Responsible Use of Electronic Media for Personnel, Intern/Student Teachers, Substitute Teachers, Volunteers, and Vendors (Version 07102014)

The following document outlines guidelines for use of the computing systems and facilities located at or operated by Gwinnett County Public Schools (GCPS). The definition of GCPS information and data resources will include any computer, server or network, or access provided or supported by GCPS, including the Internet. Use of the computer facilities includes the use of data/programs stored on GCPS computing systems, data/programs stored on CD-ROMs, DVD-ROMs, computer peripherals, or other storage media, that is owned and maintained by GCPS. The "user" of the system is the person requesting an account (or accounts) in order to perform work in support of the GCPS program or a project authorized for GCPS. The purpose of these guidelines is to ensure that all GCPS technology users share the GCPS technology resources in an effective, efficient, ethical and lawful manner.

The Board recognizes that electronic media, including the internet, provides access to a wide variety of instructional resources in an effort to enhance educational opportunities. Use of electronic resources must be in support of, and consistent with the vision, mission and goals established by the Gwinnett County Board of Education and for the purpose of AKS instructional support or administrative functions. All users of the district wide area network and/or other electronic informational services must maintain strict compliance with all applicable ethical and legal rules and regulations regarding access.

As a GCPS employee, volunteer, or vendor, you will be expected to maintain appropriate passwords to obtain access for your job and/or tasks. All GCPS-issued passwords should be changed within one week of issuance by the user if the application enables the user to do so. Not all applications allow this, but the applications where the password should be changed immediately include Active Directory, Lotus Notes, GCPS Portal, and SASI, should you be provided with these resources. Passwords should be changed every 90 days thereafter to maintain the integrity of the GCPS network.

Login information, usernames, and passwords are confidential. YOU are responsible for keeping logins secure. At no time should someone log in with your user name or password, and you should not use someone else's information. Students should never log into a teacher or staff member's computer; this must be done by the teacher or staff member.

Additionally, GCPS technology and electronic resources must not be used to:
- Harm other people.
- Interfere with other people's work.
- Use a computer to steal property.
- Gain unauthorized access to other people's files or programs.
- Gain unauthorized access to on-line resources by using someone else's password.
- Make changes to the hardware or software configuration of any machine, without following local school procedures for approval.
- Improperly using the network, including introducing software viruses and/or bypassing local school or office security policies.
- Steal or damage data and/or computers and network equipment.
- Access, upload, down load, and distribute pornographic, hate-oriented, profane, obscene, or sexually explicit material.

Failure to follow these guidelines can violate the Official Code of Georgia, OCGA, Codes 16-9-90, 16-9-91, 16-9-92, and 16-9-93, as well as United States Public Law 106-554, known as the Children's Internet Protection Act. Such use can also lead to disciplinary actions, up to and including termination of employment or contract with GCPS and criminal prosecution.

At no time should student names be broadcast or disclosed in unauthorized communications sent outside the GCPS network. For example, a teacher-initiated progress report sent through email to a parent is appropriate, but posting individually-identifiable student testing data on a non-GCPS website is not appropriate. Teachers should closely monitor classroom activities where students are communicating outside of GCPS. Such activities might be classroom-to-classroom collaborative projects, "pen pals" and web-site-related instructional activities. At no time should student privacy be compromised in these communications, nor should students' work be delivered outside of GCPS without direct supervision of the students' teacher. Student and staff data may be transmitted periodically to educational and government entities for required business purposes, but these transmissions are managed in a secure environment to maintain student and staff confidentiality. Finally, please note that GCPS technology use is subject to auditing for legitimate purposes, as well as live monitoring where appropriate.

Signatures:

Staff Member _____ Date _____