Greenville Independent School District
Student Responsible Use Policy for Technology

Greenville Independent School district makes a variety of communications and information technologies available to students through computer/network/Internet access. These technologies, when properly used, promote educational excellence in the district by facilitating resource sharing, innovation, and communication. Illegal, unethical, or inappropriate use of these technologies can have dramatic consequences, harming the district, its students, and its employees. These Responsible Use Guidelines are intended to minimize the likelihood of such harm by educating district students and setting standards which will serve to protect the district. The district firmly believes that digital resources, information, and interaction available on the computer/network/Internet far outweigh any disadvantages.

Mandatory Review

To educate students on proper computer/network/Internet use and conduct, students are required to review these guidelines at the beginning of each school year. All district students shall be required to acknowledge receipt and understanding of all guidelines governing use of the system and shall agree in writing to allow monitoring of their use and to comply with such guidelines. The parent or legal guardian of a student user is required to acknowledge receipt and understanding of the district's Student Responsible Use Guidelines for Technology. It is all staff members' responsibility to educate students about appropriate online behavior, including interactions with other individuals on social networking sites/chat rooms, and cyber bullying awareness and response. This may be done in a variety of ways, such as once a year short training sessions, one-on-one education with individual students, and/or via educational handouts. It is also the responsibility of all staff members to monitor students' online activity for appropriate behavior.

Definition of District Technology System

The district's computer systems and networks (system) are any configuration of hardware and software. The system includes but is not limited to the following:

- Telephones, cellular telephones, and voicemail technologies;
- Email accounts;
- Servers;
- Computer hardware and peripherals;
- Software including operating system software and application software;
- Digitized information including stored text, data files, email, digital images, and video and audio files;
- Internally or externally accessed databases, applications, or tools (Internet- or district-server based);
- District-provided Internet access;
- District-filtered public Wi-Fi; and
- New technologies as they become available.

Availability of Access

Acceptable Use

Computer/Network/Internet access will be used to enhance learning consistent with the district's educational goals. The district requires legal, ethical, and appropriate computer/network/Internet use.

Privilege

Access to the district's computer/network/Internet is a privilege, not a right.

Access to Computer/Network/Internet

Access to the district's electronic communications system, including the Internet, shall be made available to students for instructional purposes. Each district computer and public Wi-Fi (available for students who bring their own personal telecommunication devices) has filtering software that blocks access to visual depictions that are obscene, pornographic, inappropriate for students, or harmful to minors, as defined by the federal Children's Internet protection Act (CIPA). Filtered Internet access is provided to students as defined by CIPA. This filtering is provided at an account level basis.

Student Access

Computer/Network/Internet access is provided to all students unless parents or guardians request in writing to the campus principal that access be denied. Student Internet access will be under the direction and guidance of a district staff member. Students may also be allowed to use the local network and public Wi-Fi with campus permission. For students under the age of 13, the Children's Online Privacy Protection Act (COPPA) requires additional parental permission for educational software tools. Parents wishing to deny access to these educational tools must do so in writing to the Chief Information Officer indicating their child should be denied access to these tools.

Use of Personal Telecommunication Devices

The district's goal is to increase student access to digital tools and facilitate immediate access to technology-based information, much the way that students utilize pen and paper. To this end, the district will open a filtered, wireless network through which students in specific age groups will be able to connect privately owned (personal) telecommunication devices. Students using personal telecommunication devices must follow the guidelines stated in this document while on school property, attending any school-sponsored activity, or using the Greenville ISD network. Students will be required to install a security token on their personal device while on school property that will provide filtering at the appropriate level.

- **Greenville High School** – Students are allowed to bring personal telecommunication devices that can access the Internet for educational purposes as determined by the campus principal/classroom teacher. Students must be connected to the GISD-BYOD wireless network. This will provide Internet filtering as required by the federal Children's Internet protection Act (CIPA).

- **Greenville Middle School/Sixth Grade Center** – Students are allowed to bring personal telecommunication devices that can access the Internet for educational purposes as determined by the campus principal/classroom teacher. Students must be connected to the GISD-BYOD wireless network. This will provide Internet filtering as required by the federal Children's Internet protection Act (CIPA).

