P-8: Administrative Procedures
Acceptable Employee Use of Internet, Computers, and Network Resources

SALT LAKE CITY SCHOOL DISTRICT
Your Best Choice

REFERENCES

Board Policy P-8
Data Governance Plan
IT Security Plan

PROCEDURES FOR IMPLEMENTATION

I. Authority

A. The district has the right to place restrictions on the use of equipment, resources, and materials employees access or disclose through the district's Internet, computers, and network resources (collectively "electronic resources").

B. In general, all district employees are responsible for the efficient, ethical, and legal utilization of the district's electronic resources. Employees must therefore comply with all applicable local, state, and federal laws, board policies, and administrative procedures in their use of such resources.

II. Access to District Electronic Resources

A. Employees may be given access to the district's electronic resources, including an account and password. This access must not be shared, assigned, or transferred to another individual.

B. The district will periodically require new registration and account information from its employees. Employees must notify the district's human resource services department (HRS) of any changes in account information (address, phone, name, etc.). Once HRS updates the information, the changes should start propagating to district systems within 24 hours. If that does not occur, please contact the district's information systems department (IT department).

C. This access has not been established as a public access service or a public forum.

III. Electronic Devices Issued to Staff

A. Employees may be issued electronic devices (i.e., laptops, tablets, mobile phones, etc.) for the purpose of completing assigned tasks related to their assigned responsibilities and job position.

B. Assigned electronic devices remain the property of the district.

C. The primary purpose of district issued electronic devices is to perform the work of the district.

1. Employees may use district issued equipment for incidental personal use, so long as such use does not interfere with their ability to perform their assigned job responsibilities or disrupt the working or learning environment.

D. Mobile devices assigned to overtime exempt administrators, teachers, facilities supervisors, and IT staff may be taken home or to other non-district locations for the purpose of aiding them in their work while away from the district network. In general, non-exempt employees should not take district issued electronic devices off premise.

1. Rare exceptions must be approved in advance by the employee's supervisor.

E. In general, electronic devices issued at one location may not be relocated to another department or school; however, laptops issued to administrators or teachers may be relocated.

1. A laptop issued to a teacher should remain at the school if the teacher takes a position (i.e., academic coach, PAR coach, assessment data analyst, etc.) based at the district office or auxiliary services building.

IV. Software Procurement and Installation Procedures

A. If an employee wants to purchase or develop software for district use, the district's IT department must give written approval prior to the purchase or development.

B. No employee shall install or distribute software without the appropriate license and approval of the district's IT department.

V. Privileges

A. The use of the district's electronic resources is a privilege, not a right. Inappropriate use may result in disciplinary action up to and including termination, and when appropriate, a referral to legal authorities. An administrator or supervisor may limit, suspend, or revoke an employee's access to electronic resources at any time.

1. An employee may be subject to disciplinary action and other consequences for misuse of the district's electronic resources assigned to that employee, including instances when other individuals used the employee's assigned device or account.

B. The district uses monitoring systems to monitor and detect inappropriate use and may use tracking systems to track and recover lost or stolen equipment.
C. By accessing the district's network resources, employees acknowledge that they have read, understand, and agree to abide by the provisions of Board Policy P-8 and these administrative procedures.

VI. Acceptable Use

A. An employee's use of the district's electronic resources shall be consistent with the district's purpose, mission, and goals, and shall be for educational and professional purposes.
B. Incidental use of electronic resources for personal reasons is allowed provided that such use does not:
   1. disrupt or distract from the conduct of district business due to volume, timing, or frequency;
   2. interfere with the employee's duties;
   3. violate the provisions of these administrative procedures; and
   4. involve actions which may harm or otherwise disadvantage the district.
C. Any employee who "publishes" on the Internet must abide by the district's approved publishing procedures as outlined in the I-23: Administrative Procedures, Websites and Social Media.
D. All employees 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.

