K-20 Network Acceptable Use Guidelines/Internet Safety Requirements
Blaine School District Staff Technology User Agreement

The Blaine School Board has adopted Policy and Procedure # 2022 for use of the District Network, which requires district staff sign a user agreement. A copy of the policy is available from the District website. Below are the stipulations of this agreement. You must sign the form at the end of the document.

Network Use

1. All use of the system must be in support of education and research and consistent with the mission of the district. District reserves the right to prioritize use and access to the system.
2. Any use of the system must be in conformity to state and federal law, K-20 Network policies, and district policy. Use of the system for commercial solicitation is prohibited.
3. The system constitutes public facilities and may not be used to support or oppose political candidates or ballot measures.
4. No use of the system shall serve to disrupt the operation of the system by others; system components including hardware or software shall not be destroyed, modified, or abused in any way.
5. Malicious use of the system to develop programs or institute practices that harass other users or gain unauthorized access to any entity on the system and/or damage the components of an entity on the network is prohibited.
6. Users are responsible for the appropriateness of the material they transmit over the system. Hate mail, harassment, discriminatory remarks, or other antisocial behaviors are expressly prohibited.
7. Use of the system to access, store, or distribute obscene or pornographic material is prohibited.

Security

1. System logins or accounts are to be used only by the authorized owner of the account for the authorized purpose. Users may not share their account number or password with another person or leave an open file or session unattended or unsupervised. Account owners are ultimately responsible for all activity under their account.
2. Users shall not seek information on, obtain copies of, or modify files, other data, or passwords belonging to other users; misrepresent other users on the system; or attempt to gain unauthorized access to any entity on the K-20 Network.
3. Communications may not be encrypted so as to avoid security review.
4. Users should change passwords regularly and avoid easily guessed passwords.

Personal Security

1. Personal information such as complete names, addresses, telephone numbers and identifiable photos should remain confidential when communicating on the system. Students should never reveal such information without permission from their teacher and parent or guardian. No user may disclose, use, or disseminate personal identification information regarding minors without authorization.
2. Students should never make appointments to meet people in person whom they have contacted on the system without district and parent permission.
3. Students should notify their teacher or other adult whenever they come across information or messages they deem dangerous or inappropriate on the web or when using electronic mail, chat rooms, and other forms of direct electronic communications (i.e. Instant Message services).

Copyright

The unauthorized installation, use, storage, or distribution of copyrighted software or materials on district computers is prohibited. All users of the K-20 Network shall comply with current copyright laws.

Filtering and Monitoring

1. Filtering software and services is installed and used on all computers with access to the Internet. This attempts to block or filter access to visual depictions that are obscene, child pornography, or harmful to minors. When adults are using the Internet, obscene materials and child pornography must still be filtered or blocked.
2. Educational staff will, to the best of their ability, monitor minors' use of the Internet in school, and will take reasonable measures to prevent access by minors to inappropriate material on the Internet and World Wide Web, and restrict their access to materials harmful to minors.

General Use

1. Nothing in these regulations is intended to preclude the supervised use of the network while under the direction of a teacher or other approved user acting in conformity with district policy and procedure.
2. Personal use such as personal e-mail, personal word processing, and personal web surfing should be limited and during non-working times and is subject to public record.
3. Users should not expect that files stored on school district servers will always be private. School network administrators may review files and communications to maintain system integrity and to ensure that the network is being used responsibly.
4. All activities conducted on district owned equipment (i.e., computers, cell phones, telephones) are subject to public record. Examples of activities may be web surfing, e-mailing, web chats, voice mail, and documents. Any written communication between staff and student could be determined to be a part of student record and subject to public disclosure. This communication could include: text messaging, instant messaging, and chat rooms.
5. E-mail is considered public record. As long as an e-mail message or any is maintained on a computer or server, it constitutes an educational record and is subject to FERPA (Family Educational Rights and Privacy Act) until it is permanently deleted. Blaine School District e-mail is archived daily; therefore all e-mails are subject to public record.
6. All users must recognize that they do not have a legal expectation of privacy in any activities involving the district's technology.
7. Damages incurred by the district due to the misuse of the district's technology resources, including the loss of property, will be charged to the user. District administrators have the authority to sign any criminal complaint regarding damage to district technology.

At its discretion, the district will make a determination on whether specific uses of the K-20 Network are consistent with the regulations stated above. Under prescribed circumstances non-student or staff use may be permitted, provided such individuals demonstrate that their use furthers the purpose and goals of the district. For security and administrative purposes the district reserves the right for authorized personnel to review network use and content. The district reserves the right to remove an individual's network access privileges to prevent further unauthorized activity.
Violation of any of the conditions of use may be cause for disciplinary action.

_____	_____	_____
Staff Name	**Staff Signature**	**Date**
_____	_____	_____
Supervisor/Principal Name	**Supervisor/Principal Signature**	**Date**

Date: March 28, 2008