Board of Education
School District of Menomonee Falls
Menomonee Falls, Wisconsin 53051

Policy 363.2

COMPUTER, INTERNAL NETWORK, ELECTRONIC MAIL AND INTERNET SAFETY STUDENT ACCEPTABLE USE

The School District of Menomonee Falls provides employees and students access to the District's computer equipment and internal network and to the Internet for the purpose of furthering the educational goals and objectives of the District, the professional development of its employees, and the educational enrichment of its students. Access to these facilities is available in all District schools.

District computers and network resources may be provided for instructional, development, and management purposes for use by students and staff, subject to the policies set forth herein. District computers and networks may not be used to disrupt educational or management functions, and hardware or software shall not be introduced, destroyed, modified, copied, transferred, decompiled, disassembled, disabled, or otherwise abused in any manner. Users shall not seek information on other users on the District's network, including but not limited to their passwords, files, data, electronic mail, or other data that may be stored and accessible through said computers and networks.

School administrators will apply the same criterion of educational suitability used for other education resources when providing access to software and Internet information resources. All use of these resources shall be directly related to the education of the student, the professional development of the employee, or the management of these resources by staff and administrators of the District.

Because the Internet is a fluid environment that includes materials of questionable educational value, and because it provides access to many, constantly changing resources throughout the world, it is impossible for school administrators to review and pre-select materials that are appropriate for the use of our students and employees. The District expects its students to exercise good judgment designed to further their education at the District. Therefore, the District has adopted practices regarding access to and use of District electronic resources and networks, especially the Internet.

The District firmly believes that the valuable information, interaction, collaboration, and peer contact available on the Internet all outweigh the possibility that students and employees may inadvertently access materials that are not consistent with the educational and professional development goals of the District. Ultimately, we rely on the parents and guardians of minors to be responsible for conveying and enforcing standards that their children should follow when using electronic resources like the Internet or any other media, and we rely on our employees to use good judgment in selecting these resources for their use and students' use.

We have extensive systems and security mechanisms in place for the security, integrity, and appropriateness of the data on our networks. We respect each family's right to decide whether to allow their student(s) access to the Internet.

The District will ensure that every student's parent or guardian is notified of these network and Internet use policies and procedures in the beginning of each school year. The District reserves the right to distribute a summary of this policy at the beginning of the year, rather than the full policy and procedure. Parents will be informed of the procedure to receive a complete copy of the policy and the procedure regarding student use of computer systems. Parents must review this policy and procedure with their children, explaining its provisions in a manner in which the student understands. Parents must grant permission for the student to access the school's internal networks and the Internet before the District will assign a User ID and password to the student. In addition to this parental review, appropriate District employees will review this policy with students at appropriate times during each school year and will ensure that they have permission slips for all students who access the District's networks and the Internet.

Legal References: Wisconsin Statutes: Sections 115.38(2), 118.13, 120.12(1), 120.13(1), 121.02(1)(h), 943.70, 947.0125

Wisconsin Administrative Code PI8.01(2)(h), PI8.01(2)(k), PI 9.03(1)

United States Code: Children's Internet Protection Act, Neighborhood Children's Internet Protection Act, Children's Online Privacy Act, Federal Copyright Law, Technology Education and Copyright Harmonization Act (TEACH Act), 47 U.S.C. § 230 *et seq*., 15 U.S.C. § 6501 *et seq.*, 20 U.S.C. § 6777, Ch. 17 USC Copyright

Code of Federal Regulations: 47 C.F.R. § 54.520

Cross References: 522.7 Procedure Computer, Internal Network, Electronic Mail, and Internet Safety (Staff Policy)
771 Policy Copyrighted Materials
411.1 Policy Harassment and Bullying of Students Prohibited
448.2 Student Suspension/Explusion

Approved: January 24, 2005
Revised: June 11, 2007
Revised: April 12, 2010

A. Management, Administration, Monitoring, and Privacy

1. The District has software and systems in place that monitor and record all Internet usage. The District wants users to be aware that our security systems are capable of monitoring and recording, for each and every user, each World Wide Web site visit and the amount of time spent actively using the World Wide Web, and we reserve the right to do so at any time, without advance notice or warning to the user. No District student or employee should have any expectation of privacy as to his or her computer or Internet usage, or the privacy of any content, electronic mail message, file, download, note, or other data stored on, transmitted, or received through any District computing facility. The District may review content, computing activity and usage patterns, and may choose to publicize this data to assure that the District's computing resources are devoted to maintaining the highest standards of educational benefit and employee productivity.

