

Blackfoot School District No. 55 recognizes the importance of providing positive, productive educational experiences through the district's Internet, computer, mobile computing 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, mobile computing devices 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, including mobile computing devices, 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, mobile computing 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, mobile computing devices, and network resources and may also deny access to staff and students who violate related policies and procedures.

INTERNET SAFETY FOR STUDENTS

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.

The district will take appropriate steps to protect all students from access, through the district's computers, including mobile computing devices, 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 §18-1507, by installing and utilizing specific technology that blocks or filters Internet access to such visual depictions.

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, this district will hold annual public meetings 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 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, mobile computing 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 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. 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, mobile computing devices, 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 publishing in the student handbook. 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, mobile computing devices, 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. 698F1, Internet, Computer, Mobile Computing Devices, and Network Services User Agreement) that signifies their understanding and agreement to follow these regulations.



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: June 26, 1997

- AMENDED:** October 28, 2004
October 27, 2005
October 23, 2008
December 17, 2009
June 24, 2010
December 16, 2010
August 21, 2014
July 16, 2015
October 20, 2016
February 25, 2021

**Blackfoot School District No. 55
Internet, Computer, Mobile Computing Device
and Network Service User Agreement**

Blackfoot School District No. 55 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, each student ("user") must agree to abide by the terms and provisions as set forth in *Policy No. 698, Acceptable Use of Internet, Computer, Mobile Computing Devices and Network Resources for Students*. This Agreement applies to all district-provided Internet, computers and network resources, including district-issued mobile computing devices used on and off district premises.

Every student, regardless of age, must read and sign below:

I have read, understand and agree to abide by the terms and conditions of the [name] School District's policies regarding student use of District-provided Internet, computers, mobile computing devices and network resources (Policy No. 698). By signing this Agreement, I take full responsibility for usage and agree to indemnify and hold the school, the school district, or internet service provider (ISP) harmless from any and all loss, costs, claims, or damages resulting from user access to its Internet, computer, mobile computing devices, and network resources, including but not limited to any fees or charges incurred through purchases of goods or services by the user. Further, I understand and agree that I am responsible for damages to the district's equipment, systems, and software resulting from deliberate or willful acts.

The district makes no warranties of any kind, either express or implied, in connection with its provision of access to and use of its Internet, computer, mobile computing devices, and network resources.

I am aware that the district uses monitoring systems to monitor and detect inappropriate use. I agree to cooperate with the school in the event of an investigation into a user's use or access of the district's Internet, computer, and network resources.

I understand that failure to comply with the policy or inappropriate use of the district's Internet, computers, mobile computing devices, or network resources may result in usage restrictions, loss of access privileges, forfeiture of any fees paid for the use of any mobile computing device, and/or disciplinary action up to and including expulsion, regardless of whether the misuse was committed by me or another person. The superintendent or designee may also report the violation to law enforcement where appropriate.

I accept full responsibility for the safe and secure handling of mobile computing devices issued to me for this school year. I accept full responsibility for the proper use and safeguarding of the

device under all applicable policies. I understand that it is my responsibility to immediately report any damage, theft, or problems with the device to a teacher or administrator.

Student Signature

Date

Student's Printed Name

Address: _____

Phone Number: _____

As the parent/guardian of the above student, I understand my child's responsibility in the use and care of the mobile computing device issued by the district, and my financial responsibility in the event my student loses the device or is found to be the cause of deliberate or negligent damage to it. I understand that if he or she is found to be responsible for deliberate or negligent damage or for the loss of the device, I will be financially responsible for reasonable repair and/or replacement cost.

I have read Policy 698 and explained it to my child. I understand that my child's failure to comply with the policy or inappropriate use of the district's Internet, computers, mobile computing devices, or network resources may result in usage restrictions, loss of access privileges, forfeiture of any fees paid for the use of any mobile computing device, and/or disciplinary action up to and including expulsion, regardless of whether the misuse was committed by my child or another person.

I also understand that I will be responsible for monitoring my child's use of district-provided Internet, computers, mobile computing devices and network resources outside of the school setting.

_____ I do not wish my student to take a mobile computing device at this time.

Parent/Guardian Name (Please Print)

Parent/Guardian Signature

Date