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, 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 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.

GENERAL NETWORK INFORMATION

The District network is a service provided by the District. The system administrators are employees of the District and reserve the right to monitor all activity on the District's network. All users must submit a signed *Blackfoot School District Technology User Agreement* before obtaining a user account and password.

Because of the complex association between many government agencies and networks, the end user of this network must adhere to strict procedures. They are provided here so that users, and the parents of users who are under 18 years of age, are aware of their responsibilities. The District will modify these rules at any time circumstances and laws may dictate, by publishing the modified rule(s) on the District's website and at each school's media center. Any signature at the end of the *Blackfoot School District Technology User Agreement* is legally binding and indicates the signer has read the Terms and Conditions carefully and understands their significance.

ONLINE SERVICES

The District may provide services, either hosted by the District or by third-party vendors, that allow users to send, receive, share, store, create, and/or manipulate various media, data, and

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

communications using devices capable of accessing the Internet. Examples of these services are Google Apps for Education (GAFE), DropBox, Infinite Campus, Blackboard and Brain honey. These services may be accessible at district sites, at home, or at other private or public sites. When available, these services are provided as an educational tool, to be used solely for District educational purposes and goals. User accounts may be maintained for a certain period after a user leaves the District, to allow the user to retrieve their data and store on their personal storage, except in employment or educational termination situations. These services are a privilege and may be revoked if a user is found in violation of any part of the District Acceptable Use Policy.

INFORMATION CONTENT & USES OF THE SYSTEM

Users agree not to submit, publish, or display on the District network or online services, any information which conveys an offensive, profane, or sexually suggestive message. Users further agree not to harass or disturb by pestering or tormenting, including, but not limited to, intimidation because of a person's race, color, religion, gender, sexual orientation or ethnicity. Users agree not to use the facilities of the District's network or online services to conduct any business or business activity. Neither shall they solicit the performance of any activity which is prohibited by law. Users agree not to publish on the District's network or online services any information which contains any advertising or any solicitation of other users to use goods or services without the explicit approval of the District.

Because the network and online services provide access to other systems around the world, users (and the parent(s) of a user if the user is under 18 years of age) specifically understand that the system administrators and the District do not have control of the content of information existing on these other systems. Users, who are under 18 years of age and their parents/guardians, are advised that some systems may contain defamatory, inaccurate, abusive, obscene, profane, sexually-oriented, threatening, racially offensive, or illegal material. The District does not control such material. Nor does it condone and nor permit use of these materials on the District's network.

Parents of minors having accounts on the District network or online services should be aware of the existence of such materials and monitor home usage of the system. Users accessing such materials over the network or online services are subject to the discipline of the school/department, the District's "Student Code of Conduct" and the District's Board Policies. Such activities may also result in termination of the user's account on the District's network and online services, as well as suspension or expulsion.

ONLINE CONDUCT

Any action by a user that constitutes an inappropriate use of the District's network and/or online service, or improperly restricts or inhibits other users from using and enjoying the District's network and/or online services, is prohibited. Transmission of material, information or software in violation of any local, state or federal law is prohibited.

In consideration for the privilege of using the District's network and online services and in consideration for access to the information contained in it, users release the District's network and its operators and sponsors, the District and its staff, and all organizations, groups and institutions with which the District is affiliated, from any and all liability or claims of any nature arising from the use, or inability to use, the District's network.

The District's network and online services shall be used for educational purposes only.

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

CHILDREN'S INTERNET PROTECTION ACT POLICY (C.I.P.A.)

The District intends that all Internet safety policies and technology protection measures comply with the provisions of the Children's Internet Protection Act (CIPA), 47 USC 254(h), as amended. Accordingly, the District shall take all actions necessary and appropriate to implement and enforce the following policies with respect to student access to and use of the Internet through the District's computer network, and in accordance with the District's Student Code of Conduct.

These policies and protection measures will also be implemented and enforced as much as is feasible with any third party online service (ex. Google Apps for Education) the District maintains for educational access and use, whether by students or employees of the District.

