I-18: Administrative Procedures Acceptable Student Use of Internet, Computers, and Network Resources

SALT LAKE CITY SCHOOL DISTRICT
Your Best Choice

REFERENCES

Board Policy I-18

DEFINITIONS

Electronic Device: Any device used for audio, video, or text communication, or any other type of computer or computer-like instrument including, but not limited to cell phones, smart watches, tablets, cameras/video recorders, and or video game devices.

Parent:

For purposes of these administrative procedures and the corresponding board policy, "parent" means:

A. a biological or adoptive parent;
B. a legal guardian or other individual legally authorized to make educational decisions for the child;
C. an individual, with whom the child lives, who is acting as a parent in the absence of a natural parent or a guardian;
D. a foster parent if the authority of the biological or adoptive parents to make educational decisions on the child's behalf has been terminated or specifically limited by a court order;
E. in the absence of any individual qualified under parts A-D, a surrogate parent appointed pursuant to the Individuals with Disabilities Education Act; and/or
F. a stepparent if the stepparent is present on a day-to-day basis with the natural parent and child, and the other parent is absent from the home. A stepparent who is not present on a day-to-day basis in the home of the child does not have rights under Family Educational Rights and Privacy Act (FERPA) with respect to the child's education records. Stepparents without guardianship of a child do not have the authority to enroll or register a child in school.

"Parent" does not include the state or any political subdivision of government.

PROCEDURES FOR IMPLEMENTATION

I. Authority

A. The district has the right to, and in some instances a legal obligation to place restrictions on students' use of and access to electronic devices, and district provided computer systems, computer networks, district-adapted tools and devices, software applications, email, and the Internet (collectively "electronic resources").
B. In general, all students are responsible for the responsible, ethical, and legal utilization of the district's electronic resources. When using these resources, either on or off district property, students must comply with these administrative procedures as well as Board Policy S-3: Student Conduct and Discipline.

II. Access to District Electronic Resources

A. Through the registration process, parents and students will attest that they have read and understand these administrative procedures and the accompanying board policy ("Responsible Use Contract").
   1. Parents may terminate their student's access in accordance with Section VI.C.
B. At a minimum, teachers shall review these administrative procedures and other applicable rules and regulations with students on an annual basis, but teachers are encouraged to discuss appropriate use guidelines with students on a regular basis when they are using the district's electronic resources.
C. After enrolling in the district, all students will be provided a password in order to access the district's electronic resources.

III. Privileges

A. The use of the district's electronic resources is a privilege, not a right. Inappropriate use may result in a loss of network privileges, disciplinary action, and/or referral to legal authorities. The system administrators have the authority to close an account at any time.
   1. An administrator or faculty member may request the system administrator deny, revoke, or suspend a specific user's access and/or his/her user accounts.
B. By accessing the district's network resources, students acknowledge that they have read, understand, and agree to comply with the provisions of board policies I-18 and S-3, and their accompanying administrative procedures.

IV. Acceptable Use

A. A student's use of the district's electronic resources shall be for educational purposes only, which includes accessing and sharing information with teachers and other students, storing files, conducting research, and collaborating on projects with others.
   1. In some instances, students may be directed by their teachers to use the district's electronic resources in conjunction with their curriculum, an assessment, or a behavior support program.

B. Students are expected to abide by the generally accepted rules of network etiquette. These include, but are not limited to the following:
   1. Be polite.
   2. Do not be abusive in your messages to others.
   3. Use appropriate language.
   4. If told by a person to stop sending messages, the sender must stop.

V. Care of District Electronic Devices

A. Electronic devices used by students shall primarily be used only for educational purposes that directly relate to a school project or assignment, unless authorized by building administration. Personal use of district electronic devices by students may only be incidental and may not disrupt the learning environment.

B. Students are responsible for the proper care of each district electronic device that they use. Students and their parents may be responsible for costs associated with repairing damaged computers. Repair costs for computers may exceed $700. If a student or parent is unable to pay for repairs, alternative forms of restitution may be established with building administration.

VI. Prohibited Uses

The following uses of the district's electronic resources are prohibited:

A. Illegal use: any use that violates, or supports the violation of, federal, state, or local laws, board policy, school rules, and/or the student code of conduct (including any form of bullying, humiliation, intimidation, and harassment); use of copyrighted materials or material protected by trade secrets without appropriate authorization; any use in violation of software license agreements; and any use that constitutes plagiarism.