- **Elementary** – Students in grades K-5 are allowed to bring personal telecommunication devices for academic classroom use as determined by the campus principal/classroom teacher. Each campus will develop procedures for use and management. Students must be connected to the GISD-BYOD wireless network. This will provide Internet filtering as required by the federal Children's Internet protection Act (CIPA).

Security

A student who gains access to any inappropriate or harmful material is expected to discontinue the access and to report the incident to the supervising staff member. Any student identified as a security risk or as having violated these

Responsible Use Guidelines may be denied access to the district's system.

If a security breach or information breach is detected by GISD or third-party sources, GISD will notify students, staff, and parents of the incident. These notifications may include breaches of third-party non-GISD accounts as to promote security awareness and training to staff, students, and parents throughout Greenville Independent School district.

Other consequences may also be assigned
A student who knowingly brings prohibited materials into the school's electronic environment will be subject to suspension of access and/or revocation of privileges on the district's system, will be subject to disciplinary action in accordance with the Board-approved Student Code of Conduct, and legal action, if appropriate.

Content/Third-Party Supplied Information
Students and parents of students with access to the district's system should be aware that use of the system may provide access to other electronic communication systems in the global electronic network that may contain inaccurate and/or objectionable material.

Subject to Monitoring
Students and parents should understand that district computers, networks, user accounts, and internet usage shall not be considered confidential and is subject to monitoring by designated staff at any time to ensure appropriate use. Students should not use the computer system to send, receive or store any information, including email messages, that they consider personal or confidential and wish to keep private. GISD monitors based on account and therefore may monitor student accounts signed in at locations other than at a GISD facility as well.

All electronic files, including email messages, transmitted through or stored in the computer system will be treated no differently than any other electronic file. The district reserves the right to access, review, copy, modify, delete, or disclose such files for any purpose. Students should treat the computer system like a shared or common file system with the expectation that electronic files, sent, received, or stored anywhere in the computer system, will be available for review by any authorized representative of the district for any purpose.

Personal telecommunication devices are subject to examination in accordance with disciplinary guidelines if there is reason to believe that the Responsible Use Guidelines have been violated.

Student Computer/Network/Internet Responsibilities

District students are bound by all portions of the Responsible Use Guidelines. A student who knowingly violates any portion of the Responsible Use Guidelines will be subject to suspension of access and/or revocation of privileges on the district's system and will be subject to disciplinary action in accordance with the Board-approved Student Code of Conduct.

Use of Social Networking/Digital Tools
Students may participate in district-approved social media learning environments related to curricular projects or school activities and use digital tools, such as, but not limited to, mobile devices, blogs, discussion forums, RSS feeds, podcasts, wikis, and on-line meeting sessions. The use of blogs, wikis, podcasts, and other digital tools are considered an extension of the classroom. Verbal or written language that is considered inappropriate in the classroom is also inappropriate in all uses of blogs, wikis, podcasts, and other district-approved digital tools.

Use of System Resources
Students are asked to purge email or outdated files on a regular basis. GISD reserves the right to purge data as needed to maintain responsible use of district resources.

Password Confidentiality
Students are required to maintain password confidentiality by not sharing their password with others. Students may not use another person's system account. It is highly recommended that students use separate passwords for services as to promote password security.

Reporting Security Problem
If knowledge of inappropriate material or a security problem on the computer/network/Internet is identified, the student should immediately notify the supervising staff member. The security problem should not be shared with others.

The following guidelines must be adhered to by students using a personally-owned telecommunication device at school:

- Internet access is filtered by the district on personal telecommunication devices in the same manner as district- owned equipment. If network access is needed, connection to the filtered, wireless network provided by the district is required.
- These devices are the sole responsibility of the student owner. The campus or district assumes no responsibility for personal telecommunication devices if they are lost, loaned, damaged or stolen and only limited time or resources will be spent trying to locate stolen or lost items.
- These devices have educational and monetary value. Students are prohibited from trading or selling these items to other students on district property, including school buses.
- Each student is responsible for his/her own device: set-up, maintenance, charging, and security. Staff members will not store student devices at any time, nor will any district staff diagnose, repair, or work on a student's personal telecommunication device.
- Telecommunication devices will not be used as a factor in grading or assessing student work.
- Students who do not have access to personal telecommunication devices will be provided with comparable district-owned equipment or given similar assignments that do not require access to electronic devices.
- Telecommunication devices are only to be used for educational purposes at the direction of a classroom teacher or as stated for specific age groups.
- Campus administrators and staff members have the right to prohibit use of devices at certain times or during designated activities (i.e. campus presentations, theatrical performances, or guest speakers) that occur during the school day.
- An appropriately-trained administrator may examine a student's personal telecommunication device and search its contents, in accordance with disciplinary guidelines.

