

COMPUTER, INTERNAL NETWORK, ELECTRONIC MAIL, AND INTERNET
ACCEPTABLE USE POLICY FOR EMPLOYEES

Philosophy

The School District of West Allis-West Milwaukee provides employees and students access to the District's computers, communications systems¹, the Internet, and other technology resources 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. For the purpose of this Acceptable Use Policy (AUP), the district refers to "users" as all students, faculty, administrators, staff, community members, and others who are granted access to the district computers and network. Access to these facilities is available in all District schools.

¹ Communication systems include network, wireless access points, cell phones, instant messaging, e-mail, e-Learning platforms, and/or other emerging technologies.

The District permits responsible and safe use of Web resources for instructional and educational purposes. Web resources are a collection of tools that enable interaction on the Internet. Web resources include the Internet, e-Learning platforms, blogs, wikis, podcasts, video casts, social-bookmarking, social networking sites, multi-user role-playing environments, video games and other forms of electronic communication. Users are expected to engage in safe and acceptable use of these resources in accordance with the policies and educational objectives of the West Allis – West Milwaukee School District.

The West Allis-West Milwaukee School District firmly believes that the valuable information, interaction, collaboration, and peer contact available on the Internet all outweigh the possibility that users may access materials that are not consistent with the educational and professional development goals of the District. Ultimately, we rely on our employees to be responsible enforcing standards that they must follow when using electronic resources like the Internet or any other media to use good judgment in selecting the resources they will use that meet the District's educational goals.

Non-District-Provided Technology (Bring Your Own Device –BYOD)

The District permits use of personal technology devices by students and staff in support of teaching and learning, managing resources, and connecting with stakeholders. Personal devices must meet minimum requirements for network access. Use of personal devices is permitted so long as it does not interfere with educational or employment responsibilities and as long as the use does not hinder, disrupt or consume an unreasonable amount of network resources, violate state or federal law, or Board policies.

Users may bring personal devices into the District to access the District network. Personal devices may include laptop computers, tablets, cell phones, iPods/MP3 players, wireless devices, digital cameras, storage devices, or other electronics that may be carried on a person. The District is not liable for the loss, theft, damage, or misuse of any personal device including while on, to , or from District property or while attending school-sponsored activities.

Users that make use of any personal technology must follow all rules and guidelines of this Policy and related policies, guidelines and rules. No cameras, video recorders, cell phones or other personal devices may be used in locker rooms or rest rooms.

**COMPUTER, INTERNAL NETWORK, ELECTRONIC MAIL, AND INTERNET
ACCEPTABLE USE POLICY FOR EMPLOYEES**

The District reserves the right to confiscate and search personal devices if reasonable suspicion exists that the use of the device or technology is in violation of this policy.

The District may establish standardized guidelines regarding the use, nonuse or scope of permissible use of personal devices at the elementary and secondary levels.

Parental Opt-Out Provision

The Board of Education supports the use of technology and Web resources, to create a personalized learning environment that engages today's digital learners in developing core academic knowledge, critical thinking skills, collaboration, communication, and problem solving skills to effectively prepare students for success in today's global economy.

As part of a student's education in West Allis - West Milwaukee School District, their work, picture, and opinions may be posted on the school's website or on a school sponsored Internet project. Any student whose parents have signed a district media opt-out form should not be pictured on the school's external website or on a school sponsored Internet project.

Limitations/Privileges/Privacy

Technology resources, like any other school property, are owned by and the property of the District and subject to the District's rights under contract and law. At any time and without warning, the District may remove computer software and move or delete data stored on networked systems.

Information on the Internet is constantly changing and it is impossible to predict with certainty what information individuals might locate. Making electronic information available to individuals does not imply endorsement of that content by the District. The District is not liable for any damage suffered by a user of the system, including but not limited to, loss of data stored on or transmitted by technology resources or interruptions of service. The District is not responsible for any mistakes or negligence, liability, copyright infringements or other costs incurred by the person using the District's technology resources, or the accuracy or quality of information received over the Web resources.

Users should have no expectation of privacy in the contents of any communications or files on District technology resources, individual storage systems, or Web resources unless such expectation is granted by law. The District maintains the right to access, inspect, investigate and monitor all use and its technology resources, including all files, communications and information created on, with or transmitted using its technology resources or Web resources, and including e-mail, text messages, internet usage, and any other communications or information, without notice to or consent of the user. All such files, communications, or information can be reviewed by the District for any purpose and at any time, and may be subject to monitoring, review and disclosure pursuant to civil and criminal matters, investigatory purposes, or any other lawful reason.

COMPUTER, INTERNAL NETWORK, ELECTRONIC MAIL, AND INTERNET
ACCEPTABLE USE POLICY FOR EMPLOYEES

CIPA (Children's Internet Protection Act)

It is the policy of West Allis - West Milwaukee School District 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 the Children's Internet Protection Act [Pub. L. No. 106-554 and 47 USC 254(h)] and all other applicable laws.