B. Vandalism and/or theft: any deliberate attempt to damage the hardware, software, or information resident on the district's network or any other computer system attached through the Internet; violating, or attempting to violate, the integrity of private accounts, files, or programs; deliberately infecting a computer with a virus; hacking computers using any method; interfering with computer or network performance; interfering with another's ability to use equipment and systems; destroying data.

C. Commercial use: any use for commercial purposes or activities resulting in personal financial gain, including product advertisements and solicitations.

D. Offensive or harassing behavior: any use of material, whether visual or textual, that may be deemed profane, vulgar, pornographic, indecent, abusive, threatening, obscene, or sexually explicit; distribution of disparaging or harassing statements including those that might incite violence or that are based on race, color, pregnancy, gender identity, genetic information, national origin, sex, sexual orientation, age, disability, or political or religious beliefs; posting of anonymous messages.

E. Religious or political use: any use for a religious or political purpose, including religious proselytizing and lobbying for student body elections.

F. Security violations: using an account other than the student's assigned account; accessing, or attempting to access accounts, sites, servers, files, databases, or other systems for which a student is not authorized (e.g. "hacking" or using "spyware"); spreading computer viruses; degrading or disrupting network equipment, software, or system performance; running applications or files that create a security risk; any other action that threatens the security of the district's electronic resources.

G. Disseminating or accessing confidential information: transmitting confidential information about other individuals; violating the privacy of others by reading or posting e-mail or other private communications without obtaining the appropriate consent; providing personal addresses, phone numbers, or financial information in any network communication whether that information belongs to the student user or any other individual unless it is related to an appropriate education objective in the curriculum.

H. Unnecessary uses: downloading or streaming audio or video files, or any other files that are not directly related to course curriculum; playing non-educational Internet games; accessing or using services on the Internet that impose a fee on the student.

I. Tampering: any attempt to bypass state, district, or school security; attempting to disable or bypass the district's Internet blocking/filtering software without authorization; adding, modifying, repairing, removing, reconfiguring, or tampering with any device on the district's network infrastructure.

VII. Discipline and Termination of Accounts

A. Authorized district employees will be responsible to determine what constitutes a violation of these procedures or the corresponding board policy. Authorized district employees have the right to intercept or read a student's email, review any material, edit or remove any material which they believe may be unlawful, obscene, defamatory, abusive, or otherwise objectionable.

B. If the district intends to impose any discipline, other than revoking privileges for the remainder of the school year, the user will be afforded appropriate due process.

C. An account will be terminated when:
   1. the student's parent makes a request in writing to the principal that the account be terminated;
   2. any authorized district employee determines the account should be terminated; or
   3. a student leaves the district.

VIII. Privacy Information

Nothing is private on the network. A student has no expectation of privacy as to his/her communications on or uses of the Internet. Frequently internet sites maintain records that can be subpoenaed to identify what the user has been viewing and downloading on the Internet. The district reserves the right to monitor whatever a user does on the network.

IX. Security

A. Security is a high priority on computer networks.

B. If a security problem is identified, the user must notify the system administrator immediately. Students should not demonstrate the problem to other users.
   1. Users may not use the Internet to discuss or disseminate information regarding security problems or how to gain unauthorized access to sites, servers, files, etc.
   2. Do not share passwords with other users, and change passwords frequently.
   3. Do not leave a electronic workstation without logging out of the network.

C. Students must report any of the following to a teacher or administrator:
   1. if a student receives or obtains information to which s/he is not entitled;
   2. if a student knows of any inappropriate use of the network by others; or
   3. if a student believe the filtering software is not filtering a site or sites that should be filtered under this agreement.

X. Disclaimer

The district makes no warranties of any kind, whether expressed or implied, for the services it is providing. Electronic resources are provided on an "as is, as available" basis. The district will not be responsible for any damages a student may suffer while using its electronic resources. These damages may include but are not limited to: loss of data resulting from delays, non-deliveries, or service interruptions caused by the system or by an individual's negligence, error or omission. The district makes no promise or warranty to maintain or update its network, or the information contained therein. The district may suspend or discontinue these services at any time. Use of any information obtained via the information system is at the student's own risk. The district specifically denies any responsibility for the accuracy or appropriateness of information obtained through electronic resources.

XI. Filtering/Blocking Software

In accordance with state law and the Children's Internet Protection Act, the district utilizes and consistently configures filtering/blocking software to block access to sites and materials that are inappropriate, offensive, obscene, contain pornography, or are otherwise harmful to students. The district will utilize its best efforts to block access to such sites and materials but cannot guarantee the complete effectiveness of its filtering/blocking software.