8457 Internet Safety and Acceptable Use Policy

A. Internet Safety Policy

It is the policy of Grand Island Public Schools to comply with the Children's Internet Protection Act (CIPA) and Children's Online Privacy Protection Act (COPPA). With respect to the District's computer network, the District shall: (a) prevent user access to, or transmission of, inappropriate material via Internet, electronic mail, or other forms of direct electronic communications; (b) provide for the safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications; (c) prevent unauthorized access, including so-called "hacking," and other unlawful activities online; (d) prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; (e) obtain verifiable parental consent before allowing third parties to collect personal information online from students; and (f) implement measures designed to restrict minors' access to materials (visual or non-visual) that are harmful to minors.

1. Definitions. Key terms are as defined in CIPA. "Inappropriate material" for purposes of this policy includes material that is obscene, child pornography, or harmful to minors. The term "harmful to minors" means any picture, image, graphic image file, or other visual depiction that: (1) taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion; (2) depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and (3) taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

2. Access to Inappropriate Material. To the extent practical, technology protection measures (or "Internet filters") shall be used to block or filter Internet, or other forms of electronic communications, access to inappropriate information. Specifically, as required by the CIPA, blocking shall be applied to visual depictions of material deemed obscene or child pornography, or to any material deemed harmful to minors. Subject to staff supervision, technology protection measures may be disabled or, in the case of minors, minimized only for bona fide research or other lawful purposes.

3. Inappropriate Network Usage. To the extent practical, steps shall be taken to promote the safety and security of users of the District's online computer network when using electronic mail, chat rooms, instant messaging, and other forms of direct electronic communications. Specifically, as required by CIPA, prevention of inappropriate network usage includes: (a) unauthorized access, including so-called 'hacking,' and other unlawful activities; and (b) unauthorized disclosure, use, and dissemination of personal identification information regarding minors.

4. Supervision and Monitoring. It shall be the responsibility of all members of the District staff to supervise and monitor usage of the online computer network and access to the Internet in accordance with this policy and CIPA. Procedures for the disabling or otherwise modifying any technology protection measures shall be the responsibility of the Superintendent and the Superintendent's designees.

5. Social Networking. Students shall be educated about appropriate online behavior, including interacting with others on social networking websites and in chat rooms, and cyberbullying awareness and response. The plan shall be for all students to be provided education on these subjects within the Nebraska K-12 Language Arts Standards. The Superintendent or the Superintendent's designee shall be responsible for identifying educational materials, lessons, and/or programs suitable for the age and maturity level of the students and for ensuring the delivery of such materials, lessons, and/or programs to students.

6. Parental Consent. The District shall obtain verifiable parental consent prior to students providing or otherwise disclosing personal information online using the GIPS information system.

7. Adoption. This Internet Safety Policy was adopted by the Board at a public meeting, following normal public notice and will be reviewed as needed.

8. The District shall comply with the Nebraska Student Online Personal Protection Act and will endeavor to take all reasonable and necessary steps to protect the online privacy of all students.

B. Computer Acceptable Use Policy

This computer acceptable use policy is supplemental to the District's Internet Safety Policy.

1. Technology Subject to this Policy. This Computer Acceptable Use Policy applies to all technology resources of the District or made available by the District. Technology resources include, without limitation, computers and related technology equipment, all forms of e-mail and electronic communications, and the internet.

2. Access and User Agreements. Use of the District technology resources is a privilege and not a right. The Superintendent or designee shall develop appropriate user agreements and shall require that employees, students (and their parents or guardians), and others to sign such user agreements as a condition of access to the technology resources, as the Superintendent determines appropriate. Parents and guardians of students in programs operated by the District shall inform the Superintendent or designee in writing if they do not want their child to have access.

   The Superintendent and designees are authorized and directed to establish and implement such other regulations, forms, procedures, guidelines, and standards to implement this Policy.

