

INSTRUCTION

Student/Staff Technology Use

MONROE PUBLIC SCHOOLS

Technology Code of Conduct Administrative Guidelines

Monroe Public Schools Technology Mission

The Technology Mission Statement of the **Monroe Public Schools** is to incorporate technology into educational programs in order for the district to:

- Empower students to reach their educational and vocational goals and improve their quality of life.
- Utilize current technology to prepare all students, staff and the community for a rapidly changing global society.
- Enable problem solving, exploration and critical thinking.

District Responsibilities

Monroe Public Schools is responsible for the management of the structure, hardware and software that the district uses to allow access to information technologies for educational purposes. These include:

- Assigning and removing of member accounts on the network(s)
- Maintenance and repair of equipment
- Selection of software
- Technology Code of Conduct
- Defining the privileges/responsibilities of members
- Providing resources that support the mission of the school district within budgetary constraints
- Providing training opportunities on the use and application of information technology, including training and information on new technologies, software and media as they are acquired and put into use in the district
- Guiding students at school toward appropriate materials
- Implementation of the provisions of the federal Children's Internet Protection Act applicable to public schools.

The district does not take responsibility for members, whether staff, students, or others, who take actions or who locate resources that do not support the mission of the school district.

In addition, the Monroe Public Schools makes no warranties of any kind, whether expressed or implied, for the use of its educational technology including, but not limited to, loss of data resulting from delays, non-delivery or any service interruption. Furthermore, the Monroe Public Schools is not responsible for any damages to a user's hardware or software incurred from downloading a computer virus.

Definitions: The following definitions are used in the Administrative Guidelines.

Technology: District equipment includes but is not limited to computers, disk drives, printers, scanners, networks, video and audio recorders, cameras, photocopiers, phones, and other related electronic resources.

Software: Software includes, but is not limited to, computer software, print and non-print resources.

Networks: Networks include but are not limited to all voice, video and data systems.

Network Members: All account holders on the **Monroe Public Schools** network will be granted access to network services. The following people may hold accounts on the **Monroe Public Schools** network:

1. **Students.** Students who are currently enrolled in the district may be granted a network account upon agreement to the terms stated in the Technology Code of Conduct.
2. **Employees.** Staff members currently employed by the district may be granted a network account upon agreement to the terms stated in these guidelines.
3. **Others.** These requests will be granted on a case-by-case basis, depending on need and resource availability. If the school district makes the resources available to others, individuals or entities seeking special membership to the Monroe Public Schools' Network must complete a membership request form and must agree to abide by the terms and conditions of Network use stated in this policy. Membership will be denied for access to the Monroe Public Schools' Network for use which:
 - a. Infringes upon or compromises the legitimate educational uses of electronic information technologies.
 - b. Is prohibited by law.
 - c. Is for the purchase, sale, and/or advertisement of goods or services.
 - d. Jeopardizes resource availability for students and employees.

Cyberspace: The “area” in which computer users travel when “navigating” around on a network.

CIPA: The federal Children’s Internet Protection Act (47 USC 254).

**Privileges and Responsibilities
of Monroe Public Schools
Network Members**

Privileges

Members have the following privileges:

1. Access to available technology and network services to facilitate learning and enhance educational information exchange;
2. Use of all hardware and software authorized by the system administrator;
3. Access to information from outside resources, which meet these guidelines;

4. Use in e-mail, listserv and bulletin board communications. The Monroe Public Schools' telecommunications network is intended for legitimate school business and educational purposes only. As a monitored telecommunications network, no stated or implied guarantee is made regarding the privacy of electronic mail (E-mail) or any other telecommunications transmitted or received over this network.
5. Conditional privileges to sign up for listserves, bulletin boards and newsgroups. The criteria for these privileges require: no cost to the district or user and are limited to legitimate educational purposes which support and enhance school curriculum and business which are consistent with the mission statement.

