Appropriate Use Policy

Marion County School District

Scope

This Policy applies to all Users of district technology, including but not limited to students, faculty, and staff. It applies to the use of all district technology. These include systems, networks, and facilities administered by the MCSD Office of Information Technology, as well as those administered by individual schools and departments.

Use of district technology resources, even when carried out on a privately owned computer that is not managed or maintained by Marion County Schools, is governed by this Policy.

Policy

It is the policy of the Marion County Schools to

1. Prevent the transmission of inappropriate material via the Internet.
2. Prevent unauthorized access to materials and unlawful online activities.
3. Prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors.
4. To comply fully with the Children's Internet Protection Act.

Purpose

The Marion County School District (MCSD) is pleased to offer its student's access to the Internet. The Internet is an electronic highway connecting hundreds of thousands of computers and millions of individual users globally. This computer technology will help propel our schools through the communication age by allowing students and staff to access and use resources from distant computers, communicate and collaborate with other individuals and groups, and significantly expand their available information base.

Internet access is coordinated through a complex association of government agencies, and regional and state networks. In addition, the smooth operation of the network relies upon the proper conduct of the users who must adhere to strict guidelines. These guidelines are provided here so that you are aware of the responsibilities you are about to assume. In general, this requires efficient, ethical, and legal utilization of the network resources. If a MCSD District user violates any of these provisions, his or her account will be terminated and future access could possibly be denied.

The signature(s) at the end of this document is (are) legally binding and indicates the party (parties) who signed has (have) read the terms and conditions carefully and understand(s) their significance.

CIPA Definition of Terms:

Technology Protection Measure. The term "technology protection measure" means a specific technology that blocks or filters Internet access to visual depictions that are:

1. Obscene, as that term is defined in section 1460 of title 18, United States Code;

2. Child Pornography, as that term is defined in section 2256 of title 18, United States Code; or

3. Harmful to minors.

Harmful to Minors. - The term "harmful to minors" means any picture, image, graphic image file, or other visual depiction that:

1. Taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion;

2. 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, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and

3. Taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

Sexual Act; Sexual Contact. - The terms "sexual act" and "sexual contact" have the meanings given such terms in section 2246 of title 18, United States Code.

1. A qualifying "technology protection measure," as that term is defined in Section 1703(b)(1) of the Children's Internet Protection Act of 2000; and

   2. Procedures or guidelines developed by the superintendent, administrators and/or other appropriate personnel which provide for monitoring the online activities of users and the use of the chosen technology protection measure to protect against access through such computers to visual depictions that are (i) obscene, (ii) child pornography, or (iii) harmful to minors, as those terms are defined in Section 1703(b)(1) and (2) of the Children's Internet Protection Act of 2000. Such procedures or guidelines shall be designed to:

   a. Provide for monitoring the online activities of users to prevent, to the extent practicable, access by minors to inappropriate matter on the Internet and the World Wide Web;

   b. Promote the safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications;

   c. Prevent unauthorized access, including so-called "hacking," and other unauthorized activities by minors online;

   d. Prevent the unauthorized disclosure, use and dissemination of personal identification information regarding minors; and

e. Restrict minors' access to materials "harmful to minors," as that term is defined in Section 1703(b)(2) of the Children's Internet Protection Act of 2000.

Internet Terms and Conditions of Use

1. Users will demonstrate legal responsibility by not transmitting any material in violation of United States, Mississippi, or Marion County School District laws or regulations. This includes, but is not limited to: copyrighted materials, threatening, harassing, or obscene material, pornographic material, or material protected by trade secret.
2. Users have the responsibility to use computer resources for academic purposes only unless supervised by school staff.
3. Users may not conduct commercial activities for profit, advertise products, or conduct political lobbying on the network.
4. Users will not use the network for any illegal activity.
5. Users will not cause damage to any school equipment including hardware and software.
6. Users will not remove, exchange, or tamper with any hardware or software component from any system.
7. Users will not delete, rename, move, copy, or change any file or its properties, other than his/her personally owned files.
8. Users will not tamper with installed software and files.
9. Users will not attempt to gain access to unauthorized files.
10. Users will not damage other students' work.
11. Users will not install personal software on MCSD District technology.
12. Users will not violate copyright laws by unauthorized copying of software.
13. Users will be responsible for citing sources and giving credit to authors during the research process. All communications and information accessible via the network should be assumed to be private property.
14. Users will not install, copy, or knowingly infect a computer system with a virus.
15. Users will not use e-mail accounts for SPAM or chain letters.
16. Users will not use language that may be considered offensive, defamatory, or abusive.
17. Users will not attempt to defeat any security system.