   The technology resources are not a public forum. The District reserves the right to restrict any communications and to remove communications that have been posted.

3. Acceptable Uses. The technology resources are to be used for the limited purpose of advancing the District's mission. The technology resources are to be used, in general, for educational purposes, meaning activities that are integral, immediate, and proximate to the education of students as defined in the E-rate program regulations.

4. Unacceptable Uses.

   The following is a non-comprehensive list of unacceptable uses of the technology resources:

   a. Personal Gain: Technology resources shall not be used, and no person shall authorize its use, for personal financial gain other than in accordance with prescribed constitutional, statutory, and regulatory procedures, other than compensation provided by law.

   b. Campaigning: Technology resources shall not be used, and no person shall authorize its use, for campaigning for or against the nomination or election of a candidate or the qualification, passage, or defeat of a ballot question.

c. Technology-Related Limitations: Technology resources shall not be used in any manner, which impairs its effective operations or the rights of other technology users. Without limitation:

1. Users shall not use another person's name, log-on, password, or files for any reason, or allow another to use their password (except for authorized staff members).
2. Users shall not erase, remake, or make unusable another person's computer, information, files, programs or disks.
3. Users shall not access resources not specifically granted to the user or engage in electronic trespassing.
4. Users shall not engage in activities to gain unauthorized access to the software or unauthorized access to the system of other users.
5. Users shall not copy, change, or transfer any software without permission from the network administrators.
6. Users shall not write, produce, generate, copy, propagate, or attempt to introduce any computer code designed to self-replicate, damage, or otherwise hinder the performance of any computer's memory, file system, or software. Such software is often called a bug, virus, worm, Trojan horse, malware, or similar name.
7. Users shall not engage in any form of vandalism of the technology resources.
8. Users shall follow the generally accepted rules of network etiquette. The Superintendent or designees may further define such rules.

d. Other Policies and Laws: Technology resources shall not be used for any purpose contrary to any District policy, any school rules to which a student user is subject, or any applicable law. Without limitation, this means that technology resources may not be used:

1. to access any material contrary to the Internet Safety Policy; or to create or generate any such material.
2. to engage in unlawful harassment or discrimination, such as sending e-mails that contain sexual jokes or images.
3. to engage in violations of employee ethical standards and employee standards of performance, such as sending e-mails that are threatening or offensive or which contain abusive language; use of end messages on e-mails that may imply that the District is supportive of a particular religion or religious belief system, a political candidate or issue, or a controversial issue; or sending e-mails that divulge protected confidential student information to unauthorized persons.
4. to engage in or promote violations of student conduct rules.
5. to engage in illegal activity.
6. in a manner contrary to copyright laws.
7. in a manner contrary to software licenses.

5. Disclaimer. The technology resources are supplied on an "as is, as available" basis. The District does not imply or expressly warrant that any information accessed will be valuable or fit for a particular purpose or that the system will operate error free. The District is not responsible for the integrity of information accessed, or software downloaded from the Internet.

6. Filter. A technology protection measure is in place that blocks and/or filters access to prevent access to Internet sites that are not in accordance with policies and regulations. In addition to blocks and/or filters, the District may also use other technology protection measures or procedures as deemed appropriate.

Notwithstanding technology protection measures, some inappropriate material may be accessible by the Internet, including material that is illegal, defamatory, inaccurate, or potentially offensive to some people. Users accept the risk of access to such material and responsibility for promptly exiting any such material.

The technology protection measure that blocks and/or filters Internet access may be disabled only by an authorized staff member for bona fide research or educational purposes: (a) who has successfully completed District training on proper disabling circumstances and procedures, (b) with permission of the immediate supervisor of the staff member requesting said disabling, or (c) with the permission of the Superintendent. An authorized staff member may override the technology protection measure that blocks and/or filters Internet access for a minor to access a site for bona fide research or other lawful purposes provided the minor is monitored directly by an authorized staff member.

