Vallivue School District #139

The Vallivue School District recognizes the importance of providing positive, productive educational experiences through the district's Internet, computers/devices, 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 Section 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 provide access to Internet, computers/devices, and network services. These services are filtered, monitored, and modified for public school educational use to assure the safety of students and to limit use to educational purposes related to the mission of the district. They may not always provide the same utility and resources as private or business systems.

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/devices, 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/devices, and network resources and may also deny access to staff and students who violate related policies and procedures.

10L-09L-08L-04L-02L-D2/12/98-M10/19/10-M04/01/14

INTERNET SAFETY FOR STUDENTS

The district will provide students with Internet to help advance their learning experience. Some of the uses Internet provides students is access to email, collaboration opportunities, cloud storage, research tools, curricular content resources, and a vast knowledge base of information. That access will be restricted in compliance with the Children's Internet Protection Act (CIPA) regulations and school policies. Web browsing may be monitored and web activity records may be retained indefinitely.

The district's instructional program will include a component of Internet safety for students, including interaction on social networking sites and cyberbullying awareness and response. Each year, all educators must sign the district Teacher Verification Document form stating they are in compliance with this directive.

The district will take appropriate steps to protect all students from access, through the district's computers, to visual depictions that are obscene, contain child pornography, are harmful to minors, or depicting the sexual exploitation of a minor, as defined in Idaho Code Section 18-1507, by installing and utilizing specific technology that blocks or filters Internet access to such visual depictions.

The district's intent is to make Internet access available to further educational goals and objectives, students may find ways to access other materials as well. Filtering software is in use, but no filtering system is capable of blocking 100% of the inappropriate material available on the Internet. Vallivue School District believes that the benefits to students from access to the Internet, in the form of information resources and opportunities for collaboration, exceed any disadvantages.

The building principal or designee may authorize the disabling of the Internet filter system only for the purpose of enabling access for bona fide research or other lawful purpose. Disabling of the Internet filter system by any other staff member or student will result in disciplinary action.

As required by the Children's Internet Protection Act (CIPA), this district will hold at least one public meeting~~s~~ to receive input from parents and other patrons regarding the district's Internet safety plan, including the use of an Internet filtering service.

Any staff member, student, parent, or patron may file a complaint regarding enforcement of this policy or request that the district either block, or disable a block of, a particular website. The individual must file a written complaint with the superintendent. The superintendent will appoint a five (5) member committee, including three (3) staff members and two (2) patrons. The committee will meet with the individual who filed the request in a timely manner, allow that individual to make oral or written arguments to support the request, and make a written recommendation to the superintendent regarding whether the district should block, or disable a block of, a particular website. Upon reviewing the request and the committee's

10L-09L-08L-04L-02L-D2/12/98-M10/19/10-M04/01/14

recommendation, the superintendent will render a written decision and notify the individual who made the request. The superintendent's decision will be final.

PROHIBITED USES

The district's Internet, computers/devices, 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 Internet Technology (IT) staff, classroom teacher or building principal. 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. Cyberbullying, 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

10L-09L-08L-04L-02L-D2/12/98-M10/19/10-M04/01/14

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 district 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

10L-09L-08L-04L-02L-D2/12/98-M10/19/10-M04/01/14

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 expulsion. 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 and will be provided in writing to parents/guardians upon request. 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.

Parents have the right to limit Internet, computers/devices, or network services. The district will provide an Opt-Out form (see Policy No. 698F1 Vallivue School District Parent Opt-Out Form). This form allows parents to restrict Internet, eail, and/or Release of Directory Information.

♦ ♦ ♦ ♦ ♦ ♦ ♦

LEGAL REFERENCE:

Idaho Code Sections
- 6-210 – Recovery of Damages for Economic Loss Willfully Caused by a Minor
- 18-917A – Student Harassment – Intimidation – Bullying
- 18-1507 – Definitions – Sexual Exploitation of a Child – Penalties
- 18-1514 – Obscene Materials - Definitions
- 18-2201 – Computer Crime – Definitions
- 18-2202 – Computer Crime
- 33-132 – Local School Boards – Internet Use Policy Required

Children's Internet Protection Act, Sections 1703 to 1721, USC Section 254(h)(1)
Cowles Publishing Co. v. Kootenai County Board of Commissioners, 144 Idaho 259 (2007)

ADOPTED: as new policy 4/8/08 (replaces #603.12 Information Technology Acceptable Use and Internet Safety)

AMENDED: 1/13/09, 09/14/10, 8/12/14, 11/10/15

10L-09L-08L-04L-02L-D2/12/98-M10/19/10-M04/01/14