ON-LINE SERVICES

The Internet contains material and potential contacts that could work both to the advantage and disadvantage of members of the school community. There is no system to totally control student or staff access. Like any public place where free speech is protected, the Internet presents a challenge to members of the school community who want to benefit from its resources. Members of the school community, staff and students, must be cognizant of appropriate behavior in public situations that call for judgment.

Use of the Internet/Telecommunications

The use of the network is a privilege. People using telecommunications are responsible for what they say and do on the network. Because communication with thousands of others is so quick and easy, it is important for all to think before speaking and to show respect for other people and for their ideas.

The primary use of the Internet in schools is intended for academic research and projects conducted by students and staff of the district.

District and building facilitators will make reasonable efforts to maintain reliable service and user privacy.

Any traffic from this network that traverses another network is subject to that network's acceptable-use policy.

Users must respect other users' privacy and intellectual property.

The legal rights of software producers and network providers, and copyright and license agreements, must be honored.

Privileges

1. Students and staff have the privilege of access to the Internet to facilitate diversity and personal growth in technology, information gathering skills, and communication skills related to school projects and research.

2. Students and staff may have access to the following methods for retrieving information: file transfer protocol (FTP), telnet, and electronic mail (e-mail).

3. Students and staff may request access to newsgroups and lists from Internet in order to facilitate real-time learning with members on the network. Permission is granted at the discretion of the building facilitator.

4. E-mail messaging is available at the discretion of the building facilitator.

Responsibilities

1. Students and staff are responsible for adhering to the District's policy with respect to the use of on-line technology.

2. Only those students and staff members with prior experience or instruction shall be authorized to use the Internet in school.

3. Students and staff exercising their privilege to use the Internet as an educational resource shall also accept responsibility for all material received.

4. Students and staff will not knowingly violate the privacy of others.

5. Students and staff will accept responsibility for keeping copyrighted software of any kind from entering the school via the Internet.

6. It is the students' or staff member's responsibility to make all subscriptions to newsgroups and lists known to the building facilitator. Approval is required from the building facilitator to request a newsgroup, list, or e-mail from the network.

7. Students and staff will log all file transfers while on-line.

8. Students and staff will accept responsibility for keeping all pornographic material, inappropriate text files, or files dangerous to the integrity of the network from entering the school via the Internet.

9. It is the staff member and/or building facilitator's responsibility to maintain the privacy of electronic mail.

10. The building facilitator will be responsible for placing a log book near each computer capable of accessing the network.

11. The building facilitator or teacher of classes using the Internet is responsible for determining and discovering incorrect usage of the network.

12. The building facilitator is responsible for informing the appropriate staff members (teachers and administrators) of the actions of a student in question when misconduct has been confirmed.

Consequences

1. Students and staff not adhering to this policy will be denied access to telecommunication at school.

2. Students and staff using private Internet or bulletin board accounts may be denied access to telecommunication at school.

3. In the case of a user (student or staff member) sharing his/her password and account with another user, both users will be denied access.

4. Students and staff violating this policy will be denied access to telecommunications as follows:

   a. for violating "Responsibilities" Items #4-7

      (1) first offense: access will be denied for one (1) year
      (2) subsequent offenses:

         (a) students: access will be denied for three (3) years
         (b) staff: will be subject to disciplinary action up to and including dismissal

   b. for violating "Responsibilities" Item #8

      (1) students: access will be denied for three (3) years
      (2) staff: will be subject to disciplinary action up to and including dismissal

CURRICULUM AND INSTRUCTION – ACCESS TO ELECTRONIC MEDIA

The Committee supports the right of students, employees, and community members to have reasonable access to various information formats and believes it is incumbent upon users to utilize this privilege in an appropriate and responsible manner.

Safety Procedures and Guidelines

The Superintendent or designee shall develop and implement appropriate procedures to provide guidance for access to electronic media. Guidelines shall address teacher supervision of student computer use, ethical use of electronic media (including, but not limited to, the Internet, e-mail, and other District technological resources), and issues of privacy versus administrative review of electronic files and communications. In addition, guidelines shall prohibit utilization of networks for prohibited or illegal activities, the intentional spreading of embedded messages, or the use of other programs with the potential of damaging or destroying programs or data.

