KSD Policy

3612- District Provided Access to Electronic Information, Services, and Networks

PREAMBLE

~~Kimberly School District provides information technology for educational, research, and administrative applications by its students, faculty, and staff. This policy balances the individual's ability to benefit fully from information technology and the District's need for a secure and reasonably allocated information-technology environment. Services include voice and data, email, software, wireless access, the use of computers, servers, and other technology equipment connected to a campus wide network and the Internet. It is expected that the use of these services is directly related to educational goals and is consistent with the instructional objectives of this District.~~

Internet access and interconnected computer systems are available to Kimberly School District's students ~~and faculty~~. Electronic networks, including the internet, are a part of the District's instructional program in order to promote educational excellence by facilitating resource sharing, innovation, and communication.

In order for the District to be able to continue to make its computer network and internet access available, all users, including students, must take responsibility for appropriate and lawful use of this access. Students utilizing school-provided internet access are responsible for good behavior online. The same general rules for behavior apply to students' use of District-provided computer systems. Students must understand that one student's misuse of the network and internet access may jeopardize the ability of all students to enjoy such access. While the District's teachers and other staff will make reasonable efforts to supervise use of network and internet access, they must have student cooperation in exercising and promoting responsible use of this access and students must be held responsible and accountable for their own conduct.

Curriculum

In accordance with this policy and the Board's philosophy to ensure the safety of all students, the District shall provide an appropriate planned instructional component for internet safety which shall be integrated into the District's regular instructional program. In compliance with the Children's Internet Protection Act this instruction will include information on the safe use of social networking sites and instant messaging, the characteristics of cyber-bullying, and recommended responses.

The use of the District's electronic networks shall be consistent with the curriculum adopted by the District, as well as the varied instructional needs, abilities, and developmental levels of the students, and shall comply with the selection criteria for instructional materials and library-media center materials. Staff may, consistent with the District's educational goals, use the internet throughout the curriculum.

The District's electronic network is part of the curriculum and is not a public forum for general use.

Internet/Internet Safety

The District provides Internet filtering to prevent access to inappropriate or offensive sites.
Filtering categories shall reflect statutory requirements and the values of the community.
Filtering may also prevent or limit access to content not directly related to the educational goals of the district.

Each District computer with internet access shall have a filtering device as described in Procedure 3612P. The District shall require that any vendor, person, or entity providing digital or online library resources to the District for use by students verify they have policies and technology protection measures:

1. Prohibiting and preventing users from sending, receiving, viewing, or downloading materials that are deemed to be harmful to minors, as defined by section 18-1514, Idaho Code; and

2. Filtering or blocking access to obscene materials, materials harmful to minors, and materials that depict the sexual exploitation of a minor, as defined in chapter 15, title 18, Idaho Code.

~~District staff also monitors and supervises all Internet access. All access is logged. The district provides students and staff with the understanding and skills needed to use technology in an appropriate manner.~~

The District will also monitor the online activities of students, through direct observation and/or technological means, to ensure that students are not accessing material that is inappropriate or harmful to minors, as defined in section 18-1514 Idaho Code or as defined in 47 USC Section 254.

Filtering should also be used in conjunction with:

1. Educating students on appropriate online behavior;
2. Requiring students review and sign Form 3612F Internet Access Conduct Agreement;
3. Using behavior management practices for which internet access privileges can be earned or lost; and
4. Appropriate supervision, either in person and/or electronically.

The system administrator and/or building principal shall monitor student internet access.

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 18 and older.

NETWORK SERVICES USE AGREEMENT REQUIRED
The use of the District's technology is a privilege and not a right. Permission from parents/guardians is

required before students may access network services. All users must sign a Network Services Use Agreement at the beginning of each school year. The District will assign individual user IDs and in some cases temporary passwords for access to various services. These passwords shall meet minimum complexity criteria and refresh criteria. Under no circumstance shall these passwords be shared or divulged to anyone. Workstations and other access layer devices shall not be left unattended while the user's credentials are active.

