Responsible Use of Electronic Media for Technology Team Personnel:
Central Office Technology Personnel, Technology Support Technicians, and Local School
Technology Coordinators (Version 050509)

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 accessed through GCPS computing systems, data/programs stored on CD-ROMs, DVD-ROMs, computer peripherals, or other storage media, that is owned and maintained by the 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 operate 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, 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 the GCPS Portal, Microsoft Active Directory Services, Lotus Notes, and Student Information System (SIS). 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.

Technology Team Personnel should not maintain a list of passwords unless there is a current support activity that requires the use of the user's password. Under no circumstances should a computer's administrative passwords be changed.

The access of the network for specific GCPS employee monitoring activities, commonly referred to as "sniffing" the network or eavesdropping, is not a function of the technology team in a school. The monitoring of student technology uses is within the role of the school technologists.

The Division of Information Management and Technology has been given the charge to perform network monitoring to include specific investigations. If a technology team member feels that such an investigation should occur, he or she needs to contact his/her supervising administrator, then the supervising administrator should contact the Superintendent and the Chief Information Officer.

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, data, email, or programs.
• Gain unauthorized access to on-line resources by using someone else's password.
• 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, download, and distribute pornographic, hate-oriented, profane, obscene, or sexually explicit material.

Many system administrators and central office personnel have responsibilities to maintain the network resources and networked data. The following guidelines should be enforced at all levels to protect the rights and privacy of students and employees:
• Use and disclose the users' data and information only to the extent necessary to perform the work required to assist the user or complete job-specific tasks. Particular emphasis should be placed on restricting disclosure of the data/information to those persons who have a definite need for the data in order to perform their work in assisting the user.
• Do not reproduce the GCPS employee or staff member user's data and information unless specifically permitted by the user or in conjunction with an officially authorized activity, such as an investigation. • Refrain from disclosing a GCPS employee or staff member user's data and information to third parties unless the user provides written consent. Since the GCPS network is monitored and all traffic may be subject to review, under no circumstances are passwords to be transmitted electronically in a broadcast fashion.
• Obtain an Responsible Use Policy agreement or Non-Disclosure Agreement prior to allowing individuals to access data. These may be obtained from the GCPS Division of Information Management and Technology and the Office of the Superintendent. School principals may authorize the development or creation of student password lists only, but NOT for GCPS employees. It is recommended that student password lists be maintained by specifically designated personnel, such as the LSTC, TST, and school administrators, and be treated with appropriate care to maintain privacy on the network.

Currently, specialized access exists for the Local School Technology Team, including the Local School Technology Coordinator (LSTC), the Technology Support Technician (TST) and the Media Specialist. They are charged with the responsibility of maintaining many of the rights to GCPS network resources.

In the area of technology standards, telephone communications, and network configurations, the GCPS Division of Information Management and Technology has the final right, authority, and responsibility to review enterprise practices and ultimately resolve any discrepancies with regard to issues of security and access.

As stewards of the network in schools and specific locations, technology team members are ethically charged to troubleshoot within their area of responsibility ONLY, meaning their specific school or department. To that end, at no point should a technology team member provide or use access to network resources outside of their own areas of responsibility. Great care should be taken to use email appropriately, as email communication can easily be distributed to the wrong audiences.

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. The only exceptions to this policy are those employees who, for legitimate and legally appropriate reasons, need special access to accomplish their tasks, such as with School Resource Officers. All such exceptions will have to be cleared through the chief executive of the GCPS Division of Information Management.

At no time should student names be broadcast or disclosed in communications sent outside the GCPS network. 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.

Technology team members are not immune from disciplinary action, up to and including termination of employment and legal prosecution, should infringements occur. Tampering with, deleting, or editing information or evidence that may implicate a technology team member during an investigation may also be grounds for disciplinary action.

Signatures:

Staff   Date

Member _____   _____