Internet safety measures shall be implemented that effectively address the following:

- Controlling access by minors to inappropriate matter on the Internet
- Safety and security of minors when they are using electronic mail, chat rooms, and other forms of electronic communications
- Preventing unauthorized access, including hacking and other unlawful activities by minors online
- Unauthorized disclosure, use and dissemination of personal information regarding minors
- Restricting minors' access to materials harmful to them.

The District shall provide reasonable public notice of, and at least one (1) public hearing or meeting to address and communicate its Internet safety measures.

Permission/Agreement Form

A written parental request shall be required prior to the student being granted independent access to electronic media involving District technological resources. The required permission/agreement form, which shall specify acceptable uses, rules of on-line behavior, access privileges, and penalties for policy/procedural violations, must be signed by the parent or legal guardian of minor students (those under 18 years of age) and also by the student. This document shall be kept on file as a legal, binding document. In order to modify or rescind the agreement, the student's parent/guardian (or the student who is at least 18 years old) must provide the Superintendent with a written request.

Employee Use

Employees shall use electronic mail only for purposes related to work-related activities. Employees shall not use a code, access a file, or retrieve any stored communication unless they have been given authorization to do so. Authorization is not required each time the electronic media is accessed in performance of one's duties. Each employee is responsible for the security of his/her own passwords.

Disregard of Rules

Individuals who refuse to sign required acceptable use documents or who violate District rules governing the use of District technology shall be subject to loss or restriction of the privilege of using equipment, software, information access systems, or other computing and telecommunications technologies.

Responsibility for Damages

Individuals shall reimburse the District for repair or replacement of district property lost, stolen, damaged or vandalized while under their care.

Responding to Concerns

School officials shall apply the same criterion of educational suitability used to review other educational resources when questions arise concerning access to specific databases or other electronic media.

Audit of Use

Users with network access shall not utilize District resources to establish electronic mail accounts through third-party providers or any other nonstandard electronic mail system.

The Superintendent or designee shall establish a process to determine whether the District's education technology is being used for purposes prohibited by law or for accessing sexually explicit materials. The process shall include, but not be limited to:

1. Utilizing technology that blocks or filters Internet access for both minors or adults to certain visual depictions that are obscene, child pornography, o, with respect to computers with Internet access by minors, harmful to minors;

2. Maintaining and securing a usage log; and

3. Monitoring online activities of minors.

LEGAL REFS: 47 USC §254

CROSS REFS: IJNDB, Acceptable Use Policy – Technology

ETHICS POLICY FOR COMPUTER SYSTEMS AND INFORMATION NETWORK ACCESS

INTRODUCTION

The information networks of the District represent powerful educational resources which allow staff and students to find information anywhere in the world. Staff and students can connect to businesses, major universities, national libraries, other schools and other students around the world. The District has rules for acceptable behavior. Likewise, there are correct procedures and rules that govern the use of the information networks. If staff and students don't follow these guidelines, they may risk losing privileges to access the internet.

Students and parents will be asked to sign a statement acknowledging that they are aware of the proper procedures for using the internet.

Information networks

The District includes both stand-alone and networked computer systems. The network connects various District schools and offices. This makes sharing information and communicating with District schools and offices possible. This network supports activities which have educational value for administration, teachers and students.

The Internet is a collection of many worldwide networks that support the open exchange of information. The Internet provides immediate access to information anywhere in the world. You can look at (and print out) articles, documents and pictures that you can use in your classes. You can even get current facts about news, weather and sports.

First Steps

It is important to your teachers, your parents and your school administrators that you understand the many consequences of the computer connections that you wish to make using the information networks. It is important that you understand that your use of this educational tool is a privilege. If used properly, it can provide countless hours of exploration. Students can lose this privilege by breaking any of the network access rules.

