ADMINISTRATIVE PROCEDURE/POLICY
13-2
METHUEN PUBLIC SCHOOL
Internet / Network Acceptable Use Policy

Introduction

The Methuen Public Schools (MPS) recognizes that access to technology in school gives students greater opportunities to learn, engage, communicate, collaborate, and develop skills that will prepare them for work, life, and citizenship. Our goal is to promote educational excellence by encouraging and facilitating resource sharing, innovation, and communication. We are committed to helping students develop 21st century technology and communication skills. To that end, we provide the privilege of access to technologies for student and staff use.

Internet use that is integrated into the school curriculum fosters the development of research and information skills, encourages critical and higher level thinking, and provides expanded educational opportunities for both students and staff. While supporting the rights of students and staff to use all available tools, the Methuen Public Schools recognize that there is material on the internet that is objectionable or devoid of educational value in the context of a school setting. The Methuen Public Schools have taken steps to restrict access to inappropriate or controversial material. In addition to utilizing an internet content filter, MPS staff will closely supervise students' use of the internet.

Although guidelines cannot totally eliminate the possibility of inadvertent or intentional access to such information, we believe that they can significantly limit such possibilities. The Methuen Public Schools believe that the access to valuable resources on the Internet far outweighs the concerns that the users may procure material that is not consistent with the educational goals of the Methuen Public Schools, and we intend to maximize the Internet's educational value.

The Methuen Public Schools will insure that it adheres to the most recent Children's Internet Protection Act (CIPA) requirements of 2001 by:

- implementing an Internet filter for the purpose of blocking access to visual depictions deemed obscene, child pornography, or harmful to minors. It may be disabled for adults engaged in bona fide research or other lawful purposes.

- providing for educating minors (in this case 'minors' refer to school aged children up to the age of 17) about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyber-bullying awareness and response.

This Acceptable Use Policy outlines the guidelines and behaviors that all users are expected to follow when using school technologies or when using personally owned devices on the school campus, including:

- The MPS network is intended for educational purposes.

- All activity over the network or using district technologies may be monitored and retained.

- Access to online content via the network may be restricted in accordance with our policies and federal regulations, such as the Children's Internet Protection Act (CIPA).

- Users are expected to follow the same rules for good behavior and respectful conduct online as offline.

- Misuse of school resources can result in disciplinary action.

- MPS makes a reasonable effort to ensure users' safety and security online, but will not be held accountable for any harm or damages that result from use of school technologies.

- Users of the district network or other technologies are expected to alert IT staff immediately of any concerns for safety or security.

Technologies Covered
MPS may provide the privilege of Internet access, desktop computers, mobile computers or devices, videoconferencing capabilities, online collaboration capabilities, message boards, email, and more. This Acceptable Use Policy applies to both school owned technology equipment utilizing the MPS network, the MPS Internet connection, and/or private networks/Internet connections accessed from school owned devices at any time. This Acceptable Use Policy also applies to privately owned devices accessing the MPS network, the MPS Internet connection, and/or private networks/Internet connections while on school property. As new technologies emerge, MPS will seek to provide access to them. The policies outlined in this document cover all available technologies now and into the future, not just those specifically listed or currently available.

Usage Policies
All technologies provided by the district are intended for education purposes. All users are expected to use good judgment and to follow the specifics as well as the spirit of this document: be safe, appropriate, careful and kind; don't try to get around technological protection measures; use good common sense; and ask if you don't know.

Web Access
MPS provides its users the privilege of access to the Internet, including web sites, resources, content, and online tools. Access to the Internet will be restricted as required to comply with CIPA regulations and school policies. Web browsing may be monitored and web activity records may be retained indefinitely.

Users are expected to respect the web filter as a safety precaution and shall not attempt to circumvent the web filter when browsing the Internet. The determination of whether material is appropriate or inappropriate is based solely on the content of the material and the intended use of the material, not on whether a website has been blocked or not. If a user believes a site is unnecessarily blocked, the user should submit a request for website review through the email link provided on all blocked pages.

