

MOUNT UNION AREA SCHOOL DISTRICT

SECTION: OPERATIONS

TITLE: ACCEPTABLE USE OF
COMPUTERS AND NETWORK
SERVICES

ADOPTED: April 26, 2004

REVISED: August 24, 2009

<p>1. Purpose</p> <p>2. Authority</p> <p>3. Guidelines</p>	<p style="text-align: center;">815. ACCEPTABLE USE OF COMPUTERS AND NETWORK SERVICES</p> <p>The Board recognizes that computer networks, including the Internet, are important resources that facilitate learning and teaching, thereby enhancing the district's instructional programs. The use of computers and computer networks, most especially the internet and email, are an integral part of society today and, hence, an integral part of the curriculum as outlined in the District Technology Strategic Plan. However, some users may find ways to access material that is illegal, defamatory, inaccurate, or offensive to some people or use the networks for non-intended purposes. The Board is aware of these potential problems but still believes that the benefits that users derive from network access outweigh the disadvantages. To help prevent potential problems, the Board expects administrators, teachers, and staff to work together to help students develop the intellectual skills necessary to discriminate among available information sources, identify information appropriate to their age and developmental level, and evaluate and use obtainable information to meet the educational goals of the adopted curriculum.</p> <p>Furthermore, the Board emphasizes that access to the Internet and other computer networks is a privilege, not a right. Any inappropriate, unauthorized, or illegal use may result in the cancellation of privileges and appropriate disciplinary action.</p> <p>The Technology Director shall periodically review this policy and guidelines and recommend revisions as necessary to the Board for adoption.</p> <p>The use of the District's network, the World Wide Web, and email is a valuable part of education today and all staff shall use these and other technologies in their curricula. Therefore, all students and staff will not be permitted to use the Internet, until a signed Acceptable Use Policy Permission Form is returned to the school district. This form shall be distributed to all students on their first day of elementary and high school and kept in a file until graduation from the respective school. Every employee of the school district shall be required to sign and submit an Acceptable Use Policy form to be kept in their permanent file.</p> <p>This policy shall be published and accessible through the policy section of the District's web site (www.muasd.org/MUASD_info.htm).</p>
--	---

	<p>The following guidelines shall govern the use of the District's computer networking facilities.</p> <p><u>General</u></p> <ol style="list-style-type: none">1. The District shall not:<ol style="list-style-type: none">a. Endorse the content or quality of any information received by students and staff.b. Guarantee the accuracy of information received via the network.c. Be responsible for any user information that may be lost or damaged.d. Guarantee the availability of any information or online resource.e. Be responsible for any unauthorized charges or fees resulting from access to any network services.2. The District reserves the right to log network use, and to randomly monitor and periodically read and review e-mail messages and web sites visited by all users.3. Students and staff have the responsibility to respect and protect the rights of other users both in the District and on the various networks. <p><u>Specifically Prohibited Uses of Computer Networks</u></p> <p>The following uses of the computer networks are prohibited for both students and staff:</p> <ol style="list-style-type: none">1. The facilitation of any illegal activity.2. Commercial or for-profit activities or product advertisement.3. Hate mail, discriminatory remarks, and inappropriate, offensive or inflammatory language including profanity.4. Unauthorized or illegal installation, distribution, reproduction, or use of copyrighted materials.5. Accessing or distribution of obscene or pornographic material.6. Intentionally obtaining or modify files, passwords, or data belonging to other users.7. Impersonation of another user, anonymous communications, and/or the use of pseudonyms or quoting personal communications in a public forum without the original author's prior consent.
--	--

