

TECHNOLOGY USAGE POLICY

MISSION:

The mission of the School System is to provide an education using the best teaching techniques resulting in the use of basic, life, technological, and other necessary skills. These skills will enrich the total individual and instill a respect for the freedoms provided by our society, ultimately preparing each student to successfully meet the challenges of our rapidly changing world.

INTRODUCTION:

To ensure that students receive a quality education and that employees are able to work in a professional and intellectually stimulating environment, it is the policy of the School System to provide all students and employees with access to a variety of technology resources.

The creation of a large and varied technology environment demands that technology usage be conducted in legally and ethically appropriate ways, consistent with the Mission Statement and instructional goals of the School System.

Thus, it is the intention of the School System that all technology resources will be used in accordance with any and all School System policies and procedures as well as local, state, and federal laws and/or guidelines governing the usage of technology and its component parts. Additionally, it is implied that all students and employees of the School System will use the provided technology resources so as not to waste them, abuse them, interfere with or cause harm to other individuals, institutions, or companies.

- The administrators of each school will be responsible for establishing specific practices to enforce this policy at individual schools and to create a local policy for his or her school's unique situations.
- Parents and guardians of students are responsible for giving written permission for students to use the Internet and for the system to publish the student's name, picture, or schoolwork on the Internet. They are expected to discuss this policy with their children and to place upon the student a "parental expectation" of correct behavior when using technology resources.
- Teachers and any employee responsible for supervising students will provide general supervision of students while students are using technology resources in the employee's area of responsibility. When any employee leaves his or her area of responsibility, technology resources will be secured to the maximum extent possible to prevent unauthorized use. Students may not use technology resources unsupervised.
- This policy will be prominently displayed in all rooms throughout the system that contain one or more computers.
- This policy applies to all users that include K-12 students, employees, guests, community education teachers, and community education students.

- . All School System technology resources, regardless of purchase date, location, or fund, are subject to this policy. Computers and other technology resources purchased by individuals are subject to this policy if the computer or resource is used in any School System facility or is connected to the School System network.
- . Any questions about this policy, its interpretation, or specific circumstances shall be directed to the School System Technology Coordinator before proceeding.
- . Employees violating this policy may subject themselves to disciplinary action that could include termination, and under certain circumstances such violations could result in legal action taken against them. Users will not use the computer to engage in any illegal or criminal activity of any type.
- . For users who are not N-12 students, violations of this policy will be handled in a manner comparable to situations in which Board policy has been violated requiring disciplinary and/or legal action.
- . For N-12 students, violations of this policy constitute a Class III offense. In addition to the punishments listed under Class III, the student may lose their Internet privileges or authorization to use any and all technology resources.
- . Willful damage to a technology resource by any user will result in the user being responsible for all repair costs.
- . The School System hereby disclaims any responsibility for costs created by unauthorized use of a technology resource.

POLICY STATEMENT

The primary goal of the technology environment is to support the educational and instructional endeavors of students and employees of the School System. Resources are provided for non-commercial uses only. Use of any and all technology resources by any user is a privilege and not a right.

ACCESS:

- . An individual may only use accounts, files, software, and technology resources that are assigned to him or her.
- . Individuals may not attempt to log in to the network by using another person's account and/or password or allow someone to use his or her password to access the network, e-mail, or the Internet.
- . Individuals must take all reasonable precautions to prevent unauthorized access to accounts and data and any other unauthorized usage within and outside the School System.
- . The use of all School System technology resources is a privilege, not a right, and inappropriate or suspected inappropriate use will result in a cancellation of those privileges pending investigation.
- . The School System Technology Coordinators and/or school administrators will determine when inappropriate use has occurred and they have the right to deny, revoke, or suspend specific user accounts.

- Any user identified as a security risk may be denied access.
- Any use of technology resources that reduces the efficiency of use for others will be considered a violation of this policy.
- Users must not attempt to disrupt any computer services or data by spreading viruses, spamming or by any other means.
- Users must not attempt to modify technology resources, utilities, and configurations, or change the restrictions associated with his/her account(s), or attempts to breach any technology resources security system, either with or without malicious intent.

