Sublette County School District #9 Policy IHAJ

Adopted July 2011 Page 1

NETWORK/INTERNET USAGE POLICY

The Technology Mission of Sublette County School District #9 is to provide all staff and students with the opportunities and resources to become technologically skilled lifelong learners able to compete successfully in an increasingly complex world and to achieve their personal, educational, and workplace goals. As such, this policy becomes a means whereby the board's intent gives form and direction to district personnel to acquire and use technology in the most efficient and effective ways possible.

The Board, therefore, dedicates this "Network" and grants access to its users as a privilege to be used under the specific guidelines and limitations contained herein.

I: BOARD'S DESIRED OUTCOMES

1. Educational Technology including but not limited to Internet access, network storage, hardware, and software known from here on out as the "Network", will be appropriately integrated into instruction and management and used by all students and staff as an essential element of school improvement and student success. Improving student performance and achievement, increasing staff productivity, and assuring greater efficiency in the operations and communications of the school system are the essential reasons for the technological commitment on behalf of the Board of Education.

2. The Board expects staff and students to utilize the Internet to:

- tap into "depositories of research" i.e., ERIC, Library of Congress
- retrieve resource information for in-depth research
- complement the present "traditional" media center resources

3. The curriculum will be revised appropriately in order to integrate technology as a tool of instruction and a means for processing information in order to stimulate and augment a more powerful and productive learning environment.

II: GENERAL USAGE GUIDELINES FOR NETWORK/INTERNET

1. Access to the Internet allows students to reach out to many other people, to share information, learn concepts and research subjects. With this educational opportunity comes responsibility. The District views access to the Network/Internet as a privilege and not a right. As such, inherent with this privilege are responsibilities with which the District expects full and complete compliance. Breach of these responsibilities may result in loss of complete access privileges. The District has the right to review any material stored on the District network and to edit or remove such material as well as to monitor all network activity.

2. Inasmuch as there is material available on the Internet that could potentially be harmful and/or offensive, parental consent must be provided prior to any student's access to the Internet. It is the user

that specifically agrees not to submit, publish or display any defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive or illegal material. Ultimately, parents and guardians of minors are responsible for setting and conveying the standards their children should follow. As such, it becomes each family's right to decide whether to allow their student(s) access.

III: DISTRICT TERMS AND CONDITIONS OF ETHICAL USE

NETWORK/INTERNET

1. Use of the Network to access and/or send offensive or objectionable material or messages is strictly prohibited.

2. Use of the Network for any illegal or nefarious activity is strictly prohibited.

3. Attempting to infiltrate/access the Network in any manner and/or damaging the hardware or software components is strictly prohibited.

4. Plagiarism, regardless of whether it is print or non-print media, will not be tolerated or accepted.

5. As an education network, the Board believes that individuals must take responsibility for their actions and words. Therefore, any losses, costs, or damages, including reasonable attorney's fees incurred by the District arising out of any breach of the student/parent agreement and/or this policy becomes the responsibility of the parents or guardians.

SECURITY

1. Students/staff may not share their account or password with anyone or leave the account open or unattended.

2. Students/staff will be responsible for taking precautions to prevent viruses on the Network.

3. The illegal installation/usage of copyrighted software or files or shareware on district computers is prohibited.

4. Any software installation on district computers must have prior approval of the building administrator and the Technology Department.

5. Total loss of privileges may immediately be enacted upon anyone who attempts to improperly access, misappropriate or misuse files, data or information of either the District or others.

E-MAIL

1. E-mail messages are subject to District review at any time.

2. Staff members are allowed discretionary use of E-mail. Student use of E-mail is subject to teacher review and discretion, i.e., it is not considered to be confidential.

