TECHNOLOGY USE – INTERNET SAFETY PRACTICES AND PROCEDURES

Students are offered access to GSTEMA's technology for educational purposes related to the curriculum and education program. All uses of technology, including mobile devices, computers, software, and other technology related materials are the property of GSTEMA and are intended for the educational goals of the curriculum and education programs. The use of technology is a privilege and the students are expected to act responsibly when using equipment or accessing information through the Internet. Access to technology will be revoked if there is inappropriate use by the student.

GSTEMA will support opportunities to educate students and parents about appropriate online behavior, including interacting with others online, communicating on social networking websites and in chat rooms, and will provide opportunities for students to gain knowledge about cyber bullying and how to respond or report incidents.

Guidelines

1. **Privacy**: GSTEMA reserves the right to monitor use of technology accessed by students, staff, parents, and partners, including the right to retrieve and review any data composed, sent, received, or stored using technology networks and Internet connections, including e-mail. There is no expectation of privacy when using GSTEMA technology equipment or systems no matter where it is utilized.
2. **Cyber Bullying:** GSTEMA prohibits cyber-bullying, an act involving the use of information and communication technologies, including but not limited to e-mail, text messages, blogs, instant messages, personal web sites, on-line social directories and communities (e.g. Facebook Twitter, YouTube), video-posting sites, and online personal polling web sites, to support deliberate or repeated hostile behavior, by an individual or group, that is intended to defame, harm, threaten, intimidate, or harass students, staff members, parents, and partners, or the school during or outside school hours and on or off school premises.
3. **Usage:** Students are not to install or download any hardware, software, shareware, or freeware onto any media or network drives. Software installed by anyone other than the network administrator will be removed. Downloading of non-work related files is permitted only with an instructor's permission. Student may not copy other people's work or intrude into other people's files. All copyright laws must be respected.
4. **Access:** Use of language or accessing information that is profane, abusive, pornographic, obscene, and/or material inappropriate for the age of the user is not permitted. Unintended or accidental access should be reported to the teacher or school leader immediately. Intentional circumvention of web-filtering is prohibited. All users must have proper authorization to access the technology systems of GSTEMA. Students will be given a username and password and should not share that login information with others or allow others to login with their identification. Students must log off the computer when they are

finished with their work. Students should notify their teacher or school leader immediately if their password is compromised.

5. **Equipment Usage:** Students must not attempt to damage or destroy equipment or files. Students are responsible for GSTEMA equipment issued to them. In the event the student leaves GSTEMA or upon request by a teacher or school leader, assigned equipment must be surrendered immediately. Students must return all GSTEMA property that is in their possession. Where permitted by applicable law(s), GSTEMA will pursue reimbursement for equipment not returned upon departure or request.

   Prior to students being issued access to equipment, parents and students will be required to sign a Technology Usage Form. In the event the equipment is lost or damaged, a report needs to be filed immediately in the school office. GSTEMA does not warrant any damage to data. Students should delete their files and materials they no longer need only after checking with their teacher.

6. **Printing Resources:** Due to the expense of materials, students must obtain permission from the teacher before printing documents.

The resources available through the Internet will be integrated into student instruction. Student usage of technology and access to the Internet is permitted only in the presence and supervision of staff, the child's parent, or other designated adult school personnel. Neither GSTEMA nor our staff is responsible for the accuracy or quality of information obtained through the Internet or through GSTEMA's technology system. Some material accessible via the Internet contains illegal, defamatory, inaccurate, or potentially offensive language or images. While GSTEMA uses Internet resources to achieve educational goals, there is always a risk of students accessing other materials. However, the advantages of using technology surpass the disadvantages. Staff members will be trained in the appropriate use of technology with students, but ultimately parents of students are responsible for setting and conveying the expectations regarding the use of media and information sources at home and school.

The Children's Internet Protection Act (CIPA) is a federal law enacted by Congress to address concerns about access to the Internet and other information. Under CIPA, schools and libraries must certify that they have certain safety measure in place in order to apply for e-rate funding.

The protection measures must block or filter Internet access to pictures that are: (a) obscene; (b) child pornography; or (c) harmful to minors (for computers that are accessed by minors). Before adopting this Internet safety policy, schools and libraries must provide reasonable notice and hold at least one public hearing or meeting to address the proposal.

Schools subject to CIPA have two additional certification requirements: 1) their Internet safety policies must include monitoring the online activities of minors; and 2) as required by the Protecting Children in the 21st Century Act, they must provide for educating minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, and cyber bullying awareness and response.

Schools and libraries subject to CIPA are required to adopt and implement an Internet safety policy addressing: (a) access by minors to inappropriate matter on the Internet; (b) the safety and security of minors when using electronic mail, chat rooms and other forms of direct electronic communications; (c) unauthorized access, including so-called "hacking," and other unlawful

activities by minors online; (d) unauthorized disclosure, use, and dissemination of personal information regarding minors; and (e) measures restricting minors' access to materials harmful to them.