GREGORY-PORTLAND INDEPENDENT SCHOOL DISTRICT
STUDENT ACCEPTABLE USE GUIDELINES FOR ONLINE ACCESS, TELECOMMUNICATIONS, AND OTHER ELECTRONIC DEVICES

Student:_____ **Teacher:**_____

Campus:_____ **Grade:**_____ **Date:**_____

Gregory-Portland ISD supports the use of computers, networks, and the Internet as part of the state and district curriculum in order to help facilitate teaching and learning. The use of technology is a privilege given to students who agree to act in a considerate and responsible manner. The technology is to be used for instructional purposes to include academic research, completing class assignments, communication, publishing, technology integration, state technology proficiencies, software training and any other activity supporting the Gregory-Portland ISD technology objectives. We request that students and parents or guardians read, accept and sign the following guidelines for acceptable online behavior.

The Children's Internet Protection Act (CIPA) was signed into law on December 21, 2000 and revised in October 2008. Under CIPA, no school or library may receive discounts unless it certifies that it is enforcing a policy of Internet safety that includes the use of filtering or blocking technology. This Internet Safety Policy must protect against the access, through computers with Internet Access, to visual depictions that are obscene, child pornography, or (in the case of use by minors) harmful to minors. The school or library must also certify that it is enforcing the operation of such filtering or blocking technology during any use of such computer by minors. New requirements include educating minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, in addition to cyberbullying awareness and response.[1]

Assurance:

Some material accessible via the Internet may contain items that are illegal, defamatory or potentially offensive to some people. Action has been taken by the district to block inappropriate sites and information; however, this action is not foolproof.

User Responsibilities:

- Users are responsible for good behavior on the Internet just as they are in a school building. The Student Code of Conduct for behavior and communications apply.
- Users of an issued system account will be responsible at all times for its proper use.
- Users may not use another person's system account (i.e. UserName and Password).
- Users shall use the resources in accordance to copyright law.
- Users shall protect the security and privacy of the Gregory-Portland ISD systems and network.
- Users shall respect and protect the rights of other users.
- Users shall recognize that all data is the property of the Gregory-Portland ISD and there is no expectation of privacy. Administrators will review files and communications to maintain system integrity and ensure that users are using the system responsibly.
- Users shall only bring authorized materials into the technology system.

Users are NOT permitted to:

- Utilize district technology for non-educational purposes.
- Send, display, or use offensive or obscene language, messages, or pictures.
- Use resources to harass, insult, or attack others (i.e. Cyberbullying, E-mail, construction of websites, etc). All forms of harassment of the Internet, commonly referred to as cyberbulling, are unacceptable and viewed as a violation of this Acceptable Use Policy. Cyberbullying includes, but is not limited to the following misuses of technology: harrassing, teasing, intimidating, threatening or terrorizing another person by sending or posting inappropriate or hurtful messages, or images.
- Damage or inject viruses into computers, computer systems, or computer networks.
- Install software (i.e. games, toolbars) not approved by the Technology Dept. Administrator.
- Utilize the network for buying, selling, or promotion of commercial items for private financial or commercial gain.
- Attempt to read, delete, copy or modify the electronic mail of another user.
- Use another's password or trespass in another's folder, work or files.
- Intentionally waste limited resources, including the use of "chain letters" and messages broadcasted to mailing lists or individuals.

- Reveal the personal address or phone number of yourself or any other person without permission from your teacher.
- Use/download any peer-to-peer (PTP) software such as Napster, Morpheus, etc.
- Waste system resources. Examples: Printing items that aren't educational, and downloading large files such as games, music, videos without permission
- Utilize a false identity or impersonate another person.
- Participate in any activity that violates the rights of others or interferes with the educational purpose of the district.
- By any method bypass the district security including the content filter.

