Policy 0502.81 Student Technology and Internet Acceptable use

The District provides students with access to electronic devices, networks, information systems and the Internet to support education, research and for the conduct of school business. Students are expected to use all technology resources for purposes appropriate to the education environment at all times and will refrain from any use that is not consistent with the policies, purposes, or objectives of the West Ada School District.

Student personal use of technology that is consistent with the District's educational mission may be permitted during class when authorized by a student's teacher or appropriate administrator. 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.

Electronic Devices

The terms of acceptable use apply to all electronic devices, including personal devices. All electronic devices and communication sent on a District network shall be used in a manner consistent with the policies of the District. In the course of monitoring District networks for acceptable use, District personnel may limit or restrict electronic devices (including personal devices) from access to District resources, networks, and the Internet.

Privacy and Confidentiality

Students have no expectation of privacy in any materials that are stored, transmitted, or received via the District's electronic network or District electronic devices. 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. This includes any and all information transmitted or received in connection with such usage, including documents, email and instant messages. Users should expect that even deleted messages and documents may be recovered and reviewed by designated District personnel for a period of time after deletion.

Filtering and Logging

All District devices and networks, including the Virtual Private Network (VPN), are filtered and logged for content, sites visited, and duration of use as required by Idaho Code. This includes all guests, students, classified, certified, and administration staff. These logs are accessible and can be reviewed by designated technology staff to ensure that District technology is used for appropriate educational purposes.

Unacceptable Uses of District Technology

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:

- 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 student discipline policy, local, State, or federal law; viewing, transmitting, or downloading pornographic materials or materials that encourage others to violate local, State. or federal law; 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;
- Uses that cause harm to others or damage their property, person, or reputation, including but not limited to engaging in defamation (harming another's reputation by lies); employing another's password or some other user identifier that misleads message recipients into believing that someone other than you is communicating; reading another person's communications; sharing another person's pictures, private information, or messages without their permission; or otherwise using his or her access to the network or the Internet; Posting or sending messages anonymously or using a name other than one’s own;
- Students may not disrupt the learning atmosphere, educational programs, school activities, or the rights of others by using any communication regarding any student(s), District personnel, or District school in their social media accounts. All requirements of this policy apply to use of social media through the District network or equipment or as part of a class assignment.
- 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 will immediately notify a teacher, building administrator, or the school's system administrator if they have identified a possible security problem. Users will not intentionally look for security problems, because this may be construed as an illegal attempt to gain 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.
- Uses that jeopardize the security of student access and of the computer network or other networks on the Internet;
- Uses that waste District resources including downloading or copying very large files without permission from a teacher or are required for a school related project, unnecessary printing, and consuming excess file space on shared drives.
    - Students will use their designated directories on the network or online accounts to store documents they have created and will delete them when they are no longer needed.
    - Through routine maintenance, individual files (on network directory drives or online accounts) may be reviewed and deleted by designated technology staff.
- Uses that are commercial transactions, including commercial or private advertising. Students and other users may not sell or buy anything over the Internet. Students should not give personal information to others, including credit card numbers and social security numbers.
- The promotion of election or political campaigns, ballot issues, or proselytizing in a way that presents such opinions as the view of the District.
- Sending, receiving, viewing, or downloading obscene materials, materials harmful to minors, or materials that depict the sexual exploitation of minors.
- Disclosing identifying personal information or arranging to meet persons met on the Internet or by electronic communications.
- Sharing one’s password with others or allowing them to use one's account.
- Downloading, installing, or copying software or other files without authorization of the Superintendent or the Superintendent's designee(s).
- 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.
- Attempting to bypass internal or external security systems or controls. Students may only access the Internet using the District network.
- Plagiarism of material accessed online. Teachers will instruct students in appropriate research and citation practices.
- Using the network while access privileges are revoked.

Any conditions or activities not specifically listed above that are not consistent with the policies, purposes, and objectives of West Ada School District are prohibited.

E-M ail Retention

All email will be removed and deleted from a user's account after one hundred and ninety (190) days. The District email system does not archive email for later retrieval.

Wireless Guest Network

The District wireless network is an extension of the District network and may be accessed with a personal device by using the published username and password protocols established by the Technology Department.

By using the District guest wireless network, students agree to the following:

- This wireless network will only have access to the Internet and not allow connection to any District or school server(s), printer, or other peripheral device.
- All Internet usage will be filtered and logged according to District filtering and logging procedures.
- No technical support will be provided to make a device work on the guest network.
- Personal devices connected to the wireless network may be monitored and reviewed at any time by designated technology staff.
- Personal web accounts visited while connected to the wireless network maybe monitored and reviewed at any time by designated technology staff.
- Use of this network is a privilege and not a right, District reserves the right to limit or restrict connectivity to this network at any time and for any reason without notification.

Consequences of Inappropriate Use of Network/Internet Resources

If any user violates this policy, the user's access to the District's Internet system and electronic devices can be denied and he or she may be subject to additional disciplinary action, including but not limited to removal from appropriate class and possible expulsion from the District. The system administrator OR Superintendent's designee(s) AND the building principal will make all decisions regarding violation of this policy and any related rules or regulations. All disciplinary decisions made by the principal or his or her designee are deemed final with recommendations for expulsion following District procedure. Actions which violate local, State, or federal law may be referred to the local law enforcement agency.

A user will be required to reimburse West Ada School District for any losses, costs, or damages, including attorney’s fees, caused by inappropriate use.

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.

District Limitation of Liability

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 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. The user or, if the user is a minor, the user's parent(s)/legal guardian(s) agrees to cooperate with the District in the event the school initiates an investigation of a user's use of his or her access to its computer network and the Internet.

Legal References: Code of Idaho,18-1514, 18-2201, 18-2202, 33-132