<p>P.L. 94-553 Sec. 107 Pol. 814</p>	<ol style="list-style-type: none">8. Disrupting the work of other users.9. Destruction, modification, abuse, or unauthorized access to network hardware, software, or files.10. Access by users to material that is harmful to minors or is determined inappropriate for minors in accordance with Board policy.11. Transmission of material likely to be offensive, threatening, or objectionable to recipients.12. Copying, communicating, or modifying materials in violation of copyright laws. Failure to properly document material that is copied and pasted from an online resource is plagiarism.13. Loading or using unauthorized games, programs, files, or other electronic media.14. Creating or intentionally uploading viruses. <p><u>Network Overview</u></p> <p>The Internet is a widely recognized form of communication. The District's web site is intended to be a source of information for the entire school community, including all school staff, parents, and students. As part of the initiative to relay as much information as possible to the community, it may be necessary to publish photographs and student projects on the web site. Students shown in photographs that are published on the web site will not be identified. Captions may identify some photographs, but these captions will not include student names.</p> <p>Mount Union Area School District has several safeguards in place that protect students from accessing information that is not suited for educational purposes, including:</p> <ol style="list-style-type: none">1. In order to remain eligible for certain federal funds, to comply with the Children's Internet Protection Act, and to provide a safeguard to help prevent the accidental access of inappropriate material, Internet access will be filtered using filtering software. Use of a filtering program does not remove the responsibility of network users to restrict their online activities that comply with the guidelines and standards of the acceptable use policy.2. Server permissions that limit students to access folders and/or computers set forth by the network administrator.3. An email server that enables technology staff to monitor and track email usage, as necessary.
--	---

Use of Email

Students are not permitted to send or receive email or other forms of electronic communication without the specific approval of a teacher or administrator. Email accounts shall be provided for all MUASD employees and shall be used to support education, district administrative operations and to improve communication between staff members and parents. Electronic mail and files stored on MUASD.org servers are not guaranteed to be private. Antivirus software will be used to reduce the spread of unwanted and/or malicious files. Each user must take steps (verify that antivirus software is installed, do not open attachments from unknown servers) to reduce the spread of viruses and malicious files throughout the MUASD.org network.

Storage of Files

File storage on MUASD.org servers is provided for individuals with MUASD.org user accounts. Storing files on a server allows a user to access the files from any computer in the school district that is connected to the MUASD.org network. Users are encouraged to use the network drive to save files or as one method of backing up files (backups may also be stored on local hard drives when network drives are used for primary storage).

As with all other areas of computer use, use of the MUASD.org servers must be in support of education, academic research, or district administrative operations and must be consistent with this acceptable use policy. Files stored on MUASD.org servers are not private. The network administrator may periodically conduct searches of network files in order to identify files that require large amounts of storage space or are in violation of this policy. Files that violate this acceptable use policy may be deleted without warning under the direction of the network administrator.

Security Protocol That Users Shall Follow

1. System security is protected through the use of passwords. Each user will be issued a password. Because failure to adequately protect or update passwords could result in unauthorized access to personal or district files, employees and students shall not reveal their passwords to other individuals.
2. Network accounts shall be used only by the authorized owner of the account. Users shall not use a computer that has been logged in under another student's or staff member's name.
3. Any user identified as a security risk or having a history of problems with other computer systems may be denied access to the network.
4. Users who identify a security problem shall notify the network administrator, a teacher, or school building administrator. The discovering user shall not demonstrate the finding to other users.

Protection From Harassment and/or Unwanted or Unsolicited Communication

1. Any network user who receives threatening or unwelcome communications shall immediately report them to a teacher, school building administrator, or the network administrator.
2. Network users are reminded that electronic mail is not guaranteed to be private. The release of information such as personal address and telephone numbers by the user on the Internet shall only be permitted under limited circumstances.

Consequences for Inappropriate Use

1. Each user shall be responsible for damages s/he causes to the equipment, systems, and software resulting from deliberate or willful acts.
2. Illegal use of the network, intentional deletion, or damage to files of data belonging to others, copyright violations, or theft of services will be reported to the appropriate legal authorities for possible prosecution.
3. Loss of access and/or other disciplinary actions shall be the consequence for any behavior that does not conform to accepted rules of network etiquette, federal and state laws, or stipulations of this policy.
4. Vandalism may result in cancellation of access privileges in addition to repair costs. Vandalism is defined as any malicious attempt to harm or destroy data of another user, the Internet or other networks and equipment. This includes, but is not limited to, the uploading or creation of computer viruses.
5. The network administrator may at any time close an account of a user who is violating this policy or upon the request of a building administrator, faculty member, or staff member who is aware of a user who is violating this policy.

Account Termination

Authorized MUASD employees may disable or terminate an account as students withdraw or graduate from the district, or as faculty, staff and guests leave the district.