

Salt Lake City School District

Administrative Procedures for Board Policy P - 8

Under Revision

Title: Employee Internet Acceptable Use (AUP)
Index: P = Personnel Policies

References: [Salt Lake City School District Board Policy P - 8](#)

Definitions:

Acceptable Use: Internet use must be consistent with the Professional and Ethical Guidelines as outlined by the Utah State Office of Education. The district does not prohibit the occasional personal use of the Internet consistent with this AUP.

Prohibited Use: Any use that violates federal or state laws and/or board policy.

Procedures for Implementation:

1. Prohibited Uses: Unless specifically authorized by the superintendent or the business administrator, the following use of the district's computers, including its network and Internet access are prohibited:
 - a. Using an account other than your own and any attempt to gain unauthorized access to accounts on the network.
 - b. Attempting to obtain access to restricted sites, servers, files, databases, etc., and attempting to gain unauthorized access to other systems (e.g. "hacking").
 - c. Using non-educational Internet games.
 - d. All unmoderated chat rooms and moderated chat rooms not related to the core curriculum.
 - e. Using the Internet or network for any illegal activity. This includes, but is not limited to; distributing copyrighted material, threatening or obscene material, or material protected by trade secrets. This prohibition includes the violation of any federal, state, or local law.
 - f. Providing personal addresses, phone numbers, and financial information of any individual, other than yourself, in any network communication.
 - g. Using the Internet for commercial purposes, financial gain, personal business, product advertisement, religious or political lobbying.
 - h. Attempting vandalism defined as any intent to harm or destroy data of another user, another agency or network that is connected to the Internet. Vandalism includes, but is not limited to, the uploading, downloading, or creation of computer viruses. It also includes attempts to gain unauthorized access to a network that is connected to the Internet.
 - i. Degrading or disrupting network equipment, software or system performance.
 - j. Wasting finite network resources.
 - k. Invading the privacy of individuals or disclosing confidential information about other individuals unless directly related to your work assignment.
 - l. Posting personal communications without the original author's consent.
 - m. Posting anonymous messages.
 - n. Accessing, downloading, storing, or printing files or messages that are profane, obscene, or that use language that offends or tends to degrade others.
 - o. Harassing others and using abusive or obscene language on the network. You may not use the network to harass annoy or otherwise offend other people.
 - p. Using material which may be deemed to violate any district policy or the Professional and Ethical Guidelines as outlined by the Utah State Office of Education.
 - q. Downloading music or video files or any other files that are not directly related to the core curriculum.
 - r. Communicating threats of violence.
 - s. Using the network for plagiarism. Plagiarism is taking ideas or writing from another person and offering them as your word. Credit must always be given to the person who created the information or idea.
2. Privileges and Discipline
 - a. Internet use is a privilege, not a right. Inappropriate use may result in a loss of network privileges, referral to legal authorities, and/or disciplinary action which may include reprimand, suspension, or termination of employment. The system administrators will close an account when necessary. An administrator may request the system administrator deny, revoke, or suspend specific user access and/or user accounts.

- b. Authorized district employees will be responsible to determine what constitutes a violation of this policy. Authorized district employees have the right to intercept or read a users email, review any material and to edit or remove any material which they believe may be unlawful, obscene, defamatory, abusive, or otherwise objectionable. 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. The following processes must be followed when reporting and AUP/Internet violation:
 - 1. Notify a school administrator or system administrator.
 - 2. The school or system administrator will notify the human resource department and the appropriate law enforcement agency if necessary.
 - 3. The human resource department will guide the investigation and subsequent discipline.
 - 4. The human resource department may request assistance from Information Systems in the investigation, technical details, or damage.
 - 5. The violation and any discipline will be recorded in the employees personnel file.

3. Privacy Information

- a. Nothing is private on the network. A user has no expectation of privacy as to their Internet communications or uses. When a user accesses the Internet, it is likely that someone knows the connections that the user is making, knows about the computer the user is using, and what the user looked at while on the system. Frequently, these sites maintain records which can be subpoenaed to identify what the user has been viewing and downloading on the Internet. In addition, the district reserves the right to monitor whatever a user does on the network and to make sure the network functions properly. A user has no expectation of privacy as to his or her communications or the uses made of the Internet. In addition, under Utah's Governmental Records Access Management Act and the Federal Educational Right to Privacy Act, persons outside the district may be able to request and receive information from the district, information regarding an individual's communications and use of the network.

4. Network Etiquette

- a. Users 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; and
 - 4. Do not swear, use vulgarities or any other language inappropriate in a school setting.

5. Security

- a. Security is a high priority on computer networks. If a security problem is identified, the user must:
 - 1. Notify the system administrator immediately;
 - 2. Do not demonstrate the problem to other users. 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.;
 - 3. Do not share passwords with other users and change them frequently; and
 - 4. Do not leave a workstation without logging out of the network.
- b. You must report any of the following to a building administrator:
 - 1. If you receive or obtain information to which you are not entitled;
 - 2. If you know of any inappropriate use of the network by others;
 - 3. If you believe the filtering software is not filtering a site or sites that should be filtered under this agreement; and/or
 - 4. If you have information that users are using and/or accessing accounts other than their own.

6. Disclaimer

- a. The district makes no guarantee of the completeness or accuracy of any information provided on the network. It will not be responsible for any damages suffered because of the use of its networks. This includes loss of data resulting from delays, non deliveries, or service interruptions caused by negligence, errors or omissions. It makes no promise or warranty to maintain or update its network, or the information contained or made available to the public, or to its employees and students. The district may suspend or discontinue these services at anytime. The user assumes the risk of verifying any materials used or relied on.

- b. The district disclaims any express or implied warranty in providing its computer system and any materials, information, graphics, or processes contained therein. It makes no warranty, express or implied, nor assumes any responsibility regarding the use of its network or its contents for its accuracy, completeness, currency, use of any general or particular purpose, or that such items or use of such items would not violate or infringe on the rights of others. Access to its network is provided on a strictly "as is basis".
 - c. The district's network resources may contain hypertext or other links to Internet or computer site not owned or controlled by the district that may be of interest. The district cannot supervise or control the content of these other sites. Any information, endorsement of products, services, materials, or personal opinions appearing on such external sites, are not controlled, sponsored or approved by the district.
 - d. The district specifically disavows legal responsibility for what a user may find on another site, or for personal opinions of individuals posted on any site, whether or not operated by the district.
 - e. A user assumes the risk of use or reliance on any information obtained through the network.
 - f. The district will not be responsible for any damages a user suffers while on the system, missed deliveries or service interruptions caused, including loss of data resulting from delays, non-deliveries by negligence, errors or omissions.
7. Salt Lake City School District's Guidelines for Access and/or Accounts
- a. All users must read and agree to follow all guidelines outlined in the AUP. This agreement is formalized through the user's signature on the application. Users may be granted an account for their term of employment.
 - b. Signatures on the AUP are legally binding, and indicate that parties, who signed, have read the terms and conditions carefully and understand their significance.
 - c. Any user, who has received a password, is deemed to have received, read, understood, and agreed to the terms of the AUP.

Approved by: McKell Withers
Date: 3/28/07

Page 3 of 3