Internet Safety Policy – Policy 6320

A. **Introduction**

It is the policy of the District to: (a) prevent user access over its computer network to, or transmission of, inappropriate material via Internet, electronic mail, or other forms of direct electronic communications; (b) prevent unauthorized access and other unlawful online activity; (c) prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; and (d) comply with the Children's Internet Protection Act [Pub. L. No. 106-554 and 47 USC 254(h)].

B. **Access to Inappropriate Material**

To the extent practical, technology protection measures shall be used to block or filter Internet, or other forms of electronic communications, access to inappropriate information. Specifically, as required by the Children's Internet Protection Act, blocking shall be applied to visual depictions of material deemed obscene or child pornography, or to any material deemed harmful to minors. Subject to staff supervision, technology protection measures may be disabled or, in the case of minors, minimized only for bona fide research or other lawful purposes.

C. **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 cyberbullying awareness and response. Such training will include Internet, cell phones, text messages, chat rooms, email and instant messaging programs. (See also Policy 6116 – State Mandated Curriculum – Human Sexuality).

D. **Inappropriate Network Usage**

To the extent practical, steps shall be taken to promote the safety and security of users of the District's online computer network when using electronic mail, chat rooms, instant messaging, and other forms of direct electronic communications. Specifically, as required by the Children's Internet Protection Act, prevention of inappropriate network usage includes: (a) unauthorized access, including so-called 'hacking,' and other unlawful activities; and (b) unauthorized disclosure, use, and dissemination of personal identification information regarding minors.

E. **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 or otherwise modifying any technology protection measures shall be the responsibility of Technology Director or designated representative.

Technology and Internet Usage – Regulation 6320

The Sedalia 200 School District's technology exists for the purpose of enhancing the educational opportunities and achievement of district students. Research shows that students who have access to technology improve achievement. In addition, technology assists with the professional enrichment of the staff and increases engagement of students' families and other patrons of the district, all of which positively impact student achievement. The district will periodically conduct a technology census to ensure that instructional resources and equipment that support and extend the curriculum are readily available to teachers and students. 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.

The purpose of this policy is to facilitate access to district technology and to create a safe environment in which to use that technology. Because technology changes rapidly and employees and students need immediate guidance, the superintendent or designee is directed to create procedures to implement this policy and to regularly review those procedures to ensure they are current.

Sedalia School District #200
Acceptable Use Policy (AUP)
For the use of Computers, Mobile Devices, Cell Phones, Internet Access, and Internet Applications

Definitions

User includes anyone, including employees, students, and guests, using Sedalia School District technology, including, but not limited to, computers, networks, Internet, email, chat rooms and other forms of technology services and products.

Network is wired and wireless technology networks including school and district networks, cellular networks, commercial, community or home-based wireless networks accessible to students.

Equipment are cellular phones, 'Blackberry' [smartphone] type devices, PDAs, MP3 players, iPod type devices, and portable computers such as laptops, iPads, desktops, tablets and netbooks, as well as portable storage devices.

Acceptable Use

Technology provides students with unique and powerful ways to enhance their learning. The Sedalia 200 School District supports the use of technology for the purpose of enhancing and supporting learning and is pleased to offer Users access to computer networks so that they can access district-supplied technology to enhance learning any time of day.

It is one of the technology goals of the district to ensure that each User's interactions with technology contribute positively to the learning environment both at school and in the community. Negative use of technology through the Sedalia School District-owned devices inside or outside of our schools that degrades or defames other Users, or members of our community is unacceptable. The Sedalia School District also recognizes that Users have widespread access to both technology and the Internet; therefore, use of personal devices and connectivity is considered to be included in this Acceptable Use Policy (AUP)

Access to Sedalia School's network is a privilege, not a right. The use of technology whether owned by the Sedalia School District or devices supplied by the Users entails personal responsibility. It is expected that Users will comply with Sedalia School District rules, act in a responsible manner, and will honor the terms and conditions set by the classroom teacher, the school, and District. Failure to comply with such terms and conditions may result in temporary or permanent loss of

access as well as other disciplinary or legal action as necessary. In particular, students will be held accountable for their actions and are encouraged to report any accidental use immediately to their teacher or school administration.

