Hall County Schools Acceptable Use of Electronic Media for Personnel, Substitute Teachers, Volunteers, and Vendors

The Hall County Board of Education 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 Hall County Board of Education and for the purpose of 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, including The Georgia Professional Standards Commission Code of Ethics for Educators, and all regulations regarding access.

The following document outlines guidelines for use of the computing systems and facilities located at or operated by Hall County Schools (HCS). The definition of HCS information and data resources will include any computer (including handheld devices), server or network, or access provided or supported by HCS, including portal-delivered applications and the Internet. Use of the computer facilities includes the use of data/programs stored on HCS computing systems, data/programs stored on magnetic tape, floppy disk, jump drives, USB devices, CD-ROMs, DVD-ROMs, computer peripherals, or other storage media that is owned and maintained by HCS. The "user" of the system is the person requesting an account (or accounts) in order to perform work in support of the HCS program or a project authorized for HCS. The purpose of these guidelines is to ensure that all HCS technology users share the HCS technology resources in an effective, efficient, ethical and lawful manner. All users of HCS technology resources and facilities must agree to and sign the terms of this acceptable use agreement.

As a HCS employee, volunteer, or vendor, you will be expected to maintain appropriate passwords to obtain access for your job and/or tasks. All HCS 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 you to do this. Passwords should be changed every 90 days thereafter to maintain the integrity of the HCS network. If your password is compromised, request a new password through your building administrator.

Login information, usernames, and passwords are confidential. YOU are responsible for keeping logins secure. At no time should anyone 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.

You are responsible for ensuring that any computers or computing devices, diskettes, CD, memory sticks, USB flash drives, or other forms of storage media that you bring in from outside the school are virus free and do not contain any unauthorized or inappropriate files. Employees, volunteers, vendors, or students are not permitted to use their personal computer or computing devices to connect to the HCS network.

Additionally, HCS technology and electronic resources must not be used to:

- Harm other people (including cyber bullying and harassment).
- Interfere with other people's work.
- Steal property.
- Gain unauthorized access to other people's files or programs.
- Gain unauthorized access to online resources by using another individual's password.
- Make changes to the hardware or software configuration of any machine without following HCS technology department procedures for approval.

- Improperly use the network, including introducing software viruses and/or bypassing local school or office security policies.
- Gain personal profit by selling of goods or property in a business or personal environment.
- Solicit or distribute political information or materials.
- Steal or damage data and/or computers and network equipment.
- Download copyrighted software, music, or images, or violate any copyright laws.
- Access, upload, download, or distribute pornographic, hate-oriented, profane, obscene, sexually explicit material, or other inappropriate material.

Under no circumstances are users to upload/install any materials, program, files, or applications onto HCS computers, network equipment, or any computer systems without obtaining prior written consent of a HCS technology coordinator.

Failure to follow these guidelines may violate Georgia Laws related to computer crimes as set forth in the Official Code of Georgia, O.C.G.A. 16-9-90, 16-9-91, 16-9-93, and 16-9-93.1, as well as Title XVII of United States Public Law 106-554, known as the Children's Internet Protection Act and 20 USC 1232g, known as the Family Educational Rights and Privacy Act. Such actions can also lead to disciplinary actions, up to and including loss of access to HCS technology resources and further disciplinary actions as defined by existing HCS policies.

At no time should student names be broadcast or disclosed in unauthorized communications sent outside the HCS network. For example, teacher-initiated progress reports sent through email to a parent are appropriate, but posting individually identifiable student testing data, student pictures or video on a non-HCS website is not appropriate. Teachers should always directly supervise classroom activities, including when students are communicating outside of HCS. Such activities might be classroom-to-classroom collaborative projects, blogs, wikis, podcasts, vodcasts, networking sites, and website-related instructional activities. When utilizing web instructional resources such as, but not limited to blogs, wikis, networking sites, all posts must be teacher moderated and when possible provide closed or invitation only access. At no time should student privacy be compromised in these communications, nor should a student's work be delivered outside of HCS without direct supervision of the student's 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.

Employees who bring privately owned computers/other technology devices used in HCS environments are personally responsible for the equipment. Responsibility for the maintenance and repair of the equipment rests solely with the owner of the equipment. Any damage or theft to the equipment is the responsibility of the owner of the equipment. Software residing on privately owned computers must be privately owned and properly licensed. All devices must include up-to-date anti-virus software.

District technicians and/or school-based personnel will not service or repair privately owned hardware or software. No internal components belonging to the district shall be placed in any personal equipment, whether as enhancements, upgrades or replacement.

All HCS technology use is subject to auditing, as well as live and archived monitoring where appropriate. All deleted email is archived for 14 days. Users should have no expectation of privacy when using HCS computers, network, or equipment.

_____ _____

Employee Signature Date