Email
MPS may provide users with the privilege of email accounts for the purpose of school related communication. Availability and use may be restricted based on school policies. If users are provided with email accounts, the account(s) should be used with care. Users should not send personal information; should not attempt to open files or follow links from unknown or untrusted origins;

should use appropriate language; and should only communicate with other people as allowed by the district policy or the teacher. Users are expected to communicate with the same appropriate, safe, mindful, courteous conduct online as offline. Email usage may be monitored and as a school department, all email communications are archived for seven (7) years.

Technology Specialists who operate the system have access to all mail, including deleted messages. Messages relating to or in support of illegal activities may be reported to the authorities. All communications and information accessible via the network should be considered public property; however, the use of another person's intellectual property without that individual's prior written approval or authorization is prohibited. The school district will completely and periodically delete information from the system.

Legal Implications of Electronic Mail (Email)
For the purpose of this policy email is defined as messages created and received on an electronic mail system. The email message may be text or word processing documents, spreadsheets or other data compilations transmitted through such a system.

Email created or received by an employee of a government unit is a public record. In Massachusetts, the term "public record" is broadly defined to include all documentary materials or data created or received by any officer or employee of any governmental unit, regardless of physical form or characteristics. G.L. c. 4, sec. 7(26). Email is therefore a public record and subject to the requirements of the Public Records Law G. L. C. 66. Email messages are subject to public access through the Public Records Law G. L. C. 66. Sec.10. A determination as to whether an email message is exempt from disclosure depends upon the content of the message. G. L.C. 4. Sec. 7(26)(a-m).

Email messages may be sought through the discovery process in litigation and may be admissible in evidence. Like all electronically created and stored records, email is subject to the rules of evidence and a judge will rule on its admissibility.

Refer to the Commonwealth of Massachusetts Public Records Division SPR- Bulletin No. 1-99 dated February 16, 1999 for additional information.

Network Accounts
Do not use another individual's account or password. Do not give your password to others. Attempts to log-on to the system as another user may result in cancellation of user privileges.

Network Use Limitations
The district's computer network may not be used to disseminate commercial or personal advertisements, solicitations, promotions, destructive code (e.g., viruses, self- replicating programs, etc.), or any other unauthorized materials. Staff and students may not use the school system's Internet connection to download games or other entertainment software or to play non-educational games over the Internet. Additionally, you may not use the computer network to display, store or send (by email or any other form of electronic communication such as bulletin boards, chat rooms, Usenet groups, etc.) material that is fraudulent, harassing, embarrassing, sexually explicit, profane, obscene, intimidating, defamatory or otherwise inappropriate or unlawful.

Computer resources are not unlimited. Network bandwidth and storage capacity have finite limits, and all users connected to the network have a responsibility to conserve these resources. As such, the user must not deliberately perform acts that waste computer resources or unfairly monopolize resources to the exclusion of others. These acts include but are not limited to, streaming music or

videos for non- educational purposes, sending chain letters, spending, playing online games, or otherwise creating unnecessary loads on network traffic associated with nonbusiness-related uses of the Internet.

Social/Web 2.0 / Collaborative Content
Recognizing the benefits that collaboration brings to education, MPS may provide users with access to web sites or tools that allow communication, collaboration, sharing, and messaging among users. Users are expected to communicate with the same appropriate, safe, mindful, courteous conduct online as offline. Posts, chats, sharing, and messaging may be monitored. Users should be careful not to share personally- identifying information online.

Mobile Devices Policy
MPS may provide users with mobile computers or other devices to promote learning outside of the classroom. Users should abide by the same acceptable use policies when using school devices off the school network as on the school network. Users are expected to treat these devices with extreme care and caution; these are expensive devices that the school is entrusting to your care. Users should immediately report any loss, damage, or malfunction to IT staff. Users may be financially accountable for any damage resulting from negligence or misuse. Use of school issued mobile devices off the school network may be monitored.

Personally-Owned Devices Policy
Students should keep personally-owned devices (including laptops, tablets, smart phones, cell phones, e-readers, iPod touch) turned off and put away during school hours—unless in the event of an emergency or as instructed by a teacher or staff for educational purposes. Devices are to be used as part of classroom lessons upon teacher approval, and they should not be used in between classes or in the hallways or other common areas. Because of security concerns, when personally-owned mobile devices are used on campus, they must be used over the school network. Access to cellular connections is strictly prohibited. Gaming devices are prohibited.