A user's privilege to access educational technology resources may be restricted, suspended or revoked for violation of the Technology Code of Conduct. Access may also be inhibited by certain actions including, but not limited to, routine maintenance, device availability, daily schedules, course requirements, safety concerns and assignments or reassignments.

Responsibilities

Members have the following responsibilities:

1. Use of appropriate language. Profanity or obscenity will not be tolerated on the Network. All members should use language appropriate for school situations as indicated by school codes of conduct and teacher contracts;
2. Utilization of resources that support the school's mission. Keep all files free of pornographic, indecent, and other offensive materials;
3. Utilization of non-offensive and non-inflammatory speech. Members must respect the privileges of others both in the local community and in the Internet at large. Personal attacks are an unacceptable use of the network. You are to bring the incident to the attention of a teacher or school administrator;
4. Appropriate use of technology in the school. Use of the technology for private business, for product advertisement or political lobbying is prohibited;
5. Attendance at appropriate training sessions in the use and care of hardware, software and networks and refraining from using any technology for which they have not received training;
6. Following the rules established for the use of hardware, software, labs and networks in the school or through remote access outside of the school;
7. Legal use of technology. Use of technology for any illegal activities is prohibited. Illegal activities include, but are not limited to, tampering with computer hardware or software, unauthorized entry into computers, or knowledgeable vandalism or destruction of computer files. Such activity is considered a crime under state and federal law;
8. Keeping passwords private. All violations of this guideline that can be traced to an individual account name will be treated as the sole responsibility of the owner of that account. Under no conditions should you give your password to another user;
9. Maintaining the integrity of district technology. Deliberate attempts to degrade or disrupt system performance of the Network or any other computer system in cyberspace by spreading computer viruses is considered criminal activity under state and federal law;
10. Notification of threatening or unwelcome communications to a school administrator or teacher. Members must, however, be aware that there are many services available on the Internet that could potentially be offensive to certain groups of users. Monroe Public Schools cannot eliminate access

to all such services, nor could they even begin to identify them. Thus, individual users must take responsibility for their own actions in navigating the Network;

11. Ethical use of technology. Malicious use of technology to disrupt the use of technology by others, to harass or discriminate against others, and to infiltrate unauthorized computer systems is prohibited;
12. Appropriate use of e-mail, listserves, bulletin boards or newsgroups;
13. Obtaining prior approval from a school administrator or designee to develop a Web page or create a bulletin board;
14. Adherence to copyright, trademark or licensing agreement guidelines in the use of software, information, and attributions of authorship and in the transmission or copying of text or files on the Internet or from other sources;
15. Obtaining the original author's prior consent before re-posting personal communications. To re-post personal communications without the original author's prior consent is a violation of the author's privacy. However, all messages posted in a public forum such as newsgroups or listserves may be copied in subsequent communications, so long as proper attribution is given;
16. Use of real names. Impersonation, anonymity and pseudonyms are not allowed. Individuals must take responsibility for their actions and words;
17. Use of exemplary behavior on "virtual" field trips. When "visiting" locations in cyberspace, members must conduct themselves as representatives of their school and of the community as a whole;
18. Observation of safety precautions. Members must never send home addresses or home phone numbers over cyberspace, nor provide credit card or social security numbers. Once information is released in cyberspace, there is no way to limit or control its usage. It is important that members recognize that there is no such thing as total security in network communications.

Enforcement:

Use of the Monroe Public Schools' education technology is limited to legitimate education purposes which support and enhance school curriculum and business and which are consistent with the mission statement. The following uses are strictly prohibited and may subject the offender to restriction, suspension or termination of educational technology privileges and to appropriate disciplinary sanctions, such conduct to include, but not be limited to:

1. Unauthorized entry into a file, whether to use, read, change or for any other purpose.
2. Unauthorized transfer, deletion or duplication of a file.
3. Unauthorized use of another individual's identification or password.
4. Unauthorized access to telecommunications files or facilities.
5. Use of computing facilities, which interfere with the work of another student, faculty member, or school official.
6. Use of computing facilities to draft, send or receive inappropriate communications including, but not limited to, communications which are indecent, obscene, profane, vulgar, threatening, defamatory or otherwise prohibited by law.

