Groesbeck ISD Internet Safety Policy

The school district has technology protection measures for all computers/laptops in the school district, including computers in media centers/libraries, that block and/or filter visual depictions that are obscene, child pornography, and harmful to minors as defined in the Children's Internet Protection Act (CIPA). The school district will certify that schools in the district, including media centers and libraries, are in compliance with the Children's Internet Protection Act.

Compliance measures contained within this plan address the following:

Access by Minors to Inappropriate Matter on the Internet and World Wide Web

1. Users will not use the district system to access profane or obscene material (pornography) that advocates illegal acts of violence or discrimination toward other people (hate literature). However, a notable exception may be made for hate literature for students if the purpose of such access is to conduct research, and both the teacher and the parent approve access. District employees may access the above material only in the context of legitimate research.

2. If a user inadvertently accesses such information, they should immediately disclose the inadvertent access in a manner specified by their school. Students should immediately notify teachers, and teachers and staff should immediately notify the building administration. The Building administration should immediately notify the director of technology. This will protect users against allegations of intentionally violating the acceptable use policy.

3. The fact that the filtering technology has not protected against access to certain material does not create the presumption that such material is appropriate for users to access. Similarly, the fact that the filtering software has protected access to certain material does not create the presumption that the material is inappropriate for users to access.

4. The school district will provide students access to Internet resources only in supervised environments and has taken steps to lock out objectionable areas to the greatest extent possible, but potential dangers remain.

Safety and Security of Minors When Using Electronic Mail, Chat Rooms, Cyber-Bullying Awareness and Other Forms of Direct Electronic Communications and Unauthorized Disclosures

1. Student users will not post or share contact information about themselves or others. Personal contact information includes the student's name, along with other information that would allow an individual to locate the student, including, but not limited to, parent(s) name(s), home address/location, work address/location, or phone number.

2. Elementary and middle school students will not disclose their full name or any other personal contact information for any purpose.

3. High school students will not disclose personal contact information except to educational institutions for educational purposes, companies, or other entities for career development purposes, or with specific staff approval.

4. Students will not disclose names, personal contact information, or any other private or personal

information about other students under any circumstances. Students will not forward a message sent to them privately without the permission of the person who sent them the message.

5. Students will not agree to meet someone they have met online.

6. Students will promptly disclose to their teacher or another school employee any message they receive that is inappropriate or makes them feel uncomfortable. Students should not delete such messages until a staff member instructs them to do so.

7. Students will be educated on cyberbullying awareness and inappropriate and appropriate online behaviors and responses.

Unauthorized Access, Including "Hacking" and Other Unlawful Activities by Minors Online

1. Security is a high priority on any computer network, especially when the network involves many users. If users feel they can identify a security problem on the computer network, they must notify a network administrator or building-level administrator. The user should not inform individuals other than network or building administrators of a security problem.

2. Users are responsible for using their individual accounts and should take all reasonable precautions to prevent others from using them. Under no circumstances should a user provide their password to another person.

3. Passwords to the network should not be easily guessed by others, nor should they be words that could be found in a dictionary.

4. Attempts to log in to the network using either another user's account or as a network administrator could result in the termination of the account. Users should immediately notify a network administrator if a password is lost or stolen or if they have reason to believe that someone has obtained unauthorized access to their account. Any user identified as a security risk will have limitations placed on the usage of the network or may be terminated as a user and be subject to other disciplinary action.
5. Users will not attempt to gain unauthorized access to the district system or any other computer system through the district system or go beyond their authorized access. This includes attempting to log in through another person's account or accessing another person's files. These actions are illegal, even if only for the purpose of "browsing."

6. Users will not deliberately attempt to disrupt the computer system's performance or destroy data by spreading computer viruses or by any other means. These actions are illegal.

7. Users will not use the district system to engage in any illegal act, such as arranging for a drug sale or the purchase of alcohol, engaging in criminal gang activity, threatening the safety of a person, etc.

8. Users will not attempt to access websites blocked by district policy, including the use of proxy services, software, or websites.

9. Students will not attempt to access non-instructional district systems, such as student information systems or business systems.

10. Users will not use sniffing or remote access technology to monitor the network or other users' activity.

11. Users will not use any wired or wireless network (including third-party internet service providers) with equipment brought from home. Examples include using a home computer or laptop on the network or accessing the Internet from any device not owned by the district.

12. Users will not use district equipment, networks, or credentials to threaten employees or students or disrupt the educational program.

13. Users will not possess published or electronic material designed to promote or encourage illegal behavior, or that could threaten school safety, or use the Internet or school websites to encourage illegal behavior or threaten school safety.

14. Users will not use the district equipment, network, or credentials to send or post electronic messages that are abusive, obscene, sexually-oriented, threatening, harassing, damaging to another's reputation, or illegal.

Technology Protection Measure (Internet Filtering)

The district has selected a technology protection measure (SonicWall content filtering) for use with the district's Internet system. The filtering technology will always be configured to protect against access to material that is obscene, illegal (i.e., child pornography), and material that is harmful to minors, as defined by the Children's Internet Protection Act. The district or individual schools may, from time to time, reconfigure the filtering software to best meet the educational needs of the district or schools and address the safety needs of the students. Furthermore, the GoGuardian content filtering client also monitors the student laptops to facilitate filtering for in-district and home use of district resources.

The district technology department will conduct an annual analysis of the effectiveness of the selected filter and will make recommendations to the Superintendent regarding its selection and configuration.

The filter may not be disabled at any time that students are using the district internet system if such disabling will cease to protect against access to prohibited materials under the Children's Internet Protection Act. However, the filter may be disabled during non-student use time for system administrative purposes.

Filtering technology has been found to inappropriately block access to appropriate material. To ensure that the implementation of the technology protection measure is accomplished in a manner that retains district control over decision-making regarding the appropriateness of the material for students, does not unduly restrict the educational use of the district Internet system by teachers and students, and ensures the protection of students' constitutional right to access to information and ideas. Educators can contact the network/campus administrator to unblock access to sites blocked by the filter.

Building administrators will be granted authority to unblock access. Individuals granted authority to unblock sites must meet necessary technical proficiency standards to ensure the system's security. The technology department shall determine such standards.

To unblock a site, the authorized individual must review its content outside of the presence of any student before allowing access to the site by a student.

Reports of all instances of unblocking will automatically be forwarded to the technology director.

Board Approved: