Acceptable Use and Internet Safety Policy

The Madison County Schools' electronic network is available to students and employees, and the goal is to promote educational excellence in schools by facilitating resource sharing, innovations, and communications. As the technological environment is large and varied, the use of technology by students and employees must be legal and ethical; and it should be consistent with the educational vision, mission, and goals of the Board of Education.

The use of the Madison County Schools' network is a privilege, not a right, and each user is expected to abide by the generally accepted rules of network etiquette and the provisions in this document. Violations of these provisions, or applicable laws and regulations, may result in the loss of computer services, disciplinary action to include termination of employment and/or appropriate legal action, and/or assessment of the cost of damages to hardware/software.

Violations

112 Violation of Acceptable Use Policy (AUP) and Internet Safety - Minor

a. Accessing another individual's materials, information, or files without the permission of that person;
b. Violating copyright or otherwise using the intellectual property of another individual or organization without permission
c. Using passwords other than one's own.
d. Giving out personal information on-line such as full name, home address, phone number, etc.;
e. Using software which has not been assigned or approved by staff
f. Failing to follow a district policy while using computers or failing to follow any other policies or guidelines established by district administration, teachers, or other appropriate district staff
g. Seeking to gain or gaining unauthorized access to information resources or other computing devises
h. Accessing chat rooms, and sites selling term papers, book reports and other forms of student coursework

221 Violation of Acceptable Use Policy (AUP) and Internet Safety - Intermediate

a. Accessing, uploading, downloading, or distributing pornographic, obscene, or sexually explicit material;
b. Transmitting obscene, abusive, sexually explicit, or threatening language;
c. Using the network for commercial purposes
d. Harassing, insulting, or attacking others
e. Altering the setup of computers as set by the system administrator

326 Violation of Acceptable Use Policy (AUP) and Internet Safety – Major

a. Accessing, uploading, downloading, or distributing pornographic, obscene, or sexually explicit material;
b. Vandalizing, defined as any unauthorized access and/or malicious attempt to damage computer hardware/software or networks or destroying the data of another user, including creating, uploading, or intentionally introducing viruses
c. Gaining unauthorized access ("hacking") to resources or entities
d. Invading the privacy of individuals
e. Using personal devices (Hotspots, Myfi) to circumvent the MCSS Network

419 Violation of Acceptable Use Policy (AUP) and Internet Safety – Criminal

Any of the uses named above that violate any local, state, or federal statute

The school district maintains the right to limit the content of material that students read due to legitimate pedagogical concerns.

Because the Internet contains an unregulated collection of resources, the district cannot guarantee the accuracy of the information or the appropriateness of any material that a student/employee may encounter. Therefore, before using the district's on-line resources, each student/employee (and the parents/guardians of the student) shall sign and return an Acceptable Use Agreement. Students/Employees and parents/guardians shall agree to not hold the district responsible for materials acquired on the system, for violations of copyright restrictions, users' mistakes or negligence or any costs incurred by users.

There have been cases of the Internet being used as a tool in credit card fraud, electronic forgeries, and other forms of illegal behavior. Students and employees should be aware that these activities exist, and should exercise extreme caution to prevent themselves from becoming a victim of such scams.

Although the staff will supervise student use of the Internet while at school, we encourage parents to have a discussion with their children about values and how those beliefs should guide student activities while using the Internet.

Internet Safety

General Warning; Individual Responsibility of Parents and Users. All users and their parents/guardians are advised that access to the electronic network may include the potential for access to materials inappropriate for school-aged pupils. Every user must take responsibility for his or her use of the computer network and Internet and stay away from these sites. Parents of minors are the best guide to materials to shun. If a student finds that other users are visiting offensive or harmful sites, he or she should report such use to the person designated by the School.

Personal Safety. Be safe. In using the computer network and Internet, do not reveal personal information such as your home address or telephone number. Do not use your real last name or any other information that might allow a person to locate you without first obtaining the permission of a supervising teacher. Do not arrange a face-to-face meeting with someone you "meet" on the computer network or Internet without your parent's permission (if you are under 18).
Regardless of your age, you should never agree to meet a person you have only communicated with on the Internet in a secluded place or in a private setting.

