First Adopted: 12/18/1996
Revised: 11/15/2000
Revised: 06/20/2001
Revised: 02/19/2003
Revised: 03/19/2008
Revised: 10/15/2014
Revised: 02/18/2015
Revised: 08/17/2016

2454

Acceptable Use of Electronic Resources

Purpose

The Blue Mountain Union School District recognizes that information technology (IT) is integral to learning and educating today's children for success in the global community and fully supports the access of these electronic resources by students and staff. The purpose of this policy is to:

1. Create an environment that fosters the use of information technology in a manner that supports and enriches the curriculum, provides opportunities for collaboration, and enhances staff professional development.
2. Ensure the district takes appropriate measures to maintain the safety of everyone that accesses the district's information technology devices, network and web resources.
3. Comply with the requirements of applicable federal and state laws that regulate the provision of access to the internet and other electronic resources by school districts.

Policy

It is the policy of the Blue Mountain School District to provide students and staff access to a multitude of information technology (IT) resources including the Internet. These resources provide opportunities to enhance learning and improve communication within our community and with the global community beyond. However, with the privilege of access comes the responsibility of students, teachers, staff and the public to exercise responsible use of these resources. The use by students, staff or others of district IT resources is a privilege, not a right.

The same rules and expectations govern student use of IT resources as apply to other student conduct and communications, including but not limited to the district's harassment and bullying policies.

The district's computer and network resources are the property of the district. Users shall have no expectation of privacy in anything they create, store, send, receive or display on or over the district's computers or network resources, including personal files and electronic communications.

All emails, text, images or posts may be stored on our network and are our property. If there is use of social media through the school's network, whatever is on the network may be stored and is the property of the district. There is no expectation of privacy.

This policy restricts the use of internet and social media to appropriate use while at work. Social media use shall not interfere with an employee's work day.

The Superintendent is responsible for establishing procedures governing use of IT resources consistent with the provisions of this policy. These procedures must include:

1. An annual process for educating students about responsible digital citizenship. As defined in this policy, a responsible digital citizen is one who:

    - **Respects One's Self.** Users will maintain appropriate standards of language and behavior when sharing information and images on social networking websites and elsewhere online. Users refrain from distributing personally identifiable information[1] about themselves and others.
    - **Respects Others.** Users refrain from using technologies to bully, tease or harass other people. Users will report incidents of cyber bullying and harassment in accordance with the district's policies on bullying and harassment. Users will also refrain from using another person's system account or password or from presenting themselves as another person.
    - **Protects One's Self and Others.** Users protect themselves and others by reporting abuse and not forwarding inappropriate materials and communications. They are responsible at all times for the proper use of their account by not sharing their system account password.
    - **Respects Intellectual Property.** Users suitably cite any and all use of websites, books, media, etc.
    - **Protects Intellectual Property.** Users request to use the software and media others produce.

2. Provisions necessary to ensure that Internet service providers and other contractors comply with applicable restrictions on the collection and disclosure of student data and any other confidential information stored in district electronic resources.

3. Technology protection measures that provide for the monitoring and filtering of online activities by all users of district IT, including measures that protect against access to content that is obscene, child pornography, or harmful to minors.[2]

[1] For the purposes of this policy, "personally identifiable information" shall not include any information listed as "directory information" in the school district's annual FERPA notice.
[2] Required by Children's Internet Protection Act (CIPA), 47 U.S.C. § 254(1); 47 C.F.R. § 54.520(c)(ii)

4. Methods to address the following:[3]

    - Control of access by minors to sites on the Internet that include inappropriate content, such as content that is:

        - ✓ Dating
        - ✓ Gambling
        - ✓ Hate
        - ✓ Discrimination
        - ✓ Nudity
        - ✓ Obscene or pornographic
        - ✓ File Sharing

    - The safety and security of minors when using electronic mail, social media sites, and other forms of direct electronic communications.
    - Prevention of unauthorized online access by minors, including "hacking" and other unlawful activities.
    - Unauthorized disclosure, use, dissemination of personal information regarding minors.
    - Restriction of minors' access to materials harmful to them.

5. A process whereby authorized persons may temporarily disable the district's Internet filtering measures during use by an adult to enable access for bona fide research or other lawful purpose.[4]
6. The Blue Mountain Union School District reserves the right to create and maintain records about the use of school computers. Records of computer use, if any, will be retained for no fewer than 30 days, but may be kept longer if the need exists. The Principal, Assistant Principal, Tech Coordinator, or Systems Administrator may review these records to ensure the efficient and legal operation of the computer network. Staff and students should have no expectations of privacy when using a school computer or the computer network.

Policy Application

This policy applies to anyone who accesses the district's network, collaboration and communication tools, and/or student information systems either on-site or via a remote location, and anyone who uses the district's IT devices either on or off-site.

[3] Required by Children's Internet Protection Act (CIPA), 47 U.S.C. § 254(1); 47 C.F.R. § 54.520(c)(ii)
[4] Required by 20 U.S.C. § 6777(c)

Limitation/Disclaimer of Liability

The District is not liable for unacceptable use or violations of copyright restrictions or other laws, user mistakes or negligence, and costs incurred by users. The District is not responsible for ensuring the accuracy, age appropriateness, or usability of any information found on the District's electronic resources network including the Internet. The District is not responsible for any damage experienced, including, but not limited to, loss of data or interruptions of service. The District is not responsible for the accuracy or quality of information obtained through or stored on the electronic resources system including the Internet, or for financial obligations arising through their unauthorized use.

Enforcement

The district reserves the right to revoke access privileges and/or administer appropriate disciplinary action for misuse of its IT resources. In the event there is an allegation that a user has violated this policy, a student will be provided with notice and opportunity to be heard in the manner set forth in Policy 4300 Behavior Management.

Allegations of staff member violations of this policy will be processed in accord with contractual agreements and legal requirements.

Notice of violations of this policy by students shall be forwarded to the Principal to evaluate compliance with this policy and the appropriate implementation procedures. Students involved will be provided with notice and opportunity to be heard in the manner set forth in Policy 4300 Behavior Management. Staff member infractions will be dealt with in accordance with contractual agreements.

The Blue Mountain Union School District shall cooperate fully with local, state or federal officials in any investigation concerning to or relating to any illegal activities conducted through the use of the school's electronic resources.

Disciplinary action shall be appropriate to meet specific concerns related to the violation and, in the case of students, will focus on helping them learn how to use the electronic network in a responsible manner.

Due process procedures shall be followed in all matters pertaining to violations or perceived violations of this policy.

13 V.S.A. § 1027 (Disturbing Peace by Use of…Electronic Means)

13 V.S.A. §2605(Voyeurism)

13 V.S.A. Sections 2802 et seq. (Obscenity, minors)

15 U.S.C. Section 6501 (Children's Online Privacy Protection Act)

17 U.S.C. Sections 101-120 (Federal Copyright Act of 1976 as amended)

18 U.S.C. Section 2510 (Electronic Communications Privacy Act)

18 U.S.C. Section 2251 (Federal Child Pornography Law)

20 U.S.C. § 6777 et seq. (Enhancing Education Through Technology Act)

47 U.S.C. §254 (Children's Internet Protection Act)

47 CFR §54.520 (CIPA Certifications)

47 U.S.C. section 230 (Computer Decency Act)

Verified by _____

Date _____