~~**NO WARRANTIES**~~ Warranties/Indemnification

Network services provided by the District may not always meet student or staff requirements or be uninterrupted or error-free. It is provided on an "as-is/as available" basis. The District makes no warranties of any kind, express or implied, in connection with its provision of access to and use of its computer networks and the internet provided under this policy. The District is not responsible for any information that may be lost, damaged, or unavailable when using the network, or for any information that is retrieved or transmitted via the internet. This includes loss of data resulting from delays, non-deliveries, missed deliveries, or service interruptions caused by its negligence or the user's errors or omissions. Use of any information obtained via the internet is at the user's own risk. The District specifically denies any responsibility for the accuracy or quality of information obtained through its services. The District will not be responsible for any unauthorized charges or fees resulting from access to the internet, and any user is fully responsible to the District and shall indemnify and hold the District, its trustees, administrators, teachers, and staff harmless from any and all loss, costs, claims, or damages resulting from such 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 and attorney fees. The user or, if the user is a minor, the user's parent(s)/legal guardian(s) agrees to co-operate with the District in the event of the school's initiating an investigation of a user's use of his/her access to its computer network and the internet.

Violations/ Termination of Account

~~District administrators reserve the right, at their sole discretion, to suspend or terminate a user's access to and use of network services upon any breach of the district's Network Services Use Agreement. The user may be subject to additional disciplinary action.~~

If any user violates this policy, the student's access to the District's internet system and computers will be denied, if not already provided, or withdrawn and they may be subject to additional disciplinary action. The District Administrators/or **B**uilding Principal will make all decisions regarding whether or not a user has violated this policy and any related rules or regulations and may deny, revoke, or suspend access at any time, with their decision being final. Actions which violate local, state, or federal law may be referred to the local law enforcement agency.

If the actions of the individual are also in violation of other District discipline policies, said student shall be subject to additional possible disciplinary action based upon these policies.

Public Notification

The Internet Safety Coordinator shall inform the public via the main District webpage of the District's procedures regarding enforcement of this policy and make them available for review at the District office.

Email **(ISBA did not have anything on email- in policy, just procedures)**

Students ~~and staff~~ will use district provided email services. Limited personal use shall not interfere with the educational goals or instructional objectives of the district. Information forwarded to non-district accounts shall not contain material that would constitute a breach of confidentiality or contain educational records. All email is archived for a period of at least five years.

~~Email may be pushed to personal devices of district employees. The employee shall provide password protection for the device and exercise due diligence to protect sensitive district information.~~

The District reserves the right to access and disclose the contents of any account on its system, without prior notice or permission from the account's user. Use of an unauthorized non-district electronic mail account for district related business or classroom use is strictly prohibited.

Limits to the amount and age of saved email messages may be imposed to conserve district resources.

District e-mail addresses will not be linked to personal/social networking accounts and social websites.

Software and Equipment

To ensure compliance with applicable law, provide accurate inventory information and promote systems interoperability and compatibility only district approved software will be installed by designated personnel on networks or individual machines. Appropriate licenses must be held for all software. Licenses and installation media, physical or electronic will be retained by the tech department. Peripheral devices (including, but not limited to, printers, scanners, and storage/data devices) must be approved and installed by designated personnel. Donated equipment and software are subject to the same policies. Service and support for personal devices will not be provided by district staff. All purchases of software and equipment connected to or using district provided network services require approval by the Tech Director.

Wireless

Wireless access is provided for district approved devices. Other devices including personal student or staff devices may be provided access if resources are available. The access for personal devices will be limited to resources available to the public via the Internet. Students ~~and staff~~ are prohibited from establishing network services of any kind or interfering with district services.

Outsourcing of Services

To provide more efficient service and cost effectiveness it may be desirable to outsource various services. To ensure compatibility with existing systems, regulatory compliance, and to avoid duplication or

conflicts in service, contracts for such services require the approval of the technical director and the superintendent.

Contracts for outsourced services shall include specific language to assure the vendor will not use data for any purpose other than providing the outsourced service such as data mining for the vendor's own benefit, or re-disclose it to others without appropriate authorization. The contract shall require the vendor to give us notice of any security/data breaches, and, to the extent that user notification is legally required, such notice should preferably be in advance of user notification.

Vendors shall provide tools that allow the district to access data in the event of the need for e discovery.

The contract shall expressly make clear that all data belongs to the district and that the vendor acquires no rights or licenses, including without limitation intellectual property rights or licenses, to use the data for its own purposes.

Representation of District

Posting of any material representing the District on non-district sites is prohibited unless approved by the superintendent.

Submission to State Department of Education

This policy shall be filed with the State Superintendent of Public Instruction every five years after initial submission and subsequent to any edit to this policy thereafter.

Policy History:
Adopted on: April 8, 2003
Revision: June 20, 2013