INTERNET AND OTHER COMPUTER NETWORKS ACCEPTABLE USE AND INTERNET SAFETY POLICY

The Bixby School District is pleased to make available to students and employees access to interconnected computer systems within the district and to the Internet, the worldwide network that provides various means of accessing significant educational materials and opportunities.

In order for the school district to be able to continue to make its computer network and Internet access available, all students and employees must take responsibility for appropriate and lawful use of this access. Staff and students must understand that anyone’s misuse of the District network and Internet access may jeopardize the ability of all to enjoy such access. While the school’s teachers, administrators, directors, and other staff will make reasonable efforts to supervise individual student and employee use of network and internet access, they must have students’ and all employees’ cooperation in exercising and promoting responsible use of this access, the district technology systems, and computer equipment and networks.

Below is the Acceptable Use and Internet Safety Policy (“policy”) of the school district and the Data Acquisition Site that provides Internet access to the school district. Upon reviewing, signing, and returning this policy as the students have been directed, each student will be given the opportunity to enjoy Internet access at school and is agreeing to follow the policy. If a student is under 18 years of age, he or she must have his or her parents or guardians read and sign the policy. The school district cannot provide access to any student who, if 18 or older, fails to sign and submit the policy to the school as directed, or, if under 18, does not return the policy as directed with the signatures of the student and his/her parents or guardians.

Employees of Bixby Public Schools will, upon employment, complete and sign and internet and computer equipment and network agreement. Such agreement will be on file with the director of technology for the employee’s term of employment with the school district.

Listed below are the provisions of the agreement regarding the district technology systems, computer equipment, and computer network and internet use. If you have any questions about these provisions, you should contact the person that your school has designated as the one to whom you can direct your questions. If any user violates this policy, the student’s or employee’s access will be denied, if not already provided, or withdrawn and he or she may be subject to additional disciplinary action.

Personal Responsibility

By signing the Internet Acceptable Use and Safety Agreement, you are agreeing not only to follow the rules in this policy, but are agreeing to report any misuse of the network to the person designated by the school for such reporting. Misuse means any violations of this policy or any other use that is not included in the policy, but has the effect of harming another or his or her property.

Term of the Permitted Use

Students must obtain an Internet Access Conduct Agreement and have the form signed by the student’s parent, legal guardian or other legal custodian before using any district computer which has telecommunication capabilities. It is the responsibility of the classroom teacher, instructor, or the appropriate faculty member to insure that such form is on file before a student is permitted to use computer telecommunications equipment. A student who submits to the school, as directed, a properly signed Agreement and follows the policy to which she or he has agreed will have computer network and Internet access during the course of his/her attendance at the Bixby Public School site. Students will be asked to sign a new Agreement before they
are given access to the district computer network and Internet when they are transferred or attend a different school site within the Bixby Public School District.

Acceptable Uses

1. **Educational Purposes Only.** The school district is providing access to its computer networks and the Internet for only educational purposes. If you have any doubt about whether a contemplated activity is educational, you may consult with the person(s) designated by the school to help you decide if a use is appropriate.

2. **Unacceptable Uses of Network.** Among the uses that are considered unacceptable and which constitute a violation of this policy are the following:

   a. Uses that violate the law or encourage others to violate the law. Don’t transmit offensive or harassing messages; offer for sale or use any substance the possession or use of which is prohibited by the school district’s student discipline policy; view, transmit or download pornographic materials or materials that encourage others to violate the law; intrude into the networks or computers of others; and download or transmit confidential, trade secret information, or copyrighted materials. Even if materials on the networks are not marked with the copyright symbol, you should assume that all materials are protected unless there is explicit permission on the materials to use them.

   b. Uses that cause harm to others or damage to their property. For example, don’t engage in defamation (harming another’s reputation by lies); employ another’s password or some other user identifier that misleads message recipients into believing that someone other than you is communicating or otherwise using his/her access to the network, or the Internet; upload a worm, virus, “Trojan horse,” “time bomb,” or other unauthorized access to other computers, networks, or information systems.

   c. Uses that jeopardize the security of student access and of the computer network or other networks on the Internet. For example, don’t disclose or share your password with others; don’t impersonate another user.

   d. Uses that are commercial transactions. Students and other users may not sell or buy anything over the Internet. You should not give others private information about you or others, including credit card numbers and social security numbers.

