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

All use of electronic networks shall be consistent with the District's goal of promoting educational excellence by facilitating resource sharing, innovation, and communication. These procedures do not attempt to state all required or proscribed behaviors by users. However, some specific examples are provided. **The failure of any user to follow these procedures will result in the loss of privileges, disciplinary action, and/or appropriate legal action.**

Terms and Conditions

Acceptable Use:

1. The District provides employees with an electronic network to support education and research and for the conduct of school business. Personal use of District computers and networks outside of class is permissible, but must comply with District policy. Use is a privilege, not a right. 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 other messages.
2. Privileges – The use of the District's electronic networks is a privilege, not a right, and inappropriate use will result in a cancellation of those privileges. The system administrator (and/or building principal) will make all decisions regarding whether or not a user has violated these procedures, and may deny, revoke, or suspend access at any time. An appeal of such decisions may be made to the Superintendent within seven days. Their decision is final.
3. Unacceptable Use – The user is responsible for their actions and activities involving the network. Some examples of unacceptable uses are:
    - Using the network for any illegal activity, or to access websites encouraging illegal activity including violation of copyright or other contracts, or transmitting any material in violation of any U.S. or state law:
    - Accessing sites which allow or promote online gambling;
    - Accessing information pertaining to the manufacture of weapons or the promotion of illegal weapons;
    - Downloading the TikTok app or visiting the TikTok website;
    - Uses that cause harm to others or damage property;

- Unauthorized downloading, installation, or copying of software, regardless of whether it is copyrighted or de-virused checked for viruses;
- Installation and/or using a VPN (Virtual Private Network)
- Downloading copyrighted material for other than personal use or trade secret information;
- Viewing, transmitting, or downloading pornographic materials, materials harmful to minors, or other sexually explicit materials;
- Using the network for private financial or commercial gain;
- Wastefully using resources, such as file space;
- Hacking, attempting to bypass security systems, or gaining unauthorized access to files, resources, entities;
- Uploading a worm, virus, or other harmful form of programming and other uses the jeopardize the security of the network;
- Invading the privacy of individuals, which includes the unauthorized disclosure, dissemination, and use of information of a personal nature about anyone;
- Using another user's account or password; or some other user identifier that misleads message recipients into believing that someone other than you is communicating;
- Posting material authored or created by another person, or pictures of another person, or another person's private information or messages, without their consent;
- Posting anonymous messages; or messages using a name other than one's own;
- Using the network for commercial or private advertising;
- Uses that are commercial transactions;
- Accessing, submitting, posting, publishing, sending, or displaying any defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, harassing, or illegal material;
- Accessing sites which advocate discrimination or which promote intolerance.
- Uses amounting to harassment, sexual harassment, bullying, or cyber-bullying;
- Uses that cause harm to others or damage their property, person, or reputation, including but not limited to engaging in defamation;
- Using the network while access privileges are suspended or revoked.

- Promotion of political, personal, or religious causes in a way that presents such opinions as the view of the District;
- Disclosing identifying personal information or arranging to meet persons met on the internet or by electronic communications;

4. Network Etiquette – The user is expected to abide by the generally accepted rules of network etiquette. These include, but are not limited to, the following.
   - Be polite. Do not become abusive in messages to others.
   - Use appropriate language. Do not swear or use vulgarities or any other inappropriate language.
   - Do not reveal personal information, including the addresses or telephone numbers, of students or colleagues.
   - Recognize that District email electronic mail (e-mail) is not private. People who operate the system have access to all mail. Messages relating to or in support of illegal activities may be reported to the authorities.
   - Do not use the network in any way that would disrupt its use by other users.
5. No Warranties – The District makes no warranties of any kind, whether expressed or implied, for the service it is providing. The District will not be responsible for any damages the user suffers. 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.
6. Indemnification – The user agrees to indemnify the District for any losses, costs, or damages, including reasonable attorney fees, incurred by the District, relating to or arising out of any violation of these procedures.
7. Security – Network security is a high priority. If the user can identify a security problem on the internet, the user must notify the system administrator or building principal. The user shall not demonstrate the problem to other users. Users shall keep their account and password confidential. Users shall not use another individual's account. Attempts to log on to the internet as a system administrator will result in cancellation of user privileges. Any user identified as a security risk may be denied access to the network.

8. Vandalism – Vandalism will result in cancellation of privileges, and other disciplinary action. Vandalism is defined as any malicious attempt to harm or

destroy data of another user, the internet, or any other network. This includes, but is not limited to, the uploading or creation of computer viruses.

9. Telephone Charges – The District assumes no responsibility for any unauthorized charges or fees, including telephone charges, long-distance charges, per-minute surcharges, and/or equipment or line costs.
10. Copyright Web Publishing Rules – Copyright law and District policy prohibit the republishing of text or graphics found on the Web or on District websites or file servers, without explicit written permission.
    - For each republication (on a Website or file server) of a graphic or text file that was produced externally, there must be a notice at the bottom of the page crediting the original producer and noting how and when permission was granted. If possible, the notice should also include the Web address of the original source.
    - Employees engaged in producing Web pages must provide library media specialists with e-mail or hard copy permissions before the Web pages are published. Printed Evidence of the status of "public domain" documents must be provided.
    - The absence of a copyright notice may not be interpreted as permission to copy the materials. Only the copyright owner may provide the permission. The manager of the website displaying the material may not be considered a source of permission. is not necessarily authorized to act as a source of permission.
    - Before publishing student work employee needs to ensure there is written permission from both the parent/guardian and the student.
    - Violation of the copyright web publishing rules may result in denial of access to the network.
11. Use of Email Mail
    - The District's email system, and its constituent software, hardware, and data files, is managed by the District. The District provides e-mail to aid employees in fulfilling their duties, responsibilities and as an educational tool.
    - Email could be subject to public records requests and disclosures depending upon the subject matter of the contents of the email.
    - 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. Unauthorized access by any employee to an email account other than their own is strictly prohibited.

- Each person should use the same degree of care in drafting an email message that would be put into a written memo or document. Nothing should be transmitted in an email that would be inappropriate in a letter or memorandum.
- Email messages sent from a District account carry with them an identification of the user's internet domain. This domain name identifies the author as being with the District. Great care should be taken, therefore, in the composition of such messages and how such messages might reflect on the name and reputation of this District. Such messages reflect on the name and reputation of the district. Users will be held personally responsible for the content of any and all emails transmitted to both internal and external recipients.
- Any message received from an unknown sender should be verified as to the message's authenticity and be treated with caution and handled as directed by the system administrator. Downloading any file attached to any electronic based message is prohibited unless the user is certain of that message's authenticity and the nature of the file so transmitted.
- Use of the District's electronic mail system constitutes consent to these regulations.

12. Internet Safety

- Internet access is limited to only those "acceptable uses", as detailed in these procedures.
- Employees shall supervise students while students are using District internet access at school, to ensure that the students abide by the Terms and Conditions for internet access, as contained in Student Policy 3612 and 3612P.
- Each District computer with internet access shall be equipped with a filtering device that blocks materials that are: a) obscene, b) pornographic, or c) harmful or inappropriate for users as determined by the Superintendent or designee. The filter may also block other materials users are prohibited from accessing by District policy or procedure. The Superintendent or designee shall enforce the use of such filtering devices. Employees must use the District's filtered network for all online activities on school grounds or using District equipment. Such filter shall also block access to the TikTok website. Measures shall also be undertaken to prevent the downloading of TikTok onto any District device or via the District's electronic network.
- The system administrator, designee, and/or building principals shall monitor all internet access.

Policy Procedure History:
Adopted on: