MEDFORD LAKES BOARD OF EDUCATION

FILE CODE: 6142.10
X Monitored
X Mandated
X Other Reasons

Computer/Internet Policy

Purpose

In a support of our education mission, the Board of Education is providing employees and students with access to the District's electronic communication system, which includes Internet access. For the purposes of this policy, the term "District system: is meant to include all computing facilities (for example, hardware, software, files, and accounts) used over a communication network in support of instructing, teaching and learning.

The term "educational purpose" includes use of the system for classroom activities, professional or career development, and teacher-approved high quality, self-discovery activities. Educational technology shall be infused into the district curriculum to maximize student achievement of the Core Curriculum Content Standards.

The District system has a specific educational purpose. The purpose of the District system is to assist in preparing students for success in life and work in the 21st century by providing them with electronic access to a wide range of information and the ability to communicate with people throughout the world. Additionally, the system will be used to increase District intra-communication, enhance productivity, and assist District employees in up-grading their skills through greater exchange of information with their peers. The District system will also assist the District in sharing information with the local community, including parents, social service agencies, government agencies, and businesses.

Users may not use the District system for commercial purposes, defined as offering or providing goods or services or purchasing goods or services for personal use. Accounts or facilities are not to be used for the transmission of commercial or personal advertisements, solicitations, promotions, or for personal monetary gains or other activities inconsistent with District policy or federal and/or state statutes. Users may not disclose the password of an account or otherwise make the account available to others who have not been authorized to use the account. Users are responsible for all usage of their accounts and are expected to take appropriate safeguards to assure that their account passwords are not known to others.

The Internet constitutes an unregulated collection of resources that changes constantly, so it is not possible to totally predict or control the resources that users may locate. The board cannot guarantee the accuracy of the information or the appropriateness of materials that a user may encounter. Furthermore, the board shall not be responsible for any damage users may suffer, including but not limited to, loss of data or interruptions of service. Nor shall the board be responsible for financial obligations arising through the unauthorized use of the system.

District Responsibilities

The Superintendent will serve as the coordinator to oversee the District system and will work with other regional or, state organizations as necessary.

The building principal will serve as the building-level coordinator for the District system, will approve building-level activities, ensure teachers receive proper training in the use of the system and the requirements of this policy, establish a system to ensure adequate supervision of students using the system, maintain and execute user agreements, and be responsible for interpreting the Districts Acceptable Use Policy at the building level.

Teachers are responsible to know the Acceptable Use Policy and to supervise students in the use of the system, which is consistent with this policy.

The Superintendent or his/her appointee, will establish a process for administering their District's system which will include tasks such as the following: setting-up individual and class accounts, set quotas for disk usage on the system, establish a retention schedule, establish a District virus protection process, and other activities. System administrators

or other authorized staff, in the course of meeting their job responsibilities, are allowed full access to files and programs during maintenance, routine backup operations, or in acting to safeguard the integrity and reliability of computing facilities. Staff who are authorized such access are expected to respect the privacy of other users.

Assess to the System

District System The District's Acceptable Use Policy, set forth in Section 1, will govern all use of the District system. Students' use of the system will also be governed by each respective building's disciplinary code. Employee use will also be governed by District policy.

World Wide Web District employees and students may have access to the Web through District-owned computers. The User Agreement and Parent Permission Form will be required for all students. Parents may specifically request that their child(ren) not be provided such access by indicating this and the User Agreement and Parent Permission Form.

Student E-Mail Students may be granted e-mail access only through a classroom or building account with approval of their teacher and parents. E-mail may only be sent or received under the direct supervision of a teacher or administrator.

Employee E-Mail District employees may be provided with an individual account for job-related purposes.

Technical Services Provided Through District System

E-Mail The District may provide e-mail to allow employees and students to communicate with people from throughout the world

World Wide Web The Web provides access to a wide range of information in the form of text, graphics, photographs, video, and sound, from throughout the world. The Web is a valuable research tool for students and employees.

Blocking Software The District will acquire security software designed to block access to certain sites and will install the software on workstations where students work independently or as a whole class.

Other Add-Ons The District will acquire other add-on Internet services which may support the educational mission of the district.

A. Parental Notification and Responsibility

1. The District will notify the parents about the District's Internet access; and the policies governing its use. Parents sign an agreement to allow their students to access the Internet. Parents may request alternative activities for their child(ren) that do not require Internet access.

