SANTA FE R-X STUDENT TECHNOLOGY USAGE

Grades K-12 User Agreement

I have read the Santa Fe R-X School District Technology Acceptable Use Policy as outlined in Santa Fe R-X School District Regulation 6320 and agree to abide by its provisions. I understand that violation of these provisions may result in disciplinary action taken against me, including but not limited to suspension, or revocation of my access to district technology, and suspension or expulsion from school.

I understand that my use of the district's technology is not private and that the school district may monitor my use of district technology, including but not limited to accessing browser logs, e-mail logs, and any other history of use. I consent to district interception of or access to all communications I send, receive, or store using the district's technology resources, pursuant to state and federal law, even if the district's technology resources are accessed remotely.

Student Signature_____ Date_____

Printed Name_____ Graduation Year_____

Parent/Guardian Technology Agreement

I understand that violation of the Santa Fe R-X School District Technology Acceptable Use Policy may result in disciplinary action taken against my child, ward, or child within my care, including but not limited to suspension or revocation of my child's or ward's access to district technology, and suspension or expulsion from school.

I understand that my child's or ward's technology usage is not private and that the school district will monitor my child's or ward's use of district technology, including but not limited to accessing browser logs, e-mail logs, and any other history of use. I consent to district interception of or access to all communications sent, received or stored by my child or ward using the district's technology resources, pursuant to state and federal law, even if the district's technology resources are accessed remotely.

I agree to be responsible for any unauthorized costs arising from my child's or ward's use of the district's technology resources. I agree to be responsible for any damages incurred by my child or ward.

I give permission for my child or ward to utilize the school district's technology resources.

Circle one: YES NO

The district maintains a website. Students' pictures, likeness, and/or student's work could occasionally appear on the website as they participate in school activities.
I grant permission for a picture or likeness of my child/ward and/or work to appear on the district website, www.santafechiefs.k12.mo.us, and district social media accounts (Facebook, Twitter, Instagram, etc.).

Circle one: YES NO

Signature of Parent_____ Date_____

G Suite for Education Permission Form

I give permission for Santa Fe R-X School District to create/maintain a G Suite for Education account for my child. I realize that my child may be able to selectively share educational documents he/she chooses from his/her account.

Circle one: YES NO

Student Name (Print) _____ Parent/Guardian's Name (Print) _____

Parent/Guardian's Signature _____ Date_____

INSTRUCTIONAL SERVICES Regulation 6320

Library, Media, and Technology Services

Internet Usage

Personal Responsibility

Access to electronic research requires students and employees to maintain consistently high levels of personal responsibility. The existing rules found in the District's Behavioral Expectations policy (Board Policy/Regulation 2610) as well as employee handbooks clearly apply to students and employees conducting electronic research or communication.

One fundamental need for acceptable student and employee use of District electronic resources is respect for, and protection of, password/account code security, as well as restricted databases files, and information banks. Personal passwords/account codes may be created to protect students and employees utilizing electronic resources to conduct research or complete work.

These passwords/account codes shall not be shared with others; nor shall students or employees use another party's password except in the authorized maintenance and monitoring of the network. The maintenance of strict control of passwords/account codes protects employees and students from wrongful accusation of misuse of electronic resources or violation of District policy, state or federal law. Students or employees who misuse electronic resources or who violate laws will be disciplined at a level appropriate to the seriousness of the misuse.

Acceptable Use

The use of the District technology and electronic resources is a privilege, which may be revoked at any time. Staff and students are only allowed to conduct electronic network-based activities which are classroom or workplace.related. Behaviors which shall result in revocation of access shall include, but will not be limited to: damage to or theft of system hardware or software; alteration of system hardware or software; placement of unlawful information, computer viruses or harmful programs on, or through the computer system; entry into restricted information on systems or network files in violation of password/account code restrictions; violation of other users' rights to privacy; unauthorized disclosure, use or dissemination of personal information regarding minors; using another person's name/password/account to send or receive messages on the network; sending or receiving personal messages on the network; and use of the network for personal gain, commercial purposes, or to engage in political activity.

Students and employees may not claim personal copyright privileges over files, data or materials developed in the scope of their employment, nor may students or employees use copyrighted materials without the permission of the copyright holder. The Internet allows access to a wide variety of media. Even though it is possible to download most of these materials, students and staff shall not create or maintain archival copies of these materials unless the source indicates that the materials are in the public domain.