"Hacking" and Other Illegal Activities. It is a violation of this Policy to use the School's computer network or the Internet to gain unauthorized access to other computers or computer systems, or to attempt to gain such unauthorized access. Any use which violates state or federal law relating to copyright, trade secrets, the distribution of obscene or pornographic materials, or which violates any other applicable law or municipal ordinance, is strictly prohibited.

Online Behavior Education. All students will receive education about appropriate online behavior, including cyber bullying awareness and response and interacting with other individuals on social networking sites and chat rooms. This education will be provided through the implementation of the Technology Course of Study, through Internet Safety awareness and education programs at each school. In addition, educational materials and links regarding cyber bullying as well as safe and appropriate behavior will be placed on the System's website for access by parents and students.

Internet Filtering

The Madison County Schools, either by itself or in combination with the Internet Provider, will utilize filtering software or other technologies to prevent students from accessing visual depictions that are (1) obscene, (2) child pornography, or (3) harmful to minors. The School will also monitor the online activities of students, through direct observation and/or technological means, to ensure that students are not accessing such depictions or any other material that is inappropriate for minors.

Internet filtering software or other technology-based protection systems may be disabled by a supervising teacher or school administrator, as necessary, for purposes of bona fide research or other educational projects being conducted by students age 17 and older.

The term "harmful to minors" is defined by the Communications Act of 1934 (47 USC Section 254 [h] [7]), as meaning any picture, image, graphic image file, or other visual depiction that:
- taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion;
- depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors,
- an actual or simulated sexual act or sexual contact,
- an actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals;
- taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

Electronic Mail (Email)

The Madison County Schools provides access to electronic mail for all employees and for specific and selected student use. Such access is for his/her use in any educational and instructional business that they may conduct. Limited personal use of electronic mail is permitted as long as it does not violate Madison County Schools policy and/or adversely affect others.
Electronic mail shall not be used to promote political, religious, and/or personal gains. *The Board cannot guarantee the privacy, security, or confidentiality of any information sent or received via electronic mail. Network administrators can review e-mail, file folders, and communications to maintain system integrity and insure that users are using the system responsibly.*

Network Etiquette ("Netiquette")

Users of E-mail and other network services should be aware of the common expectations or network etiquette that users expect from one another.

- E-mail messages are not guaranteed to be private.
- When sending e-mail, make your "subject" as descriptive as possible.
- Do not post the personal address or phone numbers of students or colleagues.
- Check your e-mail frequently and delete it after reading it.
- Proofread and edit messages before they are sent, but be tolerant of errors in messages from others.
- Be careful when using sarcasm and humor: without face-to-face communications, a joke may not be taken the way it was intended.
- Do not publicly criticize or inflame others.
- Protect the privacy of other people.
- Messages written in all capitals are difficult to read and are the network equivalent of shouting.

Internet Publishing

Design and Development:
Project pages and other documents for publication may be designed and developed as desired by individual students, teachers, or groups as appropriate. The content of the school's/department's home page is left to the discretion of the school/department except for the required elements listed above.

Approval and Implementation:
The school principal/department supervisor is responsible for implementation of the homepage and the documents maintained on the server. The principal/supervisor is also responsible for maintaining a backup of the information so that a prompt recovery can be made in the event of corruption or loss.

Maintenance:
School principals/department supervisors are responsible for ensuring that all publications implemented by their respective areas are updated as necessary to maintain accurate and current content. This includes the regular review, testing, and modification of all links and the withdrawal of any documents that become inaccurate or irrelevant.

The Webmaster

The Webmaster will provide assistance as requested in the design and development of electronic documents. In addition, the Webmaster will monitor all Madison County Schools publications. Internet documents published by students and employees will normally reside on the system's server or a school or project server maintained by an individual school. As school principals/department supervisors are responsible for ensuring the integrity and recoverability of their respective servers, the Webmaster's role in implementation is limited to advising and assisting as requested.