2. The District, through appropriate management personnel, reserves the right to inspect any and all data stored in public or private areas of networked and individual storage systems of any kind, without notice or warning, and at any time or for any purpose.

3. The District uses services to identify and block Internet content that is inconsistent with the educational and professional development goals of the District. We will block access from within our networks to all such sites that we know of or that our services identify. These services endeavor to block use of the network to create, view, send, receive, store, display, or print text of graphics which may reasonably be construed to be obscene, disruptive, or harmful to the educational or working environment No blocking or filtering mechanism is capable of blocking all inappropriate content all of the time. Students and employees may not use District computers for viewing or accessing any site that contains any offensive, disruptive, or harmful material, including but not limited to those listed above. Offensive, disruptive, or harmful data include, but are not limited to any messages of files, or data which contain the following:

    - pornographic or erotic content,
    - sexual content,
    - racial slurs,
    - derogatory gender-specific comments,
    - information or instructions designed to cause physical harm to another person,
    - comments that offensively address a person's age, sexual orientation, religious beliefs, political beliefs, national origin, or disability,
    - any comment intended to frighten, intimidate, threaten, abuse, annoy, or harass another person,
    - those data or activities which invade the privacy of another person

    If a student or employee finds that he/she is connected to a site that contains any offensive, disruptive, or harmful material, including but not limited to those listed above, he/she must disconnect from that site immediately, regardless of whether that site has been previously deemed acceptable by any screening or rating program, and inform the teacher or supervisor of the incident.

    The District's goal in creating the above standards and reporting requirement is not to create an environment of fear and apprehensiveness for users accessing the Internet and internal networks, but to affirmatively set forth content standards for users to be mindful of when accessing these resources.

4. The District will fully cooperate with requests from law enforcement and regulatory agencies for logs, diaries, data, and archives on individual computing activities.

B. Systems Management, Data Integrity, and Security

1. Non-District owned hardware or software should not be introduced into the system without approval from the appropriate systems management personnel.

2. Students may only download or upload files that are specifically identified by a teacher for a specified school project. Employees shall download or upload only those materials that are applicable to their position in the District.

3. No employee or student may use District computing facilities to download or distribute software or data that is pirated, or in a manner inconsistent with its license agreement or applicable copyright law and District copyright policy. Any software or files transferred in any manner into or via the District's computing facilities becomes the property of the District, subject to the restrictions of any existing licensing agreement or applicable copyright law or policy. In any event, such downloaded files, regardless of license or license ownership, may only be used in a manner consistent with their licenses or copyrights, applicable District policy and other controlling authority.

4. Unless software or data transferred into the District's computing facilities is part of an approved educational curriculum, students and employees must understand that the unauthorized use or independent installation of non-standard data may cause computers and networks to function erratically, improperly, or cause data loss No software should be installed that is not directly related to or approved through an existing curriculum. Users should seek the assistance of qualified systems management personnel in using non-standard software and data, and must never install downloaded software to networked storage devices without the assistance and approval of appropriate personnel.

5. No employee or student may use the District's computing facilities to propagate any virus, worm, Trojan horse, trap-door program code, or any form of destructive or malicious computer instruction. Further, employees or students may not propagate any virus "warnings" via electronic mail except to alert appropriate District systems management personnel.

6. Students and employees may not intentionally delete or modify data that is used as part of an approved educational curriculum, except where the deletion or modification of said data is part of that curriculum. Users must respect the fact that, much like a library, software and data are made available for all to use and benefit from.

