Boardman Local School District

COMPUTER/INTERNET ACCEPTABLE USE POLICY

For Students

Below is the Computer Network and Internet Acceptable Use Policy and Agreement ("Policy and Agreement") of the Boardman Local School District and the Mahoning County Educational Service Center (MCESC) and the Area Cooperative Computerized Educational Service Center (ACCESS) Information Technology Site (ITC) that provides Internet access to the school district.

It is the policy of Boardman Local Schools to:(a) prevent user access over its computer network to, or transmission of, inappropriate material via Internet, electronic mail, or other forms of direct electronic communications; (b) prevent unauthorized access and other unlawful online activity; (c) prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; and (d) comply with the Children's Internet Protection Act [Pub. L. No. 106554 and 47 USC 254(h)].

The school district cannot provide access to any student who fails to sign and submit the Policy to the School as directed.

A student's use of the District's computers and Internet resources is a privilege, not a right. Student users of the District's computer network and Internet access are expected to use this technology as an educational resource.

Student computer network/Internet users are expected to behave responsibly in accessing and viewing information that is pertinent to the educational mission of the District. Students are required to abide by the generally accepted rules of network etiquette. These include, but are not limited to the following:

NETWORK ETIQUETTE

1. Use of Appropriate Language. The District's Internet system has been established for an educational purpose. As such, the District prohibits student users from using language which is inconsistent with an educational purpose. The use of the following type of language is prohibited:

    a. Criminal speech and speech used in the course of committing a crime (for example: threats to the President or to any other person, instructions on breaking into computer systems, child pornography, drug dealing, purchase

of alcohol, gang activities, etc.);

b. Speech that is inappropriate in the educational setting or violates District rules (such as obscene,profane, lewd, vulgar, threatening, harassing or discriminatory language or false or defamatory material about a person/organization; dangerous information that if acted upon could cause damage or present a danger of disruption; violations of privacy/revealing personal, private information about others); and

c. In some circumstances, such as on District sponsored student Web pages, the District may require that student publications meet a variety of standards related to adequacy of research, spelling and grammar and appropriateness of material (i.e., that school Web pages must relate to school and career preparation activities).

2. Sending, receiving, transferring, viewing, sharing or downloading obscene, pornographic, lewd or otherwise illegal materials, images, videos or photographs, including but not limited to sexually explicit images or images portraying nudity.

3. Access to Information. Students are prohibited from accessing or attempting to access the following categories of material or information on the Internet or World Wide Web:

a. material that is profane or obscene;

b. material that is pornographic, expressly including child pornography;

c. material that is harmful to minors (i.e., pictures or visual depictions which, taken as a whole, appeal to a prurient interest in nudity, sex or perverted or lewd acts);

d. material that advocates or condones the commission of unlawful acts; or
e. material that advocates or condones violence or discrimination towards other people.

4. Students are advised that the District utilizes a Technology Protection Measure that blocks or filters Internet access to the above categories of material / information, as well as other categories of material or information which the District has deemed inappropriate for viewing by students in the educational setting.

5. Online Safety/Privacy: Students are required to complete an Internet safety course. The curriculum will focus on educating students about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response. The course content will be prescribed to the building principals by a designated administrator within the District's IT Department at the beginning of each school year. The IT administrator will ensure the content is consistent with federal requirements.

6. Students are prohibited from giving out personal information for non educational reasons pertaining to themselves such as: addresses, telephone numbers, parents' work addresses or telephone numbers or the name and

location of their school, even through email correspondence unless specifically authorized by the District and with the consent of the students' parents/guardians. Students must tell their teachers and/or parents immediately if they come across information which makes them feel uncomfortable. Students must never agree to get together with someone they "meet" online without first discussing it with their parents. If their parents agree to the meeting, students must ensure that the meeting is in a public place and that they are accompanied by one of their parents.

7. Only Web 2.0/Social Networking tools and applications, including but not limited to instant messaging, chat rooms, wikispaces, blogs and other methods of interactive electronic communication, approved by a designated administrator within the IT Department, and aligned to the National Educational Technology Standards for Students (NETS*S) may be utilized for instructional purposes in the attainment of the educational goals of the District. Technology Protection Measures are in place to block or filter Internet access to non-approved Web 2.0 tools and applications. Any digital communications are subject to District review at any time. Technology Protection Measures will be used to redflag digital communications that violate OHIO or federal law or District policy. Routine maintenance and monitoring of the District's system may lead to discovery that a student has violated the law or a District policy. An individualized search of a student's profile, log files, history, etc., will be conducted if there is reasonable suspicion that a user has violated the law or District policy.

8. Electronic Mail (email): Students may only use email solutions approved by a designated administrator within the IT Department. Students must understand that there is no guarantee of privacy in their email messages and that email messages are subject to District review at any time. Technology Protection Measures will be used to redflag emails that violate the law or a District policy/rule. Routine maintenance and monitoring of the District's system may lead to discovery that the student has violated the law or a District policy/rule. An individualized search of a student's email will be conducted if there is a reasonable suspicion that a user has violated the law or District policy/rule. Email should be used only for legitimate educational purposes or as authorized by the District. Students should be courteous and respectful in their email messages to others. The use of students' email accounts will be permitted for instructional purposes aligned to the National Educational Technology Standards for Students (NETS*S) and for the attainment of the District's educational goals.

9. Plagiarism: Students are reminded that it is plagiarism to "cut/copy and paste" information from the Internet and then pass it off as their own original ideas. Students are prohibited from plagiarizing information and resources from the Internet and are reminded to cite proper sources used from the Internet.
10.Copyright Infringement: All communications and information via the network (i.e., the Internet) should be assumed to be private property and protected by copyright. Students may not reproduce copyrighted material without explicit permission of the author/owner. Only public domain software can be downloaded.