3. E-mail cannot be used for commercial, political or religious purposes.

4. E-mail is to be deleted regularly from directory to conserve file space.

IV SUPERVISION AND MONITORING

It shall be the responsibility of all District employees to supervise and monitor usage of the online computer network and access to the Internet in accordance with this policy and the Children's Internet Protection Act. Procedures for the disabling, filtering or otherwise modifying of any technology protection measures shall be the responsibility of the Technology Director or designated representatives. To make a request:

1. Follow the process prompted by the District's filtering software (or to remain anonymous, log in under log in name: 123anonymous and password: 123anonymous) and submit an electronic request for access to a web site; or

2. Submit a request, whether anonymous or otherwise, to the District's Superintendent/the Superintendent's designee.

3. Requests for access shall be granted or denied within three (3) school days. If a request was submitted anonymously, persons should attempt to access the web site requested after three (3) school days.

4. Appeal of the decision to grant or deny access to a web site may be made in writing to the Board of Education. Persons who wish to remain anonymous may mail an anonymous request for review to the Board of Education at the School District's Central Office, stating the web site that they would like to access and providing any additional detail the person wishes to disclose.

5. In case of an appeal, the Board of Education will review the contested material and make a determination.

6. Material subject to the complaint will not be unblocked pending this review process.

In the event that a District student or employee feels that a web site or web content that is available to District students through District Internet access is obscene, child pornography, or "harmful to minors" as defined by CIPA or material which is otherwise inappropriate for District students, the process described above should be followed, except any decision to filter or block web content will be made within thirty (30) days.

V: SUMMARY OF TERMS AND CONDITIONS FOR ACCEPTABLE USE

1. Acceptable Use requires compliance with the above stated Ethical Guidelines.

2. Unacceptable Use: Examples are:

- Using the network for any illegal/offensive activity as deemed inappropriate by the principal or teacher.
- Degrading or disrupting equipment or system performance.
- Gaining unauthorized access to district resources or another's files, i.e., trespassing in another's

folder, work or files.

- Posting anonymous messages to harass, intimidate or insult.
- Posting personal communications without the author's consent.
- Allowing others to access your account or divulging your password.
- Utilizing the network for the propagation of political, religious, or commercial gain.
- Use of obscene, vulgar, threatening, harassing, abusive, defamatory language or sending, receiving/displaying inappropriate graphic communications is expressly forbidden.
    - Disclose, use or disseminate personal identification information regarding students

NOTE: The principal will be the sole arbiter of what constitutes such impermissible or improper communication.

3. Privilege vs. Right: The use of Internet is a privilege, not a right, and inappropriate use will result in immediate consequences. The system administrator, superintendent, and/or principal will deem what is inappropriate use and make a final decision as to the appropriate consequences.

4. District Caveat: Beyond the reasonable clarification of "acceptable/unacceptable use" standards, the District is not responsible for restricting, monitoring, or controlling the communications of individuals utilizing the network. Therefore, we believe that parents and guardians of minors are responsible for their students to adhere to district rules/regulations governing the use of the network and Internet. To that end, the District supports and respects each family's right to decide whether or not to permit their student's access to the Internet.

5. District's Right to Monitor: Within reason, freedom of speech and access to information will be honored. However, use of the network and network storage areas may be treated similar to school lockers. Network administrator, staff or principal may monitor/access files and communications to maintain system integrity and insure that users are using the system responsibly. Users should, therefore, NOT expect that files stored on district servers will be private and confidential.

6. Copyright Requirements: Under no circumstances shall it be necessary for either staff or students to violate copyright restrictions in order to perform their duties/responsibilities properly. The Board of Education does not sanction or condone illegal duplication in any form and any employee or student

violating the district's copyright position does so at his/her own risk and assumes all liability/responsibilities.

7. Internet Use Agreement: At the beginning of each school year, every student user of the Network/Internet shall sign and return an Internet Terms & Conditions of Use Agreement. Said Agreement shall cover the following areas:

- Network/Internet acceptable use
- Security on the Network
- Network etiquette (netiquette)
- Notice of release from District liability

8. Prior to Student Access to Network/Internet: An INTERNET TERMS & CONDITIONS AGREEMENT FORM must be signed by the student and parent/guardian before any student is allowed access to the Network/Internet. In addition, the District is required to provide instruction to the student on acceptable and ethical use of the Network/Internet and proper network etiquette (Netiquette).