7. No employee or student may use the District's computing facilities to disable or overload any computer system or network, or to circumvent any system intended to protect the privacy or security of another user or the user's data.

8. All data that is transferred into the District's computing facilities must be checked for viruses before it is run or otherwise accessed. On computers where virus scanning takes place automatically, the virus scanning software must not be disabled, modified, uninstalled, or otherwise inactivated. If you are uncertain as to whether the workstation you are using is capable of detecting viruses automatically, or you are unsure whether the data has been adequately checked for viruses, you should contact appropriate site systems management personnel.

9. No student or employee may use the District's computing facilities to access or attempt to access stored materials or data that are not appropriate for their position, or are outside the scope of their education or employment duties.

C. User IDs and Passwords

1. Every student and employee accessing District computing resources will be assigned a User ID and/or password that functions as the method of access to our computing facilities. Users should guard this information as any other identifying material, such as bank account numbers. Users will be held fully accountable for activity that occurs on any District computing facility under the individual User ID and password, regardless of whether the person assigned to the User ID and password is the actual user. Therefore, great care should be taken not to share or otherwise disclose this information to another person.

2. User IDs and passwords should never be written in a conspicuous place, written down together, or shared with any third party other than authorized District personnel. If a password is lost or forgotten, (or User ID and password together), the student or employee must immediately inform appropriate systems management personnel so his/her account can be temporarily deactivated and a new password assigned.

3. The District has security facilities available to detect an intruder who may be attempting to use or guess another's User ID and password to gain access to resources they are not authorized to use. If you find that your account has become disabled because of an intruder's attempt to access our computing facilities, you should contact appropriate systems management personnel for assistance.

4. Some student users may not be granted User Ids and passwords if their foreseeable computer use will not involve storing files or accessing the Internet.

5. Passwords not disclosed to authorized District personnel may not be used.

D. Electronic Mail

1. Electronic mail should primarily be used for District business, instructional purposes, collaboration with fellow students and peers, and other activities directly related to a user's education or employment. While we recognize that a minimal and incidental amount of personal use occurs with any communications medium, we strongly discourage users from using District computing resources for personal communication, and expressly prohibit commercial use or for personal enrichment or profit.

2. Though electronic mail is a fast and relatively easy mode of communication, nothing should be included in an electronic mail message that the user would not want read by a third party.

3. Employees and students may not use District electronic mail facilities to propagate chain letters, advertising, jokes, personal files, images, offensive, disruptive, or harmful material or any other materials not directly related to their employment or education.

4. Employees and students should keep in mind that electronic mail is a written form of communication, just like a paper letter. Though electronic mail is relatively spontaneous compared with regular mail, care should be taken to use the same level of discretion and

forethought before sending a message, checking it for completeness, accuracy, and grammar just as any written correspondence.

E. World Wide Web Publishing and Use

1. District employees, staff, and teachers will lead students in activities and exercises that strengthen their research skills and enrich the educational process. This may include using search engines in a way that is appropriate for the curricular goal and cognitive level of students, using pre-determined Web resources as a group, or allowing students to independently research subjects consistent with established curriculum and content guidelines set forth herein.

2. Employees and students should read information on the World Wide Web with an evaluative and critical attitude, verifying the sources, authenticity, and accuracy of information to the best of their ability. To that end, employees will endeavor to review Web materials that will be used in classroom learning activities, and use only those that are of the highest quality.

3. Employees and students may bookmark educationally sound Web sites so they may be referred to quickly and easily, without the sometimes-tedious process of discovering the resource on one's own. These bookmarks may be saved on an individual workstation or networked storage device, and should be reviewed regularly by the user for relevance, currentness, and appropriateness to the educational and employment environment.

4. Materials published to the World Wide Web using District computing facilities are considered official District materials, and will be created by appropriate employees. Students may, upon approval of their teacher, create Web pages relating to class projects or other school-related activities. The purpose of Web pages published by the District shall be to communicate information about the District to students, parents, and the public, and to provide an instructional tool with links to other sites that correlate with current curriculum, are age-appropriate, and are reviewed in advance by appropriate District employees.