Some parts of the Internet contain material that is not suited for students. The intent of the District is to use connections on the Internet only for purposes consistent with our approved curriculum. Anyone who uses the network illegally or improperly will lose his/her privileges. The information networks cannot be used for commercial or for-profit services. The rules defined in this document describe the proper ways to use this research tool.

Who is on the Internet?

The information networks are "public places." Students must always remember that they are sharing this space with many other users. Millions of individuals may be interacting across the network at the same time. Students' actions can be "seen" by others on the network. If students use a particular service on the network, it is likely that someone knows the connections that students are making, knows about the computer software that is being used and knows what students look at while in the system. Because these connections are granted as part of the larger scope of the curriculum, the District has the right to monitor what students do on the network to make sure that the network continues to function properly for all of its users.

Student Behavior

Students are expected to use computers and the network to pursue intellectual activities, seek resources, access libraries and other types of learning activities. We want you to explore this space and discover what is available there. We want you to learn new things and share your knowledge with your friends, your parents and your teachers.

When students are using the computer network and communicating with others, they need to keep the following in mind: (1) You cannot tell how old they are or even what sex they are; (2) They can tell you anything, and you cannot be sure what they are telling you is true; and (3) Absolute privacy cannot be guaranteed in a network environment. So, you need to think carefully about what you say and how you say it.

For your own safety and for the safety of others, remember to exercise caution when you are communicating with people anywhere. Do not share your home phone number or your address with anyone. If you feel there is a problem or if you feel uncomfortable with the information someone is giving you, tell your teacher immediately.

On the other hand, you may not harass other users. You should not run the risk of breaking the law by bothering other people. If a user on the network asks that you no longer send them mail or in any other way contact them, you must stop all contact immediately. You have the right of freedom of expression, but others have the right to be free from harassment.

Because the District's computers and information networks are used as part of a school activity, your school's code of conduct applies to computer and network activities. Therefore, the Acceptable Use Policy is an extension of your school's behavior code. These rules apply to vandalism of computer equipment, unauthorized access to information, computer piracy, hacking, and any tampering with hardware or software.

These rules apply to harassing others and using abusive or obscene language on the information networks. You may not use the network to annoy, harass, or otherwise offend other people.

The rules also apply to other types of damage or information loss on the information networks that might be caused by destructive devices such as computer viruses. If you are responsible for a computer becoming infected with viruses, worms, or any other type of destructive device, you will be held liable.

Moral and Ethical Issues

The District wants to provide you with a stimulating educational environment. At the same time, we want to protect you from information that is not appropriate for you to use.

While the District wants you to use this valuable educational tool, we do not condone the use of inappropriate information on the Internet. We acknowledge that some materials exist that are inappropriate for the instructional setting and do everything we reasonably can to prevent them from being accessed. You must clearly understand that access to such material in any form is strictly forbidden. The network is designed to achieve and support instructional goals. You should avoid any information that does not support classroom learning.

Although the actual percentage of unacceptable materials is small, it can cause concern for students and parents if a student accesses those materials while doing legitimate research. If you have a question or concern regarding any materials you find, contact your teacher of computer lab operator.

Electronic Libraries

Guidelines for access to information have already been established in the Library Bill of Rights of 1980. These principles can be applied to the Internet as well. This document states that "attempts to restrict access to library materials violate the basic tenets of the Library Bill of Rights;" however, school librarians are required to devise collections that are "consistent with the philosophy, goals, and objectives of the school district." This means that students have the right to information, but the school has the right to restrict any information that does not apply to approved curriculum.

Materials on the Internet can be considered part of a vast digital library. Electronic database and information search tools to access the Internet are becoming part of school media centers and libraries, and may public libraries offer some type of Internet access as part of their services.

Using Resources

Information networks have limited capacities. The more users there are on the network, the more congested the network becomes and access to information will take longer. The following guidelines will help ease the congestion:

- Do not tie up the network with unproductive activities.
- Do not play games with others on the network or on the Internet.
- Do not download large files unless directed to do so by your teacher.
- Download only the information you need.
- Use your access efficiently. Remember, there are many students who need to use the network.

