ELECTRONIC INFORMATION ACCESS
ACCEPTABLE USE POLICY

Introduction:

The Montcalm Area Intermediate School District, hereinafter referred to as MAISD, encourages and strongly promotes the use of electronic technologies in education. MAISD provides information technology in a variety of electronic formats including Internet and electronic mail to further educational goals through the integration of technology with curriculum.

It is the policy of MAISD to: (a) prevent User access over its computer network to, or transmission of, inappropriate material via internet, electronic mail, or other forms of direct electronic communications; (b) prevent unauthorized access and other unlawful online activity; (c) prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; and (d) comply with state and national laws governing internet access and usage, such as CIPA and E-rate [Pub. L. No. 106-554 and 47 USC 254(h)].

Guidelines for the use of technology described in these regulations apply to all users of MAISD resources. Disciplinary action for misuse of resources is consistent with MAISD policies governing behavior.

Definitions

Some of the key terms used in this policy may be defined in the *Children's Internet Protection Act, otherwise known as CIPA.**

1. **Technology Protection Measure:** The term "technology protection measure" means a specific technology that blocks or filters Internet access to visual depictions that may be obscene, contain pornographic or sexual content, or otherwise harmful to minors.
2. **Obscene: The terms** as defined in Section 1460 of Title 18, United States Code;
3. **Child Pornography:** The term as defined in Section 1460 of Title 18, United States Code;
4. **Harmful to Minors:** The term "harmful to minors" means any picture, image, graphic, image file, or other visual depiction taken as a whole and with respect to minors;
   A. appeals to a prurient interest in nudity, sex, or excretion;
   B. 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 act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals;
   C. taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.
5. **Sexual Act; Sexual Contact:** The terms "sexual act" and "sexual contact" have the meanings given such terms in Section 2246 of Title 18, United States Code.
6. **Bootleg Software:** Software downloaded or otherwise in the user's possession without the appropriate permission or registration of the software including payment of fees to the owner or software distributor.
7. **FERPA:** The "Federal Education Records Protection Act" outlines rules and regulations staff must follow to protect confidentiality of certain student record information.
8. **NEOLA:** All policies as approved by the MAISD Board of Education are maintained online by NEOLA. The NEOLA web site offers easy access to current policies.

Privileges:

Users have the privilege to use hardware and software for which they have been assigned, access information from outside resources, and access MAISD internal network resources to retrieve information facilitating learning and enhancing educational information exchange.

Consequences of Inappropriate Behavior:

1. Users violating any of these Privileges and Responsibilities may be banned from using MAISD hardware and telecommunications software to access the Internet.
2. Users will be required to make full financial restitution for any unauthorized expenses incurred or any damages caused beyond normal wear and tear.
3. Users violating any of these privileges and responsibilities may face additional disciplinary and/or legal action deemed appropriate in keeping with the disciplinary policies of the MAISD, state, and federal law.

*The building administrator, system administrator, and/or superintendent will determine inappropriate use based on the Electronic Access and Use Policy. These guidelines are not all-inclusive, but only representative and illustrative. A user who commits an act of misconduct that is not listed may also be subject to disciplinary action. The user account may be closed at any time for infractions.

Responsibilities: Users are responsible for:

1. utilizing MAISD technology only for facilitating learning and enhancing educational information exchange consistent with MAISD policy.
2. making sure all food and drinks are kept out of the computer labs and a safe distance away from computers.
3. properly using and caring for hardware and software which they have been issued.
4. adhering to the rules established for the use of MAISD hardware, software, labs, and networks accessed internally or externally through remote access.
5. adhering to MAISD guidelines and copyright law as it pertains to plagiarism or the unwritten consent from the author from which it is derived.
6. all files stored or printed under his/her user account.
7. complying with FERPA rules governing the protection and confidentiality of educational records.
8. compliance with MAISD policies as approved by the Board of Education and posted online with NEOLA. Including but not limited to policy 7540 computer technology and networks, 7540.03 student acceptable use, 7540.04 staff acceptable use, 7540.05 electronic mail, 7545 electronic communication, 7543 remote access, and 7543 network access from personally owned computers and/or other web-enabled devices. Policy 7540 covers requirements for the education of minors in online safety and security, cyber-bullying, and disclosure of personal information.

Users are prohibited from:

1. using technology for personal business, commercial purposes, financial gain, product advertisement, business service endorsement, political activity, or religious or political lobbying.
2. committing or attempting to commit any willful act involving the use of the network which disrupts the operation of the network within the MAISD or any network connected to the Internet including:
   A. the use of, attempted use, or possession of computer viruses or hacking tools.
   B. illegal activity such as violation of copyright or other contracts, or transmitting any material in violation of any US or state regulation.
3. downloading or installing software on MAISD equipment from disks, CD-ROMs, electronic files, email, or any other data storage devices without prior approval.
4. downloading copyrighted material for other than legal personal, professional, or educational use.
5. gaining unauthorized access to resources or entities.
6. using or sharing another user's individual MAISD provided account or password information with the exception of MAISD group or guest accounts as specifically assigned.
7. posting material authored or created by another without his/her consent.
8. using the network while access privileges are suspended or revoked.
9. publishing or otherwise disseminating another person's identity, personal information, account or password.
10. accessing or transmitting inappropriate material which:
    A. promotes violence or terrorism, advocates destruction of property including, but not limited to, access to information concerning the manufacture of destructive devices such as explosives, fireworks, smoke bombs, or incendiary devices.
    B. is defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, harassing, or illegal.
    C. advocates or promotes violence or hatred against particular individuals or groups of individuals or superiority of one racial ethnic or religious group over another.
11. using or possessing bootleg software.
12. using unauthorized encryption software or encrypted hardware with MAISD provided technology.
13. transmitting credit card information or other persona information on the MAISD network through the use of e-mail, blog, chat, instant messenger, or other online activity.
14. transmitting student's personally identifiable information to unauthorized individuals without a signed release unless limited to standard directory information such as first name.
15. accessing the Internet through an anonymous relay.

