Guidelines for Teacher and Student access to networked information resources

Teachers and students are responsible for good behavior when using school computer networks since communications on the network are often public in nature. General school rules for behavior and communications apply. The network is provided for the teachers and students to conduct research and communicate with others; however, access to network services, i.e. Internet, will be provided to only those teachers and students who agree to act in a considerate and responsible manner.

Independent student use of telecommunications and electronic information resources will be permitted upon submission of parental permission/agreement forms (included in the Student of Conduct) signed by students and their parents/guardian, **PARENTAL PERMISSION IS REQUIRED.** Access to the Internet via School System computers is a privilege, not a right, and entails responsibility.

ACCESS:

1. Users may use only accounts, files, software, and technology resources that are assigned to him/her.
2. Users may not attempt to log in to the network by using another person's account and/or password or allow someone to use his/her password to access the network, e-mail, or the Internet.
3. Users must take all reasonable precautions to prevent unauthorized access to accounts and data and any other unauthorized usage within and outside the School System.
4. Users identified as a security risk may be denied access.
5. Any use of technology resources that reduces the efficiency of use for others will be considered a violation of this policy.
6. Users must not attempt to disrupt any computer services or data by spreading viruses, spamming or by any other means.
7. Users are not allowed to order any goods or services over the School System's network that will result in charges to the School System.
8. Users must not attempt to modify technology resources, utilities and configurations, or change the restrictions associated with his/her accounts, or attempts to breach any technology resources security system, either with or without malicious intent.
9. 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. Their decision will be final.

PRIVACY:

1. To maintain network integrity and to insure that the network is being used responsibly, local school administrators and the District System Technology Coordinator reserve the right to review files and network communications.
2. Users **should not** expect files stored on the School System network would always be private.
3. Because communications on the Internet are, often, public in nature, all users should be careful to maintain appropriate and responsible communications.
4. The School System cannot guarantee the privacy, security, or confidentiality of any information sent or received via the Internet.
5. Users should be aware that the technology staff routinely monitors and performs maintenance on file servers, email, 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.
6. Users are encouraged to avoid storing personal and/or private information on the School System and/or school technology resources.

7. The system-wide technology staff does perform routine backups of District-wide data. However, all users are responsible for storage of any critical files and/or data.
8. Student records, media center collections, and accounting information should be backed up to a disk.

ELECTRONIC MAIL:

1. The School System provides access to electronic mail for employees.
2. Access to -mail is for employee, class, and/or student use in any educational and instructional business that they may conduct.
3. Personal use of electronic mail is permitted as long as it does not violate School System policy and/or adversely affect others or the speed of the network.
4. Electronic mail should reflect acceptable standards at all time.
5. School System e-mail accounts may not be used for political or personal gains.
6. School System e-mail accounts may not be used for attempting or successfully sending anonymous messages.
7. School System e-mail accounts may not be used for sending mass e-mails.
8. School System e-mail accounts may not be used for posting or forwarding other user's personal communication without the author's consent.

Ownership of email data

The system owns all e-mail accounts and all data transmitted or stored using e-mail capabilities.

Data Retention

Individuals are responsible for saving e-mail messages as they deem appropriate. Due to finite resources, the system has the right to restrict the amount of user space on the e-mail server as necessary and to purge and remove e-mail accounts of teachers, staff and students who are no longer employed or enrolled in the system.

DATA BACKUP

The e-mail system is backed up on a regular basis as a way of recovering from a systematic loss impacting the entire email system. User files and folders are not backed up individually, and the IT staff cannot accommodate requests to restore these files or folders. While in some cases it may be possible to recover from the accidental deletion of files by a user, this is generally not feasible, and therefore each e-mail user is responsible for backing up individual messages and folders as appropriate.

APPROPRIATE USE

When using e-mail as an official means of communication, students, faculty and staff should apply the same professionalism, discretion, and standards that they would use in written business communication. Furthermore, students, faculty and staff should not communicate anything via e-mail that would not be prepared to say publicly. Students, faculty and staff may not disclose school system information in e-mail that they are privileged to access because of their position.

USER RESPONSIBILITY

The Coosa County School District maintains the school system's official e-mail system; faculty, staff and students are expected to read e-mail on a regular basis and manage their accounts appropriately. An e-mail message regarding school matters sent from an administrative office, faculty, or staff member is considered to be an official notice. Faculty, staff, or students should not use another e-mail system on the system's Network. Sharing of passwords is strictly prohibited. Each individual is responsible for his/her account, including the safeguarding of

access to the account. All email originating from an account is deemed to be authored by the account owner, and it is the responsibility of that owner to ensure compliance with these guidelines.