ADMINISTRATIVE PROCEDURE

OVERVIEW OF PURPOSE/INTENTION

The policy outlined by the Board, in reality, is a directive to administration and staff whereby it becomes a means to provide all staff and students with the opportunities and resources to become technologically skilled lifelong learners able to compete successfully in an increasingly complex world and to achieve their personal, educational, and workplace goals.

Plainly stated: There is no question that the Board, in giving financial and philosophical commitment to technology, fully expects the Network/Internet to be utilized within the curriculum. Although basic skill education still remains a paramount concern, the Board wants to see a variety of instructional methods utilizing technology when appropriate. Staff must be prepared to answer the following: What are we doing that's different, i.e., more effective and more efficient, using technology? How is technology being utilized within the curriculum? Network/Internet access provides tremendous opportunities for educational benefit. However, the District has no reasonable means for controlling the content of all communication or information disseminated on the Internet. Moreover, the District lacks the ability to monitor the dissemination of communication by every student at all times. Because pornography, defamatory or inaccurate information or information that is offensive may be accessed through the Internet and because unlawful or inappropriate student communication may serve as a basis for criminal and/or civil liability, it must be fully communicated to parents/guardians that they provide consent for student access to the Internet.

However, every reasonable and prudent effort must be made by the principal and staff to assure that the aforementioned nefarious activity be minimal. Therefore, a primary administrative objective will be to support teachers - who in turn must support students - in the responsible use of this vast reservoir of information. Two areas requiring staff attention for "responsible use" are:

- What constitutes “appropriateness?” Criteria for the selection of information, resources or instructional materials on the Internet shall be established under the authority of the Superintendent. The responsibility for selection of such materials may be delegated to the certified staff. The use of any material which may be inappropriate or controversial in some manner will be decided first by the certified staff and the building principal with the right for appeal to the Superintendent and, ultimately, to the Board of Education.
- Freedom of Speech on the Internet: Students are entitled to express themselves and to state their personal opinions as long as their expressions do not materially and substantially interfere with and disrupt the operation of the school, the freedom of others to express themselves, are not personally vindictive, and do not constitute slander. Additionally, the use of obscenities or personal attacks is prohibited. As an administrator or teacher, we must stress that the educational value of the information and the interaction available on this worldwide network outweighs the risks that users may access and/or procure material that is not consistent with the educational goals of the school district.

The following constitute annual procedures to assure appropriate use:

PROCEDURE

1. Mandated “acceptable use” sessions with staff: These have been found to be most successful. With the deluge of printed material, educators often don’t read policies or procedures as carefully as they should. The required sessions allow for verbal reinforcement of the seriousness of the commitment that teachers take on when they implement the Internet. Even small issues, such as the placement of the computer in the classroom, need to be discussed. Teachers often place computers in corners with monitors facing away from their line of sight in order that the computers “don’t disturb other students.” Another issue that should be discussed is the access to potentially objectionable material and how to limit access to said material. These and similar issues can never be covered in a simple written policy. Therefore, it is important that a face-to-face encounter with teachers occur. Specific items to discuss are:
    - Internet Safety Training – In compliance with the Children’s Internet Protection Act, each year all District students will receive internet safety training which will educate students about appropriate online behavior, including interacting with other individuals on social networking sites and in chat rooms, and cyber bullying awareness and response.
    - A comprehensive review of the policy
    - Responsibility to maintain accurate records of parental approval for access.
    - The importance of parental signature of agreement to the Internet Terms and Conditions of Use. Prior to affording individual student access, form must be signed by the student and parent. Building administrators will determine how to distribute, collect and where to store original signed copies of said agreement.
    - The importance of stressing the confidentiality of passwords and the disallowance of allowing others to use your account.
    - The importance that staff go over, in complete detail with students, what constitutes acceptable and unacceptable behavior with respect to using the Network/Internet, as well as the consequences of unacceptable use. Have staff emphasize to students that this is a privilege for which they must apply. It is NOT a right.

- Also stress the fact that the District has the right, and more importantly the responsibility, to monitor student usage/storage of material.