11.Unauthorized or Disruptive Use/Hacking: Students are prohibited from using the District network in such a way that would disrupt the use of the network by other users. Students may not create or maliciously distribute computer viruses. Students may not destroy another person's data. Students may not access or attempt to access other computer systems or access files without authorization.

12.Purchase of Products or Services: Students are prohibited from purchasing products or services through the District network. The District is not responsible for any financial obligations arising from unauthorized use of the District network for the purchase of products or services.

13.Student Passwords/Accounts: Students may not share their passwords to anyone nor allow unauthorized network access via their account.

14.Unauthorized Disclosure, Use or Dissemination of Personal Information: Students may not disclose, use or disseminate personal information about students, especially minor students, without the authorization of that student's parent/guardian and without specific authorization from the District. 15.Prohibition on Using Peer to Peer Networking Applications: Students are prohibited from using peer to peer networking applications on the Internet/World Wide Web.

Cyberbullying

Cyberbullying will not be tolerated. Harassing, dissing, flaming, denigrating, impersonating, outing, tricking, excluding, and cyberstalking are all examples of cyberbullying. Don't be mean. Don't send emails or post comments with the intent of scaring, hurting, or intimidating someone else.

Engaging in these behaviors, or any online activities intended to harm (physically or emotionally) another person, will result in severe disciplinary action and loss of privileges. In some cases, cyberbullying can be a crime. Remember that your activities are monitored and retained.

Addendum:

Examples of Acceptable Use I will:

- Use school technologies for school related activities and research.
- Follow the same guidelines for respectful, responsible behavior online that I am expected to follow offline.
- Treat school resources carefully, and alert staff if there is any problem with their operation.
- Encourage positive, constructive discussion if allowed to use communicative or collaborative technologies.

- Alert a teacher or other staff member if I see threatening/bullying, inappropriate, or harmful content (images, messages, posts) online.
- Use school technologies at appropriate times, in approved places, for educational pursuits only.
- Cite sources when using online sites and resources for research; ensure there is no copyright infringement.
- Recognize that use of school technologies is a privilege and treat it as such. Be cautious to protect the safety of myself and others. Help to protect the security of school resources.
- This is not intended to be an exhaustive list. Users should use their own good judgment when using school technologies.

Examples of Unacceptable Use I will not:

- Use school technologies in a way that could be personally or physically harmful to myself or others.
- Search inappropriate images or content.
- Engage in cyberbullying, harassment, or disrespectful conduct toward others–staff or students.
- Try to find ways to circumvent the school's safety measures and filtering tools.
- Use school technologies to send spam or chain mail.
- Plagiarize content I find online.
- Post personally identifying information, about myself or others.
- Agree to meet someone I meet online in real life.
- Use language online that would be unacceptable in the classroom.
- Use school technologies for illegal activities or to pursue information on such activities.
- Attempt to hack or access sites, servers, accounts, or content that isn't intended for my use.

This is not intended to be an exhaustive list. Users should use their own good judgment when using school technologies.

Limitation of Liability

Staff members shall report to the System Administrator or a School District Administrator any actions by students which would violate the security or integrity of any computer, network or messaging system whenever such actions become known to them in the normal course of their work duties. This shall not be construed as creating any liability for staff members for the computer related misconduct of students.

BOARDMAN LOCAL SCHOOL DISTRICT will not be responsible for damage or harm to persons, files, data, or hardware. While BOARDMAN LOCAL SCHOOL DISTRICT employs filtering and other safety and security mechanisms, and attempts to ensure their proper function, it makes no guarantees as to their effectiveness. BOARDMAN LOCAL SCHOOL DISTRICT will not be responsible, financially or otherwise, for unauthorized transactions conducted over the school network.

Google Account Deletion

Upon graduation or leaving the Boardman Local District your email and google drive will be deleted. It is your responsibility to download or transfer items you with to keep to a personal account before your last day in the district.

Image Release Statement

The Boardman Local School District is making an ongoing effort to promote the positive activities, honors, and work of our staff and students. This includes working with the local newspapers, radio, and television stations and also developing our own publications. These publications include information, likenesses, and images, which may appear on the district web site as well as in other publications. Toward that end, please note that your child's image or likeness may appear in occasional candid photos.

Unless stated otherwise and submitted in writing to the Superintendent prior to October 1 of each school year, permission is granted to the Boardman Local School District to use your child's likeness in a photograph in any and all of its publications, including website entries, without payment or any other consideration. Furthermore, it is agreed that such materials will become the property of the Boardman Local School District and will not be returned. This irrevocable authorization grants the Boardman Local School District the right to edit, alter, copy, exhibit, publish or distribute such photos for purposes of publicizing the District's programs or for any other lawful purpose. In addition, parent(s)/guardian(s) waive the right to inspect or approve the finished product, including written or electronic copy, wherein their child's likeness appears.

Violations of this Acceptable Use Policy

Violations of this policy may have disciplinary repercussions, including:

- Suspension of network, technology, or computer privileges in extreme cases
- Notification to parents in most cases

- Detention or suspension from school and school related activities • Legal action and/or prosecution

I have read and understood this Acceptable Use Policy and agree to abide by it:

_____ (STUDENT Printed Name)

_____ (STUDENT Signature)

_____ (Date)

_____ (PARENT Printed Name)

_____ (PARENT Signature)

By signing this Policy and Agreement, you are agreeing not only to follow the rules in this Policy and Agreement, but are agreeing to report any misuse of the network to the person designated by the School for such reporting. Misuse means any violation of this Policy or any other use that is not included in the Policy, but has the effect of harming another or his or her property.

Legal References ORC 3313.20, 3313.47 Children's Internet Protection Act of 2000, 47 U.S.C. 254 [h],[1]