Regulation 0403.50-AR-08 Technology and Internet Acceptable Use

The District provides personnel access to electronic devices, networks, information systems, and the Internet to support education and research for conducting school business. Personnel are required to use all technology resources for purposes appropriate to the education environment and will avoid any use that does not align with the policies, purposes, or objectives of the District.

Electronic Devices

The acceptable use terms apply to all electronic devices, including personal devices. All electronic devices and communications transmitted over the District network must adhere to District policies. While monitoring the District networks for compliance with these acceptable use standards, District personnel may limit or restrict access to District resources, networks, and the Internet for any electronic device (including personal devices).

Privacy and Confidentiality

Personnel should be aware that there is no expectation of privacy for any materials stored, transmitted, or received through the District's electronic network or devices. The District retains the authority to access, monitor, inspect, copy, review, and store all usage of its technology, including Internet access, at any time and without prior notice. This encompasses all information transmitted or received in connection with such use, including documents, emails, and instant messages. Users should understand that deleted messages and documents may still be recoverable and subject to review by designated District personnel for a specific period after deletion.

Filtering and Logging

All District devices and networks, including the Virtual Private Network (VPN), are monitored and recorded for content, sites visited, and duration of use in compliance with Idaho Code. This applies to all guests, students, classified personnel, certified personnel and administrative personnel. Authorized technology personnel can access and review these logs to ensure that District technology is utilized for appropriate educational purposes.

Sharing of Education Records

Electronic mail and documents containing confidential student information, as defined in Policy 504.6 – Education Records, are intended for designated recipients or those with a legitimate educational interest. These materials should not be forwarded or shared with individuals who do not have a legitimate educational interest.

Unacceptable Uses of District Technology

The following actions are deemed unacceptable uses and constitute a breach of this policy. Other forms of unacceptable use may arise beyond those explicitly enumerated in this document:

- Uses that violate the law or encourage others to violate the law, including but not limited to transmitting offensive or harassing messages; offering for sale, use, or purchase any substance the possession or use of which is prohibited by the District's policy, local, State, or federal law; viewing, transmitting, or downloading pornographic materials or materials that encourage others to violate local, State or federal law; Sending, receiving, viewing, or downloading obscene materials, materials harmful to minors, or materials that depict the sexual exploitation of minors; information pertaining to manufacture of weapons; intruding into the networks or computers of others; and downloading or transmitting confidential, or trade secret information.
- Intentionally 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.
    - Users must promptly notify the technology department upon identifying any potential security issues. Users are prohibited from deliberately searching for security vulnerabilities, as such actions may be deemed illegal attempts to gain unauthorized access.
- Uses amounting to harassment, sexual harassment, bullying, or cyber-bullying defined as using an electronic device, computer system, or computer network to convey a message in any format, including audio or video, text, graphics, photographic, or any combination thereof, that is intended to harm another individual, their property, person, or reputation, including but not limited to engaging in defamation (harming another's reputation by lies).
- Uses that jeopardize the security of another user's access and the computer network or other networks on the Internet; Sharing one's password with others or allowing others to use them to use one's account; posting or sending messages anonymously or using a name other than

ones' own; employing another person's password or some other user identifier that misleads message recipients into believing that someone other than you is communicating; reading another person's communication that has not been shared with you them; and sharing another person's pictures, private information, or messages without their permission.

- The misuse of District resources, such as downloading or copying large files, excessive printing, and occupying excessive file space on shared drives, is prohibited. Designated technology personnel may review and delete individual files (on network directory drives or online accounts) during routine maintenance.
- Downloading, installing, or copying software, applications, plugins, or other executable files without authorization of the Chief Technology Officer.
    - Only District-approved software will be installed by designated personnel on networks or District electronic devices. Appropriate licenses must be held for all software.
    - Peripheral devices (including, but not limited to, printers, scanners, and storage/data devices) must be approved and installed by designated personnel.
- Using District technology including the electronic mail system for:
    - Personal financial gain
    - Personal advertising or promotion
    - For-Profit business activities
    - Unapproved fundraising
    - Inappropriate public relations activities, such as solicitation for religious purposes
    - Inappropriate political purposes
    - Non-job-related purposes
- Utilizing a VPN or any other methods or software to circumvent the District's content filter, internal security systems, or external controls is strictly prohibited.
- Using the network while access privileges are revoked.

Personnel Use of Social Media

Personnel will be held responsible for the content they post on social media platforms. All personnel must adhere to District policies and regulations, ensuring that their actions do not disrupt the educational environment, interfere with school programs or activities, or infringe upon the rights of others. These requirements apply to the use of social media through the District's network or equipment.

Copyright

Users are expected to follow current copyright law. Text or multimedia files from the Internet or other electronic sources should be used in accordance with the Fair Use Guidelines established by federal copyright law and District policies and appropriately cited.

E-mail Retention

Emails will be deleted from a user's account after 190 days. Personnel can mark emails for retention for up to 390 days. The District email system does not archive emails for later retrieval.

Personal Technology Equipment and Use at Work

Personnel are prohibited from bringing personal technology equipment to the workplace, including but not limited to printers and consumer home automation products such as smart speakers. Personal devices pose a risk to the security of the District's network and can compromise the integrity of its systems and sensitive data. To ensure a secure and efficient work environment, all technology used for district purposes must comply with established security protocols and must be provided by the district. Unauthorized personal technology equipment may not be connected to the District's network or used for work-related tasks. Personnel found in violation of this policy may be subject to disciplinary action.

Wireless Guest Network

The District wireless network is an extension of the District network and may be accessed using personal devices such as laptops and mobile phones, following the established protocols provided by the Technology Department.

By using the District wireless network, the user agrees to the following terms:

- The wireless network will only have access to the Internet and will not connect to any District or school server(s), printers, projection devices, or other peripheral devices.
- All Internet usage will be filtered and logged in accordance to District filtering procedures.
- Personal devices connected to the wireless network may be monitored and reviewed at any time by designated technology personnel.

- Personal web accounts accessed while connected to the wireless network may also be monitored and reviewed at any time by designated technology personnel.
- Use of this network is a privilege, not a right. The District reserves the right to limit or restrict connectivity to this network at any time and for any reason without notification.
- The District does not offer technical support for personal devices connected to its network. Users should not anticipate that their personal devices will function on the District's wireless network. Although the District's technology department may occasionally provide limited assistance on a best-effort basis, this should not be expected or relied upon.

CONSEQUENCES OF INAPPROPRAITE USE OF TECHNOLOGY RESOURCES

Any user actions considered inappropriate by a principal, supervisor, or Chief Technology Officer, in accordance with District policy, may result in disciplinary measures. This may include termination and/or legal action, mainly if the actions restrict or inhibit other users from accessing the network or electronic information and communication systems.

If the individual's actions violate other District policies and/or regulations, said individual shall be subject to additional possible disciplinary action.

District Limitation of Liability

The District does not provide any warranties, whether express or implied, in relation to the provision of access to and use of its computer networks and the Internet as outlined in this policy. The District is not liable for any loss, damage, or unavailability of information while using the network, nor for any information retrieved or transmitted via the Internet.

The District will not be held responsible for unauthorized charges or fees incurred through Internet access. Users are fully accountable to the District and must indemnify and hold harmless the District, its Board, administrators, teachers, and personnel from all losses, costs, claims, or damages arising from the user's access to the computer network and Internet, including but not limited to any fees or charges resulting from purchases made by the user.

Furthermore, users (or their parents/legal guardians if the user is a minor) agree to cooperate with the District in the event of an investigation into the user's use of the District's computer network and Internet access.