With the increased usage of free educational applications on the Internet, digital storage areas, containing less sensitive User information, may or may not be located on property of the school, district, or county. In some cases, data will not be stored on local servers. Therefore, Users should not expect that files and communication are private. The Sedalia School District reserves the right to monitor Users' online activities and to access, review, copy, and store or delete any electronic communication or files and disclose them to others as it deems necessary. **Users should have no expectation of privacy regarding their use of school district property, network and/or Internet access or files, including email.**

The Sedalia School District has a private and secure system for sensitive school records, which will be managed by school district Technology Staff.

Terms and Conditions
These are examples of inappropriate activity on the Sedalia school district network, but the district reserves the right to take immediate action regarding activities 1) that create security and/or safety issues for the district's network, Users, schools, network or computer resources; 2) that expend district resources on content it determines lacks legitimate educational content/purpose; or 3) other activities as determined by the school district as inappropriate.

Violating any state or federal law or municipal ordinance, such as: Accessing or transmitting pornography of any kind, obscene depictions, harmful materials, materials that encourage others to violate the law, confidential information or copyrighted materials.

Criminal activities that can be punished under law.

Selling or purchasing illegal items or substances.

Obtaining and/or using anonymous email sites, spamming, spreading viruses.

Causing harm to others or damage to their property.

Using profane, abusive, or impolite language; threatening, harassing, or making damaging or false statements about others or accessing, transmitting, or downloading offensive, harassing, or disparaging materials. Deleting, copying, modifying, or forging other Users' names, emails, files or data, disguising one's identity, impersonating other users, or sending anonymous email.

Damaging computer equipment, files, data or the network in any way, including intentionally accessing, transmitting or downloading computer viruses or other harmful files or programs, or disrupting any computer system performance.

Using any district computer/mobile devices to pursue "hacking," internal or external to the Sedalia School District, or attempting to access information protected by privacy laws.

Accessing, transmitting or downloading large files, including "chain letters" or any type of "pyramid schemes."

Using web sites, email, networks, or other technology for political uses or personal gain.

The Sedalia School District's internet and intranet property must not be used for personal benefit.

Users must not intentionally access, create, store or transmit material that may be deemed to be offensive, indecent, obscene, intimidating, or hostile; or that harasses, insults or attacks others.

Advertising, promoting non-school district sites or commercial efforts and events

Users must adhere to all copyright laws.

Users are not permitted to use the network for non-academic related bandwidth intensive activities such as network games or transmission of large audio/video files or serving as a host
for such activities.

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. This includes the use of proxy sites used to bypass the school district's filter**

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.

Cybersafety and Cyberbullying
All Users - Despite every effort for supervision and filtering, all Users and Students' parents/guardians are advised that access to the network may include the potential for access to content inappropriate for school-aged students. Every User must take responsibility for his or her use of the network and make every effort to avoid those types of content. Every User must report security or network problems to a teacher, administrator, or system administrator.

Personal Safety – In using the network and Internet, Users should not reveal personal information such as home address or telephone number.

Confidentiality of User Information – Personally identifiable information concerning students may not be disclosed or used in any way on the Internet without the permission of a parent or guardian. Users should never give out private or confidential information about themselves or others on the Internet.

Active Restriction Measures – Sedalia School District will utilize filtering software or other technologies to prevent Users from accessing visual depictions that are (1) obscene, (2) pornographic, or (3) harmful to minors. Attempts to circumvent or 'get around' the content filter are strictly prohibited, and will be considered a violation of this policy. The Sedalia School District will also monitor the online activities of Users through direct observation and/or other technological means.