PRIVACY:

- To maintain network integrity and to insure that the network is being used responsibly, the School System Technology Coordinator is responsible for reviewing files and network activity. Equipment and software will be used to monitor how resources are being used and what sites on the Internet are being accessed. Due to this requirement users will have a diminished expectation of privacy when using the School System' network or other resources.
- Because communications on the Internet are, often, public in nature, all users should be careful to maintain appropriate and responsible communications.
- The School System cannot guarantee the privacy, security, or confidentiality of any information sent or received via the Internet.
- Users should be aware that the technology staff routinely monitors and performs maintenance on file servers, e-mail, workstations, the Internet, user accounts, telephones, and telephone systems. During these procedures, it may be necessary to review e-mail and/or files stored on the network.
- Users are encouraged to avoid storing personal and/or private information on the School System and/or school's technology resources.

BACKING UP SOFTWARE

- Student administrative records, media center collections, application software that maintains student records (i.e. Accelerated Reader) and accounting information must be backed up on a timely basis to disk, tape, or CD-ROM by the person primarily responsible for the information.
- The System-wide technology staff will perform backups to certain servers and other software; however, this is not the primary back up and all users are responsible for backing up personal files.

COPYRIGHT:

- Duplication of any copyrighted software is prohibited unless specifically allowed for in the license agreement and then, should occur only under the supervision and direction of the Technology Coordinator.
- A backup copy of all purchased software programs should be made and, thus, become the working copy.

FILE: IFBGC
GARB
(Continued)

- . All original copies of software programs, including those purchased with departmental funds, and hardware will be stored in a secure place.
- . If a single copy of a given software package is purchased, it may only be used in one computer at a time. Multiple loading or "loading the contents of one disk onto multiple computers," is NOT allowed.
- . If more than one copy of a software package is needed, a site license, lab pack, or network version must be purchased. The School System Technology Coordinator with the person requesting the software will be responsible for determining how many copies should be purchased.
- . The School System Technology Coordinator is authorized to sign license agreements for a school within the system. Copies of any system-wide license agreements must be signed by the School System Technology Coordinator and/or Superintendent and distributed to all schools that will use the software.
- . The School System Technology Coordinator must install all software in use on the local or wide area networks and/or individual workstations within the School System. The School System Technology Coordinator will grant exceptions to this requirement, in writing, on a case-by-case basis.
- . Users are not authorized to install software and should not purchase software without consulting the technology staff.
- . Users are not authorized to make copies of any software or data without the knowledge and permission of the School System Technology Coordinator.
- . Any questions about copyright provisions should be directed to the School System Technology Coordinator.
- . Illegal copies of software may not be created or used on school equipment.
- . The legal and ethical practices of appropriate use of technology resources will be taught to all students and employees in the system (i.e. during lab orientation, network orientation, faculty meetings, etc).
- . Web page authors will be held responsible for the contents of their pages. Do not "borrow" icons or graphics from other pages without documented permission.

ELECTRONIC MAIL:

- . Electronic mail access is for the individual's use in any educational and instructional business that he or she may conduct.
- . Personal non-commercial uses of electronic mail are permitted as long as it does not violate School System' policy and/or adversely affect others or the speed of the network.
- . Electronic mail should reflect professional standards at all time.
- . School System' e-mail accounts may not be used for political or personal gain.
- . School System' e-mail accounts may not be used for attempting or successfully sending anonymous messages.
- . School System' e-mail accounts may not be used for sending mass e-mails except for authorized messages in the conduct of the School System's business.

- . School System' e-mail accounts may not be used for posting or forwarding other user's personal communication without the author's consent.

INTERNET:

- . The intent of the School System is to provide access to resources available via the Internet with the understanding that faculty, staff, and students will access and use information that is appropriate for his/her various curricula.
- . Internet access is provided for students to allow them to conduct research.
- . Students will gain access to the Internet by agreeing to conduct themselves in a considerate and responsible manner and by providing written permission from their parents.
- . Students will be allowed to conduct independent research on the Internet upon the receipt of the appropriate permission forms.
- . Permission is not transferable, and therefore, may not be shared.
- . Resources that will be used in the classroom will be screened for content prior to their introduction.
- . All school rules and guidelines for appropriate technology usage shall apply to usage of the Internet.

INTERNET FILTERING:

- . Internet access for all users is filtered and monitored through one central point.
- . Internet access is filtered by URL, IP address and content.
- . Internet searches are filtered by keyword and content.
- . URLs and IP addresses may be added to or deleted from the list by the School System office. The staff member requesting the change is responsible for ensuring that the site is appropriate for use before requesting the site to be unblocked.
- . Software is used to track which computer has contacted which Internet site, at what time.