Security

1. Users will not access the network using another user's account.
2. Users should consider their login and password private and should not reveal this information.
3. Users will not divulge information, personal or otherwise, about themselves or other users.
4. Users will immediately report to MCSD District authorities any attempt by other Internet users to engage in inappropriate conversations or personal contact.
5. Users should not expect that files stored on school-based computer to remain private. Authorized staff will periodically inspect personal folders and logs of network usage will be kept at all times.

6. Users are not allowed access to the computer operations area, and access is restricted to those responsible for operation and maintenance. No individuals are allowed in MCSD server or equipment rooms unless they are under close and immediate supervision of an IT staff member or authorized staff member. Tampering with equipment is prohibited.
7. Users consent to the use of scanning programs for security purposes by bringing any personal computers or technology onto school grounds.
8. Users consent to having user actions logged in order to facilitate recovery from system malfunction and for other management purposes.

Individual schools may create additional guidelines and procedures consistent with this policy. Such guidelines and procedures will be appropriate for the electronic information resources being used and the student served at the school. There will be consequences for any user who fails to follow MCSD District and school guidelines and policies. The consequences may include paying for damages, denial of access to technology, detention, suspension, or expulsion. In severe cases, the MCSD District will involve law enforcement authorities.

Users may not alter the MCSD network infrastructure by installing any unauthorized networking equipment including (but not limited to) hubs, switches, routers, or wireless access points of any kind without the express permission of the MCSD Information Technology Department. It is also a violation to install any devices or programs on the MCSD network or any other PC or computing device connected to the MCSD network that are designed to alter, reshape, affect, monitor, or intercept network traffic.

The MCSD Information Technology Department may terminate or limit the network connectivity of any user whose online activities are deemed detrimental to the health of the network.

1. Software Copyright Laws

The Marion county School District has made technology available to all staff and students. Computers, computer networks, the Internet, and computer software have been made available for the purpose of enhancing education in the classroom. The MCSD District is also committed to adhering to all copyright laws. All employees and students of the MCSD District are to abide by copyright laws as specified by the software's publishers and distributors.

The following rules have been put in place to ensure that no employee or student of the MCSD District violates any federal, state, or local regulation of copyright laws.

a. No software will be installed on any District computer without the proper license.
b. The only individual that signs software license agreements for the MCSD District is the Director of Technology.
c. Each department and/or school will establish a central location to store software licenses to be reviewed on demand.

d. Permission must be obtained from the MCSD District Director of Technology to duplicate any software product or distribution media.
e. Employees must receive permission from their principal and the MCSD District Director of Technology before purchasing software for District use.
f. Principals shall be responsible for enforcement of this policy at their individual school.

2. Violations

Employees who violate the United States Copyright Laws do so at their own risk and assume all liability for their actions. They shall also be subject to disciplinary action for willful infringement of the law or for using District equipment for duplication that is prohibited.

Marion County School District
Internet Safety Policy

Introduction
It is the policy of the Marion County School District to: (a) prevent user access over its computer network to, or transmission of, inappropriate material via Internet, electronic mail, or other forms of direct electronic communications; (b) prevent unauthorized access and other unlawful online activity; (c) prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; and (d) comply with the Children's Internet Protection Act [Pub. L. No. 106-554 and 47 USC 254(h)].

Definitions
Key terms are as defined in the Children's Internet Protection Act.

Access to Inappropriate Material
To the extent practical, technology protection measures (or "Internet filters") shall be used to block or filter Internet, or other forms of electronic communications, access to inappropriate information.

Specifically, as required by the Children's Internet Protection Act, blocking shall be applied to visual depictions of material deemed obscene or child pornography, or to any material deemed harmful to minors.

Subject to staff supervision, technology protection measures may be disabled for adults or, in the case of minors, minimized only for bona fide research or other lawful purposes.

Inappropriate Network Usage

To the extent practical, steps shall be taken to promote the safety and security of users of the Marion County School District online computer network when using electronic mail, chat rooms, instant messaging, and other forms of direct electronic communications.

Specifically, as required by the Children's Internet Protection Act, prevention of inappropriate network usage includes: (a) unauthorized access, including so-called 'hacking,' and other

unlawful activities; and (b) unauthorized disclosure, use, and dissemination of personal identification information regarding minors.

Education, Supervision and Monitoring

It shall be the responsibility of all members of the Marion County School District staff to educate, supervise and monitor appropriate usage of the online computer network and access to the Internet in accordance with this policy, the Children's Internet Protection Act, the Neighborhood Children's Internet Protection Act, and the Protecting Children in the 21st Century Act.

Procedures for the disabling or otherwise modifying any technology protection measures shall be the responsibility of The Technology Director or designated representatives.
The Marion County School District or designated representatives will provide age-appropriate training for students who use the Marion County School District Internet facilities. The training provided will be designed to promote the Marion County School District's commitment to:

I. The standards and acceptable use of Internet services as set forth in the Marion County School District's Internet Acceptable Use Policy;

II. Student safety with regard to:

   a. safety on the Internet;

   b. appropriate behavior while on online, on social networking Web sites, and in chat rooms; and

   c. cyberbullying awareness and response.

