KSD Policy 5450
Employee Electronic Mail and On-Line Services Usage

~~Electronic mail ("e-mail") is defined as a communications tool whereby electronic messages are prepared, sent and retrieved on personal computers. On-line services (i.e., the Internet) are defined as a communications tool whereby information, reference material and messages are sent and retrieved electronically on personal computers.~~

Internet access and interconnected computer systems ~~may~~ ~~be~~ are available to the District's employees. 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.

Employees may, consistent with the computer use policies of the District and the District's educational goals, use approved internet sites throughout the curriculum.

The District email and internet systems are provided for educational purposes ~~only~~. The District's electronic network is part of the curriculum and is not a public forum for general use.

Because of the unique nature of e-mail/Internet, and because of the District's desire to protect its interest with regard to its electronic records, the following rules have been established to address e-mail/Internet usage by all employees:

~~The District e-mail and Internet systems are intended to be used for educational purposes.~~

~~Use for informal or personal purposes is permissible within reasonable limits.~~

~~All e-mail/ Internet records are considered District records and should be transmitted only to individuals who have a need to receive them.~~

~~Additionally, District records, e-mail/Internet records are subject to disclosure to law enforcement or government officials or to other third parties through subpoena or other process. Consequently, employees should always ensure that the educational information contained in e-mail/Internet messages is accurate, appropriate and lawful.~~

Uses

The use of the District's electronic network must be in support the education and/or research, and in furtherance of the District's stated educational goals and legitimate school business purpose.

Use for other informal or personal purposes is permissible within reasonable limits provided it does not interfere with work duties and complies with District policy. All email and internet records are considered District records and should be transmitted only to

individuals who have a need to receive them and only relating to educational purposes. Employees have no expectation of privacy in any materials that are stored, transmitted, or received via the District's electronic network or District computers. The District reserves the right to access, 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, including email and instant messages.

Unacceptable Uses of Network

The following are considered examples of unacceptable uses and constitute a violation of this policy. Additional unacceptable uses can occur other than those specifically listed or enumerated herein:

1. Uses that violate the law or encourage others to violate the law including local, State, or federal law; accessing information pertaining to the manufacture of weapons; intruding into the networks or computers of others; and downloading or transmitting confidential, trade secret information, or copyrighted materials;

2. Uses that cause harm to others or damage their property, person, or reputation, including but not limited to engaging in defamation; employing another's password or some other user identifier that misleads message recipients into believing that someone other than you is communicating; reading or sharing another person's communications or personal information; or otherwise using their access to the network or the internet;

3. Uploading a worm, virus, other harmful form of programming or vandalism; participating in hacking activities or any form of unauthorized access to other computers, networks, or other information. Employee will immediately notify the school's system administrator if they have identified a possible security problem;

4. Downloading the TikTok app or visiting the TikTok website;

5. Uses amounting to harassment, sexual harassment, bullying, or cyber-bullying (defined as using a computer, computer system, or computer network to convey a message in any format that is intended to harm another individual);

6. Uses that jeopardize the security of access and of the computer network or other networks on the internet; uses that waste District resources;

7. Uses that are commercial transactions, including commercial or private advertising;

8. The promotion of election or political campaigns, issues dealing with private or charitable organizations or foundations, ballot issues, or proselytizing in a way that

presents such opinions as the view of the District;

9. Sending, receiving, viewing, or downloading obscene materials, materials harmful to minors, materials that depict the sexual exploitation of minors, or other inappropriate materials;
10. Sharing one's password with others or allowing them to use one's account;
11. Downloading, installing, or copying software or other files without authorization of the Superintendent or the Superintendent's designee;
12. Posting or sending messages anonymously or using a name other than one's own;
13. Attempting to access the internet using means other than the District network while on campus or using District property;
14. Sending unsolicited messages such as advertisements, chain letters, junk mail, and jokes;
15. Sending emails that are libelous, defamatory, offensive, or obscene;
16. Notifying patrons or the public of the occurrence of a school election by providing anything other than factual information associated with the election – such as location, purpose, etc. Such information shall not promote one position over another;
17. Forwarding or redistributing the private message of an email sender to third parties or giving the sender's email address to third parties without the permission of the sender; and/or
18. Downloading or disseminating copyrighted or otherwise protected works without permission or license to do so.
19.

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 employees. 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 employee 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. Employees 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.

Records and Privacy

The District provides e-mail and Internet access and requires employees to use them in the performance of their duties for the District. All school district business conducted electronically will be done so utilizing Kimberly School District provided services.

Access to non-district services for the purpose of collaboration related to district assigned duties may be approved by an immediate supervisor on a limited time, case by case basis.

E-mail messages and Internet records are to be treated like shared paper files, with the expectation that anything in them is available for review.

District records, including email and internet records may be subject to public records requests, disclosure to law enforcement or government officials, or to other third parties through subpoena or other processes. The Superintendent or their designee may review any and all email of any employee, at any time, with or without cause. Consequently, employees should always ensure that all information contained in email and internet messages is accurate, appropriate, and lawful. When sending student records or other confidential information by email, employees shall be aware of the security risks involved and shall take all steps directed by the ~~Internet Safety Coordinator~~ District to reduce such risks.

The ~~Internet Safety Coordinator~~ District shall provide directions to employees on how to send student records or other confidential information by email in a secure manner if that need arises.

When communicating with students and parents by email, employees should use their District email rather than a personal email account. Email and internet messages by employees may not necessarily reflect the views of the District. Abuse of the email or internet systems, through excessive and/or inappropriate personal use, or use in violation of the law or District policies, will result in disciplinary action, up to and including termination of employment.

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.

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

Internet Access Conduct Agreements

Each employee will be required to sign the Procedure 5450F Employee Electronic Mail and Online Services Use Policy Acknowledgment upon the adoption of this policy or upon hiring.

Warranties/Indemnification

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. 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 employees 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.

Violations

If any employee violates this policy, they may be subject to disciplinary action. The system administrator ~~and/or the Internet Safety Coordinator~~ and/or the building principal or Superintendent will make all decisions regarding whether or not a user has violated this policy and any related rules or regulations. Actions which violate local, State, or federal law may be referred to the local law enforcement agency.

~~The use of this policy is coordinated with the District provided Internet Services Policy #'s 3612 R and 3612 F.~~

Policy History:
Adopted on: Nov. 21, 2003
Revised on: August 19, 2015
Revised on: October , 2025

Legal References	Description
531 P.2d 588 (1975)	Board of County Commissioners v. Idaho Health Fac. Auth.
IC § 18-6726	TikTok Use by State Employees on a State-Issued Device Prohibited
Idaho Executive Order	2022-06