Student Acceptable Use Policy Agreement

The School District of Greenville County provides computer, network, e-mail, and Internet access to students as part of the learning environment. While these systems have the power to deliver a huge number of resources to our classrooms, their ability to serve students depends on the responsible and ethical use of them by every student.

GCS may install software and/or hardware to monitor and record all information system resources, usage, including e-mail and Web site visits. The district retains the right to record or inspect any and all files stored on district systems.

Students shall have no expectation of privacy with respect to district information system resource usage. Students are advised that serious disciplinary action may result from evidence of prohibited activity obtained through monitoring or inspection of electronic messages, files, or electronic storage devices. Illegal activity involving district information system resource usage may be referred to appropriate authorities for prosecution.

"Acceptable use" of these systems is use that is consistent with the instructional goals of the District. If you break "acceptable use" rules, you may lose the privilege to use both classroom computers and/or the Internet. Further disciplinary and/or legal action may be taken at the discretion of school administration.

The District takes reasonable precautions by using filtering software to keep inappropriate Internet sites and e-mail out of the classroom. The District does not supervise individual e-mail accounts, a Parent Portal is available that permits the supervision of your child's e-mail account.

Please note that parents may choose for their child not to have access to the Internet at school; however, students who do not have access to the Internet will not be able to access e-mail or web based programs that teachers may be using in class. Your child has agreed to the terms and conditions of this document upon acceptance of the school district handbook. Violation of any of the terms or conditions will result in disciplinary action and/or involvement of law enforcement.

Treat computer equipment with care and respect – Willful destruction of any computer equipment or software will be considered vandalism, and may warrant the involvement of local law officials.

Parents and guardians, by you and your child agreeing to this acceptable use policy you will insure that GCS computer equipment is handled with care and respect. Only GCS ETS personnel are allowed to repair or modify GCS computer equipment hardware and software.

Do not add, modify, repair, remove, reconfigure or otherwise tamper with any device on the network infrastructure including, but not limited to: wireless network devices, workstations, printers, servers, cabling, switches/hubs, routers, etc

Do not perform unauthorized access, use, or attempt unauthorized access or use of District information systems.

"Hacking tools" Hacking tools" which may be used for "computer hacking" as defined in the South Carolina Computer Crime Act, may not be possessed on any district premise or run or loaded on any district system. Do not use school computers for illegal activities such as planting viruses, hacking, or attempted unauthorized access to any system. This is an automatic recommendation for expulsion.

Do not use a cell phone or PDA to access the Internet on school premises.

Any written text, graphics or executable files created, downloaded, displayed, or exchanged with another student or teacher must be for education-related purposes only.

Do not bypass or attempt to bypass any of the District's security or content filtering safeguards.

Do not use school computers for commercial purposes.

Follow copyright laws at all times – See District copyright policies for more information. If you have questions about the legality of using software, text, graphics, or music you find online, ask your teacher or media specialist for guidance.

Keep your password secret – You will be held responsible for all computer activities associated with your password.

For example, if you share your password with your friend and he/she signs on as you and breaks one of the rules outlined above, you will be held responsible.

Do not allow another person to use the computer under your district login.

All online communication must be polite and not threatening or offensive in any way – All students in grades 3-12 are issued e-mail accounts. The District has the right to review any e-mail sent or received using District equipment and e-mail accounts. E-mail accounts should be used for educational and district purposes only.

Do not give out personal information or photos through online communications (i.e. e-mail, cell phone, PDA, etc). Never give out your phone number, social security number, full name, age, home address, or any other personal information.

Home directories are provided to students for educational related work. Students should not store personal or non-school related work in home directories. The District reserves the right to review the contents of a student's home directory.

Please contact your school if you do not want your child to have access to the Internet and e-mail.

"Internet Safety Policy" (Staff and Students)

This rule includes provisions to address access by minors to inappropriate matter on the Internet and World Wide Web; the safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communication; unauthorized access, including so-called "hacking" and other unlawful activities by minors online; unauthorized disclosure, use, and dissemination of personal identifications regarding minors; and measures designed to restrict minors' access to materials harmful to minors.