2. The District Acceptable Use Policy contains restrictions on accessing inappropriate material. There is a wide range of material available on the Internet, some of which may not be fitting with the particular values of the families of the students. Although every effort will be made to closely monitor students' use of the Internet and their compliance with the Student Acceptable Use Policy, it is not practically possible for the District to monitor all internet activities. Therefore, it is imperative that the user be held accountable for the appropriate utilization of the technology.

3. The District will provide students and parents with guidelines for student safety while using the Internet.

B. District Limitation of Liability

1. The District makes no warranties of any kind, either expressed or implied, that the functions or the services provided by or through the District system will be error-free or without defect. The District will not be responsible for any damage users may suffer, including but not limited to, loss of data or interruptions of service. The District is not responsible for the accuracy or quality of the information obtained through or stored on the system. The District will not be responsible for financial obligations arising though the unauthorized use of the system.

C. Due Process

1. The District will cooperate fully with local, state, or federal officials in any investigation concerning to or relating to any illegal activities conducted through the District system.
2. In the event there is an allegation that a student has violated the District Acceptable Use Policy, the student will be provided with notice of the alleged violation and an opportunity to present an explanation before an administrator.

3. Disciplinary actions will be tailored to meet specific concerns related to the violation and to assist the student in gaining the self-discipline necessary to behave appropriately on an electronic network. If the alleged violation also involves a violation of other provisions of the respective building's disciplinary code, the violation will be handled in accord with the applicable provision of the respective building's disciplinary code.

4. Employee violations of the District Acceptable Use Policy will be handled in accord with District policy.

D. Search and Seizure

1. System users have a limited privacy expectation in the contents of their personal files on the District system. All files and information stored on the District system are the property of the District. Network administrators may review files and communications to maintain system integrity and ensure that users are using the system responsibly. Users should not expect that files stored on District servers will be private.

2. Routine maintenance and monitoring of the system may lead to discovery that the user has or is violating the District Acceptable Use Policy, the respective building's disciplinary code, or the law.

3. An individual search will be conducted if there is reasonable suspicion that a user has violated the law or the respective building's disciplinary code. The nature of the investigation will be reasonable and in the context of the nature of the alleged violation.

4. District Employees should be aware that their personal files may be discoverable.

E. Copyright and Plagiarism

1. District policies on copyright will govern the use of material accessed through the District system. Because the extent of copyright protection of certain works found on the Internet is unclear, employees will make a standard practice of requesting permission from the holder of the work if their use of the material has the potential of being considered an infringement. Teachers will instruct students to respect copyright and to request permission when appropriate.

2. District policies on plagiarism will govern use of materials accessed through the District system. Teachers will instruct students in appropriate research and citation practices.

3. Computer users shall not attempt or knowingly seek, provide, view, use, delete, modify information in, or obtain copies of files or programs belonging to other computer users without the permission of those users. Searching through non-public directories, libraries, or any other storage media to find unauthorized information is likewise prohibited. Further, computer users must not use the facilities to plagiarize or claim the intellectual or literacy property of others.

   Users granted access to administrative data in which individuals are identified must respect the confidentiality of these data. Disclosure of data pertaining to students, for example, should be in accordance with the Family Rights and Privacy Act.

   On most facilities, security systems are in place to prevent unwanted or unauthorized access. Any defects or weakness discovered in security systems, should be reported to the building principal. Under no circumstances should computer users, other than authorized system administrators, access or attempt to access system security programs or files.

F. Academic Freedom, Selection of Material, Student Rights to Free Speech

1. Board policies on Academic Freedom and Free Speech will govern the use of the Internet.

2. When using the Internet for class activities, teachers will select material that is appropriate in light of the age of the students and that is relevant to the course objectives. Teachers will preview the materials and sites they require or recommend students access to determine the

appropriateness of the material contained on or accessed through the site. Teachers will provide guidelines and lists of resources to assist their students' in channeling their research activities effectively and properly. Teachers will assist their students in developing the skills to ascertain the rightfulness of information, distinguish fact from opinion, and engage in discussions about controversial issues while demonstrating tolerance and respect for those who hold divergent views.

3. Within reason, freedom of speech and access to information will be honored. During school, teachers of younger pupils will guide them toward appropriate materials. Outside of school, families bear the same responsibility for such guidelines as they exercise discretion with information sources such as television, telephones, movies, radio, and other potentially offensive media.