Students are expected to be responsible for safe Internet communications practices outlined below:

- Never meet anyone in person whom you have met online.
- Remember to never give any personal information about yourself unless given permission from a teacher or Administrator.
- Be civil and polite online.
- Report any activity that makes you uncomfortable or if someone sends you inappropriate e-mail.
- Remember that you never really know who the other person is online.
- Notifying a teacher or technology administrator of possible security problems.
- Disclosing information concerning any information he/she knows about that are inappropriate or cause discomfort.
- The use of certain online chat rooms, wikis, blogs, forums and other Web 2.0 tools may be allowed only in controlled, teacher supervised settings, and for valid instructional purposes. All other use is inappropriate. Sites must be approved by the Curriculum Director and the Technology Department.
- If a student uses e-mail accounts and social networking sites on a school computer, the teachers must monitor all communications and have access to the students account.
- Notifying a responsible school professional if he/she mistakenly accesses inappropriate information.

District Authority and Responsibilities:

The district may revoke user privileges, remove user accounts, and refer to legal authorities when there are violations (i.e. unauthorized or inappropriate network use, breach of security, vandalism, and copyright infringement). Potential disciplinary action includes use of computers only under direct supervision, limitation or loss of access to the GPISD computer network as well as other disciplinary action up to and including expulsion. In addition, the Superintendent or designee may also take other disciplinary action on a case by case basis. Gregory-Portland offers no warranties of any kind, whether expressed or implied, for the services provided.

The district will strive to help students and teachers to learn to use technology appropriately and ethically. The October 2008 changes to the Protecting Children in the 21st Century Act added a new educational requirement to the Children's Internet Protection Act (CIPA). CIPA requires all school districts to educate students regarding cyberbullying and the appropriate online behaviors, such as interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response. Instruction may include:

- Use of information technology in the classroom
- Internet safety
- Cyberbullying
- Avoiding plagiarism
- The concept, purpose and significance of copyright so that pupils can distinguish between lawful and unlawful online downloading, and the implications of illegal peer-to-peer network file sharing.

Other District Authorities and Responsibilities include:

- The district will purchase and implement a content filter.
- The district will not be responsible for financial obligations arising from unauthorized use of the system.
- The district cannot guarantee that information or other content accessed from the Internet is not harmful, nor is the District liable if the accessed content should be harmful.
- The district may limit, restrict or extend computing privileges and access to its resources on a case by case basis.
- The district reserves the right to determine which network services will be provided through school district resources.
- The district reserves the right to deny computer privileges to any user identified as a security risk or having a history of problems with other computer systems. The determination of risk shall be the responsibility of a district administrator.
- The district reserves the right to examine any user files, should the security of a computer system be threatened or unacceptable use is suspected.
- The district reserves the right to view and monitor all applications provided by the district through the network, including e-mail and everyday technology usage.

- The district shall not be responsible for student information that is lost, damaged or unavailable due to technical problems or user error.
- The district specifically denies any responsibility for the accuracy or quality of information available on the Internet and does not imply endorsement of the content.
- The district reserves the right to determine if any activity not appearing in this document constitutes an acceptable or unacceptable use of the computer facilities or network resources.

Disciplinary Action:

The use of technology resources is a privilege, not a right. Improper use may result in any of the following disciplinary actions depending on the severity of the violation, including but not limited to any of the following:

- Disciplinary actions regarding inappropriate student behavior will be determined at the building level consistent with existing practices.
- Restriction from using District Technology may be for a length of time ranging from one day to a year.
- Loss of the privilege of having a network account or Internet access.
- Required to pay for any unauthorized expenses or damages.
- Users may face additional disciplinary action consistent with the District Code of Conduct as determined by the Superintendent or designee.

*Teachers or Administrators may sign on restricted users to allow students to fulfull the Technology TEKS.

Higher level violations may carry stricter consequences depending on the situation. Higher level violations may include:

- Use of the computer/equipment in any way that may harass, defame or demean others with language, image or threats.
- Attempt to use or discover anyone else's password.
- Write, produce, generate, copy, propagate, or attempt to introduce any computer code designed to self-replicate, damage, or otherwise hinder the performance of any part of the technology system (i.e. bug, virus, worm, Trojan Horse).
- Assemble or disassemble computers/equipment without written authorization from the Technology Department.
- Attempts to harm or destroy district equipment or data, or any other agencies' equipment or data.
- Purposely access or post (say or send) materials that are abusive, obscene, sexually-oriented, threatening, harassing, damaging to another's image, or illegal.
- Hack or alter programs or files belonging to other users. For example, changing, erasing or renaming anyone else's files, programs, email or disks.

