

Instruction

Access to Electronic Networks

Electronic networks, are a part of the District's instructional program and serve to promote educational excellence by facilitating resource sharing, innovation, and communication.

The term electronic networks includes all of the District's technology resources, including, but not limited to:

1. The District's local-area and wide-area networks, including wireless networks (Wi-Fi), District-issued Wi-Fi hotspots, and any District servers or other networking infrastructure.
2. Access to the Internet or other online resources via the District's networks or to any District-issued online account from any computer or device, regardless of location.
3. District-owned or District-issued computers, laptops, tablets, phones, or similar devices.

The Superintendent shall develop an implementation plan for this policy and appoint system administrator(s).

The School District is not responsible for any information that may be lost or damaged, or become unavailable when using the network; or for any information that is retrieved or transmitted via Internet. Furthermore, the District will not be responsible for any unauthorized charges or fees resulting from access to the Internet.

Curriculum and Appropriate Online Behavior

The use of the District's electronic networks shall: (1) be consistent with the curriculum adopted by the District as well as the varied instructional needs, learning styles, abilities, and developmental levels of the students, and (2) comply with the selection criteria for instructional materials and library resource center materials. As required by federal law and Board policy 6:60, *Curriculum Content*, students will be educated about appropriate online behavior, including but not limited to: (1) interacting with other individuals on social networking websites and in chat rooms, and (2) cyber-bullying awareness and response. Staff members may, consistent with the Superintendent's implementation plan, use the Internet throughout the curriculum.

The District's electronic network is part of the curriculum and is not a public forum for general use.

Acceptable Use

All use of the District's electronic networks must be: (1) in support of education and/or research, and be in furtherance of the goals stated herein, or (2) for a legitimate school business purpose. Use is a privilege, not a right. Users of the District's electronic networks have no expectation of privacy in any material that is stored on, transmitted, or received via the District's electronic networks or District devices.

General rules for behavior and communications apply when using electronic networks. The District's administrative procedure, *Authorization for Electronic Network Access*, contains the appropriate uses, ethics, and protocol. Electronic communications and downloaded material, including files deleted from a user's account but not erased, may be monitored or read by school officials.

Internet Safety

Technology protection measures shall be used on each District computer with Internet access. Each District computer with Internet access shall have a filtering device that protects against Internet access by both adults and minors to visual depictions that are: (1) obscene, (2) pornographic, or (3) harmful or inappropriate for students, as defined by federal law and as determined by the Superintendent or designee. The Superintendent or designee shall enforce the use of such filtering devices. An administrator, supervisor, or other authorized person may disable the filtering device for bona fide research or other lawful purpose, provided the person received prior permission from the Superintendent or system administrator.

The Superintendent or designee shall include measures in this policy's implementation plan to address Internet use at the District as follows:

1. Ensure staff supervision of student access to online electronic networks,
2. Restrict student access to inappropriate matter as well as restricting access to harmful materials,
3. Ensure student and staff privacy, safety, and security when using electronic communications,
4. Restrict unauthorized access, including "hacking" and other unlawful activities, and
5. Restrict unauthorized disclosure, use, and dissemination of personal identification information, such as, names and addresses.

Authorization for Electronic Network Access

Each staff member must sign the District's *Authorization for Electronic Network Access* as a condition for using the District's electronic network. Each student and his or her parent(s)/guardian(s) must also sign the *Authorization before being granted unsupervised use*.

Confidentiality

All users of the District's computers to access the Internet shall maintain the confidentiality of student records. Reasonable measures to protect against unreasonable access shall be taken before confidential student information is loaded onto the network.

Violations

The failure of any user to follow the terms of the District's administrative procedure, Acceptable Use of the District's *Electronic Network*, or this policy, will result in the loss of privileges, disciplinary action, and/or appropriate legal action.

Google Apps for Education:

The Google Apps for Education for Students Suite, with the exception of Gmail, will be available to students in grades K-12. The following Google Apps for Education's Productivity Tools will be available for the appropriate grade bands: Calendar (K-12), Classroom (K-12), Docs: docs, spreadsheets, slides (K-12), Drive (K-12), Gmail (5-12), and Sites (K-12). These accounts will allow students and teachers to communicate and collaborate in a safe and structured manner.

Restrictions for Student Google Accounts:

All student accounts will begin with each student's ID number followed by @students.sd308.org. All accounts will be password protected. Students in grades 5-8 can only send and receive emails from other School District 308 teachers, students and approved domains. Students in grade 9-12 will be able to send and receive emails from within and outside of School District 308 domain.