3. **Netiquette.** All users must abide by rules of network etiquette, which include the following:

   a. Be polite. Use appropriate language. No swearing, vulgarities, suggestive, obscene, belligerent, or threatening language.

   b. Avoid language and uses which may be offensive to other users. Don’t use access to make, distribute, or redistribute jokes, stories, or other material which is based upon slurs or stereotypes relating to race, gender, ethnicity, nationality, religion, or sexual orientation.

   c. Don’t assume that a sender of e-mail is giving his or her permission for you to forward or redistribute the message to third parties or to give his/her e-mail address to third parties. This should only be done with permission or when you know that the individual would have no objection.
d. Be considerate when sending attachments with e-mail (where this is permitted). Be sure that the file is not too large to be accommodated by the recipient’s system and is in a format which the recipient can open.

Supervision and Monitoring
It shall be the responsibility of all staff of the Bixby Public Schools 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 the Superintendent or designated representatives. Unacceptable uses of computer and electronic communications resources includes use that jeopardizes personal safety, use that involves illegal and prohibited activities, and use that threatens the security of the District’s technology resources.

Education
Students will be annually provided instruction on acceptable and safe use of the internet including appropriate behavior. Specifically, students will be educated about interacting with other individuals on social networking Web sites and in chat rooms and cyber bullying awareness and response.

Internet Safety

1. General Warning: Individual Responsibility of Parents and Users. All users and their parents/guardians are advised that access to the electronic network may include the potential for access to materials inappropriate for school-aged students. Every user must take responsibility for his or her use of the computer network and Internet and stay away from these sites. Parents of minors are the best guides to materials to shun. If a student finds that other users are visiting offensive or harmful sites, he or she should report such use to the person designated by the school.

2. Personal Safety: Employees and students shall not use the District’s technology resources in any manner that jeopardizes or poses a threat to personal safety. The following directives are essential to ensuring personal safety:

   a. Users shall not post personally identifiable information about themselves or others. For example, it is not permissible to put people’s photographs on the web and identify them by name.

   b. Student users shall not agree to meet or meet with someone they have met online, without parental approval.

   c. Student users shall promptly disclose to their instructor or another school employee any message the user receives that is inappropriate or makes the user feel uncomfortable.

   d. Users shall receive or transmit communications using only District-approved and District-managed communication systems. For example, users may not use free, web-based e-mail, messaging, videoconferencing or chat services, except in special situation for educational purposes where arrangements have been made in advance and approved by the District’s authorized supervisory personnel and the Director of Technology.

   e. Users shall not attempt major repair of District-owned technology resources without the assistance of the District support mechanism. Major repair is defined as any repair or modification which has the potential to impact the District infrastructure, more than one workstation, disrupt business operations or requires the user to add or remove hardware. However, users are encouraged to perform troubleshooting and minor repairs in conjunction with the District technology support segment.
3. **Illegal Activities.** It is a violation of this policy to use the school’s computer network or the Internet to gain unauthorized access to other computers or computer systems, or to attempt to gain such unauthorized access. Any use which violates state or federal law relating to copyright, trade secrets, the distribution of obscene or pornographic materials, or which violates any other applicable law or municipal ordinance, is strictly prohibited. The emerging and fast-paced developments in technology make it impossible for the District to anticipate every potential use or misuse of its technology resources. Accordingly, users are instructed that the District’s technology is not to be used for illegal activities. Among other things, users are expected to abide by the following:

a. Users shall not plagiarize works that are found on the Internet or any other electronic resource. Plagiarism is presenting the ideas or writings of others, as one’s own.