Interactive Web 2.0 Tools
Technology provides an abundance of opportunities for Users to utilize interactive tools and sites on public websites that benefit learning, communication, and social interaction.

Users may be held accountable for the use of and information posted on these sites if it detrimentally affects the welfare of individual users or the governance, climate, or effectiveness of the school(s). From time to time, teachers may recommend and use public interactive sites that, to the best of their knowledge are legitimate and safe. As the site is "public" and the teacher, school, and district is not in control of it, all Users must use their discretion when accessing information, storing, and displaying work on the site. All terms and conditions provisions in this AUP also apply to User-owned devices utilizing the Sedalia schools network.

Student Use of Interactive Web 2.0 Tools
Online communication is critical to the students' learning of 21st Century skills, and tools such as blogging, podcasting, and chatting offer an authentic, real-world vehicle for student expression. Student safety is the primary responsibility of teachers.

Therefore, teachers need to ensure the use of classroom blogs, student e-mail, podcast projects, email chat features, or other Web interactive tools follow all established Internet safety guidelines including:

The use of blogs, podcasts or other web 2.0 tools is considered an extension of the classroom. Therefore, any speech that is considered inappropriate in the classroom is also inappropriate in all uses of blogs, podcasts, or other web 2.0 tools. This includes—but is not limited to—profanity, racist, sexist, or discriminatory remarks.

Students using blogs, podcasts or other web tools are expected to act safely by keeping ALL personal information out of their posts.

Students should NEVER post personal information on the web (including, but not limited to, last names, personal details such as address or phone numbers, or photographs).
Students should NEVER, under any circumstances, agree to meet someone they have met over the Internet.
Any personal blog a student creates in class is directly linked to the class blog which is typically linked to the student profile and therefore must follow these blogging guidelines. In addition to following the information above about not sharing too much personal information (in the profile or in any posts/comments made), students need to realize that anywhere they use the blog login it links back to the class blog. Therefore, anywhere that login is used (posting to

a separate personal blog, commenting on someone else's blog, etc.), the account should be treated the same as a school blog and should follow these guidelines.

Students should never link to web sites from their blog or blog comments without reading the entire article to make sure it is appropriate for a school setting.

Students using such tools agree to not share their user name or password with anyone besides their teachers and parents and treat Web posting spaces as classroom spaces. Speech that is inappropriate for class is also inappropriate for a blog.

Students who do not abide by these terms and conditions may lose their opportunity to take part in the project and/or be subject to consequences appropriate to misuse.

Student Use of Mobile Devices
When the Sedalia School District provides students with mobile devices such as iPads for use both in school as well as away from school. The District-owned devices follow the stipulations outlined in this AUP.

School Administration and District Technology staff may search the student's memory device if they feel school rules have been violated, which may include, but are not limited to, audio and video recording, photographs taken on school property that violate the privacy of others, or other issues regarding bullying, etc.

Students may not use an audio recording device, video camera, or camera (or any device with one of these, e.g. cell phone, laptop, tablet, etc.) to record media or take photos during school unless they have permission from both a staff member and those whom they are recording.

These rules apply to student-owned devices as well. A student-owned mobile device is a non-district supplied device used while at school or during school or district-sponsored activities. The students may use the student-owned mobile devices in class only with the teacher's expressed permission.

Student Supervision and Security
The Sedalia School District does provide content filtering controls for student access to the Internet using the district's network as well as reasonable adult supervision, but at times inappropriate, objectionable, and/or offensive material may circumvent the filter as well as the supervision and be viewed by students. Students are to report the occurrence to their teacher or the nearest supervisor. Students will be held accountable for any deliberate attempt to circumvent Sedalia School District's technology security and supervision.

Students using mobile and cellular devices while at school, during school or district-sponsored activities are subject to the terms and conditions outlined in this document and are accountable for their use.

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 termination of user privilege.

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 termination