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

- Sending or displaying offensive messages or pictures
- Using obscene language
- Harassing, insulting, or attacking others
- Damaging computers, computer systems, or computer networks
- Violating copyright laws
- Using another's account
- Trespassing in another's folder, work, or files
- Intentionally wasting limited resources
- Employing the network/computers for commercial purposes

Violations may result in a loss of access as well as other disciplinary or legal action.
Additional disciplinary action may be determined at the building level in line with existing practice regarding inappropriate language or behavior.

G. District Web Site

1. District Web Site The District may establish a Web site and Web page that will present information about the District. The Superintendent, or his/her appointee will be designated the Webmaster, responsible for maintaining the District Web site.

2. School or Class Web Pages Schools and classes may establish Web pages that present information about the school or class activities. The building principal may designate an individual to be responsible for managing the school Web site. The building principal will establish a process and criteria for the posting of material including links to other sites on these pages. Teachers will be responsible for submitting material for approval for their sites and for maintaining their class sites.

3. Extracurricular Organization Web Pages With the approval of the building principal and under close supervision by teachers, extracurricular organizations may establish Web pages. The principal will establish a process and criteria for the posting of material, including links to other sites, on these pages. Materials presented on the organization Web page must relate specifically to organization activities. Organization Web pages must include the following notice: ***"This is a student extracurricular organization Web page. Opinions expressed on this page shall not be attributed to the District."***

H. District Acceptable Use Policy

The following uses of the District system are considered sensible measures for all people to adhere to:

1. Jeopardizing Personal Safety (Restrictions are for students only)

a. Users will not post personal contact information about themselves or other people. Personal contact information includes address, telephone number school address, work address, etc.

b. Users will promptly disclose to their teacher or other school employee any electronic communication they receive that is inappropriate or makes them feel uncomfortable.

2. **Illegal Activities**
   a. Users will not attempt to gain unauthorized access to any other computer system through the District system, or go beyond their authorized access. This includes attempting to log in through another person's account or access another person's files. These actions are illegal, even if only for the purpose of "browsing".

   b. Users will not make deliberate attempts to disrupt the computer system performance or destroy data by spreading computer viruses or by any other means. These actions are illegal.

   c. Users will not use the District system to engage in any other illegal act.
   d. You will not make any malicious attempt to harm or destroy any equipment or data of another user or the network that is connected to the system.

3. **Comprising System Security**
   a. Users are responsible for the use of any individual accounts and should take all reasonable precautions to prevent others from being able to use an account.

   b. You will immediately notify a teacher or the system administrator if you have identified a possible security problem. Do not go looking for security problems, because this may be construed as an illegal attempt to gain access.

   c. Users will avoid the inadvertent spread of computer viruses by following recommended virus protection procedures if they download software.

   d. It is recommended that all computer disks used on the District system be internally distributed. In the event that a disk from outside must be used, a teacher using appropriate virus protection software will perform a virus check.

4. Inappropriate Language
   a. Restrictions against inappropriate language apply to public messages, private messages, and material posted on Web pages.

   b. Users will not use obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful language.

   c. Users will not post information that, if acted upon, could cause damage or a danger of disruption.

   d. Users will not engage in personal attacks, including prejudicial or discriminatory attacks.

   e. Users will not harass another person. Harassment is persistently acting in a manner that distresses or annoys another person. If a User is told by a person to stop sending them messages, they must stop.

   f. Users will not knowingly or recklessly post false or defamatory information about a person or organization.

5. **Disregarding Respect for Privacy**
   a. Users will not re-post a message that was sent to them privately without permission of the person who sent them the message.

   b. User will not post private information about another person.

6. Disregarding Respect for Resource limits
   a. Users will use the system only for educational purposes and professional or career development activities.

   b. Users will not download files unless it is approved by the teacher or administrator and it is absolutely necessary.

c. Users will not post chain letters or engage in "spamming". Spamming is sending an annoying or unnecessary message to a large number of people.

d. Users with access to e-mail will check their e-mail frequently and delete unwanted messages promptly.

e. Real-time conferencing where administrators have no control over the content of messages received are strictly prohibited. This includes but not limited to instant messaging, chat rooms, message boards, internet groups, etc. are prohibited.

f. The printing facilities of the network/computer should be used judiciously. Printing for other than approved educational purposes is prohibited.

7. Plagiarism and Copyright Infringement

a. Users will not plagiarize works that they find on the Internet. Plagiarism is taking the ideas or writings of others and presenting them as if they were originals to the user.

b. Users will respect the rights of copyright owners. Copyright infringement occurs when an individual inappropriately reproduces a work that is protected by a copy right. If a work contains language that specifies acceptable use of that work, the user should follow the expressed requirements. If the user is unsure whether or not they can use a work, they should request permission from the copyright owner.