5. Creation and publishing of Web pages is subject to the following guidelines:

   a. Pages and the data contained thereon belong to the District, and should reflect quality work and accurate information.

   b. Contents must adhere to this Acceptable Use Policy, applicable privacy policies and laws, applicable copyright policies and laws, and other established District policies.

   c. Information published on District web pages should be education-related, non-confidential, and non-commercial. However, advertising for non-profit, school-sponsored organizations is acceptable.

   d. All pages should be created to facilitate easy loading and viewing of graphics and audiovisual materials by the user of the page, whether internal or outside the District, and subject to the restrictions contained in this Acceptable Use Policy.

   e. Links to commercial or personal Web pages shall not be made from any District web page, except where such linking would serve a legitimate educational purpose, and the content on the entire linked site would not violate any provision of this Acceptable Use Policy.

f. District web pages shall not contain the following items without the written consent of an adult pupil or a minor pupil's parent or guardian, or in the case of information about an employee, the employee:

- Students' full names, electronic mail addresses, telephone numbers, street addresses, or any other identifying information.
- Identifying photographs, video, or likenesses of students and staff.
- Employees' personal electronic mail addresses, personal telephone numbers, street addresses, or any other identifying information of a personal nature. Web pages may contain an employee's name, title, work telephone number, work electronic mail address, the building or facility they are employed in, and other work-related information to facilitate communication with parents and other outside correspondents.

6. District web pages should be updated regularly on a schedule determined by appropriate District systems management personnel. Links to outside pages must be reviewed and checked regularly for accuracy. Staff shall be responsible for complying with all District policies and rules and ensuring the content of each District web page and online forum is professional and consistent with the educational mission of the District. Building principals shall review the content of District web pages for purposes of determining compliance with District policies and rules. Any questions from staff regarding the content of District web pages should be directed to the building principal.

7. The District encourages the development of an online educational community through interaction and communication in the District's online classroom forums, District web pages, and other online communication tools. Sharing the work of students with other staff and students throughout the District is a means of fostering the educational community and furthering the educational mission of the District. Use of online forums for classroom discussion and assignments by students and staff is another means of fostering the educational community and furthering the educational mission of the District. Students may use the District's online forums and the work of students may be published on the District's Web pages provided that written consent is provided by the adult pupil or the minor pupil's parent or guardian to allow for such use and disclosure. District web pages and online forums are accessible by District students, staff, parents and guardians, and may be accessible by the public.

8. Students shall demonstrate proper etiquette when using District computers and networks. Each employee and student using the Web and other Internet facilities of the District shall identify himself or herself honestly, accurately, and completely at all times. No employee or student may purport to represent the District or its views, policies, or opinions without the advance approval of the Superintendent, and must refrain from political advocacy, endorsement of products, services, or educational methods, or communication with any media outlet or public forum without such advance approval.

F. Internet Safety

1. The District strives to further its educational mission. In furtherance of that mission, it is the policy of the District to:
   (a) prevent the access or transmission of inappropriate content in its computers and over its networks through electronic mail or other forms of communication;

(b) promote the safety and security of minors using the District's computers, electronic mail, chat rooms, text messaging, instant messaging and other forms of communications;
(c) prevent unauthorized access (such as "hacking") and other unlawful activities;
(d) prevent unauthorized online disclosure, use, or dissemination of student personally identifiable information; and
(e) comply with CIPA—the Children's Internet Protection Act, N-CIPA, and all other applicable laws.

2. The District prohibits users of the District's computers or networks from using, accessing, storing or transmitting inappropriate content through the District's computers and networks. Examples of inappropriate content include offensive, profane, abusive, harassing, sexually explicit, threatening or obscene language or visual depictions, as well as pornography and child pornography. Additionally, inappropriate content includes any content in violation of the District's policies and rules, including policies and rules regarding discriminatory conduct, bullying or harassment. The District also prohibits the use of its computers and networks for fostering any acts of academic misconduct, including cheating or plagiarism.