2. Staff Awareness of the following:

A. Have staff review Network etiquette with their students.

B. Have staff review General Usage Guidelines outlined in Policy.

C. Have staff review "penalties" associated with abuse. Specifically, action may include, but not necessarily be limited to:

- Suspension or revocation of computing privileges
- Reimbursement
- Legal action - including action to recover damages
- Referral to administrator for further disciplinary action.

D. Have staff review both ethical use (in Policy) and common unethical practices such as

- Unauthorized and time consuming recreational game playing.
- Sending chain letters or unauthorized mass mailings
- Using the computer for personal gain or illegal purposes, i.e. advertisements, political mailings, religious use, etc .

E. Finally, have staff go over "Terms and Conditions of Usage" so that students thoroughly understand the terms and conditions as well as their responsibility to ensure that they follow said terms.

UNDER NO CIRCUMSTANCES

a. Similar to a "safety test" given in a shop class, no student is to be allowed access to the Network/Internet without the District providing instruction on the appropriate and ethical use of the Network/Internet and Internet etiquette.

b. Is the student to be allowed access without the District having in their possession (1) a signed application and (2) an Internet use agreement form.

Dear Parent/Guardian:

Your child is being offered Internet electronic access on the Sublette School District #9 network. To have access, your child requires your permission to do so. With access, he/she will be able to communicate with other schools, colleges, organizations and students around the world. He/She will also have the opportunity to reach out to people around the globe to share information, learn concepts, and research virtually any topic. With this educational opportunity offered by Sublette District #9 also comes responsibility. It is imperative that your child read the enclosed Internet Terms and Conditions of Use Agreement and you discuss it together. At the time your child is given a logon name and password to

use on the computer, it is extremely important that the rules be followed. Failure to follow the rules may result in disciplinary action which may include the loss of the privilege to use this educational tool.

Please remember that you are legally responsible for your child's actions. Therefore, it is absolutely critical that, under no circumstances, your child allow anyone to know their password. Although we have established acceptable use procedures which the teacher will review with your child, please be aware that there exists on the Internet, material that this district deems unacceptable and/or objectionable which your child could access. It is not possible for us to always provide direct supervision of all students, and we cannot control material available on other networks all over the world. We encourage you to consider the potential of your child being exposed to inappropriate material in your decision of whether or not to sign the informed consent form. If you choose to do so, please be aware that the parent/guardian must accept responsibility for providing guidance on Internet use and conveying standards to your child to follow when accessing and/or exploring Internet sites. You should also be aware of the following "Conditions of Use" within district policy:

• Any costs/expenses Incurred by the District, including reasonable attorneys' fees, due toimproper downloading , purchasing, or transmission of material/Information in violation of any local/state/federal laws becomes the express liability of the parent/guardian.

• Costs incurred by the District for vandalism, i.e., any malicious attempt to harm or destroy another's data, the District Network, or other agency's networks become the express liability of the parent or guardian. This includes, but is not limited to, the deliberate uploading, downloading or creation of computer viruses.

• Use or misuse of information obtained via the Sublette District #9 network is "at your own risk." After you have read and discussed this with your child and you have both agreed to the conditions and responsibilities inherent with the privilege of accessing the District's Network and Internet, please return with the appropriate signatures to the school.

INTERNET TERMS AND CONDITIONS OF USE AGREEMENT

The "Terms and Conditions of Use" agreement is provided so that you are aware of the responsibilities you are about to acquire in accessing the Internet. Because Internet access is coordinated through a complex association of government agencies and state networks, the smooth operation of the network relies upon the proper conduct of end users who must adhere to strict guidelines. In general, usage requires efficient, ethical and legal use of the Network/Internet resources. Therefore, if any user of the Sublette School District #9 network violates any of these provisions, his or her access may be denied.

Your signature(s) on the reverse side of this page are legally binding and indicate the party (parties) who signed has/have read the terms and conditions carefully; fully understand their significance; and are willing to abide by the INTERNET TERMS AND CONDITIONS OF USE as summarized below and outlined completely in District Policy IHAJ.