Web Pages

The Internet is a worldwide system of networks, which makes a vast quantity of information and resources available to anyone who has a computer, a modem, and an Internet access account. Examples of documents, which Madison County Schools students and employees might publish on the Internet, include job vacancies, school assignment information, bus routes, student project information and other information of public interest. All web pages created by students and student organizations on the district's computer system will be subject to treatment as a district-sponsored publication.
Accordingly, the district reserves the right to exercise editorial control over such publications.

Content published via the Madison County Schools network must comply with the following regulations:

- All publications must comply with all policies and regulations of the district and all state, federal and international laws concerning copyright, intellectual property and use of computers.
- All Madison County Schools publications should reside on the district's communication network. Any exceptions must be approved by the Director of Technology.
- All content must be appropriate, decent, in good taste, and not intended to harass or demean individuals or groups.
- Correct grammar and spelling should be used.
- Publications must include a statement of copyright, when appropriate, and indicate that permission has been secured to include copyrighted materials.
- Factual information must be documentable.
- Only a student's first name will be used when publishing student work and/or pictures. Pictures that are a part of student publishing will not include any identifying information. Under no circumstances, will a student's home address or phone number be included.

- Links to other sites should be scrupulously researched to make sure that the linked site is free from objectionable material. The following disclaimer should be posted on the school's web page; “The links in this area will let you leave the school and school district site. The linked sites are not under the control of the school/district, and the school/district is not responsible for the contents of any linked site or any link contained in a linked site, or any changes or updates to such sites. The school/district is providing these links to you only as a convenience, and the inclusion of any link does not imply endorsement of the site by the school/district".
- Publications must identify affiliation with Madison County Schools.
- All publications must provide a link to the Madison County Schools home page.
- The date of creation and the date last updated are required on all publications.
- All publications must include the e-mail address of the person maintaining the page.
- All publications must include the statement, "Madison County Schools does not discriminate in admission, treatment, or access to program or activities on the basis of race, color, national origin, religious preference, disability, age, gender, sexual orientation, citizenship, non-English speaking ability, or homeless status, except as provided by the law or policy."
- Commercial use (advertisements, business logos, etc.) is prohibited. (A listing of school adopters is permitted)
- Documents should be high quality and structured for clarity and readability.
- All publications must be reviewed and approved as described below.
- Written permission must be on file for all students/employees pictures to be placed on the page.
- Permission must be granted, and on file, for all original work (poems, stories, artwork, etc.) done by students/employees that is posted on the page.

Security

Security on any computer system is a high priority, especially when the system involves many users. If you feel you can identify a security problem on the Madison County Schools network, please contact Computer Services. Do not demonstrate the problem to other users. Do not use another individual's account without written permission from that individual. Attempts to login to any system, program, or network as an administrator may result in cancellation of user privileges.

Occasionally, individuals are issued passwords in order to access programs as part of the tasks they perform. It is each individual's responsibility to protect the integrity of those passwords, and password sharing is strictly prohibited.

Any individual identified as a security risk or having a history of problems with other computer systems may be denied access.

Copyright Restrictions

All copyright laws and regulations, in all formats, including electronic-based works or processes will be enforced.

Material that may be copyrighted: "Any tangible medium of expression now known or later developed, which can be perceived, reproduced, or otherwise communicated either directly or with the aid of a machine, i.e. books, videos, pictures, etc." (Public Law 94-553 [U.S. Code 17] January 1, 1978.

Public or private educational institutions must comply with copyright laws. A 1980 amendment to the 1976 Copyright Act gives computer programs the same basic protection as other original works of authorship. All material, including graphics, available on the Internet is copyright protected unless otherwise stated. It is illegal to make or distribute copies of copyrighted material without proper authorization.

Madison County Schools licenses the use of copies of computer software from a variety of outside companies. Madison County Schools does not own the copyrighted software or it's related documentation and, except for a single copy for backup purposes or unless expressly authorized by the copyright owner(s), does not typically have the right to reproduce it for use on more than one computer, unless district licenses have been obtained.
Madison County Schools students/employees are not permitted to install their personal copies of any software on the system's computers unless specifically authorized by the licensee. Madison County Schools students/employees are not permitted to copy software from the system's computers and install it on home or any other computers unless specifically authorized by the licensee.