WEB PUBLISHING:

- . The School System' web server cannot be used for profit, commercial purposes, to express personal opinions, or to editorialize.
- . Acting on behalf of the Superintendent, the School System Technology Coordinator will periodically review all web pages that are posted on the School System web server. The School System Technology Coordinator will remove any content that is in violation of this policy or that could adversely affect students, employees, or the school system
- . Pictures and other personally identifiable information should only be used with permission in writing from the parent or guardian of the student involved. No full names should be used--only first name, last initial. No written permission is required for in-school broadcasts (i.e. morning news, announcements, class profiles, etc.)
- . All web page authors are responsible for insuring that parental permission has been granted before using a student's name (first name and last initial only), picture or schoolwork on a web page.

- . All links should be checked regularly to make sure they are current and working.
- . Pages that are not updated in a timely fashion, that contain inaccurate or inappropriate information, or contain links that do not work will be removed and the author will be notified.
- . Unfinished pages will not be posted until they are fully functional.
- . Teacher created web pages, stored on a commercial or private server, may be a link from a teacher created web page stored on the School System Internet server.
- . Student posting of personal information of any kind is prohibited. Personal information includes: home and/or school address, work address, home and/or school phone numbers, full name, social security number, etc.
- . No written permission is required to list faculty/staff and their school contact information (phone extension, e-mail address, etc.)
- . Written consent will be required for posting of any employee photographs.
- . Infringement of copyright laws, obscene, harassing or threatening materials on web sites are against the law and are subject to prosecution.

PARENTAL PERMISSIONS:

No student's name, picture, or work will be published on the Internet without written parental permission. Parental permission will be granted or denied as part of the technology use agreement. It is the responsibility of the person posting the information to determine if parental permission has been granted.

EXAMPLES OF INAPPROPRIATE USE OF RESOURCES:

The following activities are examples of inappropriate activities for any School System' computer, network, network equipment, e-mail system, or the Internet. This list is not all-inclusive. Anything that would be considered inappropriate in "paper form" is also considered inappropriate in electronic form.

- . Using another user's password or attempting to find out another user's password
- . Sharing your own password
- . Trespassing in another user's files, folders, home directory, or work
- . Saving information on ANY network drive or directory other than your personal home directory or a teacher specified and approved location
- . Downloading, installing, or copying programs or other executable software of any kind onto a workstation, your home directory, or any network drive
- . Harassing, insulting, or attacking others via technology resources
- . Damaging or altering computers, computer systems, computer networks, or network equipment (this includes changing workstation configurations such as screen savers, backgrounds, printers, BIOS information, preset passwords, etc.)
- . Attempting to interrupt the flow of data across the network
- . Intentionally wasting limited resources such as disk space and printing capacity
- . Accessing inappropriate web sites (sites containing information that is violent, illegal, satanic, lewd, pornographic, etc.)

FILE: IFBGC
GARB
(Continued)

- . Sending, displaying, or downloading offensive messages or pictures
- . Using obscene, racist, profane, discriminatory, threatening, or inflammatory language
- . Participating in on-line chat rooms without the permission or supervision of an adult staff member
- . Posting any false or damaging information about other people, the school system, or other organizations
- . Posting of any personal information about another person without his or her written consent
- . Broadcasting network messages and/or participating in sending or perpetuating chain letters
- . Violating copyright laws
- . Plagiarizing of materials that are found on the Internet
- . Using technology resources to create illegal materials (i.e. counterfeit money, fake identification, false official records, etc.)
- . Altering, attempting to alter, or allowing another to alter the setup of any server
- . Adding or attempting to add or deleting or allowing another to add or delete software, hardware, peripheral equipment from a server
- . Interrupting or attempting to interrupt or change or allowing another to interrupt or attempt to interrupt or change data flow on the network
- . Failing to properly guard against unauthorized use of a password
- . Using any School System technology resource for personal gain, commercial or political purposes
- . Using alternate Internet service provider connections to the School System's internal network unless expressly authorized and properly protected by a firewall or other appropriate security device(s)
- . Employee personal computers may not be connected to the school network
- . Non-network Internet uses by School System employees must also conform to this policy.

SOURCE: Cullman City Board of Education, Cullman, AL
ADOPTED: 2000; REVISED: Jan. 27, 2003
LEGAL REF.: The Code of Alabama, 16-11-9, 16-21-1 to 3