A SUMMARY OF ACCEPTABLE AND UNACCEPTABLE USAGE GUIDELINES:

NETWORK/INTERNET

1. Use of the Network to access and/or send offensive or objectionable material or messages is strictly prohibited. The district filters all internet access and restricts access to material harmful to minors.

2. Use of the Network for illegal/nefarious activity is strictly prohibited.

3. Attempting to infiltrate/access or "hack" the District's computing system or other entities systems and/or damage the software components is strictly prohibited.

4. As an education network, the Board believes that individuals must take responsibility for their actions and words. Exemplary behavior is expected on "virtual" field trips. When "visiting" sites on the Internet, users must conduct themselves as representatives of both their respective schools and the community as a whole. Conduct that is in conflict with the responsibilities outlined herein may result in the loss of network privileges.

NOTE: The District reserves the right to monitor internet, email and other direct electronic communications as well as files stored on District computer/servers. Therefore, users should NOT expect these to be either private or confidential.

SECURITY

1. Students/staff may not share their account or password with anyone or leave the account open or unattended.

2. Students/staff will be responsible for taking precautions to prevent viruses on the Network.

3. The illegal installation/usage of copyrighted software or files or shareware on district computers is prohibited.

4. Any software installation on district computers must have prior approval of the building administrator and the Technology Department.

5. Total loss of privileges may immediately be enacted upon anyone who attempts to improperly access, misappropriate or misuse files, data or information of either the District or others.

6. The student is responsible for making back-up copies of documents critical to them.

7. The district and its employees will not disclose, use or disseminate personal information regarding minors.

NETWORK ETIQUETTE (NETIQUETTE)

1. Always be polite and avoid sending any abusive, obscene or harassing language (flaming).

2. Do not reveal your personal address or phone numbers of students or colleagues.

3. Effort must be made to delete unnecessary files from the directory to conserve fileserver hard disk space.

4. Do not use the network in such a way that you would disrupt the use of the network by other users, i.e., downloading large files during prime time; sending mass messages; annoying other users using write functions.

NOTICE OF PROVISION TO RELEASE DISTRICT FROM LIABILITY

• Any costs/expenses incurred by the District, including reasonable attorneys' fees, due to improper downloading, purchasing, or transmission of material/information in violation of any local/state/federal laws becomes the express liability of the parent/guardian.

• Costs incurred by the District for vandalism, i.e., any malicious attempt to harm or destroy another's data; the District Network; or other agencies networks become the express liability of the parent or guardian. This includes, but is not limited to, the uploading/downloading or creation of computer viruses.

• Use/misuse of information obtained via the District Network is "at your own risk."

REMEMBER: INTERNET ACCESS IS A PRIVILEGE, NOT A RIGHT, AND ACCESS REQUIRES RESPONSIBILITY.

STUDENT AGREEMENT

I have read, understood and agree to abide by the INTERNET TERMS AND CONDITIONS OF USE AGREEMENT - as outlined herein. I further understand that any violation of the terms and conditions of this agreement is unacceptable, unethical and very possibly, illegal. I further agree to and understand that, should I commit any violation of the terms and conditions of agreement, my access privileges may be revoked; disciplinary action may be taken; and/or appropriate legal action may be filed.

STUDENT SIGNATURE _____DATE_____

PARENT/GUARDIAN AGREEMENT

As parent or guardian of _____, I have read the INTERNET

TERMS AND CONDITIONS OF USE AGREEMENT as outlined on the reverse side of this page. I understand that access to the Network and to the Internet is designed strictly for educational purposes. However, I also recognize that it is impossible for Sublette School District #9 to restrict access to all controversial materials on the Internet and I will not hold the school district responsible for controversial or offensive materials acquired or use and misuse of information acquired on the Internet. I understand and accept that, as a parent/guardian, I am legally responsible for any liability that happens as a result of my child's use/misuse of the Internet. I hereby give Sublette School District #9 permission to allow my child access to the Internet.

Parent consents to allow school to use Internet (Web site) operators to offer online programs for the benefit of students and the school system, such as for communication regarding homework, facilitating online testing and/or communication regarding grades.

The school requires that the service provider assure the school that it has in place a procedure or security system to maintain the confidentiality of any personal information that the service provider could have access to.