A. General Access

The smooth operation of the network, Internet, and e-mail services relies on the proper conduct of the end users who must adhere to strict guidelines. These guidelines are provided so that students and staff are aware of their responsibilities when using these technologies. In general, this requires efficient, ethical, and legal utilization of the network resources. Because access to the network provides connections to other computer systems located all over the world, users (and parents of students who are users) must understand that neither the District nor any District employee controls the content of the information available on the systems. Every effort will be made by the District to monitor and restrict ready access to known objectionable sites; however, the District does not condone the use of controversial of offensive materials and cannot be held responsible for such use.

B. Technology Protection Measures

In compliance with the Children's Internet Protection Act ("CIPA"), 47 U.S.C. § 254 (h), the District uses technological devices designed to filter and block the use of any of the District's computers with Internet access to retrieve or transmit any visual depictions that are obscene, child pornography, or "harmful to minors" as defined in the CIPA. Though the district makes reasonable efforts to filter such Internet content, the district cannot warrant the effectiveness of its Internet filtering due to the dynamic nature of the Internet

Adult users of a District computer with Internet access may request that the "technology protection measures" be temporarily disabled by the chief building administrator of the building in which the computer is located for bona fide research purposes or other lawful purposes not otherwise inconsistent with this administrative rule.

C. Education, Supervision, and Monitoring

It shall be the responsibility of all district school staff to educate, supervise, and monitor appropriate usage of online computer network and access to the Internet in accordance with this policy, CIPA, and the Protecting Children in the 21st Century Act.

D. Terms and Conditions of Use

1. Acceptable Use

The purpose of the District's educational network is to support research and education by providing access to unique resources and the opportunity for collaborative work. All use of the network, Internet, and e-mail services must be in support of education and research and consistent with the educational objectives of the District. Use of other networks or computing resources must comply with the guidelines governing those networks. Transmission of any material in violation of any federal or state laws or regulations is prohibited; this includes, but is not limited to, copyrighted material, threatening or obscene material, or material protected by trade secret. Access to computer systems, personally assigned district computing devices, and networks owned or operated by the District imposes certain responsibilities and obligations on users and is subject to District policies and local, state, and federal laws. Acceptable use is always ethical, reflects honesty, and shows restraint in the consumption of shared resources. It demonstrates respect for intellectual property, ownership of information, system security mechanisms, and the individual's rights to privacy and freedom from intimidation, harassment, and unwarranted annoyance.

2. Procedures for Use

1. Administrators and teachers may access the Internet or e-mail for educational or work-related purposes at any time, which is not disruptive and does not interfere with the performance of other responsibilities by the employee.
2. The District will notify parents/guardians about the District network, related safety issues, and issues governing its Internet through a general letter to all parents. Parental permission is not required for use of the Internet, but parents will be notified they have the right to file a Parent/Guardian Denial Form available from the school principal if they do not want their child(ren) to have access to Internet resources.
3. A student's parent of guardian must sign a Student E-mail Account Agreement in order for that student to be granted an individual e-mail account. The parent/guardian may withdraw approval at any time through a written request directed to the student's teacher or principal.
4. All computer, Internet usage and e-mail usage by District employees and students must be consistent with the Greenville County School District mission and policies.

3. Rules Governing Use

Permitted Uses of Internet and E-mail

- **Users** will utilize the system for educational and professional or career development activities only, except as permitted in Article III (F).
- **Users** may download text and other non-executable files attached to e-mail messages or from the Internet for school-related business only.
- **Users** will check their e-mail frequently, delete unwanted messages promptly, and stay within their e-mail quota. Be aware that the system administrator may delete e-mail at any time.

General Prohibitions

- **Users** may not use the District system for commercial purposes, defined as offering or providing goods or services or purchasing goods or services for personal use. Greenville County School District will not be responsible for any obligations resulting from any unauthorized use of the system.
- **Users** may not use the system for political activities.
- **Users** will not post chain letters or engage in spamming. Spamming is sending an unnecessary message to a large number of people.