All devices are on a use at your own risk policy. The School District is not accountable for loss, damage, theft, etc.

Please remember, this Acceptable Use Policy applies to privately-owned devices accessing the MPS network, the MPS Internet connection, and private networks/ Internet connections while on school property. Virus protection for PC's is required.

Users who cannot access the MPS network or who may have technical issues with their technology tool need to take care of this issue by working with the user's manual that came with the device outside of the classroom. These are not MPS devices and the district in not allocating resources at this time to troubleshoot issues.

Security
Users are expected to take reasonable safeguards against the transmission of security threats over the school network. This includes not opening or distributing infected files or programs and not opening files or programs of unknown or untrusted origin. If you believe a computer or mobile device you are using might be infected with a virus, please alert IT. Do not attempt to remove the virus yourself or attempt to download any programs to help remove the virus.

You are responsible for any misuse of your account, even if the inappropriate activity was committed by another person. Therefore, you must take steps to ensure that others do not gain unauthorized

access to your account. In addition, you may not use your account to breach security of another account or attempt to gain unauthorized access to another network or server.

Your password provides access to your account. Sharing your password and account access with unauthorized users is prohibited. You should take care to prevent others from using your account by keeping your password secure since you will be held responsible for such use. Do not leave an unsupervised computer logged on to the network.

Downloads
Users should not download or attempt to download or run .exe programs over the school network or onto school resources without express permission from IT staff. You may be able to download other file types, such as images or videos. For the security of our network, download such files only from reputable sites, and only for education purposes.

Netiquette
Users should always use the Internet, network resources, and online sites in a courteous and respectful manner. Users should recognize that among the valuable content online there is also unverified, incorrect, or inappropriate content. Users should only use trusted sources when conducting research via the Internet. Users should remember not to post anything online that they wouldn't want students, parents, teachers, or future colleges or employers to see. Once something is online, it's out there—and can sometimes be shared and spread in ways you never intended.

Plagiarism
Users should not plagiarize (or use as their own, without citing the original creator) content, including words or images, from the Internet. Users should not take credit for things they didn't create themselves, or misrepresent themselves as an author or creator of something found online. Research conducted via the Internet should be appropriately cited, giving credit to the original author.

Personal Safety
Users should never share personal information, including phone number, address, social security number, birthday, or financial information, over the Internet without adult permission. Users should recognize that communicating over the Internet brings anonymity and associated risks, and should carefully safeguard the personal information of themselves and others. Users should never agree to meet in real life someone they meet online without parental permission. If you see a message, comment, image, or anything else online that makes you concerned for your personal safety, bring it to the attention of an adult (teacher or staff if you're at school; parent if you're using the device at home) immediately.

MPS makes an attempt to protect private information but users who submit personal information online do so at their own risk.

Cyber-bullying
Cyber-bullying will not be tolerated. Harassing, dissing, flaming, denigrating, impersonating, outing, tricking, excluding, and cyber-stalking are all examples of cyber-bullying. Don't be mean. Don't send emails or post comments with the intent of scaring, hurting, or intimidating someone else. Engaging in these behaviors, or any online activities intended to harm (physically or emotionally) another person, will result in severe disciplinary action and loss of privileges. In some cases, cyber-bullying can be a crime. Remember that your activities are monitored and retained.

Social Media Policy

The district has a separate Social Media Policy that applies to all staff, and may have implications for students. By signing the Acceptable Use Policy users are acknowledging they have been made aware of the Social Media Policy and agree to abide with the requirements of the Social Media Policy. Violations of the Social Media Policy are in effect violations of the Acceptable Use Policy.

Vandalism
Any verified acts of vandalism will result in cancellation of privileges. Vandalism is defined as any malicious attempt to harm or destroy the data of another user, the Methuen Public Schools' network, or other networks that are connected to our system through the Internet. This includes, but is not limited to, the uploading or creation of computer viruses.

Privacy
Staff and students are given access to computers and the Internet to assist them in furthering the educational process. Users should have no expectation of privacy in anything they create, store, send or receive using the district's computer equipment. In addition the district, through its designees, reserves the right to monitor, examine, evaluate and disclose all aspects of the technology resources and their use.