7. Use of computing facilities, including telecommunications facilities, to interfere with the operation of the computing system.
8. Violation of copyright, trademark, trade secrets or licensing agreement.
9. Use of computing facilities for the purchase, sale, and/or advertisement of goods or services.

Monitoring and enforcement may also occur during “non-school” hours, e.g., before and after school, weekends, vacations, summer.

CIPA Special Provisions:

1. In compliance with the federal Children's Internet Protection Act (47 USC 254 (h) and (l)), not later than June 30, 2002 there shall be instituted for the School District's computers and computer network a technology protection measure that protects against Internet (which, as used in this policy, includes the World Wide Web) access by both adults and minors to material which is: obscene; child pornography, or; harmful to minors.
 - A. The term "minors" means individuals under the age of eighteen (18) years.
 - B. The term "child pornography" means any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where: 1) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; 2) such visual depiction is, or appears to be, of a minor engaging in sexually explicit conduct; 3) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct; or 4) such visual depiction is advertised, promoted, presented, described, or distributed in such a manner that conveys the impression that the material is or contains a visual depiction of a minor engaging in sexually explicit conduct.
 - C. The term "materials harmful to minors" means any communication, picture, image, graphic image file, article, recording, writing, or other matter of any kind 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 to minors.
2. The activities of students on School District computers and computer network shall be monitored by the teacher responsible for the class for which the computer activity is being conducted, and/or by School District personnel designated by the Superintendent of Schools.
3. No person shall use any School District computer, computer equipment, or School District-provided Internet connection to access sexually explicit or obscene material.
4. When using School District computers, computer equipment or Internet connections for electronic mail, chat rooms, bulletin boards or any other form of direct electronic communication, no student shall disclose any personal information (including, but not limited to, names, addresses, telephone numbers and photographs) about other students or School District staff. Students shall be discouraged from disclosing personal information about themselves in electronic mail, chat rooms, bulletin boards or any other form of direct electronic communication through the Internet.
5. School District computers, computer equipment and Internet connections shall not be used by any person to access another person's accounts, files, data or information without authorization, or for

any unlawful activity. The interference with others' accounts, files, data, or information is prohibited.

6. The School District reserves the right to monitor and review all use of its computers, computer equipment, and computer network (including, but not limited to, Internet activity and external/internal electronic mail, files and data); no user of the School District's computers, computer equipment or computer network shall have any expectation of privacy with respect to use of the School District's computers, computer equipment or computer network.
7. No person shall engage in any activity which is detrimental to the stability or security of the School District's computers, computer equipment or computer network, or use School District computers, computer equipment, or computer network in any way which is detrimental to the stability or security of others' computers, computer equipment or computer networks, including, but not limited to, the intentional or negligent introduction of viruses, or the vandalism or abuse of hardware or software.
8. No person shall use the School District's computers, computer equipment or computer network in violation of copyright laws, including, but not limited to, the installing, downloading, copying or using of copyrighted software without proper authority.
9. No person shall, in the course of using the School District's computers, computer equipment or computer network, impersonate another person or user; no person shall reveal a password of another person or user.
10. No person shall use the School District's computers, computer equipment or computer network for commercial purposes.
11. Violation of this policy may result in disciplinary action, as well as restriction, suspension or termination of access to the School District's computers, computer equipment and/or computer network. In addition, referral may be made to law enforcement authorities.

Consequences of Inappropriate Behavior:

Any member who does not comply with the Technology Code of Conduct may lose Network privileges. Repeated or severe infractions of the policy may result in permanent termination of privileges. Members will be required to make full financial restitution for any unauthorized expenses incurred or any damages caused.

The school administrator will determine what is inappropriate use based on the Technology Code of Conduct. The school administrator may close an account at any time for infractions.