3. Applicable laws require the District to implement technology protection measures such as filters and blocks to prevent online access to inappropriate content Specifically, technology protection measures must be applied to depictions of obscene material or child pornography, and to any material deemed "harmful to minors" under CIPA. The District uses commercially reasonable technology protection measures that allow it to meet CIPA's requirements. In certain limited circumstances reserved to the discretion and decision of the Superintendent or the Superintendent's designee (an administrator, supervisor or other authorized person), the technology protection measures may be disabled, circumvented, or minimized for those demonstrating a bona fide research need to access such filtered or blocked materials, or for other lawful purposes.

4. The ultimate responsibility for appropriate use is the sole responsibility of the individual user. The District understands that a determined user may be able to access inappropriate content on the District's network and that it is impossible to guarantee that users will not gain access to content that may constitute offensive, objectionable or controversial content, The user or the minor user's parent or guardian should not interpret such access as the District's endorsement that the site is CIPA/N-CIPA-compliant or is acceptable, or both. The use of or access to such inappropriate information violates this Policy and other District Policies, which may result in suspension of technology privileges, legal action, and discipline up to and including suspension and expulsion for students and discipline up to and including discharge for employees.

5. The District's prevention of inappropriate network usage includes: (a) preventing minors from accessing inappropriate content online; (b) promoting the safety and security of users of the District's online computer network when using electronic mail, chat rooms, text messaging, blogging, instant messaging, and other forms of communication; (c) preventing unauthorized access (such as "hacking"), vandalism, and other unlawful activities; (d) preventing the unauthorized disclosure, use, and dissemination of a student's personally identifiable information; and (e) restricting access to materials that are harmful to minors. The District uses commercially reasonable measures to promote the online safety and security of information and users of its network and computers, such as firewalls, anti-virus software, and the technology protection measures described above.

6. In order to facilitate the District in its compliance with CIPA , N-CIPA, and other laws and in furtherance of the District's education mission, in the event that a user accesses inappropriate information through the District's network or in the event a user circumvents, disables or modifies the District's network technology protection measures, then the user must immediately report such

action—whether intentional or unintentional—or any other possible misuse by any person of the District's computer system to the teacher, building administrator or authorized District personnel.

7 District staff shall supervise and monitor the use of the District's computers and network by students, in accordance with this policy and applicable law. The District may monitor District computer and network activities by any users for any content, including inappropriate content. District staff shall also be responsible for training and educating District students regarding compliance with District Policy.

G. Resource Considerations

1. Students and employees with Internet access should not use District computing facilities to transfer images, video, or sound materials unless there is an explicit educational purpose for such a transfer. The regular and widespread transfer of such large amounts of data creates a significant burden on any computing facility. Rather than transferring large files via the public Internet, users should ideally download a large amount of data once, then distribute it to others using the District's faster internal network.

2. Whenever possible, students and employees should schedule communications-intensive operations such as large file transfers, video downloads, mass emailing, or the use of streaming audiovisual technology for times when other users are not likely to be performing the same activity.

3. Students and employees will be granted a limited amount of space on the District's networks to store electronic mail, files, and other data. Users may not exceed this quota without the advance approval and assistance of appropriate systems management personnel, and users at their storage limit may find that their access to some resources will be automatically restricted or disabled to ensure that the resource will be equally available for everyone to use at all times.

4. The District may, at any time and without warning, move or delete data stored on networked systems to efficiently allocate computing resources to all users. While every reasonable attempt will be made to inform users of such modifications or deletions, users should preserve important or sensitive data on a disk or other removable storage medium, and particularly recognize that there may be circumstances when such a notification will not be possible, such as at the end of an academic year or during a vacation period.

H. Enforcement

1. Any user who fails to comply with District policy and rules or who is identified as a security risk or having a history of problems with computing systems may be denied access to the District's computing facilities, with or without advance notice, warning, or opportunity to cure a defect that may result in such a revocation of privileges.