VII. Care of assigned equipment

A. Employees are responsible for the proper care and security of district issued devices, both on and off district property.
B. Employees should ensure that district issued mobile devices are properly secured in their offices or classroom, e.g., by locking devices in a car or cabinet, and/or locking the classroom/office door that contains the device(s).
C. Employees must report a lost or stolen device to building administration and to the IT department immediately.
   1. If a device is stolen, a report also should be made immediately with local police.
D. It is understood that the employee is responsible for any damage to or loss of property if the authorized device has been removed from district premises.
E. If necessary, the district may reduce an employee's payroll check to cover the replacement cost of the property if it is not returned. If the employee's last payroll check has already been issued, or is not sufficient to cover the cost of replacement, the employee will work with the district to promptly pay for any unreturned/damaged equipment.

VIII. Prohibited Uses

A. The following uses of the district's electronic resources are prohibited and just cause for termination of use privileges, disciplinary action, and/or legal action.
   1. Illegal use: any use that violates, or supports the violation of, federal, state, or local laws, and/or board policy; any unauthorized use of copyrighted materials or material protected by trade secrets; any use in violation of software license agreements; any use that constitutes plagiarism; any use to view, create, distribute, or store pornographic or indecent material in any form, including material involving children.
   2. Vandalism and/or theft: any deliberate attempt to damage the hardware, software, or information residing 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.
   3. Commercial use: any use for commercial purposes or activities resulting in personal financial gain, including product advertisements and solicitations.
   4. Offensive or harassing behavior: any use of material, whether visual or textual, that may be deemed profane, vulgar, abusive, threatening, obscene, or sexually explicit; distribution of disparaging or harassing statements including those that might incite violence or that are based on race, national origin, sex, sexual orientation, age, disability, or political or religious beliefs; posting of anonymous messages.
   5. Religious or political use: any use for a religious or political purpose, including religious proselytizing and lobbying for student body elections.
   6. Security violations: using an account other than your own; accessing, or attempting to access accounts, sites, servers, files, databases, or other systems for which an employee 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.

7. Disseminating or accessing confidential information: transmitting confidential information about other individuals or information that is classified as other than "public" under Utah's Government Records Access and Management Act (GRAMA) without proper authorization; violating the privacy of others by reading or posting e-mail or other private communications without obtaining the appropriate consent.
8. Unnecessary uses: downloading or streaming audio or video files, or any other files that are not directly related to ordinary course of business; forwarding or replying to chain letters, pyramid schemes, "contests" or "fast cash" schemes; and posting or sending advertisements, unauthorized solicitations, mass cross-postings, and uninvited mass mailings.
9. 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.

IX. Violations and Discipline

A. Authorized district employees will be responsible for determining what constitutes a violation of these procedures. Authorized district employees have the right to intercept or read a user's 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, the employee will be afforded appropriate due process.

B. The following processes must be followed when reporting a violation:
   1. Notify a school administrator or the district's IT department.
   2. The school administrator or member of the IT department will notify HRS, and the appropriate law enforcement agency, if necessary.
   3. HRS will guide the investigation and subsequent discipline.
   4. HRS may request assistance in the investigation from the IT department.
   5. Any substantiated violation and imposed discipline will be recorded in the employee's personnel file.

C. If in the course of performing his/her job duties, a member of the IT department views an image on a computer or other electronic device that is or appears to be child pornography, state law requires the IT staff member to immediately report the finding of the image to state or local law enforcement, the Cyber Tip Line at the National Center for Missing and Exploited Children, or the chief information officer.

X. Privacy of Information

A. Nothing is private on the network. The district's electronic resources are district property. Employees should recognize there is no expectation of privacy as to their use of the district's electronic resources. Therefore, employees shall have no expectation of privacy in anything they create, store, send, delete, receive, or display on or over the district's electronic resources, including personal files. The district reserves the right to monitor, track, and log network access and use; monitor fileserver space utilization; and deny access to prevent unauthorized, inappropriate, or illegal activity.