Members violating any of these privileges and responsibilities may face additional disciplinary action deemed appropriate in keeping with the adopted disciplinary policies and guidelines of the school district. Discipline may include requirements for additional training sessions and/or legal action.

Challenges:

Challenges to district staff/student discipline shall be made as established by Board adopted policy.

GUIDELINES FOR STUDENT USER

The Monroe Public Schools' telecommunications network is intended for legitimate school business and educational purposes only. As a monitored telecommunications network, no expressed or implied guarantee is made regarding the privacy of electronic mail (E-mail) or any other telecommunications transmitted or received over this network.

The network is provided for students to conduct research and communicate with others. Access to network services is given to students who agree to act in a considerate and responsible manner. Access is a privilege -- not a right.

Students are responsible for appropriate behavior on school computers and networks just as they are in a classroom or on school property. Communications on the network are often public in nature. General school rules for behavior apply.

Users of the district computers and networks are responsible for their behavior and communications over those technologies. It is presumed that users will comply with district standards and will honor the agreements they have signed. At school, teachers will guide students toward appropriate materials. However, the district may not be able to restrict, monitor or control the communications of individuals utilizing the networks.

School administrators or their designee may review files and electronic communications to maintain system integrity and insure that users are using the system responsibly. Users should not expect that files stored on district servers will always be private. Outside of school, families bear the same responsibility for such guidance as they exercise with information sources such as television, telephones, movies, radio and other potentially offensive media.

As outlined in Board policy and procedures on student privileges and responsibilities (Student Code of Conduct), copies of which are available in school offices, the following are not permitted:

- Sending or displaying indecent, pornographic and/or offensive messages or pictures
- Using obscene language
- Harassing, insulting or attacking others
- Damaging computers, computer systems or computer networks or other technologies
- Violating copyright, trademark or licensing agreement laws
- Using another's password
- Trespassing in another's folders, work, mail or files
- Intentionally wasting limited resources
- Employing the network for commercial purposes
- Any other actions deemed inappropriate by the administration
- Any violation of the Children's Internet Protection Act.

Violations may result in a loss of access as well as other disciplinary or legal action.

**FOR STUDENT USE
USER AGREEMENT AND PARENT PERMISSION FORM
FOR ELECTRONIC INFORMATION TECHNOLOGIES**

We are pleased to offer students of the Monroe Public Schools learning community access to electronic information technologies including computer networks for electronic mail and the Internet. To gain access to technology, e.g., e-mail and the Information Superhighway, all students must complete the attached form and return it to their teacher. Students under the age of 18 must also obtain written parental permission. Students 18 and over must sign their own forms.

Access to electronic information technologies will enable students to explore thousands of libraries, databases and bulletin boards while exchanging messages with other network users throughout the world. Families should be warned that some material accessible via the Internet and other networks may contain items that are illegal, defamatory, inaccurate or potentially offensive to some people. While our intent is to make access available to further educational goals and objectives, students may find ways to access unacceptable materials as well. We believe that the benefits to students from access to the Information Superhighway in the form of information resources and opportunities for collaboration exceed any disadvantages, which include data security, integrity or accuracy. But ultimately, parents and guardians of minors are responsible for setting and conveying the acceptable standards that their children should follow when using media and electronic information sources.

**USER AGREEMENT AND PARENT PERMISSION FORM
FOR STUDENT USE**

As a user of Monroe Public Schools' Electronic Information Technologies, I hereby AGREE to comply with the stated guidelines - communicating over networks in a responsible fashion while honoring all relevant laws and restrictions. I am aware that the Monroe Public Schools reserves and will exercise the right to review, audit, intercept, access, and disclose all matters on the Monroe Public Schools' e-mail systems at any time, with or without notice, and that such access may occur during of after the regular school day.

Student Signature

Date

As the parent or legal guardian of the student signing above, I GRANT permission for my child to access district computer services such as electronic mail and the Internet. I UNDERSTAND that students and parents/guardians may be held liable for violations. I UNDERSTAND that some materials on networks may be objectionable, but I ACCEPT responsibility for guidance of use - setting and conveying standards for my child to follow when selecting, sharing or exploring information and media.