b. Users shall respect the rights of copyright owners. Copyright infringement occurs when the user inappropriately reproduces a work that is protected by a copyright. Users shall not illegally copy protected works, or make copies of such works available. Users are responsible for observing any copyright or licensing agreement that may apply when downloading materials. Users may not download any material for which a fee or license agreement is required without the approval of appropriate District supervisory personnel. Users shall not install any software (including public domain software or freeware) which is not on the District’s approved software list.

c. District staff will not support or maintain any computer operating system or application software that does not meet District standards.

d. Illegal installation of copyrighted software is prohibited. Illegal copying of software from any District computer, network, or program diskette is prohibited. Computer software and data protected under copyright laws may not be downloaded or uploaded to a computer owned or leased by the District without the written consent of the copyright holder. Any software or data located on a computer or file server owned or leased by the District found to be in violation of copyright laws will be removed.

e. Users shall not attempt to gain unauthorized access or attempt to go beyond authorized access to District resources or to any other computer system. This includes attempting to log in through another person’s account or access another person’s files.

f. Users shall not make deliberate attempts to disrupt the District’s computer system or other portions of the technology resources or destroy data by spreading computer viruses or by any other means.

g. Users shall not congest the District’s technology resources or interfere with the work of others within or outside of the District when accessing the Internet, including the transmission or posting of messages that are intended or likely to result in the loss of the recipient’s work or systems.

h. Users shall not use the District’s technology resources to engage in any activities which interfere with the operation of the District or its educational programs or compromise the safety and security of the District’s technology resources.

4. **Inappropriate Communications.** Inappropriate communications are prohibited and may result in removal of access, or other disciplinary action including suspension from school or termination of employment.

a. Users shall not use, view, download, copy, send, post or access obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful information, communications, language, images or video, or material that advocates illegal acts, violence, or discrimination towards others. Restrictions against inappropriate language, images or video apply to public messages, private messages, material posted on web pages, and files stored or created on the District’s technology resources.
b. If a user mistakenly accesses inappropriate information, the user must immediately inform his/her teacher or the network supervisor of the location of that information.

c. Parent or guardians should instruct the student user if there is additional material that they think it would be inappropriate for their child to access. The District fully expects that student users will follow the instructions of their parents or guardians in this matter.

d. Users shall not post information that could cause damage or pose a danger of disruption to the operations of the technology resources or the District.

e. Users shall not harass another person. Harassment is persistently acting in a manner that distresses or annoys another person. If a user is told by another person to stop any activity which that person finds harassing, the user must stop immediately. Individuals who believe they are the victim of harassment should immediately contact their supervisor, campus administrator, or the Superintendent.

f. Users shall not knowingly or with reckless indifference post messages that are false or defame or libel any person or organization, or that infringe the privacy rights of others.

5. **Confidentiality of Student 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 or, if the student is 18 or over, the permission of the student himself/herself. Users should never give out private or confidential information about themselves or others on the Internet, particularly credit card numbers and Social Security numbers. A supervising teacher or administrator may authorize the release of directory information, as defined by law, for internal administrative purposes or approved educational projects and activities.

6. **Active Restriction Measures.** The school, either by itself or in combination with the Data Acquisition Site providing Internet access, will utilize filtering software or other technologies to prevent students from accessing visual depictions that are (1) obscene, (2) Child Pornography, or (3) harmful to minors. The school will also monitor the online activities of students, through direct observation and/or technological means, to ensure that students are not accessing such depictions or any other material which is inappropriate for minors. It is the policy of the Bixby Public Schools to comply with the Children’s Internet Protection Act [Pub. L. No. 106-554 and 47 U.S.C. 254 (h)].

Internet filtering software or other technology-based protection systems may be disabled by a supervising teacher or school administrator, as necessary, for purposes of bona fide research or other educational projects being conducted by students age 17 and older.