8. Inappropriate Access to Material

a. Users will not use the District system to access material that is profane or obscene (pornography), that advocates illegal acts, or that advocates violence or discrimination toward other people (hate literature).

b. If a user inadvertently accesses such information, they should immediately disclose the inadvertent access in a manner specified by their school. This will protect users against an allegation that they have intentionally violated the Acceptable Use Policy.

9. Use of District Portable Devices

a. Equipment will be directly signed out and accounted for by the classroom teacher

b. Theft or damages due to neglect will be subject to payment for damages as listed in section I1.

c. Teachers will be responsible to secure any portable devices n their classroom before leaving their classroom at all times.

d. Portable classroom devices may not be brought home at any time by students.

e. Applications may only be placed on the portable devices by the Technology Department.

f. All purchased applications must receive prior approval from the Technology Department and appropriate supervisor.

I. Internet Safety

1. **Determination of Consequences for Violations**

The Superintendent of Schools shall determine the particular consequences for violation of this policy.

Individuals, following an investigation will be notified in writing of violating this policy and shall be subject to the consequences as indicated in Policy 6142.10 and other appropriate discipline or actions, which include but are not limited to:

- Use of Computer Network(s)/Computers only under direct supervision
- Suspension of network privileges
- Revocation of network privileges
- Suspension of computer privileges

- Revocation of computer privileges
- Suspension of employment
- Dismissal
- Legal action and prosecution by the authorities

2. <u>Compliance with Children's Internet Protection Act</u>

The District has technology protection measures for all computers in the school district, including computers in media centers/libraries, that block and/or filter visual descriptions that are obscene, child pornography and harmful to minors as defined in this policy and in the Children's Internet Protection Act. The District will certify the schools in the District, including media centers/libraries are in compliance with the Children's Internet Protection Act and the District enforces Policy 6142.10.

Compliance with Neighborhood Children's Internet Protection Act

Policy 6142.10 and this Regulation establish an Internet safety policy and procedures to address:

1. Access by minors to inappropriate matter on the Internet and World Wide Web
2. The safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications
3. Unauthorized access, including "hacking" and other unlawful activities by minors online
4. Unauthorized disclosures, use, and dissemination of personal identification information regarding minors
5. Measures designed to restrict minors' access to materials harmful to minors

Notwithstanding the visual depictions defined in the Children's Internet Protection Act and as defined in 2,3, and 4 above. The board shall determine Internet material that is inappropriate for minors. The Board will provide reasonable public notice and a public hearing during a regular monthly Board meeting or during a designated special Board meeting to address and receive public community input on the Internet safety policy - Policy and Regulation 6142.10

Date Reviewed: May 16, 2001, August 20, 2003, May 21, 2008; November 12, 2012
Adopted: June 20, 2001, September 10, 2003, August 20, 2008; November 12, 2012

MEDFORD LAKES BOARD OF EDUCATION **FILE CODE: 6142.10**

X Monitored
X Mandated
PROCEDURES **X Other Reasons**

STUDENT – ACCEPTABLE USE POLICY – COMPUTER/INTERNET ACCESS

In support of our educational mission, the Board of Education is now offering Internet access for student use. This document contains the Acceptable Use Policy for your use of the District system. For the purpose of this policy, the term "District system: is meant to include all computing facilities (for example, hardware, software, files, and accounts) used over a communication network in support of instructing, teaching, and learning.

A. Educational Purpose

1. Internet access has been established for a specific educational purpose. The term "educational" purpose includes classroom activities, career development, and limited, teacher approved, high-quality, self-discovery activities.

2. The District system has not been established as a public access service or a public forum but limited public access may be offered at the Board's discretion. The Board of Education has the right to place reasonable restrictions on the material you access or post through the system. You are also expected to follow the rules set forth in your respective building's disciplinary code and the law in your use of the District system.

3. You may not use the District system for commercial purposes. This means you may not offer, provide, or purchase products or services through the District system.

4. You may not use the District system for political lobbying. But you may use the system to communicate with elected representatives and to express your opinion on political issues where appropriate.

B. Student Internet Access

1. Students may have access to Internet World Wide Web Information resources through their classroom, library, or school computer lab.