B. The district shall cooperate fully with local, state and federal officials in any investigation concerning or related to illegal activities. In addition, under GRAMA and the Family Educational Rights and Privacy Act, persons outside the district may be able to request and receive information regarding an employee's communications and use of electronic resources.

XI. Personally Identifiable Information

A. Personally identifiable information (PII) is information that, alone or in combination, is linked or linkable to a specific individual that would allow a reasonable person in the school/district community, who does not have personal knowledge of the relevant circumstances, to identify the individual with reasonable certainty.
   1. Examples of PII include an individual's social security number, biometric records, date and place of birth, mother's maiden name, employee's home address, etc.
   2. Employees shall not provide any student PII to a non-district employee, include websites and software, without the written permission of the district's Chief Information Officer,
   3. Student PII that is not considered directory information should only be shared with district employees who have a right and need to know such information.

B. The district's Data Governance Plan outlines the processes that employees must understand and comply with in regard to protecting student data. The plan is available at: https://www.slcschools.org/departments/business-administration/information-technology/student-data-privacy/documents/data-governance-plan/english/.
   1. Employees should also be familiar with the district's IT Security Plan, available at: https://www.slcschools.org/departments/business-administration/information-technology/student-data-privacy/documents/it-security-plan/english/.

C. Employees must annually take the on-line data privacy trainings before having any access to student PII.

D. Employees shall only access PII for those students/staff for which they have a right and a need to know such information as determined by their job position.

E. PII shall not be stored on any personal (non-district provided) cloud-based storage utility such as Google Drive, Dropbox, etc.

F. Employees who store PII on a district mobile device must take all necessary precautions to protect the device from being compromised, lost, or stolen. If a device containing PII is compromised, lost, or stolen, the loss must be reported to the immediate supervisor and the district's IT department.

XII. Ownership of Messages, Data and Documents

A. Except where required by law, all information contained in the district's electronic resources are district property. Therefore, all information created, sent, received, accessed, or stored using these electronic resources is district property.

B. Upon termination of employment, the district is under no obligation to provide access to personal files or other information stored on the district's electronic resources.

1. Employees must return all district computers and equipment that is within their possession upon their separation from district employment.

XIII. Security

A. Security is a high priority on computer networks because of multiple users.

B. Every employee must take appropriate security measures to protect his/her computer from unauthorized access. Such measures include, but are not limited to, locking the computer when you are away from the device, and locking doors to offices/rooms when no employee is present to monitor access.

C. If a security problem is identified, the user must notify the system administrator immediately. Employees must not demonstrate the problem to other users.

D. You must report any of the following to a school administrator or the IT department:

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; or
4. if you have information that users are using and/or accessing accounts other than their own.

XIV. Filtering/Blocking Software

The district utilizes and consistently configures filtering/blocking software to block access to sites and materials that are inappropriate, offensive, and obscene, contain pornography, or are otherwise harmful to district personnel as required by federal and state law. Filtering/blocking software is continuously in effect on the district's electronic resources on and off-site. The district will utilize its best efforts to block access to such inappropriate sites and materials but cannot warrant the complete effectiveness of its filtering/blocking software.

XV. 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 an employee 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 employee 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 employee's own risk. The district specifically denies any responsibility for the accuracy or appropriateness of information obtained through electronic resources.

XVI. Guest Computer/Network Access

The district provides guest wireless access to non-employee and non-student users such as presenters, vendors, consultants, auditors, school community council members, PTA members and other such individuals who help meet the educational and business needs of the district. Guest access is NOT intended for students, teacher or district employee use. Guest access only allows a limited number of connections and does not allow printing or access to other internal district functions and is filtered to comply with the Child Internet Protection Act. All activity on the guest wireless network is logged. All guests who use the district guest network or use a district computer must comply with Board Policy P-8 and these administrative procedures.