General Warning and Individual Responsibility of Parents and Users

All student users and student parents/guardians are advised that access to the electronic network and online services, including the Internet and World Wide Web, may include the potential for access to materials inappropriate for school-aged pupils. Every user must take responsibility for his or her use of the computer network and Internet, and must not access these sites. Parents of minors are the first and best source of guidance as to what materials to avoid. If a student finds that other users are visiting offensive or harmful sites, he or she should report such use to a teacher or administrator.

Personal Safety

In using the computer network and Internet, including electronic mail (email), blogging, chatting, texting or any other forms of electronic communication, students are advised not to reveal personal information, such as a home address or telephone number. Students are not to use their last name or provide any other information which might allow a person to locate them, unless they first obtain the permission of a supervising teacher. Students are not to arrange a face-to-face meeting with a person the student has only met through the computer network or Internet without the student's parent's permission (unless the student is 18 years or older). Regardless of age, a student should never agree to meet such a person in a secluded place or in a private setting.

Confidentiality of Student Information

No user shall disclose personally identifiable information concerning students on the Internet without the permission of a parent or guardian, or if the student is 18 or over, the permission of the student. Student users should never disclose private or confidential information about themselves or others on the Internet, particularly credit card numbers and Social Security numbers.

Users may not publish any student information that is deemed private or personal information in a way that is publicly accessible, unless required by District policy or by state or federal law.

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, 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 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, 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:

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

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.

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

iii. For-profit business activities.

iv. Unapproved fundraising.

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

vi. Inappropriate political purposes.

NETWORK/ONLINE SERVICES ETIQUETTE

Users shall abide by generally accepted rules of network and online etiquette. These include, but are not limited to:

- Be polite. Do not get abusive with messages to others.
- Use appropriate language. Do not swear, use vulgarities or any other inappropriate language. Illegal activities are strictly forbidden.
- Note that electronic mail (e-mail) is not guaranteed to be private. People who operate the system do have access to all mail. Messages relating to or in support of illegal activities may be reported to the authorities.

There is no expectation of privacy.

- Do not use the network in such a way that it would disrupt the use of the network by other users.

ELECTRONIC MAIL

Electronic mail (e-mail) is an electronic message sent by, or to a user, in correspondence with another person having Internet mail access. Messages received on the District's network and/or online services are normally retained for 120 days or until deleted by the recipient. A canceled District network account will not retain its e-mail. Users are expected to remove old messages in a timely fashion. E-mail privacy is not guaranteed. Personally identifiable information about students is not to be sent via email.

A. The District System Administrator will determine procedures for retention and removal of all e-mail on the District network.

B. The District System Administrator will cooperate fully with District administrators to facilitate internal investigations regarding suspected violations of the network or law.

The District reserves the right to cooperate fully with local, state or federal officials in any investigation concerning or related to any e-mail transmitted on the District's network.

COPYRIGHTED MATERIAL

Each user shall follow all copyright laws regarding the use, duplication, application, distribution and/or re-purposing of intellectual property (e.g. software, text, video, visual images, audio/music). Each user shall make certain no copyrighted material is used without explicit permission of the copyright holder (e.g., author, programmer, producer, developer, and publisher).

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

DISK USAGE

System administrators reserve the right to set quotas for disk usage on the System. A user who exceeds the quota is required to delete files to return to compliance. The District may take measures to enforce these measures should a user choose not comply.

SECURITY

Security on any computer system or service is a high priority, especially when the system involves many users. If a user can identify a security problem on the District's network or service, the user must notify a system administrator. The user should not demonstrate the problem to others. Passwords to the system or online service should not be easily guessable by others, nor should they be words which could be found in a dictionary. Passwords should not be shared with any other users or family members. Attempts should not be made to log in to the system or online service using another user's account. Users should immediately notify a system administrator if their passwords are lost, stolen, or if there is reason to believe that someone has obtained unauthorized access to their accounts**.** Any user identified as a security risk, or having a history of problems with other computer systems or services, may be denied access to the District's network and online services.