The term “harmful to minors” is defined by the Communications Act of 1934 (47 USC Section 254 (h) (7), as meaning any picture, image, graphic image file, or other visual depiction that
- taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion;
- depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals;
- Taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

7. **Security of District’s Technology.** The District invests and spends substantial financial and personnel resources to provide students and staff with technology resources appropriate for the diverse educational and training interests associated with educational objectives in a technology rich world. Users are required to adhere to the highest standards of use to avoid compromise or destruction of the District’s resources. Security with respect to the District’s technology resources requires adherence to the following:
a. Users shall access the Internet in a manner which does not compromise the security and integrity of the District’s technology resources, such as allowing intruders or viruses into the District’s technology resources. Users wishing to download any document, file or software from non-District sources must observe District policies and procedures for virus checking and system security.

b. Users are responsible for their individual logon passwords and e-mail account passwords and should take all reasonable precautions to prevent others from being able to use these passwords. Users shall not share e-mail passwords, provide e-mail access to an unauthorized user, or access another user’s e-mail without authorization.

c. A computer logged into the District wide area network or the internet should not be left unattended. Users are responsible for all transactions made under their User ID and Password.

d. Users must immediately notify the e-mail administrator if they identify a possible security problem.

e. Users are responsible for the appropriate storage and backup of their data.

f. Employee personal computers not owned by the school district shall not be used in school except with permission of the superintendent or the superintendent’s designee. Student owned computers may be used at the discretion and permission of the classroom teacher and the principal.

g. The administration, faculty or staff of the District may request a system administrator to deny, revoke or suspend specific user accounts for violation of these policies or procedures.

Privacy

Network and Internet access is provided as a tool for your education. The school district reserves the right to monitor, inspect, copy, review and store at any time and without prior notice any and all usage of the computer network and internet access and any and all information transmitted or received in connection with such usage. All such information files shall be and remain the property of the school district and no user shall have any expectation of privacy regarding such materials. The superintendent or designee shall have access to all materials loaded or stored on the district’s computers. Accordingly, no user of the district’s computers shall be deemed to have a privacy right in any programs, files or data, including contents of business or personal e-mail, loaded or stored on district computers.

Failure to Follow Policy

The user’s use of the computer network and Internet is a privilege, not a right. A user who violates this policy, shall at a minimum, have his or her access to the computer network and Internet terminated, which the school district may refuse to reinstate for the remainder of the student’s enrollment in the school district. A user violates this policy by his or her own action or by failing to report any violations by other users that come to the attention of the user. Further, a user violates this policy if he or she permits another to use his or her account or password to access the computer network and Internet, including any user whose access has been denied or terminated. The school district may also take other disciplinary action up to and including termination of employment for employees and suspension from school for students. If Federal and/or State laws are violated, the offender is also subject to being reported to the proper authorities for prosecution.

Warranties/Identification
The school district makes no warranties of any kind, either express or implied, in connection with its provision of access to and use of its computer networks and the Internet provided under this policy. It shall not be responsible for any claims, losses, damages, or costs (including attorney’s fees) of any kind suffered, directly or indirectly, by any user or his or her parent(s) or guardian(s) arising out of the user’s use of its computer networks or the Internet under this policy. By signing this policy, users are taking full responsibility for his or her use, and the user who is 18 or older, or in the case of a user under 18, the parent(s) or guardian(s) are agreeing to indemnify and hold the school, the school district, the Data Acquisition Site that provides the computer and Internet access opportunity to the school district and all of their administrators, teachers, and staff harmless from any and all loss, costs, claims, or damages resulting from the user’s access to its computer network and the Internet, including but not limited to any fees or charges incurred through purchases of goods or services by the user. The user or, if the user is a minor, the user’s parent(s) or guardian(s) agree to cooperate with the school in the event of the school’s initiating an investigation of a user’s use of his or her access to its computer network and the internet, whether that use is on a school computer or on another computer outside the school district’s network.

Updates

Users, and if appropriate, the user’s parents/guardians, may be asked from time to time to provide new or additional registration and account information or to sign a new policy, for example, to reflect developments in the law or technology. Such information must be provided by the user (or his/her parent or guardian) or such new policy must be signed if the user wishes to continue to receive service. If after you have provided your account information, some or all of the information changes, you must notify the person designated by the school to receive such information.

Adoption Date: November 13, 2000
Revision Date: August 12, 2002
Revision Date: June 14, 2010