Because these services or programs will necessitate giving access to student personal information to the Internet or Web site operators that host or facilitate these programs, the school must represent that it has parental permission for this and your execution of this policy/handbook shall be considered permission.

PARENT/GUARDIAN SIGNATURE _____ DATE _____

Distribution:

Original copy to be filed in Principal's Office.

Principal's Office to notify all teachers and the Technology Department of those students that have not submitted a signed copy of this Internet Terms and Conditions of Use Agreement.

Sublette County School District 9

District Technology Access

Staff Acceptable Use Policy (AUP)

Sublette County School District 9 (SCSD9) provides staff and students with access to technology equipment, software, and network resources. Use of these tools shall be encouraged where such use supports learning, collaboration, educational research, and administrative and state mandated functions. The primary use of said network resources, including the internet, shall be for school district related work.

SCSD9 employees must ensure that they:

• comply with current local, state and federal laws and regulations

• do not create unnecessary risk to the school district by their misuse of technology and/or network resources

• use computer and network resources in an acceptable way

Access

Staff who have completed the following will be issued an account with network access, internet and email:

Attended AUP training

Reviewed Staff AUP

Submitted a signed AUP agreement form

Staff will be expected to do each of these things on a yearly basis in order to maintain access to their account.

Supervisory Responsibilities

The use of district filtering services does not disqualify the requirement for staff to supervise student use of technology. Some inappropriate material may pass through the filter. The following are some guidelines concerning the use of district technology and network resources.

• Staff must be sure that students using technology resources are supervised at all times

• Staff may only allow qualified student users to have access. A qualified student is one that has signed the student AUP and has not had network privileges revoked

• Staff may NOT login for students who do not have an account

• Staff must take all reasonable precautions to prevent unauthorized student use

• Staff must notify the Technology Department or appropriate administrator if a student violates the AUP

User Responsibilities

Staff are expected to be good citizens of the network including, but not limited, to the following:

• Log on to only your own account

• Log off the network or lock the screen when leaving your computer

• Log off the network at the end of the day (this allows for proper backing up of network files)

• Notify Technology Department if you encounter inappropriate materials or sites

• Report any security problems immediately

• Keep all passwords private and secure

• Take all reasonable precautions to protect access to your account

• Be aware of potential viruses

• Practice printing conservation

• Protect the privacy of staff and students. Do not disclose, use or disseminate personal information regarding minors.

• Observe copyright guidelines (i.e. no illegal downloading of audio, video or other files)

• Avoid unnecessary system traffic (i.e. no streaming audio or video unless part of your curriculum)

• Only use high bandwidth education applications approved by the building administrator

Unacceptable Use of Technology

The following are examples of unacceptable use of technology and/or network resources:

• Purposely accessing or viewing obscene, pornographic, hateful, profane, illegal or objectionable materials or sites

• Distributing, disseminating or storing images, text or materials that might be considered indecent, pornographic, obscene or illegal

• Distributing, disseminating or storing images, text or materials that might be considered discriminatory, offensive or abusive, in that the context is a personal attack, sexist or racist, or might be considered harassment

• Accessing sites that promote any illegal activity

• Accessing copyrighted information in a way that violates the copyright (i.e. downloading videos or music)

• Installing software without authorization from building administrator and Technology Department

• Downloading and/or installing software or any copyrighted materials belonging to third parties, unless this download is covered or permitted under a commercial agreement or other such license

• Purposely introducing any form of computer virus, malicious software or malware into the school district's network or its computers

• Engaging in practices that threaten the network (i.e. opening non-requested or suspicious attachments)

• Changing network and/or security settings on school computers

• Assembling, disassembling, connecting, or disconnecting technology or network equipment without prior consent of the Technology Department

• Moving technology equipment or software to another location without prior consent of the

Technology Department

• Accessing, modifying, or deleting folders or files other than your own

• Breaking in to the school district's systems, unauthorized areas or unauthorized use of a password

•Undertaking deliberate activities that waste staff effort or network resources

• Broadcasting unsolicited personal views on social, political, religious or other non-district related matters including unsolicited commercial or advertising material

• Excessive personal use

• Using the network for financial gain (i.e. auctions, eBay, gambling)

• Using the network to perpetrate any form of fraud (including software, video or music piracy)

• Publishing defamatory and/or knowingly false material about SCSD9, your colleagues and/or students on social networking sites, 'blogs' (online journals), 'wikis', or any other online publishing format

District Email Access

Email is the District's most effective method of communication. All staff members are entitled to email accounts so they may communicate with district employees as well as parents and community members. All of the above technology policies apply to the use of email.