Personal Safety

- **Students** will not post or e-mail personal contact information about themselves or other people unless it is in conjunction with a specific teacher-approved assignment or approved college/career communication. Personal contact information includes address, telephone number, school address, etc.
- **Students** will not agree to meet with someone they have met online without their parent/guardian's approval.

- **Students** will promptly disclose to an administrator, teacher, or other school employee any message they receive that is inappropriate or makes them feel uncomfortable.

Illegal Activities

- **Users** will not attempt to gain unauthorized access to the e-mail system, the District Web pages, or any other computer systems through Greenville County School District e-mail and/or Internet and/or network access. Users will not attempt to perform functions that exceed their authorized access. This includes attempting to log in through another person's account or access another person's files. These actions are illegal.
- **Users** will not make deliberate attempts to disrupt the computer system performance or destroy data by spreading computer viruses or by any other means. These actions are illegal.
- **Users** will not use the District system to engage in any other illegal act, such as arranging for a drug sale or the purchase of alcohol, engaging in criminal gang activity, threatening the safety of another person, or any other activity that violates existing District policies or procedures. Reference to such activities will not even be made in a joking manner or as a prank.
- **The District** will notify law enforcement should illegal activities take place.

System Security

- **Users** will not share their account information (User ID and/or password) or attempt to log in to another user's account. Any sharing of User ID or password will result in immediate restriction or removal of account privileges. The only potential exception is the sharing of information with IT staff if requested for troubleshooting purposes.
- **Users** will immediately notify the IT staff if they have identified a possible security problem (students should notify a teacher and/or principal). Do not actively seek security problems but immediately report any potential issues that are found.
- **Users** will not download or install any unauthorized software or install any unauthorized hardware.
- **Users** will not run any executable files attached to an e-mail message.
- **Users** will not knowingly use portable data storage devices, which contain viruses or in any other way knowingly spread computer viruses.

Use of Appropriate Language - Restrictions against inappropriate language may apply to public messages, private messages, and material posted on Web pages.

- **Users** will not use obscene, profane, lewd, vulgar, rude, inflammatory, threatening, disrespectful, or gang related language or symbols.
- **Users** will not post or e-mail information, which could cause damage or a danger of disruption.
- **Users** will not engage in personal attacks, including prejudicial or discriminatory remarks.
- **Users** will not harass another person. Harassment is persistently acting in a manner that distresses or annoys another person. If a user is told by a person to stop sending messages, he/she must stop.
- **Users** will not use any language in an e-mail that threatens another person, whether it is the recipient of the message or a third party.
- **Users** will not knowingly or recklessly post false or defamatory information about a person or organization.

Access to Inappropriate Material

- **Users** will not use the District system to access or send material that is profane, lewd, vulgar, indecent, libelous, or obscene, e.g., pornography, that advocates illegal acts, or that advocates violence or discrimination towards other people, e.g., hate literature.
- **Adult Users** who mistakenly access inappropriate information or images should immediately report this to ETS. This will initiate proceedings to have the materials blocked.
- **Students** who mistakenly access inappropriate information or images should immediately report this to the attending teacher. ETS should be notified if it is deemed warranted. This will protect the users against an allegation that they have intentionally violated the Acceptable Use Policy.
- **Students** are expected to follow parental guidance regarding limitation of access to additional types of inappropriate materials.

Respect for Privacy

- **Users** will not repost or e-mail a message that was sent to them privately without permission from the person who originally sent the message.
- **Users** will not post or e-mail private information about another person.

E. Penalties for Improper Use

An employee who violates the terms of this administrative rule or otherwise misuses e-mail or the Internet to access or send inappropriate material will be subject to disciplinary action, up to and including discharge. In addition, the privilege of accessing the Internet and e-mail services also will be subject to cancellation. Students who violate the terms of this administrative rule or who otherwise misuses their access to e-mail or the Internet also will be subject to disciplinary action in accordance with the District Student Behavior Code. Internet and e-mail access privileges also may be cancelled. Violations of the laws of the United States or the State of South Carolina also may subject student or employee users to criminal prosecution. If a user incurs unauthorized costs, the user, as well as the user's parents if the user is a student, will be responsible for all such costs.