GPISD Wireless Infrastructure:

Principals may allow students to bring their own technology devices (laptops, smart phones, eReaders, iPads, etc.) to use at specific times during the school day. Student use of these devices requires teacher permission in the classroom. Principals may also designate certain areas for personal technology devices to be used. These designated areas may include the cafeteria, library, auditorium, or other areas to be determined by the principal. If devices are allowed, principals will notify parents and students of these designated areas.

Students are required to use the GPISD wireless infrastructure where available. Students using their personal cellular Internet service instead of the school wireless infrastructure are subject to discipline as outlined in the AUP and Student Handbook. Campus Administrators have the authority to grant permission to use personal Cellular Internet Service in designated time and places on campus. Students must abide by the rules listed on the AUP(Acceptable Use Policy) regarding any network connected equipment.

The GPISD technology department will not maintain or configure any non-district equipment. Students are responsible for maintaining and/or configuring the BYOD (Bring your Own Device) to the GPISD wireless network. Once devices recognize the wireless network, users must sign in with their network user id and password. Internet usage will be monitored and filtered to meet Federal regulations.

GPISD will not be responsible for any lost, broken, or stolen personal equipment. GPISD is not responsible for any phone charges that cellphone accounts may accrue while in use on school property.

Electronic Mail

A user is responsible for all e-mail originating from the user's ID or password.

- Forgery or attempted forgery of e-mail messages is illegal and is prohibited.
- Unauthorized attempts to read, delete, copy or modify e-mail of other users are prohibited.
- Users are prohibited from sending unsolicited electronic mail to more than 5 addresses per message, per day, unless the communication is a necessary, employment-related function or an authorized publication. Users should not send or perpetuate pyramid-generating messages, like chain letters and any other "Send this important message to everyone you know!!!" gimmicks.
- All users must adhere to the same standards for communicating online that are expected in the classroom and that are consistent with district policies, regulations and procedures.

District's Disclaimer of Liability:

The District shall not be liable for users' inappropriate use of electronic communication resources or violations of copyright restrictions or other laws, users' mistakes or negligence, and costs incurred by users. The District shall not be responsible for ensuring the accuracy, age appropriateness, or usability of any information found on the Internet. Users should not expect that files stored on school or district based machines, including e-mail messages from school computers to be private. The contents of files can be reviewed by technology personnel for purpose of system maintenance, problem solving, to investigate an instance of believed violation of district guidelines, or simply to randomly check the system for user compliance, or any other purpose.

STUDENT ACCEPTABLE USE GUIDELINES FOR ONLINE ACCESS

Student Agreement:

I have read the guidelines for acceptable online behavior, understand the guidelines, and agree to comply with them as stated above. Should I violate the guidelines, I understand that I may lose computer privileges at my school and face additional disciplinary action up to and including expulsion.

Student Signature: _____ Date: _____

Parent/Guardian Agreement:

As the parent or legal guardian of the minor student signing above, I grant permission for the above student to access the computer based electronic communications system services such as electronic mail and the Internet. I understand that some materials on the Internet may be objectionable, but I accept responsibility for providing guidance to the above student on Internet use both inside and outside of the school-setting and conveying standards for the above student to follow when selecting, sharing, or exploring information and media. I have read the guidelines and understand them.

Parent/Guardian Signature: _____ Date: _____

Student Agreement:
I have read the guidelines for acceptable online behavior, understand the guidelines, and agree to comply with them as stated above. Should I violate the guidelines, I understand that I may lose computer privileges at my school and face additional disciplinary action up to and including expulsion.

Student Signature: _____ Date:_____

Parent/Guardian Agreement:
As the parent or legal guardian of the minor student signing above, I grant permission for the above student to access the computer based electronic communications system services such as electronic mail and the Internet. I understand that some materials on the Internet may be objectionable, but accept responsibility for providing guidance to the above student on Internet use both inside and outside of the school-setting and conveying standards for the above student to follow when selecting, sharing, or exploring information and media. I have read the guidelines and understand them.

Parent/Guardian Signature:_____ Date:_____