User Responsibilities:

• Check email daily and delete unwanted items (i.e. sent, calendar and notes)

• Stay within email space limits on the server

• Honor the rights to privacy of other network users

• Subscribe only to mailing lists that are relevant to professional development

• Unsubscribe to mailing lists before vacations or other extended absences from school

• Messages sent to "Everyone" should be used sparingly for school communications and student welfare related purposes

• Follow standard online etiquette

Unacceptable Uses of Email:

• Sending or sharing confidential or inappropriate information about students or staff

• Sending or sharing communications that express personal opinions on an issue not related to teaching or the school environment

• Sending or sharing offensive messages or pictures

• Using obscene language

• Insulting or harassing others

• Excessive personal use of district email

• Posting chain letters or frivolous messages

Users should not expect that e-mail and files stored on district servers will be private. Network administrators, under the direction of school administration, may open, monitor or review files and communications at any time to maintain system integrity. E-mails and files may be opened, monitored and reviewed at any time to ensure that staff members are using the system responsibly and in

conformance with this policy. Also, remember that all electronic communications in a school are public domain and therefore could be accessed by anyone.

SCSD9 has attempted to provide a safe network environment. Staff members are advised that using the district's system might provide access to information that contains inaccurate or objectionable material.

Accessing information on the internet is ultimately the responsibility of the user. The district does not condone the use of obscene or other objectionable materials. Such materials are prohibited in the school environment.

Responsibility for Data

The Technology Department will take an active role in backing up data on the servers. However, statistics show that backups usually don't restore correctly. Therefore, each staff member is ultimately responsible for backing up their own data in at least two different locations to ensure that their data is not lost (i.e. on computer locally, on server, on an external storage device, etc.). The Technology Department will take an active role in monitoring the disk space on all servers. Users who are taking up a greater than average amount of disk space will be notified and educated in storage management.

Monitoring

SCSD9 accepts the use of computers and network resources as a valuable educational and administrative tool. However, misuse of computers and network resources can have a negative impact upon employee productivity, student learning and the reputation of the school district. Software installed by users on district computers must be related to the district mission and/or the individual's educational work. Software that causes the workstation to become unstable or consume excessive network resources may be removed by technology staff.

The school district maintains the right to examine any systems owned by the District and/or connected to the network and inspect any data recorded in those systems. In order to ensure compliance with this policy, the school district also reserves the right to use monitoring software in order to check upon the use and content of computers and network resources.

Sanctions

Where it is believed that an employee has failed to comply with this policy, the employee's supervisor will be notified and the school district's disciplinary procedure will be followed. If the employee is found to have breached the policy, they will face a disciplinary penalty ranging from a verbal warning to dismissal.

Users must acknowledge their understanding of this policy by submitting a signed staff AUP form. Failure to adhere to this policy and its regulations may result in suspension or cancellation of user privileges and may result in disciplinary action up to dismissal. District Due Process procedures will apply.

STAFF AUP FORM

Users (all school district employees, contractors or temporary staff) must acknowledge their understanding of the Staff Acceptable Use Policy (AUP) by submitting this form yearly. Failure to adhere to this policy and its regulations may result in suspension or cancellation of user privileges and may result in disciplinary action up to dismissal. District Due Process procedures will apply.

I have read and agree to the terms of the Staff Acceptable Use Policy for the 2010-11 school year. A copy of this policy has been provided for my records.

_____

Staff Member Signature Today's Date

Return this form to the

SCSD9 Technology Department

Amended: May 22, 2013