7. Monitoring. Use of the technology resources, including but not limited to internet sites visited and e-mail transmitted or received, is subject to monitoring by the administration and authorized IT Department personnel at any time to maintain the system and insure that users are using the system responsibly, without notice to the users. Users have no privacy rights or expectations of privacy with regard to use of the District's computers or Internet system. All technology equipment shall be used under the supervision of the Superintendent and the Superintendent's designees.

8. Sanctions. Violation of the policies and procedures concerning the use of the District technology resources may result in suspension or cancellation of the privilege to use the technology resources and disciplinary action, up to and including expulsion of students and termination of employees. Use that is unethical may be reported to the Commissioner of Education. Use that is unlawful may be reported to the law enforcement authorities. Users shall be responsible for damages caused and injuries sustained by improper or non-permitted use.

If a student believes that a website has been improperly blocked by technology protection measures used to block and filter Internet access, the following procedures shall be followed:

1. The challenged material will remain as is until a final decision is rendered.
2. At any time in the process where appropriate forms are not filed or appropriate steps are not followed the objection is voided.
3. If a complaint is in writing, the letter should be acknowledged promptly, including an invitation to the complainant to a conference at the school;
4. If the matter cannot be resolved satisfactorily at the school level, the principal shall:
    a. ask for a "Citizen's Request for Reconsideration of Internet Materials" form (attached);
    b. offer to send the "Request for Reconsideration" form describing the situation to the associate superintendent for student services;
    c. send a brief written statement describing the situation to the associate superintendent for student services;
    d. assure the complainant that they will be contacted promptly by the associate superintendent for student services; and
    e. explain that the internet materials will not be changed while a decision is pending.
5. Upon receipt of the "Request for Reconsideration" form, the Associate Superintendent for Student Services shall take appropriate action to see that the material is reviewed. If warranted, a meeting of an advisory committee shall be called.
    a. Committee members may include a student if appropriate, IT staff, teacher, media specialist, parent, and/or BOE member.
    b. Committee members shall review the internet material in advance of the meeting.
    c. Committee members shall report their findings to the Associate Superintendent for Student Services.

6. Upon receiving the advisory committee's report, the Associate Superintendent for Student Services shall make a decision, notify the complainant by letter and explain any appeal procedures.

Legal Reference: Children's Internet Protection Act, 47 USC § 254
Children's Online Privacy Protection Act, 15 U.S.C. § 6501
FCC Order adopted August 10, 2011
47 USC § 254(h)(1)(b); 47 CFR 54.500(b) and 68 FR 36932 (2003) (E-rate restrictions)
Neb. Rev. Stat. § 49-14,101.01 (Political Accountability and Disclosure Act)
LB 512 (2017).

Policy Adopted: 12-6-99
Policy Revised: 9-15-05
Policy Revised: 11-8-07
Policy Revised: 06.12.2012
Policy Revised: 12.14.2017
Policy Revised: 06.14.2018 – Public Hearing
Policy Revised: 06.10.2021

GRAND ISLAND PUBLIC SCHOOLS

8457.1 REQUEST FOR RECONSIDERATION OF INTERNET MATERIAL

Complainant:
Name:
Email:
Phone:
Address:

School Building:
Principal:
Date complaint filed:

Internet material in question:
Complaint initiated by:
Telephone:
Address:
Email:

Do you represent Yourself ____ Other group or organization ____

PLEASE RESPOND TO THE FOLLOWING. USE ADDITIONAL PAPER IF NEEDED.

1. Is the resource part of the curriculum, library collection, or other?
2. Have you read/viewed this material in its entirety?
3. To what in the material do you object? (Please be specific)
4. What do you feel might result from the use of this material?
5. What would you like your school to do about this material?
6. What material would you recommend?
7. Do you desire to meet with the Materials Review Committee to discuss this material?
    a. Yes____ No ____

_____
Signature of Complainant

_____
Date

PLEASE SUBMIT THIS FORM TO THE BUILDING PRINCIPAL