardian before providing the information.
- Students should not post photographs of themselves in social media or on websites that are available to the public.
- Students should not arrange a face-to-face meeting with someone they "meet" on the Internet or by email without parental/guardian permission.
- Students should not respond to messages that are suggestive, obscene, belligerent, threatening, or make a student feel uncomfortable. If a student receives such a message, he or she should

provide a copy of the message to his or her parent or guardian immediately. If the message requires school action the student's parent should provide a copy to the principal and file a harassment/bullying complaint.

The District recommends that parents/guardians read and follow the U.S Department of Justice Guidelines for Parents/Guardians on Internet Safety located at:
https://www.justice.gov/criminal-ceos/children-internet-safety

Disciplinary Actions
Violations of this policy and guidelines governing the use of technology, may result in disciplinary action which could include loss of network access, loss of technology use, suspension or expulsion, or other appropriate disciplinary action. Violations of local, state or federal law may subject students to prosecution by appropriate law enforcement authorities.

No Expectation of Privacy
The District's electronic network is part of the curriculum and is not a public forum for general use. Users should not expect that email or files stored on District servers and/or Google domains will be private. The District reserves the right to log technology use, to monitor fileserver space utilization by users, and to examine users' files and materials as needed, and at its discretion. Users must recognize that there is no assurance of confidentiality with respect to access to transmissions and files by persons outside, or from persons inside the District.

Program Agreement
The District is pleased to offer our students access to the District's computers/Chromebooks, network, internet, and other technology, including related hardware and software devices issued through a 1:1 program, (the "District Technology") for educational purposes. The District Technology is issued to students for their own personal, school-related uses at school. All District Technology issued under the 1:1 program, including computers/Chromebooks, are educational tools and may only be used in that capacity. Any use of the District Technology for other purposes (such as personal purposes) must be minimal only, and failure to comply may lead to termination of rights under the 1:1 program.
The agreement waiver must be filled out on-line in family access prior to the student receiving the electronic device.

Costs:
Manufacturer defects will be covered by the manufacturer's warranty and/or by the District. Each student is required to pay a service fee. Damage or loss that is the result of a student's failure to exercise reasonable care or willful conduct in violation of any District policy or procedure governing the use of the computer/Chromebook will not be covered by insurance. If District Technology is damaged, stolen, or lost while signed out to a student and the damage or loss is not covered by insurance or the manufacturer's warranty, the student will have the sole responsibility of paying replacement and repair costs.

If the computer/Chromebook is stolen/missing, the district must be notified within twenty-four (24) hours of the discovery of the theft.

District Technology Return:
When a student withdraws from enrollment at District, or has his or her rights terminated, the student must return any District Technology issued by the technology department immediately. In no event shall the student retain the District Technology for more than two school days after the date of such expiration, withdrawal or termination. If a student fails to return the District Technology in a timely fashion, the student and his or her parent or guardian will be subject to paying replacement costs.

Appeal Process:
If a student receives consequences for a violation of the 1:1 program or if the parent is required to pay replacement or repair costs, the student's parent or guardian may appeal by requesting an appeal in

writing within ten school days of notification of the decision to issue consequences or of notification of payment due. All requests for appeal must be addressed to the District Administrator and should include a full description of the parent or guardian's reasons for disagreeing with the decision. The District Administrator or designee will then review the decision and will respond to the parent within ten school days after receipt of the request for appeal. A meeting may be held by the District Administrator or designee to obtain additional information from the student, the parents and/or guardian and/or District staff, in the District Administrator discretion. The District Administrator or designee's decision on appeal shall be final.

All Property must be returned to the Suring Technology Department pending the resolution of any appeal. Fees will be assessed pursuant to this policy if not timely returned.

District Technology Transport and Use:

Once District Technology is issued to the student, the student and his or her parent or guardian are responsible for the District Technology at all times that the District Technology is signed out to the student. Students and their parents or guardians must take reasonable care to protect and properly use District Technology issued under the program at all times. Among other things, this means:

- The District is not responsible for district technology, including chromebook, assigned to a student at any time, including when they are left unsupervised in a classroom, hallway, locker or elsewhere on school property.
- The student is the only authorized user of his/her assigned Chromebook or other District Technology. Students may not share or trade their Chromebook or other District Technology with other individuals, including other students, other than school officials.
- Chromebooks and other District Technology must not be marked with markers, stickers or other similar materials.
- District applied labels, asset tags and other identifiers may not be removed from computers or other District Technology.
- Food and drink should not be used near Chromebooks or other District Technology.

Revised August 29, 2019