SPAM & VIRUS

DUE TO THE COMPLEX NATURE OF E-MAIL, IT IS IMPOSSIBLE TO GUARANTEE PROTECTION AGAINST ALL SPAM AND VIRUS INFECTED MESSAGES. IT IS THEREFORE INCUMBENT ON EACH INDIVIDUAL TO USE PROPER CARE AND CONSIDERATION TO PREVENT THE SPREAD OF VIRUSES. IN MANY CASES VIRUSES APPEAR TO BE SENT FROM A FRIEND OR CO-WORKER, THEREFORE ATTACHMENTS SHOULD ONLY BE OPENED WHEN THE USER IS SURE OF THE NATURE OF THE MESSAGE. DO NOT FORWARD THE MESSAGE.

INTERNET:

1. The intent of the School System is to provide access to resources available via the Internet with the understanding the faculty, staff, and students will access and use information that is appropriate for his/her various curricula.
2. All school rules and guidelines for appropriate technology usage shall apply to usage of the Internet.
3. Teachers will screen all Internet resources that will be used in the classroom prior to their introduction.
4. 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/guardians.
5. Students will be allowed to conduct independent research on the Internet upon the receipt of the appropriate permission forms.
6. Permission is not transferable, and therefore, may not be shared.

INTERNET FILTERING:

1. Internet access for all users is filtered, through one central point, by URL and IP address.
2. Internet searches are filtered by keywords.
3. URLs and IP addresses may be added to or deleted from the filtered list by the School System office.
4. Only administrators and staff members may request review of filtered sites.

WEB PUBLISHING:

1. The School System's web server cannot be used for profit, commercial purposes, to express personal opinions, or to editorialize.
2. All home pages will be reviewed by the local school and/or District Technology Coordinator before being added to the School System's School World Wide Web Server.
3. The Technology Staff reserves the right to reject all or part of a proposed Home page.
4. Home pages may only be placed on the Web server by a local school or School System Technology Coordinator.
5. All pages posted on the School System's web server must be written with an approved editor.
6. Each posted page must include the following: the school location, date of last update, and email address.
7. All posted work must be of publishable quality with regard to spelling, usage, and mechanics.
8. All web page authors are responsible for the maintenance of their own pages.
9. All links should be checked regularly to make sure they are current and working.
10. 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.
11. Unfinished pages should not be posted until they are fully functional.
12. Teacher created web pages stored on a commercial or private server may be linked from a teacher created web page stored on the School System Internet server.

13. Pictures and other personally identifiable information should only be used with permission in writing from the parent/guardian of the student involved. No full names should be used – only first name, last initial. No written permission is required for in-school broadcast (i.e. morning news, announcements, class profiles, etc.) Please refer to the Student Code of Conduct for clarification, and when in doubt, please ask for further clarification.
14. 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.
15. No written permission is required to list faculty/staff and their school contact information (phone extension, email address, etc.)
16. Written consent will be required for posting of any employee photographs.
17. Infringement of copyright laws, obscene, harassing or threatening materials on web sites are against the law and are subject to prosecution.

PARENTAL PERMISSIONS:

It is the responsibility of the staff posting information on the web, requesting videos, designing publicity of public relations information to obtain written parental permission prior to student access to the Internet (See the Student Code of Conduct).

EXAMPLES OF INAPPROPRIATE USE OF RESOURCES:

The following activities are examples of inappropriate activities for any School System network, 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.
1. Using another user's password or attempting to determine another user's password.
2. Sharing your own password.
3. Trespassing in another user's files, folders, home directory, or work.
4. Saving information on ANY network drive or directory other that your personal Home Directory OR a teacher specified and approved location.
5. Downloading, installing, or copying software of any kind onto a workstation, your home directory, or any network drive.
6. Harassing, insulting, or attacking others via technology resources.
7. Damaging computers, computer systems, or computer networks (this includes changing workstation configurations such as screen savers, backgrounds, printers BIOS information, preset passwords, etc.)
8. Intentionally wasting limited resources such as disk space and printing capacity.
9. Accessing inappropriate web site (sites containing information that is violent, illegal, satanic, sexual, etc.)
10. Sending, displaying, or downloading offensive messages or pictures.
11. Using obscene, racist, profane, discriminatory, threatening, or inflammatory language.
12. Participating in on-line chat rooms without the permission/supervision of an adult staff member.
13. Posting any false or damaging information about other people, the school system, or other organizations.
14. Posting any personal information about another person without his/her consent.
15. Broadcasting network messages and/or participating in sending/perpetuating chain letters.
16. Violating copyright laws.
17. Plagiarism of materials that are found on the Internet.
18. Use of technology resources to create illegal materials. (i.e., counterfeit money, fake identification, etc.)
19. Use of any School System Technology resource for personal gain, commercial or political purposes.
20. The knowing transmission of a message containing a computer virus.
21. The misrepresentation of the identity of the sender of an e-mail.