2. Students may be provided with e-mail access only under their teacher's direct supervision using a classroom account.

3. You and your parent must sign the User Agreement and Parent Permission Form to be granted Internet access on the District system. This Agreement must be renewed on an annual basis. Your parent can withdraw their approval at any time.

4. No personal Web pages may be attached to our District system.

C. Unacceptable Uses

The following uses of the District system must be adhered to:

1. Jeopardizing Personal Safety
    a. You will not post personal contact information about yourself or other people. Personal contact information includes your address, telephone, school address, work address, etc.

b. You will promptly disclose to your teacher or other school employee any electronic communication message you receive that is inappropriate or makes you feel uncomfortable.

2. Illegal Activities
    a. You will not attempt to gain unauthorized access to the District system or to any other computer system through the District system or go beyond your authorized access. This includes attempting to log in through another person's account or access another's person files. These actions are illegal, even if only for the purpose of "browsing".

    b. You will not make deliberate attempts to disrupt the computer system or destroy data by spreading computer viruses or by any other means. These actions are illegal.

    c. You will not use the District system to engage in any other illegal act.

    d. You will not make any malicious attempt to harm or destroy any equipment or date of another use on the networks that connected to the system

3. Compromising System Security
    a. You are responsible for your use of any account and should take all reasonable precautions to prevent others from being able to use or access your account. Under no conditions should you provide your District password to another person.

    b. You will immediately notify a teacher or the system administrator if you have identified a possible security problem. Do not go looking for security problems, because this may be construed as an illegal attempt to gain access.

    c. You will avoid the inadvertent spread of computer viruses by following recommended virus protection procedures if you download software.

    d. It is recommended that all computer disks used on the district system be internally distributed. In the event that a disk from outside must be used, a virus check will be performed by a teacher using appropriate virus protection software.

4. Inappropriate Language
    a. Restrictions against inappropriate language apply to public messages, private messages, and material posted on Web pages.

    b. You will not use obscene, profane, lewd, vulgar, rude inflammatory, threatening, or disrespectful language.

    c. You will not post information that could cause damage or a danger of disruption.

    d. You will not engage in personal attacks, including prejudicial or discriminatory attacks.

    e. You will not harass another person. Harassment is persistently acting in a manner that distresses or annoys another person. If you are told by a person to stop sending them messages, you must stop.

    f. You will not knowingly or recklessly post false or defamatory information about a person or organization.

5. Game Playing
    a. Game playing is permitted on the system only when the terminal is not needed for other purposes and the game conforms to the curricular goals of the District. Game playing over dial-up links or other inter-machine communications is prohibited, unless authorized by a teacher or administrator.

6. Disregarding Respect for Privacy
    a. You will not re-post a message that was sent to you privately without permission of the person who sent you the message.

    b. You will not post private information about another person.

7. Disregarding Respect for Resources Limits.
    a. You will use the System only for educational purposes.

    b. You will not download files unless authorized by a teacher or an administrator and absolutely necessary.

       You will not post chain letters or engage in "spamming". Spamming is sending annoying or unnecessary messages to a large number of people.

    c. In the event that you are provided with a student e-mail account you will check your e-mail frequently, delete unwanted messages promptly, and stay within your e-mail quota.

    d. Real-time conferencing where administrators have no control over the content of messages received are strictly prohibited. This includes but not limited to instant messages, chat rooms, message boards, Internet groups, etc., are prohibited.

    e. The printing facilities of the computer network/computer should be used judiciously. Printing for other then approved educational purposes is prohibited.

8. Plagiarism and Copyright Infringement
    a. You will not plagiarize works that you find on the Internet. Plagiarism is taking the ideas or writings of others and presenting them as if they were yours.

    b. You will respect the rights of copyright owners. Copyright is infringement occurs when you inappropriately reproduce a work that is protected by a copyright. Copyright laws can be very confusing. If you have questions, ask a teacher. If you are unsure whether you can use a work found, or if you have questions, ask a teacher.

