

STUDENT USE OF TECHNOLOGY (INTERNET)

The district encourages Internet access at schools to provide learning and communication opportunities for students and staff that support district's educational mission. Since the Internet is a vast and expanding resource that holds appropriate and inappropriate opportunities for students and staff, this policy is set forth to communicate acceptable and unacceptable Internet use at schools.

Students and staff should be aware that computer files and communications over electronic networks, including e-mail and voice-mail, are not private. The district reserves the right to monitor these systems at any time without advance notice or consent.

Staff Responsibility

1. Carefully read Board Policy 6163.4 and Administrative Regulation 6163.4 Student Use of Technology and sign the Staff Internet Use Agreement.
2. Make sure students and parents/guardians have signed the Internet Use Agreement before access is granted.
3. Take precautions to eliminate inappropriate access by using the filter proxy and appropriate supervision.
4. Direct questions to the principal or district technology coordinator if any part of the policy is unclear.

Parent/Guardian Responsibility

1. Carefully read Board Policy 6163.4 and Administrative Regulation 6163.4 Student Use of Technology and sign the Student Internet Use Agreement.
2. Make sure that your child understands the policy.
3. Direct questions to the school principal or staff if any part of the policy is unclear.

Student Responsibility

1. Carefully read Board Policy 6163.4 and Administrative Regulation 6163.4 Student Use of Technology (to the extent possible for younger children) and sign the Student Internet Use Agreement.
2. Follow the rules of use
3. Direct questions to parents/guardians or staff if any part of the policy is unclear.

Acceptable Internet Use

Internet access is available to students and staff for educational and professional purposes. Examples of acceptable uses include, but are not restricted to:

1. Researching curriculum topics.
2. Communicating with peers and experts.
3. Completing collaborative curriculum projects.
4. Participating in electronic field trips.
5. Working on individualized or group distance-learning projects.
6. Obtaining copyrighted material in accordance with copyright laws.
7. Staying abreast of current news and events.
8. Researching colleges or universities.
9. Researching career options.
10. Publishing educationally related information.
11. Finding educational grant-writing and contest opportunities.

Unacceptable/Illegal Internet Use

Internet access is NOT made available to students and staff for NON-educational or NON-professional purposes. It is NOT a right; it is a privilege that can be restricted/removed at any time. Examples of unacceptable/illegal uses include, but are not restricted to:

1. Transmitting or publishing personal information such as your name, address, telephone number, parent's/guardian's work address/telephone number or school name without permission.
2. Using or tampering with an account owned by another user without authorization.
3. Using the system for commercial or political use that is unrelated to educational purposes.
4. Installing or downloading software on a school computer without permission from authorized staff.
5. Transmitting harmful matter that is threatening, obscene, disruptive or sexually explicit.
6. Transmitting harmful matter that could be construed as harassment or disparagement of others based on their race, national origin, sex, sexual orientation, age disability, religion or political beliefs.
7. Promoting unethical practices or any activity prohibited by law or district policy.
8. Violating copyright laws.
9. Using ideas or writings from another person without giving credit to the author (plagiarism).
10. Libeling another person.
11. Causing damage to any school district property.
12. Maliciously accessing, altering, deleting, disrupting, damaging or destroying any computer system, computer network or computer program.

STUDENT USE OF TECHNOLOGY (INTERNET)

AR 6163.4 (d)

13. Reading or altering other users' electronic mail or files without permission.
14. Using network software that is prohibited by the network administrator.
15. Demonstrating any network security breaches to other users.

In addition,

1. Students shall not disclose, use or disseminate personal identification information about themselves or others when using electronic mail or other forms of direct electronic communication. Students are also cautioned not to disclose such information by other means to individuals located through the Internet without the permission of their parents/guardians.

Personal information includes the student's name, address, telephone number, Social Security number, or other individually identifiable information.

2. Students shall not use the system to encourage the use of drugs, alcohol or tobacco, nor shall they promote unethical practices or any activity prohibited by law or Board policy.

(cf. 3513.3 - Tobacco-Free Schools)

3. Copyrighted material shall not be placed on the system without the author's permission. Students may download copyrighted material for their own use only.

(cf. 6162.6 - Use of Copyrighted Materials)

4. Students shall not intentionally upload, download or create computer viruses and/or maliciously attempt to harm or destroy district equipment or materials or manipulate the data of any other user, including so-called "hacking."

(cf. 5131.5 - Vandalism, Theft and Graffiti)

5. Students shall not read other users' electronic mail or files. They shall not attempt to interfere with other users' ability to send or receive electronic mail, nor shall they attempt to delete, copy, modify or forge other users' mail.
6. Students shall report any security problem or misuse of the services to the teacher or principal.

The district reserves the right to monitor any on-line communications for improper use. Electronic communications and downloaded material, including files deleted from a user's account, may be monitored or read by district officials to ensure proper use of the system.

(cf. 5145.12 - Search and Seizure)

The principal or designee shall make all decisions regarding whether or not a student has violated Board policy or the district's Acceptable Use Agreement. The decision of the principal or designee shall be final.

Violations

Unacceptable and/or unethical use of the Internet will be cause for revoking network privileges and/or disciplinary action and for possible legal action when an individual uses the network for:

1. Illegal activities which violate local, state, and/or federal laws;
2. Inappropriate use which violates the intended use of the network;
3. Obscene activities that violate generally accepted social standards.

If a student is accused of any violations, he/she has all of the rights and privileges that exist with other kinds of school infractions. The school has the right to restrict or terminate Internet access for violators. The school also has the right to monitor network activity in whatever forms necessary to maintain the integrity of the system. Students should have no expectation

of privacy. After a fair hearing, students who are found to have violated the rules for network behavior may be subject to the following:

1. Suspension and/or revocation of Internet access.
2. Suspension and/or revocation of computer access.
3. School suspension.
4. School expulsion.
5. Legal action and prosecution by authorities.

No Warranty

The district makes no warranties with respect to the Internet and specifically assumes no responsibilities for:

1. The content of any advice or information received by an account holder from a source outside the district or any costs or charges incurred as a result of seeking or accepting such advice;
2. Any costs, liability, or damages caused by the way the account holder chooses to use his/her Internet access;
3. Any consequences of service interruptions or changes, even if these disruptions arise from circumstances under the control of the district;
4. Guaranteeing that a student without a parent/guardian consent to use the Internet will never gain access to the network.