Fulton City School District
Electronic Information Resources Acceptable Use Policy
Faculty and Staff Regulation

Electronic information resources form a global information infrastructure used by educators, businesses, the government, the military, and organizations. In school and libraries, electronic information resources can be used to educate and inform. As such, electronic information resources are similar to books, magazines, video, CD-ROM, and other information sources.

Faculty/staff access to both hardware and software may be provided at a level above that given to students. Not only does this mean that faculty/staff shall have greater control over the system, but that their access shall carry with it a greater burden of responsibility.

Fulton City School District provides access to electronic mail and the Internet for school district business and/or educational purposes. Every effort is made to maintain the integrity of the system but at times users may experience errors or interruptions in service while accessing the district networks. The district is not liable for any losses or damages resulting in corrupted data or inability to access data. Precautions are taken to protect networked computers from viruses however the district does not guarantee that media brought out of the district are virus free and is not liable for any delays or damages caused by them.

Scope

This regulation applies to **all** District employees and other authorized users of the Fulton School District computer systems.

Access Rights

The Superintendent or his/her designee shall establish levels of access for users according to each employees job duties. Access for employees and other authorized users may include, but is not limited to, the right to:

- Access or submit financial and property records
- Access buildings through the use of security codes
- Access to staff data such as personnel and payroll records
- Submit reports to other governmental agencies
- Communicate with other district staff and colleagues within and outside the school district
- Access student records
- Assign and access student work

Responsibilities:

To use your account responsibly.

- Never reveal your password to anyone.

- Prohibit student access to the computer through an open teacher/staff account. Students should only use the system when logged in under their own USER ID.
- Student teachers and practicum students should only use the system when logged in under their own USER ID.
- Substitute teachers (excluding long term replacement substitutes) are not authorized to use the district network. Students under their supervision should not be accessing the network.
- Never logon under your User ID and allow someone else to access the network.
- Logoff the network when leaving the machine unattended.

To see to it that hardware and software under his/her supervision is being used responsibility:

- Do not assign courseware to students who have not been taught to operate it properly.
- Do not allow students to operate hardware until they have been properly trained in its use.
- Carefully preview any materials, software and Internet sites before providing access or distributing to students. It is important that material of an inappropriate nature not be passed along to students, or be made available to students, even if inadvertently.
- Do not request installation of software on your computer that is not licensed to the school as it may place you in violation of copyright laws. The Technical Support Personnel may install software purchased by individual teachers on building machines only if the media becomes the property of the school district and remains in the possession of the building Technology Teacher Assistant/Aide, except for CD-ROM's required to run the program.
- Do not allow or provide unsupervised access to electronic information resources. Open searches on the Internet should only be conducted by students when the teacher is providing one-on-one supervision.
- Student teachers and practicum students should be involving students in Internet activities only under the direct supervision of their master teacher. The master teacher **must** be in the room at all times while students are on the Internet.
- Substitute teachers shall not have access to the Internet and should never be conducting an Internet activity with the students.

To use the system responsibly.

- Do not send or forward without authorization confidential school district information or confidential information about district employees or students.
- Do not use electronic communications to distribute materials or otherwise promote, or solicit other system users on behalf of commercial ventures, political or religious causes, charitable organizations, or other causes or groups.
- Do not send any electronic communications that cause the district to incur liability, such as ordering goods, unless specifically authorized.
- Do not access or display materials that are profane or obscene; or condone violence or discrimination towards other people or other inappropriate materials.
- Provide appropriate supervision of students when accessing the Internet, including students using e-mail and other forms of direct electronic communications.
- Provide instruction to your students regarding the District's requirements, expectations and student's obligations when accessing the Internet. Notify your students that they are not to reveal personal information without authorization including last name, address, and phone number when using e-mail, chat rooms and other forms of direct electronic communications.
- The use of chat rooms is limited to teacher directed activities on educational sites that use ID's and passwords or other means to control access. The use of chat software such as AOL Instant Messenger, Yahoo Chat, MSN Chat, MS Messenger and ICQ is prohibited.

- Document incidents of inadvertent access to inappropriate material and give the documentation to the building Technology Teacher Assistant/Aide.
- Do not use the District's computer resources for personal, commercial or other inappropriate purposes (this includes personal e-mail). Unauthorized software and/or files may be removed without notice.
- Request and distribute materials through electronic means appropriately. The use of mass emails places huge demands on network resources and should be used only with permission of your supervisor. Staff should forward any email communication intended for a large group of people such as the entire building or all district staff, to their supervisor (in the case of teachers to their building principal) who will then forward the email to the appropriate audience at their discretion. Union Officials, when communicating official union business, are not required to seek the permission of their district supervisors.
- Do not have any expectation of privacy with regard to e-mail or anything stored on Fulton district equipment. All files and data on district machines become the property of the Fulton School District. Inappropriate usage of files or messages shall result in disciplinary action. Messages relating to or in support of illegal activities shall be reported to the authorities and you may be liable for civil and criminal consequences.
- Use only the e-mail program that is authorized and has been set-up by the district for staff use. The use of Free Mail or Internet Service Provider Mail (e.g. AOL, Yahoo, Hot Mail) is prohibited.
- The use of streaming audio and video places huge demands on network resources and should be used with discretion. Please use streaming audio and video in a responsible manner and not in a frivolous manner that wastes network resources (bandwidth, storage space, etc.). Students should access, download and store video and audio files with their teacher's permission only.
- Do not attempt to bypass any network security measures. Accessing the district network from outside using remote access, a program such as PC Anywhere or Virtual PC, is prohibited.
- To prevent infection by viruses, delete e-mail with attachments if it is from someone you do not know.
- Do not use the system to engage in illegal activities, you may be liable for civil and criminal consequences.
- Do not load software on district machines. All software shall be installed district technical support personnel. After installation all media (diskettes/CD-ROM's) shall remain in the possession of the Technology Teacher Assistant/Aide, locked in a suitable location, except for CD-ROM's required to run the program.

Rewritten: October 7, 2004
Approved: November 9, 2004