9. Inappropriate Access to Material
    a. You will not use the District system to access material that is profane or obscene (pornography), that advocates illegal acts, or that advocates violence or discrimination towards other people (hate literature).

    b. If you mistakenly access inappropriate information, you should immediately tell your teacher or another District employee. This will protect you against a claim that you have intentionally violated this policy.

    c. Your parents should instruct you if there is additional material that they think it would not be appropriate for you to access. This District fully expects that you will follow your parent's instructions in this manner

D. Your Rights

1. Free Speech

    a. Your right to free speech applies also to your communications on the Internet. The District system is considered a limited forum, similar to the school newspaper, and therefore the District may restrict your speech for valid educational reasons. The District will not restrict your speech on the basis of a disagreement with the opinions you are expressing.

    b. As outlined in Board policy and procedures on pupil rights and responsibilities, copies of which are available in school offices, the following are not permitted:

    - Sending or displaying offensive messages or pictures
    - Using obscene language
    - Harassing, insulting, or attacking others
    - Damaging computers, computer systems, or computer networks
    - Violating copyright laws
    - Using another's account
    - Trespassing in another's folders, work, or files
    - Intentionally wasting limited resources
    - Employing the network/computer's for commercial purposes

2. Search and Seizure

    a. You should expect only limited privacy in the contents of your personal files on the District system. The situation is similar to the rights you have in the privacy of your locker.

    b. Routine maintenance and monitoring of the District system may lead to discovery that you have violated this Policy, your respective building's disciplinary code, or the law.

    c. An individual search will be conducted if there is reasonable suspicion that you have violated this Policy, your respective building's disciplinary code, or the law. The investigation will be reasonable and related to the suspected violation.

3. Due Process

    a. The District will cooperate fully with local, state, or federal officials in any invest related to any illegal activities conducted through the District system.

    b. In the event there is a claim that you have violated this Policy or your respective building's disciplinary code in your use of the District system, you will be provided with a written notice of the suspected violation and an opportunity to present an explanation before an administrator.

    c. If the violation also involves a violation of other provisions of your respective building's disciplinary code, it will be handled in a manner described in your respective building's disciplinary code. Additional restrictions may be placed on your use of your Internet account.

E. Limitation of Liability

The District makes no guarantee that the functions or the services provided by or through the District system will be error-free or without defect. The District will not be responsible for any damage you may suffer, including but not limited to, loss of data or interruptions of service. The district is not responsible for the accuracy or quality of the information obtained through or stored on the system.

The District will not be responsible for financial obligations arising through the unauthorized use of the system.

F. Internet Safety

The District has technology protection measures for all computers in the school district, including computers in media centers/libraries, that block and/or filter visual descriptions that are obscene, child pornography and harmful to minors as defined in this policy and in the Children's Internet Protection Act. The District will certify the schools in the District, including media centers/libraries are in compliance with the Children's Internet Protection Act and the District enforces Policy 6142.10.

Compliance with Neighborhood Children's Internet Protection Act

Policy 6142.10 and this Regulation establishes an Internet safety policy and procedures to address:

1. Access by minors to inappropriate matter on the Internet and World Wide Web
2. The safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications
3. Unauthorized access, including "hacking" and other unlawful activities by minors online
4. Unauthorized disclosures, use, and dissemination of personal identification information regarding minors
5. Measures designed to restrict minors' access to materials harmful to minors

Notwithstanding the visual depictions defined in the Children's Internet Protection Act and as defined in 2,3, and 4 above. The board shall determine Internet material that is inappropriate for minors. The Board will provide reasonable public notice and will hold a public hearing during a regular monthly Board meeting or during a designated special Board meeting to address and receive public community input on the Internet safety policy - Policy and Regulation 6142.10

G. Violations

Violations of the Acceptable Use of Computer/Internet Access Procedures may result in a loss of access as well as other disciplinary or legal action. Disciplinary action shall be taken as indicated n Policy and Regulation 6142.10, Acceptable Use of Computer/Internet Access, Pupil Discipline Policy and Regulation 5131, Suspension and Expulsion Policy and Regulation 5114, as well as possible legal action and reports to the legal authorities and entities.

1. Determination of Consequences for Violations

    a. The particular consequences for violations of this policy shall be determined by the Principal's designee in matters relating to the use of computer/internet access and by the Principal in the matters of school suspension. The Superintendent or designee and the Board shall determine when school expulsion and/or legal action or actions by the authorities are the appropriate course of action.

    b. Individuals violating this policy shall be subject to the consequences as indicated in Regulation 6142.10 and other appropriate discipline, which includes buy is not limited to:

        - Use of Computer/Internet Access only under direct supervision
        - Suspension of network privileges
        - Revocation of network privileges
        - Suspension of computer privileges
        - Revocation of computer privileges
        - Suspension from school
        - Expulsion from school, and/or
        - Legal action ad Prosecution by the authorities

Decisions of on the consequences may be appealed in accordance with Policy and Regulation 5145.6 Pupil Grievances.