F. Warranty

The District makes no warranties of any kind, whether expressed or implied, for the service it is providing. The District will not be responsible for any damages suffered by any user. This includes loss of data resulting from delays, non-deliveries, misdirected deliveries, or service interruptions caused by the system's negligence, user errors, or omissions. Use of any information obtained via the Internet is at the user's own risk. The District specifically denies any responsibility for the accuracy or quality of information obtained through its services.

G. Security

Security on any computer system is a high priority, especially when the system involves many users. If a student or employee believes he/she has identified a security problem on the network, he/she must notify the administrator for the school or ETS. Do not demonstrate the problem to other users. Attempts to log on to any network as a system administrator will result in cancellation of user privileges. Any user identified as a security risk or having a history of problems with other computer systems may be subject to severe restrictions, cancellation of privileges, or other disciplinary and/or legal action.

H. User Privacy

E-mail messages sent or received via a District-issued e-mail account and all other electronic files created using District resources or stored with District resources are property of the District. The District reserves the right to examine, restrict, or remove any material that is on or passes through its network, just as it does any other work or material generated or brought to school by staff or students. Access to electronic information related to any student or staff member will be governed by the same policies that would apply to that information if it were not in electronic form.

I. School Board Policies

All documents on the District's server(s) must conform to Board policies and regulations, as well as established school guidelines. Copies of Board policies are available on Board Docs. Persons developing or maintaining Web documents are responsible for complying with these and other policies. Some of the relevant issues and related Board policies include the following:

1. Electronic transmission of materials is a form of copying. As specified in District policy, no unlawful copies of copyrighted materials may be knowingly produced or transmitted via the District's equipment, including its Web server(s).
2. Documents created for the Web and linked to District Web pages must meet criteria for use as an instructional resource.
3. Any links to District Web pages that are not specifically curriculum-related must meet the criteria established in the District Internet Authorized Use policy. Any other non-curricular materials should

be limited to information about other youth activities, agencies, or organizations which are known to be non-sectarian, exclusively devoted to community interests or child welfare, non-profit, and non-discriminatory. Web page links may not include entities whose primary purpose is commercial or political advertising.

4. All communications via District Web pages will comply with the District Acceptable Use for Network, Internet, and E-mail Services Policy and the District Student Behavior Code. Offensive behavior that is expressly prohibited by this policy includes religious, racial, and sexual harassment and/or violence.

5. Any student information communicated via District Web pages must comply with District policies on Data Privacy and Public Use of School Records.

6. Links to external websites (e.g. blogs, forums, social networking sites, non-instructional sites) from a district/school/teacher website or from a district e-mail signature are prohibited.

7. Blogs or forums used for instruction must reside on district web servers.

8. Personal blogs and social networking sites must not link to any district web site or district e-mail address.

J. OTHER

1. Material on a Web page reflects an individual's thoughts, interests, and activities. Such Web pages do not, in any way, represent individual schools or the District, nor are they endorsed or sanctioned by any individual school or the District. Concern about the content of any page(s) created by students or staff should be directed to the building principal of that school or to that school's media specialist.

2. Given the rapid change in technology, some of the technical standards outlined in this rule may require change throughout the year. Such changes will be made with approval of the Superintendent. This rule may be updated on an annual basis or more frequently if required

VI. Access Control Rule

Public information is available at the GCS web site, and Internal Use Only information is available on the GCS internal web sites without a login. Access to Confidential or other sensitive information is granted only when a legitimate business need has been demonstrated and access has been approved in advance by the information Owner. Access to special hardware and software must be restricted based on business need. Education Technology Services ("ETS") will develop and maintain specific written procedures regarding access control.

VII. Systems Application and Development Rule

ETS will develop and maintain specific written procedures for systems application and development. All systems and applications development and/or changes must adhere to GCS security policies, rules, and standards.

VIII. Education Technology Systems Operations Rule

ETS shall develop and maintain specific written procedures for systems operations, including system security.

IX. Information System Procurement Rule

A formal risk assessment shall be performed for all GCS information system procurement and grants. This risk assessment shall be used by ETS to determine the controls needed to mitigate risk to acceptable levels or to deny the purchase or grant.