Wendell School District No. 232 recognizes the importance of providing positive, productive educational experiences through the district's Internet, computer, and network services. To promote this objective and protect its staff and students, the board authorizes the superintendent or designee to:

1. Prohibit and prevent school computers and other school owned technology-related services from sending, receiving, viewing or downloading materials that are deemed to be harmful to minors, as defined by Idaho Code §18-1514.

2. Prohibit and prevent unauthorized online disclosure, use, or dissemination of personally identifiable information of students.

3. Select and employ technology protection measures on the district's computers to filter or block Internet access to obscene materials, materials harmful to minors, and materials that depict the sexual exploitation of a minor, or other information that is determined to be in violation of district policies.

4. Establish and enforce appropriate disciplinary measures to be taken against persons violating this policy.

5. Handle complaints regarding the enforcement of the district's Internet use policies and procedures.

6. Establish procedures to remove a user's files without prior notice after an account has been inactive for a specified period of time.

The district will limit Internet access to materials that enrich and support the curriculum and educational needs of users, contribute to the delivery of efficient and effective business or educational functions, and expedite professional district communications.

PRIVACY

Use of the district's technology resources is a privilege and not a right. Access has not been established as a public access service or a public forum. The district reserves the right to monitor, inspect, copy, review, delete, and/or store at any time and without prior notice any and all results of usage of the Internet, computers, network resources, and any and all information transmitted or received in connection with such usage. All such information will be and remains the property of the district and users have no expectation of privacy regarding such materials. The district has the right to place restrictions on the use of the district's Internet, computers, and network resources and may also deny access to staff and students who violate related policies and procedures.

Employees must use district technology in a professional, legal, and responsible manner. Use of district technology for personal business must be kept to a minimum and must conform to district policies and procedures and state and federal laws and regulations.

When acting within the capacity of a district employee, communication from any location and using any type of equipment, owned by the district or otherwise, must reflect professional integrity and responsibility and not have an adverse effect on students or on the performance of an employee's duties for the district.

PROHIBITED USES

The district's Internet, computers, and network resources may only be used for approved district activities and educational purposes. All users must fully comply with this policy and immediately report any violations or suspicious activities to the building principal or designee. Prohibited uses of district technology include, but are not limited to:

1. Causing Harm to Individuals or to Property

    a. Use of obscene, profane, vulgar, inflammatory, abusive, threatening, disrespectful language or images.

    b. Making offensive, damaging, or false statements about others.

    c. Posting or printing information that could cause danger or disruption.

    d. Bullying, hazing or harassing another person.

    e. Deleting, copying, modifying, or forging other users' names, e-mails, files, or data.

    f. Disguising one's identity, impersonating other users, or sending an anonymous email.

    g. Posting personal information (e.g. phone number, address) about oneself or any other person, except to responsible agencies.

2. Engaging in Illegal Activities

    a. Participating in the sale, purchase or promotion of illegal items or substances.

    b. Accessing or transmitting:

        i. Pornography of any kind.

        ii. Obscene depictions.

iii. Harmful materials.

iv. Materials that encourage others to violate the law.

v. Confidential information.

vi. Copyrighted materials without authorization or as provided by fair use regulations.

c. Attempting to disrupt the computer system or destroy data by any means.

3. Breaching System Security

a. Sharing one's or another person's password with others.

b. Entering another person's account or accessing another person's files without authorization.

c. Allowing others to gain access to one's individual account.

d. Interfering with other users' ability to access their accounts.

e. Allowing student access to sensitive data.

f. Attempting to gain unauthorized access to another computer.

g. Using software or hardware tools designed to interfere with or bypass security mechanisms.

h. Utilizing software or hardware applications that are not approved for business use.

i. Attempting to evade the district's computer filtering software.

4. Improper Use or Care of Technology

a. Accessing, transmitting or downloading large files, including posting chain letters or engaging in spamming.

b. Attempting to harm or damage district technology, files or data in any way.

c. Alteration of configured equipment, including the addition of unauthorized passwords and user accounts.

d. Leaving an account open or unattended.

e. Attempting to remedy a security problem and not informing a school official.

f. Failing to report the abuse of district technology.

g. Installing, uploading or downloading unauthorized programs.

h. Copying district software for personal use.

i. Using district technology for:

   i. Personal financial gain.

   ii. Personal advertising or promotion.

   iii. For-profit business activities.

   iv. Unapproved fundraising.

   v. Inappropriate public relations activities such as solicitation for religious purposes.

   vi. Inappropriate political purposes.

CONSEQUENCES FOR INAPPROPRIATE USE

Failure to comply with this policy or inappropriate use of the district's Internet, computers, or network resources may result in usage restrictions, loss of access privileges, and/or disciplinary action up to and including termination. The superintendent or designee may also report the violation to law enforcement where appropriate.

Users are responsible for damages to the equipment, systems, and software resulting from deliberate or willful acts.

NOTICE

The district will inform staff, students, parents/guardians and other users about this policy through posting on the district website and by other appropriate methods. A copy of this policy will be available for review at the district office. The district will also file this policy with the state superintendent of public instruction every five years.

By accessing the district's Internet, computers and network resources, users acknowledge awareness of the provisions of this policy and awareness that the district uses monitoring systems to monitor and detect inappropriate use.

All students and staff are required to sign a technology user agreement (see Policy No. 519F1, Internet, Computer and Network Services User Agreement) that signifies their understanding and agreement to follow these regulations.

♦ ♦ ♦ ♦ ♦ ♦ ♦

LEGAL REFERENCE:
Idaho Code Sections
33-132 – Local School Boards – Internet Use Policy Required

ADOPTED: August 19, 2014

AMENDED: November 19, 2021