Access to Inappropriate Materials:

Technology protection measures (or "filtering") shall be used to block or filter Internet access to inappropriate information promoting safety and security of Users accessing the MAISD Network.

Subject to staff supervision, technology protection measures* may not be disabled but may be minimized for educational purposes.

Specifically, as required by the Children's Internet Protection Act, our protection measures prevent inappropriate network usage and Internet access by staff and minors on the Internet including: (a) unauthorized access, including so-called "hacking", and other unlawful activities by minors; and (b) unauthorized disclosure, user and dissemination of personal identification information regarding minors. Specifically as required by Federal law, filtering shall be applied to visual depictions of material deemed obscene, child pornography, or to any material deemed harmful to minors.*

Network Etiquette:

Users are expected to abide by the generally accepted rules of network etiquette. These include, but are not limited to the following:

1. Be polite. Do not be abusive in your message to others.
2. Use appropriate language. Do not use profanity, vulgarities, and other inappropriate language.
3. Do not reveal the personal address or phone numbers of yourself or any other person without prior permission.
4. Electronic mail transferred through the MAISD Network is the property of the MAISD and is not guaranteed private. System Administrators have access to all electronic data including email and messaging. Messages relating to or in support of illegal activities may be reported to authorities.
5. Do not use the network in such a way that would be disruptive to others.
6. All publications, information, files, and programs accessible via the network should be assumed to be private property; therefore, should be given copyright consideration.
7. All User files, records of access on MAISD equipment, or any other resources accessible by means of MAISD equipment should be considered MAISD property and is subject to control and inspection without notice to the user. While MAISD does not, as a matter of course, review users' activities, users acknowledge they have no expectation of privacy, privileges may be suspended or revoked without notice and, in the event a user's access is alleged to violate law, referral to appropriate law enforcement authorities may occur.

In addition, at the beginning of each school year, students receive education in appropriate online behavior, interacting with others on social networking, web sites, chat rooms and other electronic communications, and recognizing and responding to cyberbullying.

Supervision and Monitoring

It shall be the responsibility of MAISD staff to supervise and monitor student computer network and Internet access in accordance with MAISD policy and state and federal laws.

District technology staff shall maintain, monitor, and support district-owned technology by directly accessing these resources or utilizing remote access tools.

Procedures for the disabling or otherwise modifying any technology protection measures shall be the responsibility of the Montcalm Area Intermediate School District or designated representatives.

System Security:

Users will not attempt to gain unauthorized access to the MAISD network and/or computer resources or any other computer system through the MAISD system or go beyond their authorized access. This includes attempting to log in through another person's account or access another person's files.

Users 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.

Users may not download or install software on MAISD equipment from disks, CD-ROMs, electronic files, email, or any other data storage devices without prior approval.

Users are responsible for their individual account and should take all reasonable precautions to prevent others from being able to use the account. A user will not provide their password to another person other Technology Department staff. Other than the User, only a Technology Department staff member may change, reset, or otherwise use a Users password for the purposes of system administration or technical support.

Users will immediately notify a teacher or Technology Department of potential security problems. Do not demonstrate the problems to other users. Do not go looking for security problems, because this may be construed as an illegal attempt to gain access.

ELECTRONIC INFORMATION ACCESS
ACCEPTABLE USE POLICY

AGREEMENT

By using MAISD technology resources I agree to abide by such rules and regulations as illustrated in the MAISD Acceptable Use Policy, Board of Education policy, and as may be further amended from time-to-time by the MAISD and/or Network Administrator. Policies are available on the MAISD web site and in the Staff Handbook.

Accessing MAISD technology resources indicates acceptance of all district and Board of Education policy.

Photographs taken with MAISD equipment, stored on the Network, or otherwise contracted by the MAISD are property of the MAISD. Such photographs and supporting documentation may be used on the MAISD web site for the staff directory, program and event descriptions, and other informational purposes. Users objecting to the display of a photo may contact the MAISD Technology Department to have it removed. Use of student photographs may only contain a first name unless a release is signed by the parent.

RETURN TO:

Please sign and return this page to the MAISD Business Office.

_____ _____

Signature of User Date

If under 18 years old: As the parent or legal guardian of a minor, I agree to this agreement and will indemnify the MAISD for any fees, expenses, or damages incurred as a result of the minor's use or misuse of technology equipment and /or resources.

_____ _____

Signature of Parent/Guardian Date

Please forward questions or comments to:

Information Technology Department

E-mail: contact@maisd.com

Phone: 616-225-4700

Mail: 621 New Street, PO Box 367, Stanton, MI 48888