

STUDENT USE OF THE INTERNET AND ELECTRONIC COMMUNICATIONS

The internet, and electronic communications (e-mail, video conferencing, LMS platforms, district-supported digital learning platforms, and other forms of electronic communication) have vast potential to support curriculum and student learning.

Use of the internet and electronic communications require students to think critically, analyze information, write clearly, use problem-solving skills, and hone computer and research skills that employers demand. Use of these tools also encourages an attitude of lifelong learning and offers an opportunity for students to participate in distance learning activities, ask questions of and consult with experts, communicate with other students and individuals, and locate material to meet educational and personal information needs.

The internet and electronic communications are fluid environments in which students may access materials and information from many sources, including some that may be harmful to students. While it is impossible to predict with certainty what information students might locate or come into contact with, the district shall take reasonable steps to protect students from accessing material and information that is obscene, pornographic, or otherwise harmful to minors. Students shall take responsibility for their own use of district technology devices to avoid contact with material or information that may be harmful to minors. For purposes of this policy, "district technology device" means any district-owned computer, hardware, software, or other technology that is used for learning purposes and has access to the Internet.

Blocking or filtering obscene, pornographic, and harmful information

Technology that blocks or filters material and information that is obscene, pornographic, or otherwise harmful to minors, shall be installed on all district computers having internet or electronic communications access. Students shall report access to material and information that is inappropriate, offensive, or otherwise in violation of this policy to the supervising staff member or other school personnel. If a student becomes aware of other students accessing such material or information, he or she shall report it to the supervising staff member or other school personnel.

No expectation of privacy

District technology devices are owned by School District 27J and are intended for educational purposes at all times. Students shall have no expectation of privacy when using district technology devices. School District 27J reserves the right to monitor, inspect, copy, review, and store (at any time and without prior notice) all records of usage of district technology devices, including all internet activity, browser history, and electronic communications, access and transmission/receipt of materials, and information. All material and information accessed/received through district computers and computer systems shall remain the property of the school district.

Unauthorized and unacceptable uses

Students shall use district technology devices in a responsible, efficient, ethical, and legal manner.

Because technology and ways of using technology are constantly evolving, every unacceptable use of district technology devices cannot be specifically described in policy. Therefore, examples of unacceptable uses include, but are not limited to, the following:

No student shall access, create, transmit, retransmit, or forward material or information:

- that promotes violence or advocates destruction of property including, but not limited to, access to information concerning the manufacturing or purchasing of destructive devices or weapons
- that is not related to district education objectives
- that contains pornographic, obscene or other sexually oriented materials, either as pictures or writings, that are intended to stimulate erotic feelings or appeal to prurient interests in nudity, sex or excretion
- that harasses, threatens, demeans, or promotes violence or hatred against another person or group of persons in violation of the district's nondiscrimination policies.
- for personal profit, financial gain, advertising, commercial transaction, or political purposes
- that plagiarizes the work of another without express consent
- that uses inappropriate or profane language likely to be offensive to others in the school community
- that is knowingly false or could be construed as intending to purposely damage another person's reputation
- in violation of any federal or state law or district policy, including but not limited to copyrighted material and material protected by trade secret
- that contains personal information about themselves or others, including information protected by confidentiality laws
- using another individual's Internet or electronic communications account without written permission from that individual
- that impersonates another or transmits through an anonymous remailer
- that uses a teacher device for access to the network without supervision
- that installs any software, including shareware, freeware, games, or packaged software or utilities onto district computers without authorization from the school principal and approval from the district IT department

Security

Security on district technology devices is a high priority. Students who identify a security problem while using district technology devices must immediately notify a supervising staff member or other school personnel. Students should not demonstrate the problem to other users. Logging on to the Internet or electronic communications as a system administrator is prohibited.

Students shall not:

- use another person's password or any other identifier
- gain or attempt to gain unauthorized access to district technology devices
- read, alter, delete or copy, or attempt to do so, electronic communications of other system users
- leave 27J-issued technology device unattended while logged into their account
- share their login information with anyone else
- change any computer settings or configurations
- attempt to disable or bypass the district web filter
- disable virus protection

- download games, music, freeware
- play games with other users on the Internet
- purchase items using district computers

Any user identified as a security risk, or as having a history of problems with technology, may be denied access to the Internet, electronic communications and/or district technology devices.

Safety

In the interest of student safety and security, the district shall educate students about appropriate online behavior, including cyberbullying awareness and response, interacting on school LMS platforms, online discussions, video conferencing, and other forms of direct electronic communications.

When using 27J devices or 27J accounts, students shall not reveal personal information, such as home address or phone number, social security number, or credit card information while using the Internet or electronic communications. Without first obtaining permission of the supervising staff member, students shall not use their last name or any other information that might allow another person to locate him or her when communicating with non-27J persons. Students shall not arrange face-to-face meetings with persons met on the Internet or through electronic communications.