Inappropriate Use

Inappropriate use includes, but is not limited to, those uses that violate the law, that are specifically named as violations in this document, that violate the rules of network etiquette, or that hamper the integrity or security of this computer/network/Internet system or any components that are connected to it.

The following actions are considered inappropriate uses, are prohibited, and will result in revocation of the student's access to the computer/network/Internet.

Violations of Law
Transmission of any material in violation of any federal or state law is prohibited. This includes, but is not limited to:

1. threatening, harassing, defamatory or obscene material;

2. copyrighted material;
3. plagiarized material;
4. material protected by trade secret; or
5. blog posts, Web posts, or discussion forum/replies posted to the Internet which violate federal or state law.

Tampering with or theft of components from district systems may be regarded as criminal activity under applicable state and federal laws. Any attempt to break the law using a district computer/network/Internet account may result in prosecution against the offender by the proper authorities. If such an event should occur, the district will fully comply with the authorities to provide any information necessary for legal action.

Modification of Computer
Modifying or changing computer settings and/or internal or external configurations without appropriate permission is prohibited. Modifying the physical computer is prohibited at all times.

Transmitting Confidential Information
Students may not redistribute or forward confidential information without proper authorization. Confidential information should never be transmitted, redistributed or forwarded to outside individuals who are not expressly authorized to receive the information. Revealing personal information about oneself or others, such as, but not limited to, home addresses, phone numbers, email addresses, or birthdates is prohibited.

Vandalism/Mischief
Any malicious attempt to harm or destroy district equipment, materials, or data; or the malicious attempt to harm or destroy data of another user of the district's system, or any of the agencies or other networks to which the district has access is prohibited. Deliberate attempts to degrade or disrupt system performance are violations of district policy and administrative regulations and may constitute criminal activity under applicable state and federal laws. Such prohibited activity includes, but is not limited to, the uploading or creating of computer viruses.

Vandalism as defined above is prohibited and will result in the cancellation of system use privileges.
Students committing vandalism will be required to provide restitution for costs associated with system restoration and may be subject to other appropriate consequences. [See the Student Code of Conduct.]

Intellectual Property
Students must always respect copyrights and trademarks of third-parties and their ownership claims in images, text, video and audio material, software, information and inventions. The copy, use, or transfer of others' materials without appropriate authorization is not allowed.

Copyright Violations
Downloading or using copyrighted information without following approved district procedures is prohibited.

Plagiarism
Fraudulently altering or copying documents or files authored by another individual is prohibited.

Impersonation
Attempts to log on to the computer/network/Internet impersonating a system administrator or district employee, student, or individual other than oneself, will result in revocation of the student's access to computer/network/Internet.

Illegally Accessing or Hacking Violations

Intentional or unauthorized access or attempted access of any portion of the district's computer systems, networks, or private databases to view, obtain, manipulate, or transmit information, programs, or codes is prohibited. Engaging in any hacking activities or providing district information to others that threaten the confidentiality, integrity, or availability of the district's resources are violations in which are punishable by the Student Code of Conduct as well as by law.

File/Data Violations
Deleting, examining, copying, or modifying files and/or data belonging to other users, without their permission is prohibited.

System Interference/Alteration
Deliberate attempts to exceed, evade or change resource quotas are prohibited. The deliberate causing of network congestion through mass consumption of system resources is prohibited.

Email and Communication Tools

Email and other digital tools such as, but not limited to blogs and wikis, are tools used to communicate within the district. The use of these communication tools should be limited to instructional, school-related activities, or administrative needs.