Methuen Public Schools is committed to protecting private information of staff and students contained within emails or other online transmissions.

While we cannot guarantee the privacy or confidentiality of information within electronic documents, which is public information, the following procedure will help to protect the privacy and confidentiality of such information.

1. Remember when sending emails regarding students to use ONLY the student identification numbers and the first initial of both their first and last name eg: John Smith would be J.S.#12345.
2. Remember when sending emails regarding staff to use ONLY the staff member's initials and job eg: John Smith teacher would be J.S. teacher.

Examples of Acceptable Use
I will:

- ✓ Use school technologies for school-related activities.
- ✓ Follow the same guidelines for respectful, responsible behavior online that I am expected to follow offline.
- ✓ Treat school resources carefully, and alert staff if there is any problem with their operation.
- ✓ Encourage positive, constructive discussion if allowed to use communicative or collaborative technologies.
- ✓ Alert a teacher or other staff member if I see threatening, inappropriate, or harmful content (images, messages, posts) online.
- ✓ Use school technologies at appropriate times, in approved places, for educational pursuits.
- ✓ Cite sources when using online sites and resources for research.
- ✓ Recognize that use of school technologies is a privilege and treat it as such.
- ✓ Be cautious to protect the safety of myself and others.
- ✓ Help to protect the security of school resources.
- ✓ This is not intended to be an exhaustive list. Users should use their own good judgment when using school technologies

Examples of Unacceptable Use
*I will **not***:

- ✓ Use school technologies in a way that could be personally or physically harmful.

- ✓ Attempt to find inappropriate images or content; intent to seek inappropriate images or content is a violation of this Acceptable Use Policy.
- ✓ Create a personal mobile "hot-spot" or use a "proxy site" for the purpose of circumventing network safety measures and filtering tools.
- ✓ Create, distribute or deploy multi-user servers or gaming software on or within the MPS network.
- ✓ Engage in cyber-bullying, harassment, or disrespectful conduct toward others.
- ✓ Use of obscene, inflammatory, harassing, threatening, or abusive language or images
- ✓ Try to find ways to circumvent the school's safety measures and filtering tools; intent to circumvent safety measures and filtering tools is a violation of this Acceptable Use Policy.
- ✓ Use school technologies to send spam or chain mail.
- ✓ Plagiarize content I find online.
- ✓ Post or otherwise disclose personally-identifying information, about myself or others.
- ✓ Agree to meet someone I meet online in real life.
- ✓ Use language online that would be unacceptable in the classroom.
- ✓ Use school technologies for illegal activities or to pursue information on such activities.
- ✓ Attempt to hack or access sites, servers, or content that isn't intended for my use.
- ✓ Access materials or use email for nonacademic purposes or for purposes that are not approved by the staff member in charge
- ✓ Tamper with data and files being used by others.
- ✓ Use school accounts for personal messages, political lobbying, union messages, gambling, or business transactions, advertising, or commercial (offering or providing products or services) activities.
- ✓ Use or transmit materials that violates copyright laws

This is not intended to be an exhaustive list. Users should use their own good judgment when using school technologies.

Limitation of Liability
MPS will not be responsible for damage or harm to persons, files, data, or hardware.

While MPS employs filtering and other safety and security mechanisms, and attempts to ensure their proper function, it makes no guarantees as to their effectiveness.
MPS will not be responsible, financially or otherwise, for unauthorized transactions conducted over the school network.

Violations of this Acceptable Use Policy
Violations of this policy may have disciplinary repercussions, including:

- Suspension or termination of network, technology, or computer privileges;
- Notification to parents;
- Detention or suspension from school and school-related activities;
- Employment disciplinary action, up to and including termination of employment;
- Legal action and/or prosecution.

The Methuen Public Schools will provide staff with Internet guidelines and training and support in the appropriate and effective use of the internet. The school system will inform parents about Internet guidelines through the use of letters, school newsletters, and handbooks. Additionally, the Methuen Public Schools will continually evaluate tools and software which can potentially assist staff in implementing guidelines, effectiveness, manageability, and any cost for initial purchase and upgrades will be considered.