Parent Signature of Students under 18

Date

Name of Student

Birth date

School

FOR EMPLOYEE USE

**USER AGREEMENT FORM
FOR ELECTRONIC INFORMATION TECHNOLOGIES**

We are pleased to offer employees of the Monroe Public Schools learning community access to electronic information technologies including computer networks for electronic mail and the Internet. To gain access to technology, e.g., e-mail and the Information Superhighway, all employees must complete the attached form and return it to their supervisor.

Access to electronic information technologies will enable employees to explore thousands of libraries, databases and bulletin boards while exchanging messages with other network users throughout the world. Employees should be warned that some material accessible via the Internet and other networks may contain items that are illegal, defamatory, inaccurate or potentially offensive to some people. While our intent is to make access available to further educational goals and objectives, employees may find ways to access unacceptable materials as well. We believe that the benefits to employees from access to the Information Superhighway in the form of information resources and opportunities for collaboration exceed any disadvantages, which include data security, integrity or accuracy. But ultimately, employees are responsible for setting and conveying the acceptable standards that are expected by the school district when using media and electronic information sources.

**USER AGREEMENT AND FORM
FOR EMPLOYEE USE**

As a user of Monroe Public Schools' Electronic Information Technologies, I hereby AGREE to comply with the stated guidelines - communicating over networks in a responsible fashion while honoring all relevant laws and restrictions. I am aware that the Monroe Public Schools reserves and will exercise the right to review, audit, intercept, access, and disclose all matters on the Monroe Public Schools' e-mail systems at any time, with or without notice, and that such access may occur during of after the regular school day.

Employee Signature

Date

Employee Name (Print)

School/Department

GUIDELINES FOR EMPLOYEE USER

The Monroe Public Schools' telecommunications network is intended for legitimate school business and educational purposes only. As a monitored telecommunications network, no expressed or implied guarantee is made regarding the privacy of electronic mail (E-mail) or any other telecommunications transmitted or received over this network.

The network is provided for employees to conduct research and communicate with others. Access to network services is given to employees who agree to act in a considerate and responsible manner. Access is a privilege -- not a right.

Employees are responsible for appropriate behavior on school computers and networks just as they are in any instructional setting. Communications on the network are often public in nature. General district rules for behavior apply.

Users of the district computers and networks are responsible for their behavior and communications over those technologies. It is presumed that users will comply with district standards and will honor the agreements they have signed. However, since the district may not be able to restrict, monitor or control the communications of individuals utilizing the networks, self-monitoring is essential and expected for all employees.

School administrators or their designee may review files and electronic communications to maintain system integrity and insure that users are using the system responsibly. Users should not expect that files stored on district servers will always be private. Outside of school, employees bear the same responsibility for such guidance as they exercise with information sources such as television, telephones, movies, radio and other potentially offensive media.

As outlined in Board policy and procedures, copies of which are available in school offices, the following are not permitted:

- Sending or displaying indecent, pornographic and/or offensive messages or pictures
- Using obscene language
- Harassing, insulting or attacking others
- Damaging computers, computer systems or computer networks or other technologies
- Violating copyright, trademark or licensing agreement laws
- Using another's password
- Trespassing in another's folders, work, mail or files
- Intentionally wasting limited resources
- Employing the network for commercial purposes
- Any other actions deemed inappropriate by the administration
- Any violation of the Children's Internet Protection Act.

Violations may result in a loss of access as well as other disciplinary or legal action.

Adopted: May 28, 1996

Revised: October 9, 2001

Acceptable Use Policy Verification Statement

My signature below indicates that I have received and reviewed the Monroe Public School's Acceptable Use Policy and agree to abide by the information contained therein.

Name: _____

PLEASE PRINT CLEARLY

Assignment: _____ Bldg.: _____

Signature: _____ Date: _____

**Return to the Technology Department prior to a
User Account & Password being issued to you.**