Date reviewed: May 16, 2001, August 20, 2003, May 21, 2008
Date adopted: June 20, 2001, September 10, 2003, August 20, 2008

MEDFORD LAKES BOARD OF EDUCATION **FILE CODE: 6142.10**

X Monitored
X Mandated
REGULATION **X Other Reasons**

MEDFORD LAKES SCHOOL DISTRICT
TERMS AND CONDITIONS FOR NETWORK ACCESS

The Medford Lakes School District is pleased to offer the students and staff of Medford Lakes Borough access to the district's computer networks. To gain access to e-mail, Internet and the local network, all students 18 years of age and under must obtain parental permission. An "internet User Contract" must be signed and returned to the school before access will be granted.

Access to the Internet will allow the exploration of thousands of resources worldwide. Electronic mail (a-mail) will allow the exchange of messages with computer users throughout the world. Parents and students are warned that some materials accessible on the Internet may contain Items that are inaccurate, defamatory, Illegal, or offensive. While it is our intent to make the Internet available for research and to promote educational objectives, there is the potential of gaining access to other materials as well. We believe that the benefits to staff and students greatly outweigh any potential disadvantages. Ultimately parents and guardians of minors are responsible for setting and conveying standards that their children should follow. The Medford Lakes Board of Education supports and respects each family's right to decide whether or not to apply for network access.

Rules for Network Access

1. The use of a network account must be in support of education and research consistent with the educational objectives of the district, school, and teacher.
2. Transmission of any material in violation of U.S., State or local regulation is prohibited. This includes, but is not limited to, copyrighted material, threatening or obscene material, or material protected by trade secrets.
3. Use for product advertisement, political lobbying, or personal financial or material gain is prohibited.
4. Use for commercial activities by for-profit Institutions is prohibited.
5. Be polite. Do not write or send threatening or abusive messages to others.
6. Use appropriate language. Use of obscene or degrading language is prohibited.
7. It is recommended that the user not reveal their personal address or phone number. Distributing the address or phone number of another person is prohibited.
8. Network resources, Information, and electronic mail are not guaranteed to be private. Persons operating the system have access to all network resources. Any Items containing inappropriate material or relating to Illegal activities will be reported to the appropriate authorities.
9. Do not use the network in a manner that would disrupt the use of the network by others. This Includes, but is not limited to, sending mass e-mail messages, attempting to Infect the system with a computer virus, attempting to "crash the system", intentionally wasting network resources, or annoying other users in any fashion.
10. Accessing any account other than the one assigned to you is prohibited. This includes, but is not limited to, guessing or stealing another user's account access. Certain "public" accounts allow access to resources such as the school's library. These "public" accounts are considered open to all users.
11. Allowing another user to gain access to your account is prohibited. Do not give anyone your password.
12. Us of the network to facilitate plagiarism is prohibited. No user shall misrepresent another person's work as their own, or allow their work to be misrepresented as belonging to someone else.

It is understood that access to the computer networks in the Medford Lakes School System is a privilege, not a right. Failure to abide by the rules in this document could result in the revocation of access disciplinary action, or legal action, as deemed appropriate. The rules, procedures, terms and conditions apply to all users.

The Medford Lakes Board of Education does not discriminate on the basis of race, color, national origin, age, religion, marital status, sex or handicap in employment, educational programs, or activities.

Medford Lakes School District

INTERNET USER AGREEMENT AND PARENT/GARDIAN PERMSSION FORM

As the parent or legal guardian of the minor student signing below, I have read the Terms and Conditions for Network Access. I understand that this access is designed for educational purposes, and the Medford Lakes School District has made access available for this purpose. I recognize that it is Impossible for the Medford Lakes School District to restrict access to controversial material, and I will not hold them responsible for the materials this student may acquire on the network.

I understand that individuals and families may be liable for violations. I understand that some materials on the Internet may be objectionable, but I accept responsibility for guidance of Internet use.

Further, I accept full responsibility for supervision, if and when my child's use is not in a school setting. I hereby give my permission for my child to access networked computer services such as electronic mail and the Internet.

Parent/Guardian (Print Name): Signature of Parent/Guardian:

_____ _____

Date:_____

Daytime Phone:_____Evening Phone:_____

Student

I have read the Terms and Conditions for Network Access. I hereby agree to comply with the stated Terms and Conditions. I further understand that violation of the regulations is unethical and may constitute a criminal offense. Should I commit any violation, my access privileges may be revoked, school disciplinary action taken, and/or appropriate legal action Initiated.