All students are issued Office 365 and Google accounts. Students should check email frequently, delete unwanted messages promptly, and stay within the email server space allocations. Email attachments are limited to 25MB or smaller. Internet access to personal email accounts is not allowed. Students should keep the following points in mind:

1. **Perceived Representation**
Using school-related email addresses, blogs, wikis, and other communication tools might cause some recipients or other readers of the email to assume that the student's comments represent the district or school, whether that was the student's intention.

2. **Privacy**
Email, blogs, wikis, and other communication within these tools should not be considered a private, personal form of communication. Private information, such as home addresses, phone numbers, last names, pictures, or email addresses, should not be divulged. To avoid disclosing email addresses that are protected, all email communications to multiple recipients should be sent using the blind carbon copy (bcc) feature.

3. **Inappropriate Language**
Using obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful language in emails blogs, wikis, or other communication tools is prohibited. Sending messages that could cause danger or disruption, personal attacks, including prejudicial or discriminatory attacks are prohibited.

4. **Political Lobbying**
Consistent with State ethics laws, district resources and equipment, including, but not limited to, emails, blogs, wikis, or other communication tools must not be used to conduct any political activities, including political advertising or lobbying. This includes using district email, blogs, wikis, or other communication tools to create, distribute, forward, or reply to messages, from either internal or external sources, which expressly or implicitly support or oppose a candidate for nomination or election to either a public office or an office of a political party or support or oppose an officeholder, a political party, or a measure (a ballot proposition). These guidelines prohibit direct communications as well as the transmission or forwarding of emails, hyperlinks, or other external references within emails, blogs, or wikis regarding

any political advertising.

5. Forgery

Forgery or attempted forgery of email messages is prohibited. Attempts to read, delete, copy or modify the email of other system users, deliberate interference with the ability of other system users to send/receive email, or the use of another person's user ID and/or password is prohibited.

6. Junk Mail/Chain Letters

Generally students should refrain from forwarding emails which do not relate to the educational purposes of the district. Chain letters or other emails intended for forwarding or distributing (spamming) to others is prohibited.

Student Email Accounts and Electronic Communication Tools

Electronic communication is an important skill for 21st Century students. By providing this tool, the district is equipping students with the skills necessary for success in the business. All students are given access to a district created Office 365 and Google account. These accounts are set up with the student's user ID.

Students must abide by the guidelines established at Email and Communication Tools. Student email accounts will be available for use while they are currently enrolled in the district. Parents wishing to deny access to district email must do so in writing to the Executive Director of Technology. Student email accounts may be provided directly by the district, through the content management system of an approved online course, or through a district-approved provider.

Consequences of Agreement Violation

Any attempt to violate the provisions of this agreement may result in revocation of the student's access to the computer/network/Internet, regardless of the success or failure of the attempt. In addition, school disciplinary and/or appropriate legal action may be taken.

Denial, Revocation, or Suspension of Access Privileges

With just cause, the System Administrator and/or building principal, may deny, revoke, or suspend computer/network/Internet access as required, pending an investigation.

Warning

Sites accessible via the computer/network/Internet may contain material that is illegal, defamatory, inaccurate or controversial. Each district computer/mobile device with Internet access has filtering software that blocks access to visual depictions that are obscene, pornographic, inappropriate for students, or harmful to minors, as defined by the federal Children's Internet Protection Act. The district makes every effort to limit access to objectionable material; however, controlling all such materials on the computer/network/Internet is impossible, even with filtering in place. With global access to computers and people, a risk exists that students may access material that may not be of educational value in the school setting.

Disclaimer

The district's system is provided on an "as is, as available" basis. The district does not make any warranties, whether expressed or implied, including, without limitation, those of merchantability and fitness for a particular purpose with respect to any services provided by the system and any information or software contained therein. The district does

not guarantee that the functions or services performed by, or that the information or software contained on the system will meet the system user's requirements, or that the system will be uninterrupted or error free, or that defects will be corrected. Opinions, advice, services, and all other information expressed by system users, information providers, service providers, or other third-party individuals in the system are those of the providers and not the district. The district will cooperate fully with local, state, or federal officials in any investigation concerning or relating to misuse of the district's electronic communications system.