2. The District reserves the right to report all violations or suspected violations of District, local, State, or Federal laws and policies to the appropriate administrator, agency, or law enforcement authority, and may cooperate fully in the investigation of any activity that may violate established law or policy.

3. The District reserves the right to randomly and periodically review any files and use of the network and to investigate suspected or reported violations of this policy or the law. Violations of this acceptable use policy will be investigated by appropriate District personnel. The scope and nature of the district's investigation will be determined by the nature and seriousness of the alleged violation. Where appropriate, disciplinary action will be taken against students and employees violating any provision of this policy, as provided for by Board policy.

Legal References: Wisconsin Statutes: Sections 115.38(2), 118.13, 120.12(1), 120.13(1), 121.02(1)(h), 943.70, 947.0125

Wisconsin Administrative Code PI8.01(2)(h), PI8.01(2)(k), PI 9.03(1)

United States Code: Children's Internet Protection Act, Neighborhood Children's Internet Protection Act, Children's Online Privacy Act, Federal Copyright Law, Technology Education and Copyright Harmonization Act (TEACH Act), 47 U.S.C. § 230 *et seq*., 15 U.S.C. § 6501 *et seq*., 20 U.S.C. § 6777, Ch. 17 USC Copyright

Code of Federal Regulations: 47 C.F.R. § 54.520

Cross References: 522.7 Procedure Computer, Internal Network, Electronic Mail, and Internet Safety (Staff Policy)
771 Policy Copyrighted Materials
411.1 Policy Harassment and Bullying of Students Prohibited
448.2 Student Suspension/Explusion

Revised: January 24, 2005
Revised: June 11, 2007
Revised: April 12, 2010

As a user of the School District of Menomonee Falls Computer System, I recognize and understand that the District's computer systems are to be used for educational purposes only and in the interests of the District, and that all equipment, software, messages and files are the exclusive property of the District. I understand that use of the computer systems for non-educational purposes or in violation of District Policy is strictly prohibited. I agree not to use the computer systems in a way that is disruptive, offensive, or harmful to myself, others or to the District. Further, I agree not to use a password that has not been disclosed to the District or to share or disclose my password with others. I agree not to use pass codes, access a file or retrieve any stored communication, other than where authorized, unless there has been prior clearance by a teacher or District administrator. I agree not to copy, send or receive copyrighted or confidential materials without permission.

I am aware that the District reserves, and will exercise the right, to review, audit, intercept, access and, if necessary, disclose all matters on the District's computer systems when legitimate purposes require it. I am aware that the District may exercise these rights with or without notice. I am aware that use of a password or code does not guarantee confidentiality, privacy or restrict the District's right to access electronic communications.

STUDENT

I understand and will abide by the Computer, Internal Network, Electronic Mail, and Internet Safety Policy and related Policies and Rules. Should I commit any violation, I understand that the District may take appropriate legal action, disciplinary action up to and including suspension or expulsion, and other action to preserve the integrity of the District's property and networks. If I am an adult student, then I consent to the use of the District's online forums and web pages and to the disclosure of my personally identifiable information and the disclosure or showcase of my image and work on District web pages and online forums where consent may be required under this Policy.

Name (please print):_____

Signature:_____

Date:_____ Grade:_____

PARENT OR GUARDIAN:

As the parent or guardian of this student, I have read the Computer, Internal Network, Electronic Mail, and Internet Safety Policy. I understand that this access is designed for educational purposes. I recognize that it is impossible for the School District of Menomonee Falls to restrict access to all controversial materials, and I will not hold them responsible for materials acquired on the network. I consent to my student's use of the District's online forums and web pages and the disclosure of my student's personally identifiable information and the disclosure or showcase of his or her image and work on District web pages and online forums where consent may be required under this Policy. I hereby give permission to issue accounts for my child and certify that the information contained in this form is correct.

Parent or Guardian's Name (please print):_____

Signature:_____

Date:_____