Student (Print name here) _____

Student Signature_____

Medford Lakes School District

EMPLOYEE INTERNET USER AGREEMENT

I have read the Terms and Conditions for Network Access. I understand that this access is designed for educational purposes, and the Medford Lakes School District has made access available for this purpose. I recognize that it is impossible for the Medford Lakes School District to restrict access to controversial material, and I will not hold them responsible for the materials that may be acquired on the network.

I understand that individuals may be liable for violations. I understand that some materials on the Internet may be objectionable, but I accept the responsibility of Internet access networked computer services such as electronic mail and the Internet.

I have read the Terms and Conditions for Network Access. I hereby agree to comply with the stated Terms and Conditions. I further understand that violation of the regulations is unethical and may constitute a criminal offense. Should I commit any violation, my access privileges may be revoked, school disciplinary action taken, and/or appropriate legal action Initiated.

EMPLOYEE (Print Name): EMPLOYEE Signature:

_____ _____

Date:_____

TECHNOLOGY

Monitored:

Indicator 8.1

Mandated:

47 U.S.C. 254(h), known as the Children's Internet Protection Act and the implementing federal regulations, require board policy on acceptable use of the Internet for districts receiving certain federal funds, as well as the installation of blocking software to prevent access to unacceptable areas of the Internet.

No Child Left Behind also requires policy on safe student access to the Internet.

Other Reasons:

N.J.S.A. 18A:36-35 prohibits the publication on district web sites of "personally identifiable information" about students without prior written parental consent. "Personally identifiable information" is defined as student names, photos, addresses, email addresses, phone numbers and locations and times of class trips.

This is a topic of critical concern, because technology has important implications for all aspects of district operations.

TECHNOLOGY (continued)

Recommendation:

A policy directing the development of a technology plan that effectively integrates technology into district programs, practices and operations. The policy should include a section on the entire system of electronic communications and whatever other sections apply to your district system – acceptable use of the Internet, web sites, e-mail for staff and/or students, district rights and responsibilities, parental responsibilities, etc. Include assurances of the installation of blocking software if your district receives

E-rate discounts for Internet access or federal funds for some other technological uses. According to federal law, filters should block visual depictions that are obscene, child pornography, or harmful to minors. All forms of "hacking" should be prohibited. Assure monitoring of student online activities.

Sanctions for student misuse of the system should be included in your student code of conduct or regulations for policy 5131 *Conduct/discipline*. Sanctions for staff misuse would be addressed in negotiated agreements and applicable laws and regulations. List other related policies in your cross references.

Abbott districts will want to add assurances that they are in compliance with all requirements of administrative code, including provision for a full-time technology coordinator in each high school and each Whole School Reform elementary school. Include assurances that technology will be infused into all aspects of the curriculum and will be effectively applied to student achievement of the Core Curriculum Content Standards.

Legal References:

N.J.S.A. 2A:38A-1 et seq.	Computer System
N.J.S.A. 2C:20-25	Computer Related Theft
N.J.S.A. 18A:7A-11	Annual report of local school district; contents; annual report of commissioner; report on improvement of basic skills
N.J.S.A. 18A:36-35	School Internet websites; disclosure of certain student information prohibited
N.J.A.C. 6A:10A-1.1 et seq	Improving Standards-Driven Instruction and Literacy and Increasing Efficiency in Abbott School Districts
See particularly: *N.J.A.C. 6A:10A, Appendix A*	
N.J.A.C. 6A:30-1.1 et seq.	Evaluation of the Performance of School Districts
17 U.S.C. 101	United States Copyright Law
47 U.S.C. 254(h)	Children's Internet Protection Act

N.J. v. T.L.O. 469 U.S. 325 (1985)
O'Connor v. Ortega 480 U.S. 709 (1987)
No Child Left Behind Act of 2001, Pub. L. 107-110, 20 U.S.C.A. 6301 et seq.
Manual for the Evaluation of Local School Districts

Possible Cross References:

*1111	District publications
*3514	Equipment
3543	Office Services
*3570	District records and reports
4118.2/4218.2	Freedom of speech (staff)
*5114	Suspension and expulsion
*5124	Reporting to parents/guardians
*5131	Conduct/discipline
*5131.5	Vandalism/violence
*5142	Pupil safety
5145.2	Freedom of speech/expression (students)
*6144	Controversial issues
*6145.3	Publications
6161	Equipment, books and materials

*Indicates policy is included in the Critical Policy Reference Manual.