Access to electronic mail (E-mail) is a privilege and designed to assist students and employees in the acquisition of knowledge and in efficiently communicating with others. The District E-mail system is designed solely for educational and work related purposes. *E-mail files are subject to review by District and school personnel.* Chain letters, "chat rooms" or Multiple User Dimensions (MUDs) are not allowed, with the exception of those bulletin boards or "chat" groups that are created by teachers for specific instructional purposes or employees for specific work related communication.

Students or employees who engage in "hacking" are subject to loss of privileges and District discipline, as well as the enforcement of any District policy, state and/or federal laws that may have been violated. Hacking may be described as the unauthorized review, duplication, dissemination, removal, damage, or alteration of files, passwords, computer systems, or programs, or other property of the District, a business, or any other governmental agency obtained through unauthorized means.

To the maximum extent permitted by law, students and employees are not permitted to obtain, download, view or otherwise gain access to "inappropriate matter" which includes materials that may be deemed inappropriate to minors, unlawful, abusive, obscene, pornographic, descriptive of destructive devices, or otherwise objectionable under current District policy or legal definitions.

The District and school administration reserve the right to remove files, limit or deny access, and refer staff or students violating the Board policy to appropriate authorities or for other disciplinary action.

Privileges

The use of District technology and electronic resources is a privilege, not a right, and inappropriate use will result in the cancellation of those privileges. All staff members and students who receive a password/account code will participate in an orientation or training course regarding proper behavior and use of the network. The password/account code may be suspended or closed upon the finding of user misuse of the technology system or its resources.

Network Etiquette and Privacy

Students and employees are expected to abide by the generally accepted rules of electronic network etiquette. These include, but are not limited to, the following:

1. System users are expected to be polite. They may not send abusive, insulting, harassing, or threatening messages to others.

2. System users are expected to use appropriate language; language that uses vulgarities or obscenities, libels others, or uses other inappropriate references is prohibited.

3. System users may not reveal their personal addresses, their telephone numbers or the addresses or telephone numbers of students, employees, or other individuals during E-mail transmissions.

4. System users may not use the District's electronic network in such a manner that would damage, disrupt, or prohibit the use of the network by other users.

5. System users should assume that all communications and information is public when transmitted via the network and may be viewed by other users. The system administrators may access and read E-mail on a random basis.

6. Use of the District's electronic network for unlawful purposes will not be tolerated and is prohibited.

Services

While the District is providing access to electronic resources, it makes no warranties, whether expressed or implied, for these services. The District may not be held responsible for any damages including loss of data as a result of delays, non-delivery or service interruptions caused by the information system or the user's errors or omissions. The use or distribution of any information that is obtained through the information system is at the user's own risk. The District specifically denies any responsibility for the accuracy of information obtained through Internet services.

Security

The Board recognizes that security on the District's electronic network is an extremely high priority. Security poses challenges for collective and individual users. Any intrusion into secure areas by those not permitted such privileges creates a risk for all users of the information system.

The account codes/passwords provided to each user are intended for the exclusive use of that person. Any problems, which arise from the user sharing his/her account code/password, are the responsibility of the account holder. Any misuse may result in the suspension or revocation of account privileges. The use of an account by someone other than the registered holder will be grounds for loss of access privileges to the information system.

Users are required to report immediately any abnormality in the system as soon as they observe it. Abnormalities should be reported to the classroom teacher or system administrator.

The District shall use filtering, blocking or other technology to protect students and staff from accessing internet sites that contain visual depictions that are obscene, child pornography or harmful to minors. The District shall comply with the applicable provisions of the Children's Internet Protection Act (CIPA), and the Neighborhood Internet Protection Act (NCIPA).

Vandalism of the Electronic Network or Technology System

Vandalism is defined as any malicious attempt to alter, harm, or destroy equipment or data of another user, the District information service, or the other networks that are connected to the Internet. This includes, but is not limited to the uploading or the creation of computer viruses, the alteration of data, or the theft of restricted information. Any vandalism of the District electronic network or technology system will result in the immediate loss of computer service, disciplinary action and, if appropriate, referral to law enforcement officials.

Consequences

The consequences for violating the District's Acceptable Use Policy include, but are not limited to, one or more of the following:

1. Suspension of District Network privileges;
2. Revocation of Network privileges;
3. Suspension of Internet access;
4. Revocation of Internet access;
5. Suspension of computer access;
6. Revocation of computer access;
7. School suspension;
8. Expulsion; or
9. Employee disciplinary action up to and including dismissal.