Virtual Field Trips

The information networks offer many opportunities for "virtual field trips" to distant locations. The District considers all connections to remote locations as field trips The rules that apply to student conduct on field trips apply to these virtual electronic field trips as well. It is important that you realized that you represent your school and the school district when you use the information networks and be on your best behavior.

Legal Issues

A. The Law

In the Commonwealth of Massachusetts it is a felony to intentionally access any computer system or network for the purpose of:

1) devising or executing any scheme or artifice to defraud or extort, or
2) obtaining money, property, or services with false or fraudulent intent, representations, or promises.

It is also a felony to maliciously access, alter, delete, damage or destroy any computer system, computer network, computer program, or data. Penalties include fines and/or imprisonment. Anyone committing acts of this kind will face disciplinary action by the school and legal action by the authorities. The person will be punished to the full extent of the law.

Some examples of offenses are changing or deleting another user's account, changing the password of another user, using an unauthorized account, damaging any files, altering the system, or using the system to make money illegally. You may not cause damage to any school or District property. This includes the information networks.

B. Plagiarism

Plagiarism is "taking ideas or writing from another person and offering them as your own." Credit should always be given to the person who created the article or the idea. The student who leads readers to believe that what he/she are reading is the student's original work when it is not is guilty of plagiarism.

Be careful when you are using the information networks. Cutting and pasting ideas into your own document is very easy to do. When using someone else's work, be sure that you give credit to the author. When you do this, your teacher will know which ideas are yours, and you will not be guilty of plagiarism.

C. Copyright

According to the Copyright Act of 1976, "Fair Use" means that you may freely use any information that you legally find on the information networks as long as you so only for scholarly purposes. You may not plagiarize or sell what you find. For example, if you find a copy of *Microsoft Works* or any other commercial copyrighted or licensed software on the Internet, you may not legally copy it. These software packages must be purchased or licensed before you can legally use them. If, however, you find an article about the use of *Microsoft Works* on the Internet, you may legally copy it as long as you give credit to the author and do not sell the article for profit.

Additionally, you may not make copies of any commercial software program diskettes except for backup purposes. Illicit copying of computer software (piracy) is a felony. It is also a violation of copyright law to knowingly accept or use software or data which has been obtained by illegal means. If you need to copy something and are unsure if it's okay to do so, please ask your teacher or network administrator.

ACCEPTABLE USE POLICY - TECHNOLOGY
Administrative Procedures for Implementation

1. Commercial use of the system/network is prohibited.
2. The District will provide training to users in the proper use of the system/network.
3. The District will provide each user with copies of the Acceptable Use Policy and Procedures.
4. Copyrighted software or data shall not be placed on the District system/network without permission from the holder of the copyright and the system administrator.
5. Access will be granted to employees with a signed access agreement and permission of their supervisor.
6. Access will be granted to students with a signed access agreement and permission of the building administrator or designee(s).
7. Account names will be recorded on access agreements and kept on file at the building level.
8. Passwords will be provided by the network administrator.
9. Passwords are confidential. All passwords shall be protected by the user and not shared or displayed.
10. Students completing required course work will have first priority for after hour's use of equipment.
11. Principals or their designee will be responsible for disseminating and enforcing policies and procedures in the building(s) under their control.
12. Principals or their designee will ensure that all users complete and sign an agreement to abide by policies and procedures regarding use of the system/network. All such agreements are to be maintained at the building level.
13. Principals or their designee will ensure that training is provided to users on appropriate use of electronic resources.
14. Network Administrators or a designee shall be authorized to monitor or examine all system activities, including electronic mail transmissions, as deemed appropriate to ensure proper use of electronic resources.
15. Network Administrators or a designee shall be responsible for establishing appropriate retention and backup schedules.
16. Technology Director or a designee shall be responsible for establishing disk usage limitations, if needed.
17. Individual users shall, at all times, be responsible for the proper use of accounts issued in their name.
18. The system/network may not be used for illegal purposes, in support of illegal activities, or for any activity prohibited by District policy.
19. System users shall not use another user's account.
20. System users should purge electronic information according to District retention guidelines.
21. System users may redistribute copyrighted material only with the written permission of the copyright holder or designee. Such permission must be specified in the document or in accordance with applicable copyright laws, District policy, and administrative procedures.
22. System administrators may upload/download public domain programs to the system/network. System administrators are responsible for determining if a program is in the public domain.
23. Any malicious attempt to harm or destroy equipment, materials, data, or programs is prohibited.