The District uses an Internet content filtering system to limit access to material that is harmful to students, obscene or disruptive to the educational or work environment. The District uses software designed to filter and block access to pornographic Internet sites. The District uses commercially reasonable technology protection measures designed to comply with CIPA's requirements. The District reserves the right to block sites that do not enhance educational activities or are not in compliance with CIPA. Procedures for the disabling or otherwise modifying any technology protection measure shall be the responsibility of the Manager of Technology Services or designated representative.

No technology measure can block 100% of inappropriate content so the District emphasizes the importance of responsible use and of parent and staff supervision in monitoring use of technology.

Education, Supervision, and Monitoring

It shall be the responsibility of all instructional members of the District and parents to: educate, supervise and monitor appropriate use of the online computer network and access to the Internet in accordance with this Policy. The principal or designee will keep records of Internet safety training students receive.

The District will promote safe online activity for students and educate students about appropriate online behavior, including interacting with other individuals on social networking websites and cyber-bullying awareness and response. As specific Web tools are used in individual classrooms, instruction for proper behavior and etiquette when using those tools will be provided. This includes, but is not limited to:

- Teaching students how to locate and evaluate appropriate electronic sources;
- Teaching students information literacy skills, including understanding of copyright, ethical practice and data privacy; and,
- Teaching students about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyber-bullying awareness and response.

Cyber-Bullying, Harassment, and Defamation

The District's systems may not be used to create, view, send, receive, store, display, or print text or graphics which may be reasonably construed to be obscene, disruptive, or harmful to the educational environment. Users should not engage in activities on the Internet that are sexually explicit or drug related. The District reserves the right to determine, at its sole discretion, whether materials fit into these categories.

COMPUTER, INTERNAL NETWORK, ELECTRONIC MAIL, AND INTERNET
ACCEPTABLE USE POLICY FOR EMPLOYEES

Users will not engage in or in any manner partake in or be a party to cyber-bullying, harassment or defamation. This includes impersonating others, teasing, intimidation, sending/posting inappropriate, hurtful, or false email messages, instant messages, text messages, digital pictures, images, or video.

Acceptable Use Guidelines for All Users

Users should not become involved in any activity on the Internet which would violate the policies of the District. The following actions are prohibited:

- Use of an account other than one's own or misrepresentation of identity
- Use, access, storage, or transmittal of inappropriate content (Examples of inappropriate content include offensive, profane, drug-related, sexually explicit, obscene language or visual depictions, as well as pornography)
- Intentionally bypassing District filters, including the use of proxy sites
- Use the District resources for political advocacy
- Use of District resources to propagate chain letters or advertising
- Use of District resources for commercial purposes, personal financial gain, or fraud
- Plagiarism or representing the work of others as one's own
- Accessing, changing, destroying, or sharing computer files that do not belong to the user
- Revealing personal data of students and staff (Examples of personal data include social security numbers, credit card information, personal addresses or telephone numbers)
- Illegally transferring software or other copyrighted material
- Damaging or modifying computers or networks
- Intentional or neglectful transmission of viruses or other destructive computer files
- Hacking into District or external computers

Consequences

Inappropriate use of the District's technology resources, Web resources or District property and any other violation of District policies, guidelines or rules may result in suspension of technology privileges, report to criminal authorities, legal action, and discipline up to and including discipline up to and including discharge. Specifically, employees are notified that sexually explicit or pornographic content has no place in the District and violators who use or access such content will face severe consequences including termination. In addition, violations may result in financial charges for repair, replacement or services, as well as legal action. Appeals may be made in accordance with appropriate Board policies, procedures, employee contracts and handbooks.

The District will cooperate fully with local, state or federal officials in any investigation related to any illegal activities conducted through the District's systems.

**COMPUTER, INTERNAL NETWORK, ELECTRONIC MAIL, AND INTERNET
ACCEPTABLE USE POLICY FOR EMPLOYEES**

The complete computer use rule (522.6-Rule, Computer, Internal Network, Electronic Mail, and Internet Acceptable Use Policy for Employees Provisions) can be found on the District's website: www.wawm.k12.wi.us. This policy and the accompanying rule (522.6-Rule) are to be read in conjunction with one another and one shall not limit or restrict enforcement of the other. If there is confusion regarding a provision in the policy, the rule should be consulted for clarification.

LEGAL REF.: Sections 120.13 Wisconsin Statutes
943.70
947.0125
968.27 – 968.27
Electronic Communications Privacy Act of 1986

CROSS REF.: 522.6-Rule, Computer, Internal Network, Electronic Mail, and Internet Acceptable Use Policy for Employees Provisions

APPROVED: April 2, 2001

REVISED: February 24, 2003
June 14, 2010
April 9, 2012