Students will have access to a self-service portal to troubleshoot; students in grades 5-12 will be able to use this portal for password recovery. Students will need to answer three security questions, which they have selected during the initial set up, in order to recover their password. If students answer incorrectly, there will be one staff member per building who will have access to reset student passwords.

Upon graduation, students will have access to their Google Apps for Education files through Google Takeout. This process exports each student's digital work into a downloadable zip file. This process will allow students to continue to access their digital work as they continue their education after high school.

Filtering of Emails:

School email accounts must comply with the Federal Children's Internet Protection Act (CIPA). Student emails will be filtered, just as Internet access at school is filtered, to ensure student safety online. School District 308 uses filtering tools and makes every effort to block inappropriate content.

Opting Out:

If a parent/guardian has concerns about a child access to email through a Google account, a parent may contact the child's principal to opt out.

1:1 Device Program:

District 308 may issue an electronic device to District 308 students. The term 'device' may refer to a singular item or multiple items. All devices remain at all times the property of District 308. Each student and his or her parent(s)/guardian(s) must sign the *1:1 Device Program Agreement* agreeing to accept full responsibility for and proper care and treatment of the device as a condition of being issued and using a District 308 device. If the equipment becomes lost, stolen, or has become damaged through negligence or misuse, the parent/guardian agrees to replace and/or repair the device or reimburse School District 308 for the costs of such replacement/repair.

The District retains the right to revoke the privileges of use and may take disciplinary actions if the user does not comply with the conditions stated throughout the student handbook, this Policy, and as further set forth below:

1. The device shall be used for educational purposes only.
2. The District may seize and review the device at any time.
3. The device shall not be used in an unethical manner.
4. If a student is taking an extended vacation, they must return the device to the District before the start of the vacation. Upon their return, they will be re-issued the device.
5. The device must be turned in prior to the end of the school year in substantially the same condition as it was issued.
6. Students who leave the district must return the device to the Technology Department located at the District Administration Center at the time they leave the district. Failure to return the device within three days of withdrawal from the District may result in legal action, including but not limited to filing a police report and/or civil action.
7. The student is expected to follow classroom rules and expectations with the device at all times.
8. In the event the device is damaged, stolen, or lost, the student and/or the parent/guardian should contact the school immediately. Filing a police report may be advised.
9. The device shall be used only by the student to whom it was assigned. Use of the device by someone other than the student to whom it is assigned is in violation of District Policy.
10. The student will not receive official transcripts until all District owned technology has been returned to the District and/or the District has been reimbursed.

Damage to Device:

The District understands that accidents happen. Every case of damage will be assessed and evaluated to determine if the proper measures to keep the device safe were taken.

- If the student does not use proper care with the device resulting in damage, the student's parent/guardian may be responsible for repair or replacement costs.
- The determination of whether damages to the District device were accidental or due to negligent care and handling will be at the sole discretion of the District technology team working with the building administration.
- If the student has multiple cases of damage, that student may lose their device privileges for that school year.

Repair Costs:

The following are repair/replacement costs in case of damage to a student's device. The total charged amount shall be paid to the District.

- Broken Screen - \$70.00
- Broken Keyboard - \$23.00
- New Motherboard - \$185.00
 - Charging Port - \$59.00
 - Headphone Jack - \$59.00
- Battery Replacement - \$50.00
- Trackpad - \$ 6.00
- SSD - \$122.00
- Power Supply - \$20.00
- All Other Repairs - \$59.00
- Device Replacement - \$276.00
- Accessories (market cost)

LEGAL REF: 20 U.S.C. §7131, Elementary and Secondary Education Act.
47 U.S.C. §254(h) and (l), Children's Internet Protection Act.
47 C.F.R. Part 54, Subpart F, Universal Service Support for Schools and Libraries.
115 ILCS 5/14(c-5), Ill. Educational Labor Relations Act.
720 ILCS5/26.5.

CROSS REF: 5:100 (Staff Development Program), 5:170 (Copyright), 6:40 (Curriculum Development), 6:60 (Curriculum Content), 6:210 (Instructional Materials),6:230 (Library Resource Center), 6:260 (Complaints About Curriculum, Instructional Materials, and Programs), 7:130 (Student Rights and Responsibilities), 7:190 (Student Discipline), 7:310 (Restrictions on Publications and Written or Electronic Material), 7:315 (Restrictions on Publications: High Schools), 7:345 (Use of Educational Technologies: Student Data Privacy and Security).

Revised: October 22, 2007
Adopted: November 5, 2007
Revised: October 13, 2015
Adopted: November 9, 2015
Revised: October 11, 2016
Adopted: October 24, 2016
Reviewed: January 11, 2021
Approved: January 25, 2021
Reviewed: November 15, 2021
Approved: December 6, 2021