VANDALISM

Vandalism is strictly prohibited, and is defined as any malicious attempt to harm or destroy the data or computer system of another user, whether on the District's network, or any of the agencies or other networks or services that are connected to Blackfoot School District. Vandalism includes the uploading or creation of computer viruses. It also includes illegal or unauthorized entry to another person's files, accounts, computers, or computer system, or an attempt to gain such access (e.g., hacking). Abuse of Technology constitutes a violation of the District's **"**Student Discipline Handbook" including suspension or expulsion.

TERMINATION OF ACCOUNT

The District reserves the right, in its sole discretion, to suspend or terminate the user's accounts access to and use of the District's network and online services upon any suspected breach of these Terms and Conditions. Before a suspension or termination or as soon as practicable, the user will be informed of the suspected breach and be given an opportunity to present an explanation.

ENFORCEMENT PROVISIONS

In order to ensure adherence to the Terms and Conditions, the District reserves the right to monitor all activity on the system and associated online services and to inspect any data, including e-mail stored on the system and associated online services. Privacy is not guaranteed.

Violations of the Terms and Conditions will result in disciplinary action according to the policies of the District's Board and the Student Discipline Handbook.

TECHNOLOGY USE PROCEDURES OPPORTUNITIES

Every student has the opportunity to use available technology resources designated for student access for the purpose of educational growth. The trust that defines the District educational community requires that technology resources be used for educational purposes consistent with

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

the mission of the District, unselfishly, with good manners, responsible behavior, and for the good of the community as a whole. These procedures apply to all technology resources.

RESPONSIBILITIES

1. Authorized usage. Students using technology as an educational resource shall also accept the responsibility for the preservation and care of that technology. Only those students with appropriate and explicit authorization may use any technology.

It is the student's responsibility to obtain written permission from an authorized person before removing any technology resource from the school premises. Each student who takes possession of equipment acknowledges that s/he will be the sole operator, whether on or off District premises.

It is the student's responsibility to incur no charges when accessing electronic resources (e.g., databases, bulletin boards, e-mail, Internet) unless authorized by the supervising teacher or designated individual. Payments for unauthorized charges are the responsibility of the student. Authorized access is to be limited to District accounts and excludes personal accounts.

2. School/departmental policies and procedures. It is the student's responsibility to follow policies and procedures established by each school/department for the use of any technology. It is the student's responsibility to follow the directions of the teacher or designated individual in the use/access of all technology.

It is the student's responsibility to keep food, drink and other harmful objects away from technological systems as directed by the school/department. It is the student's responsibility to monitor content and volume of printed documents as well as files in their online storage as directed by the school/department. If multiple copies of a document are needed, a copy machine should be used instead of a printer.

3. Use of copyrighted intellectual property. It is the student's responsibility to follow all copyright laws regarding the use, duplication, application, distribution and/or re-purposing of intellectual property (e.g., software, text, video visual images, audio/music). It is the student's responsibility to make certain no copyrighted material is used without explicit permission of the copyright holder (e.g., author, programmer, producer, developer, and publisher).

4. Privacy of property of individuals and/or the District. It is the student's responsibility to respect the privacy of others, and to maintain his/her own privacy, regarding electronic resources and passwords. Students shall not access, copy, or modify passwords, files, e-mail, voice mail, or other materials belonging to other users without explicit authorization of the supervising teacher or designated individual. In the case of suspected misuse or threat to an electronic system, system administrators have the right and responsibility to review passwords, files, e-mail, voice mail or other materials stored on any District system by users.

5. Video usage. It is the student's responsibility to secure permission from the supervising teacher or designated individual to air a video production. Appropriate visual, textual, and audio content is expected. It is the student's responsibility to obtain the appropriate consent of people, places, and/or events being shown in a video production. Particular attention should be paid to brand names of products or services shown in the presentation.

It is the student's responsibility to be aware that certain individuals and events may be precluded from video productions due to religious or cultural objections. The supervising teacher or

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

designated individual will assist the student in making appropriate decisions as referred to below in #6.