24. Deliberate attempts to degrade or disrupt system performance may be viewed as violations of District policy and/or as criminal activity under applicable state and federal laws. This includes, but is not limited to, the uploading or creation of computer viruses.
25. Vandalism will result in the cancellation of system privileges and will require restitution for costs associated with hardware, software, and system restoration.
26. Forgery or attempted forgery is prohibited.
27. Attempts to read, delete, copy, or modify the electronic mail of other users or to interfere with the ability of other users to send/receive electronic mail is prohibited.
28. Use appropriate language; swearing, vulgarity, ethnic or racial slurs, and other inflammatory language is prohibited.
29. Pretending to be someone else when sending/receiving message is prohibited.
30. Transmitting or viewing obscene material is prohibited.
31. Revealing personal information (addresses, phone numbers, etc.) is prohibited.
32. The District will cooperate fully with local, state, or federal officials in any investigation concerning or relating to misuse of the District's system/network.

A user who violates District policy or administrative procedures will be subject to suspension or termination of system/network privileges and will be subject to appropriate disciplinary action and/or prosecution.

File: IJNDC

MONOMOY REGIONAL SCHOOL DISTRICT
ACCEPTABLE USE POLICY

The District recognizes that computers are used to support learning and to enhance instruction. Computer information networks allow people to interact with many other computers and networks. It is a general policy that all computers are to be used in a responsible, efficient, ethical and legal manner.

The District declares unethical and unacceptable behavior as just cause for taking disciplinary action, revoking information network access privileges, and/or initiating legal action for any activity through which an individual:

- Uses the information networks for illegal, inappropriate, or obscene purposes, or in support of such activities. Illegal activities shall be defined as those which violate local, state, and/or federal laws. Inappropriate use shall be defined as a violation of the intended use of the network, and/or purpose and goal. Obscene activities shall be defined as a violation of generally accepted social standards for use of a publicly-owned and operated communication vehicle;
- Uses the information networks for any illegal activity, including violation of copyrights or other contracts violating such matters as institutional or third party copyright, license agreements and other contracts;
- Degrades or disrupts equipment or system performance on network or standalone machines;
- Damages, destroys, or sabotages computer or communication equipment of any sort;
- Removes computer related property from school grounds without written permission;
- Uses District computing resources for commercial or financial gain or fraud;
- Steals data, equipment, or intellectual property;
- Gains unauthorized access to the files of others, or vandalizes the data or files of another user;
- Gains or seeks to gain unauthorized access to resources or entities;
- Forges electronic mail messages, or uses an account owned by another user;
- Invades the privacy of individuals;
- Posts anonymous messages; or
- Possesses any data which might be considered a violation of these rules in paper, magnetic (disk), or any other form.
- Consequence of Violations

Consequences of violations include but are not limited to:

- Suspension of information network access;
- Revocation of information network access;
- Suspension of network privileges;
- Revocation of network privileges;

- Suspension of computer access;
- Revocation of computer access;
- School Suspension;
- School expulsion; and
- Legal action and prosecution by the authorities.

Remedies and Recourses

Anyone accused of any of the violations has all the rights that would normally apply if such person were accused of school vandalism or any other illegal activity.

The District has the right to restrict or terminate information network access at any time for any reason. The District further has the right to monitor network activity in any form that it sees fit to maintain the integrity of the information network.