III. Compliance with the E-rate requirements of the Children's Internet Protection Act ("CIPA").

Following receipt of this training, the student will acknowledge that he/she received the training, understood it, and will follow the provisions of the District's acceptable use policies.

Communicating Safely Online - Use of the internet and online collaboration is an important part of being in high school. However, there are still risks involved when engaging in online conversation. Students will recognize and report any warning signs of online predators. Students will engage in safe online relationships and not participate in inappropriate dialogue with others online. Students will identify strangers and avoid risky online behavior. Students will report any inappropriate communication or possible online predators with a trusted adult.

Security of Information - Sharing of information online can be a great way to accomplish a task or work on a project collaboratively. However, there are certain bits of information that students should not share online or with others. Students will not share any of the following:
- Passwords
- Personal information/inappropriate photos of yourself
- Personal information/inappropriate photos of others

Internet Privacy - Many websites collect information from visitors for advertising or data collection purposes. Students will:

- Recognize and analyze online privacy terms.
- Understand the how and why companies collect their information so they can make informed decisions before providing personal information to a website.
- Guard against phishing, scamming and identity theft.

Research and Information Literacy

Searching - Students will use a variety of search engines to search for information and content. Students will understand the functions of effective keywords and categories to find useful and relevant information online.

Research and Evaluation - Students will choose websites with high-quality information and when possible, use multiple sources to find their information. Students will properly cite online resources. Students will be able to identify online advertisements and spam on websites and understand the purpose behind those advertisements.

Digital Citizenship

The internet is a powerful community of connected people. That connection requires levels of responsibilities to one another. Part of being a good digital citizen is using technology in a responsible, appropriate way. Digital media plays an important role in a student's life and in our society. Below are some specific areas to address with high school students when learning how to grow their digital citizenship.

Social Media & Email - Students will have access to a school email account after receiving some basic training on email etiquette. Please know that all email can be viewed by teachers, administrators, or parents. Email should be written with thought of the audience and purpose. Online school-approved social media sites are allowed. Students will learn about interaction, risks, and responsible use on both school- approved and other social media sites that they may encounter. Abuse or misuse of district email may require disciplinary action.

Commenting Responsibility - As use of social media and other age-appropriate websites becomes available to high school students, it's important for students to understand the positive and negative aspects of their digital life. Students will recognize the importance of context in posting or viewing online images. Students will post appropriate comments in online and social communities. These comments, like anything else on the internet, have a certain amount of digital permanence and can affect reputation down the road. Students will display respect and thoughtfulness online by not posting comments that are negative, inappropriate, or personal about others or themselves.

Digital Ethics - Students will use the internet and digital tools to produce content and projects. Students will not present the work of others as their ow work: (otherwise known as plagiarism) Students will not intentionally delete or damage another student's digital work.. Students will ask for permission prior to posting videos o photos of students or staff members online. When working projects or any other work with online resources, students will follow copyright and creative commons laws.

Cheating -With the use of mobile devices. there may be temptation to cheat and share test or assignment information on a non-collaborative project. Students willnot use technology and/or mobile devices to share confidential schoolconren.t with other students.

Cyberbullying - Cyberbullying is the use of digital technologies or mobile devices to harass, threaten, embarrass or torment another student. Minors can be convicted in a court of law of being a cyberbully. This can happen both directly and indirectly.
In order to avoid this students will:

- Identify strategies for dealing with cyberbullying responsibly.
- Analyze and report any offensive online behavior or interactions to a trusted adult
- Create positive online communities rooted in trust and respect.
- Think before you send or post
- Recognize and identify factors that intensify cyberbullying, including what role they play in escalating or de-escalating online cruelty

Students will NOT:
Publish information that is harmful or embarrassing to others
Facilitate in the spreading of rumors via online platforms.
Participate in online polls, “bash"sessions, or other activities that are harmful to others.

"Sexting" or other inappropriate online interactions - like cyberbullying, "sexting",or the transmission of inappropriate images or messages digitally, can result in conviction in a court of law. Students will understand. the role of digital technologies in relationships. Students will not actively participate in the sharing of inappropriate photos and/or information of themselves or others.

Self-Expression and Identity - There can be a difference between an online versus offline identity. Students need to be aware of these differences and realize that how they present themselves online can affect their relationships, sense of self, and reputations. Students will identify the risks of assuming different personas online and what it means to be genuine in an online context.

Digital Footprint –Information you post on the internet can affect your future. Colleges and fulltime employers look at an individual's digital footprint as a toolduring the admission or hiring process. Students will consider the possible benefits and risks before sharing information online and consider how this affects their reputation and digital self.

Adoption

This Internet Safety Policy was adopted by the Board of the Marion County School District at a public meeting, following normal public notice, on May 14th, 2012.