6. Appropriate use. It is the student's responsibility to keep material inappropriate for school use from being used or created on District technology systems (including electronic resources, and textual, video, and/or audio materials). Students are responsible for reporting inappropriate sites to their supervising teacher.

It is the student's responsibility to not use any technology in a manner which conveys an offensive, profane or sexually suggestive message, or to use technology to harass, disturb by pestering or tormenting, including but not limited to intimidation because of a person's race, color, religion, gender, sexual orientation or ethnicity.

7. Damage, vandalism or destruction of technological systems.

- Students using technology shall respect the integrity of technological systems and information. It is the student's responsibility to make sure no technology is destroyed, modified, relocated or abused in any way.
- Virus protection software is installed on the District's network to protect the information stored there as well as the integrity of the network. The student will not attempt to compromise the virus protection software.
- It is the student's responsibility to not use or develop files that infiltrate, harm, or damage components of a computer or computing system/network. It is a student's responsibility to keep infected files off District computers, networks, and online services.

8. Violations and misuse. It is the student's responsibility to report any violations or misuse of technology to the supervising teacher or designated individual.

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 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 and Network Services User Agreement) that signifies their understanding and agreement to follow these regulations.

DISCIPLINARY ACTION

The consequences of violating these technology procedures constitutes a violation of the District's "Student Discipline Handbook".

♦ ♦ ♦ ♦ ♦ ♦ ♦

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

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

ATTACHMENT: Computer Network Service User Agreement - 698F1

TECHNOLOGY USER AGREEMENT
(Board Policy 698F1)

I, _____, a student or employee of Blackfoot School District, understand and agree to comply with the *Acceptable Technology Use Policy Terms and Conditions*. Further, I understand, agree and shall comply with the following terms and conditions:

1. The use of the District's network, associated software, network accounts, and online services is a privilege and responsible use is required. Some examples of irresponsible use would include, but not be limited to, unapproved software, unlicensed software, key logging software or hardware devices, the placing of unlawful information on the system, or information which conveys an offensive, profane, sexually suggestive message, or harasses or disturbs by pestering or tormenting, including, but not limited to, intimidation because of a person's race, color, religion, gender, sexual orientation or ethnicity in either public or, upon registration of complaint, private messages or other systems that are accessed through the District's network. The District will be the sole arbiter of what constitutes irresponsible use.

2. The District's network or online services may not be used for conduct or communication that embarrasses, harms or in any way distracts from the good reputation of the District, its staff, students or any organizations, groups, or institutions with which the District's network is affiliated. The District will be the sole arbiter of what constitutes unacceptable behavior. It also includes illegal or unauthorized entry or attempt to gain access to another person's data, accounts, computers, or computer systems.

3. The District reserves the right to review any material stored on District-provided storage or services to which any users have access and will edit or remove any material which the District, in its sole discretion, believes may be unlawful, or constitutes irresponsible use as set forth in paragraph one, above. Any individual, who uses, sends, receives or stores information via the District's network or online services has no expectation of privacy associated with such actions.

4. All services and features on the District's network and associated online services are intended for educational or professional use. Any commercial or unauthorized use of those features or services, in any form**,** is expressly forbidden.

5. In consideration of the privilege of using the District's network and associated online services and in consideration of access to these, I release the District's network, its operators and sponsors, the District and its staff, and all organizations, groups and institutions with which the District is affiliated, from any liability and from any claims I may have, of any nature, arising from my use, my inability to use, and from others' use of the District's network or online services.

6. My access to the District's network and online services is subject to such rules and regulations of system usage as may be established by the administrators of the system, which may be changed from time to time. Violation of this network agreement may result in disciplinary action.

User Signature: _____ Date: _____

Print Name: _____

PARENT OR GUARDIAN (If you are student, a parent or guardian must also sign.)

Parent or Guardian (please print): _____

Signature: _____ Date: _____

cc: Student or Personnel File