Vandalism

Vandalism will result in cancellation of privileges and may result in legal action and/or disciplinary action, including suspension and/or expulsion, in accordance with Superintendent policy concerning suspension, expulsion and other disciplinary interventions. Vandalism is defined as any malicious or intentional attempt to harm, destroy, modify, abuse or disrupt a district technology device, the operation of any network within the school district or any network connected to the Internet, the operation of any form of electronic communications, the data contained on any network or electronic communications, the data of another user, or usage by another user. This includes, but is not limited to, the uploading or creation of computer viruses and the use of encryption software. Damage to 27J issued devices may result in a fee per the One2Web student handbook and school board policy.

Unauthorized content

Students are prohibited from using or possessing any software applications, mobile apps, or other content that has been downloaded or is otherwise in the user's possession without appropriate registration, payment of any fee, and approval by the 27J IT department.

Assigning student projects and monitoring student use

School District 27J will make reasonable efforts to see that the internet and electronic communications are used responsibly by students. Administrators, teachers and staff have a professional responsibility to work together to monitor students' use of the internet and electronic communications, help students develop the intellectual skills needed to discriminate among information sources, identify information appropriate to their age and developmental levels, and evaluate and use information to meet their educational goals. Students shall be given specifically defined objectives and search strategies prior to accessing information on the internet and through electronic communications.

Opportunities shall be made available on a regular basis for parents to observe student use

of the internet and electronic communications in schools per 27J school visitor policies.

Staff members assigned to supervise student use shall have received training in internet and electronic communications, safety, and monitoring student use.

Student use is a privilege

Use of the internet and electronic communications demands personal responsibility and an understanding of the acceptable and unacceptable uses of such tools. Student use of the internet, electronic communications, and district technology devices is a privilege, not a right. Failure to follow the use procedures contained in this policy shall result in the loss of the privilege to use these tools and restitution for costs associated with damages, and may result legal action and/or disciplinary action, including suspension and/or expulsion, in accordance with Board policy concerning suspension, expulsion and other disciplinary interventions. The school district may deny, revoke, or suspend access to district technology or close accounts at any time.

School district makes no warranties

The school district makes no warranties of any kind, whether expressed or implied, related to the use of district technology devices, including access to the internet and electronic communications services. Providing access to these services does not imply endorsement by School District 27J of the content, nor does School District 27J make any guarantee as to the accuracy or quality of information received. The district shall not be responsible for any damages, losses or costs a student suffers in using the internet and electronic communications. This includes loss of data and service interruptions. Use of any information obtained via the internet and electronic communications is at the student's own risk.

Cell Phones and Digital Cameras

Students that have cell phones with digital camera features shall not share any digital photos or video footage of students or staff with anyone unless written permission is obtained by the person being photographed. Cell phone usage by students during the school day is permitted when directed by a teacher - see Superintendent Policy JICJ for specifics.

Sexting

Sexting is defined as the act of sending, receiving, viewing, or reading any sexually explicit text messages, photo messages, video messages, or voice messages. Sexting is considered inappropriate for the school setting and therefore prohibited on school grounds or at school events. In some cases, sexting is considered sexual harassment and bullying, and can result in severe legal ramifications. Anyone involved in violating this policy or involved in this violation will have their phone confiscated for the remainder of the school day or event with their parents being notified about the incident as soon as possible. And appropriate disciplinary consequences per the 27J discipline matrix will be implemented whether on a personal device or 27J-issued technology device.

Video and Camera Usage on School Grounds

It is the responsibility of School District 27J to provide a safe, secure learning and working environment for students and staff. Video (camera) surveillance is utilized in schools and on school property to maintain safety and security. Although video surveillance may not always prevent incidents from happening, it does provide an additional deterrent and can provide valuable evidence in the event of an incident.

In all cases:

1. The recording of specific events may and will be used in the prosecution of crimes against property, students and staff.
2. For the protection and privacy of students and staff, recordings will only be made available to school and law enforcement officials, parents/guardians, or other legal authorities as noted in 3.
3. Parents/guardians or students who wish to view a videotape in response to disciplinary action taken against a student may request such viewing access.

On district property:

1. School District 27J places cameras in locations to provide the best possible views. These cameras are in operation 24 hours a day, seven days a week. Therefore, anyone who walks in view of these cameras may be recorded.
2. Recordings are the property of School District 27J and are not ordinarily considered as part of the student's record.

LEGAL REFS.: 20 U.S.C. 6751et seq. (*Enhancing Education Through Technology Act of 2001*)

47 U.S.C. 254(h) (*Children's Internet Protection Act of 2000*)

47 C.F.R. Part 54, Subpart F (*Universal Support for Schools and Libraries*)

C.R.S. [22-87-101](#) et seq. (*Children's Internet Protection Act*)

CROSS REFS.: [AC](#) - Nondiscrimination & Equal Opportunity

[EHC](#) - Use of the Internet

[JB](#), Equal Educational Opportunities

[JK](#) - Student Code of Conduct

[JICJ](#) - Cell Phone and Electronic Devices

Adopted: August 25, 2020