Madison County Schools employees learning of any misuse of software or related documentation within the school system shall notify the Computer Services Department. Unauthorized reproduction of software is a federal offense. Offenders can be subject to civil damages up to $100,000 per title copied and criminal penalties including fines up to $250,000 per work copied and imprisonment up to five years per title copied.

Any Madison County Schools employee, who knowingly makes, acquires, or uses unauthorized copies of computer software licensed to Madison County Schools or who places or uses unauthorized software on the system's premises or equipment shall be subject to disciplinary action, as appropriate.

Madison County Schools does not condone and specifically forbids the unauthorized duplication of software.

Electronic Communication Devices

Students are permitted to keep personal wireless devices only in locations approved by the principal or his/her designee. The Board assumes no responsibility for theft, loss, or damage to any personal/wireless communication device.

The principal or his/her designee may approve the use of such devices during medical emergencies, natural disasters, after regular school hours, at events or under circumstances in which the use of the devices serves safety, instructional, and/or convenience without disrupting academic or school operations. Principals or their designees will also have the authority to further restrict or deny the use of personal/wireless communication devices by any student to prevent the misuse, abuse, or violation of school rules regarding the use of such devices. School officials may read, examine, or inspect the contents of any such device upon reasonable suspicion that the device contains evidence of a violation of Board policy, the Student Code of Conduct, or other school rules.

Violations of this policy will be handled the same as other similar violations of policies, rules, and procedures by students in school. Personal, wireless communication devices may be confiscated from students who violate this policy and will be returned only to parents.

Alabama State Department of Education Suggested Guidelines for the Search of Digital Devices Seized During the Administration of a Secure Test

Please note that these guidelines were created with the assumption that students (and preferably parents) have been notified (verbally and in writing when at all possible) that: (1) the possession of a digital devices is strictly prohibited during the administration of a secure test; (2) if the device is used during the administration of a secure test, the device will be confiscated and is subject to a search; and (3) if the device is used during the administration of a secure test, the student's test will automatically be invalidated.

The suggested guidelines are as follows and are subject to change as testing requirements change:

1. Assuming that a student is observed in the possession of or use of a digital device during the administration of a secure test, the device will be confiscated by the test administrator. "Smart phones" and wearable devices should temporarily be turned off to help prevent any remote-access data-wipe.
2. The test administrator should deliver the device as soon as practicable to a school administrator.
3. A "chain of custody" list should be kept to record everyone who had possession of the device and when the device was transferred to someone else. The device should be stored by the school administrator in a secure location until the next step is taken.
4. For the purpose of determining whether a search of a digital device should take place, the school administrator should:
    a. Learn the facts regarding the seizure of the device from the test administrator, and
    b. Determine whether it is reasonable under all the circumstance to believe that the student could have been using the device to cheat or for some other unpermitted purpose.
5. If the school administrator determines that the student was merely in possession of the digital device then it may be returned to the student in accordance with the school system's policy.
6. If the school administrator believes that it is reasonable to suspect the student was using the device for an impermissible purpose then he or she may search the device, limiting the search to only what is necessary to reasonable determine whether the student was cheating, copying secure test information, or violating a school rule. The school administrator should follow the local policy requirements regarding the search of student property.
7. If no wrongful activity is discovered on the device then it may be returned to the student in accordance with the school system's policy.
8. If wrongful activity is discovered on the device regarding the test at issue or, if other wrongful activity is inadvertently discovered on the device, then the school administrator should secure the device in accordance with the school system's policy and notify the system test coordinator, school system attorney, or local superintendent as appropriate.
9. Following a search in which wrongful activity is discovered, and when the device is a "smart phone," the device should be turned off after the search to help prevent a potential remote-access data-wipe.
10. Any disciplinary actions should be taken in accordance with the school system's disciplinary policy.
11. Test irregularity reports should be completed in accordance with the Alabama State Department of Education's student assessment handbook.
12. In any situation involving the search and seizure of a student's property, a school administrator should consult with his or her supervisor in accordance with the school system's policy.