R 6320 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. Similarly, the use of any District computer to access sites which allow the user to conceal their objective of accessing inappropriate material is not permitted.

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.

Internet Access

In compliance with the Children's Internet Protection Act ("CIPA"), 47 U.S.C. § 254, the District uses technological devices designed to filter and block the use of any District computer with Internet access to retrieve or transmit any visual depictions that are obscene, child pornography, or "harmful to minors" as defined by CIPA and material which is otherwise inappropriate for District students.

Due to the dynamic nature of the Internet, sometimes Internet websites and web material that do not fall into these categories are blocked by the filter. In the event that a District student or employee feels that a website or web content has been improperly blocked by the District's filter and this website or web content is appropriate for access by District students, the process described below should be followed:

1. Follow the process prompted by the District's filtering software (or to remain anonymous, log in under log in name: 123anonymous) and submit an electronic request for access to a website, 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 days. If a request was submitted anonymously, persons should either attempt to access the website requested after three days or log back in at 123anonymous to see the status of the request.

4. Appeal of the decision to grant or deny access to a website 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 website 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 website 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 set forth in Regulation 6241 should be followed.

Adult users of a District computer with Internet access may request that the "technology protection measures" be temporarily disabled by the chief building administrator of the building in which the computer is located for lawful purposes not otherwise inconsistent with this Policy.

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.

STUDENT POLICY & PROCEDURES

Acceptable Uses of Technology

Access to the Internet is an unparalleled opportunity to interact with the world. The opportunity brings with it a number of responsibilities. Your access to the electronic network and resources within the Sturgeon R-V School District may be revoked for abusive conduct. Abuses include, but are not limited to the following examples:

- Accessing private files (even if those files are unprotected).
- Accessing or participating in chat rooms without teacher instruction or supervision.
- Attempting to break the security system.
- Illegally copying software.
- Placing unlawful information on or throughout the computer system.
- Using obscene, abusive, or otherwise objectionable language, messages, images, or symbols.
- Accessing pornographic materials.
- Accessing inappropriate text files.
- Attempting to harm or destroy data, files, or another user.
- Uploading or downloading of computer viruses, games, or programs.
- Harming or destroying the wide area network (WAN) or other networks connected to the WAN.
- Using the network to facilitate illegal activity.
- Using the network for commercial or "profit" purposes.
- Using the network for product advertisement.
- Misrepresenting other users on the network.
- Intentionally modifying passwords belonging to other users.
- Accessing and participating in relationships pages, trying to meet or contact people through these pages, or leaving e-mail or other personal information on these pages so that you can be contacted by other participants on these pages.

Inappropriate or illegal use of the network facilities could result in additional disciplinary and legal action. Parents and/or guardians may be held accountable for inappropriate use by their child. Any parental requests for disallowing Internet use by their child at school will need to be in writing and submitted by the parent to the building principal.

ACCEPTABLE USE OF TECHNOLOGY GUIDELINES
STURGEON R-V SCHOOL DISTRICT

Access to the Internet is an unparalleled opportunity to interact with the world. The opportunity brings with it a number of responsibilities. Your access to the electronic network and resources within the Sturgeon R-V Schools MAY BE REVOKED for abusive conduct. Suspensions may also be a result of inappropriate conduct. Remember that our Internet Provider is MoreNet and they DO track any misuse!

ABUSES include, but are not limited to, the following examples:

1. Accessing private files (even if those files are unprotected).

2. Accessing or participating in electronic mail without teacher instruction or supervision.

3. Attempting to break the security system.

4. Illegally copying software.

5. Placing unlawful information on or throughout the computer system.

6. Using obscene, abusive or otherwise objectionable language or messages.

7. Accessing pornographic materials.

8. Accessing inappropriate text files.

9. Attempting to harm or destroy data, files or another user.

10. Uploading or downloading games, programs, or computer viruses.

11. Harming or destroying the Wide Area Network or other networks connected to the Wide Area Network.

12. Harming or destroying computer hardware and other peripherals—as well as __NO__ food and drink around or near the computer hardware or peripherals.

13. Using the network to facilitate illegal activity.

14. Using the network for commercial or "profit" purposes.

15. Using the network for product advertisement.

16. Misrepresenting other users on the network.

17. Intentionally modifying passwords belonging to other users.

18. Accessing and participating in relationship pages, instant messaging, chat rooms (or any other way to distribute PERSONAL information or trying to meet or contact people through these pages, so that you can be contacted by other participants--inside or outside our Local Area Network).

I have read the guidelines above and understand the consequences that may be a result of not following them.

_____ _____
Student's Signature   Parent Signature (K-8 grades)

_____ _____
Teacher Name   Class