COMPUTER /ONLINE SERVICES
(Acceptable Use and Internet Safety)

The Middletown City School District provides an electronic communications network that allows District-authorized individuals internal access to District information resources and external access to the Internet. Access to the District network and the Internet is a privilege granted to individuals to support education, research and District business and is therefore subject to certain restrictions as may be set forth by the Board of Education or the Superintendent. The provisions of these regulations apply to any individual granted access to the District network and include all aspects of network use, including any and all information/data. Violation of any provisions of these regulations may result in disciplinary action, up to and including termination.

I. Access to Information

The District provides individuals access to information systems, including the Internet and the District network. The District is not liable if an individual chooses to access an inappropriate Web site or use network access inappropriately, regardless of the type of system or equipment used.

A. Acceptable Uses

1. Support District goals;
2. Promote student achievement;
3. Serve as a resource for information retrieval;
4. Encourage career development and educational advancement;
5. Enhance communication and collaboration among staff, parents and community members;
6. Assist non-instructional staff in performing District duties;
7. Limited personal use;

Individuals may have limited personal Internet use to briefly perform tasks essential to daily living. For example, employee use of the Internet to locate contact information for childcare providers, businesses or medical providers would be acceptable in most cases. However, these activities are limited to those that do not congest, delay or disrupt service or cause any other burden on the District network or equipment.

B. Unacceptable Uses

The Board of Education expects all employees to act in a professional and responsible manner at all times. Transmission of material in violation of any federal or state law or regulation or District policy or regulation is strictly prohibited.

Unacceptable uses include, but are not limited to, the following types of conduct:

1. Any act that may be harmful to minors including accessing and distributing material that may be harmful to minors;
2. Taking any actions that may disrupt the District network;
3. Knowingly introducing or attempting to introduce viruses or other malware into the network;
4. Unauthorized access ("hacking") into computer systems or networks, including logging into a computer with a District-issued account and allowing any other individual access. Employees will be responsible for all actions that occur while others are logged into their accounts;
5. Encouraging or committing unlawful acts or using the District network to promote illegal activities, including accessing gambling, firearms, hate, criminal, pornographic or obscene or terrorism-related sites;
6. Using discriminatory, defamatory, offensive, threatening, intimidating or harassing statements or language, including degrading others based on their race, national origin, sex, sexual orientation, age, disability, religious or political beliefs;
7. Violating copyright laws, including illegally duplicating software or plagiarizing;
8. Accessing proxy avoidance sites;
9. Cyberstalking;
10. Utilizing the District network for commercial purposes such as operating a business for personal or monetary gain;
11. Providing political or campaign information or lobbying for a political cause or candidate that is not directly connected to an instructional activity or exempted by the Superintendent or designee;
12. Posting a student's image on the Web site when the parents of said student have signed a media restriction form;
13. Sharing protected or confidential District information/data with unauthorized persons or for unauthorized purposes;
14. Posting personal information about students or staff without proper authorization;
15. Distributing material protected by trade secret; and
16. Use of religious statements in email, including email signatures and/or handles with religious statements.

II. Social Computing Guidelines

MCSD supports the use of blogs, wikis and other forms of user-generated media; however, inappropriate use of such media can reflect poorly on the district and the individual and can be cause for disciplinary action, up to and including dismissal. The following guidelines are provided to guide employees in making appropriate content choices:

A. Know and follow District Conduct Guidelines. Be aware that all laws, policies regulations and guidelines describing appropriate conduct between employees and students apply to employee conduct on any social network, whether or not the communication occurs using the District Network or other communications technologies

B. Do not link personal web pages and social networking site pages to the District web site.

C. Expect to be held personally responsible for the content published on blogs, wikis or any other form of user-generated media, District or non-District. Be mindful that online published content will be available in the public domain for an undetermined period of time, over which users have little or no control. Employees must protect their privacy.

D. Use name and, when relevant, role at District when discussing District or District-related matters. Write in the first person. Clearly state that content is based on personal opinion and does not represent the position of District.

E. When publishing content related to work done for or associated with the District to any website outside of the District use a disclaimer such as: "The postings on this site are my own and do not necessarily represent the District's positions, strategies or opinions>" or, "This link is not under the control of the Middletown City School District. The District is not responsible for the contents of any linked site or any link contained in a linked site, or any changes or updates to such sites. The district is providing this link to you only as a convenience, and the inclusion of any link does not imply endorsement of the site by the District."

F. Respect copyright, fair use and financial disclosure laws.

G. Respect the audience for the website. Do not use ethnic slurs, personal insults, obscenity, or engage in any conduct that would not be acceptable in MCSD'S workplace. Show proper consideration for others' privacy and for topics that may be considered objectionable or inflammatory.

H. Find out who else is blogging or publishing on a particular topic and cite them as a reference.

I. Use a personal District email account in any communication with students in blogs, wikis or other social networking sites.

III. Monitoring and Filtering

A. Monitoring
The District has the right to inspect and monitor any district system accessed by any individual at all times.

B. Filtering

The District will maintain or subscribe to centralized software to provide Internet control and filtering. The filtering software is intended to allow Internet access while, to the extent possible, inhibiting access to content that is obscene, pornographic, harmful to minors or that promotes gambling, use of illegal drugs, hate speech or other illegal behavior. The filtering software is also intended to prohibit access to sites for online merchandising, alternative journals and games. The District will make every effort to update the filtering software daily.

IV. Privileges

The use of any of the District systems is a privilege, not a right. Inappropriate access, use or other violation of the provisions of this regulation may result in disciplinary action under appropriate federal or state statutes or termination from the District. All activity conducted using District property, including but not limited to documents, pictures, Web sites, phone call logs and/or email is the property of the District; it is therefore not confidential or private and is subject to disclosure under Ohio Public Records Laws.

V. Disclaimer

The Board of Education will not be responsible for any damages suffered, including loss of data resulting from delays, non-deliveries, service interruptions or an individual's mistakes or negligence, costs incurred by individuals or the accuracy or quality of information received from the Internet. The individual accepts personal responsibility for any information obtained via the District network.

VI. Security

Maintaining the security of the District network is a high priority. Attempts to tamper with the network, individual accounts or software applications or to access the network using the name and password of another individual or to share a password will result in disciplinary action, up to and including termination. Electronic mail is not private; system administrators have access to all email as part of their normal job functions. Email messages relating to or in support of illegal activities will be reported to the authorities, and appropriate disciplinary action will follow.

VII. Vandalism

Vandalism of the District network or computer systems will result in disciplinary action, up to and including termination. Vandalism is defined as any malicious attempt to harm or destroy network or computer equipment and/or data of anyone connected to the network. This includes, but is not limited to, uploading, creating or transmitting computer viruses or worms. Network and computer system vandalism, including unauthorized access, is a criminal law violation.

VIII. Exceptions

Any exception to this policy must be granted on an individual basis by the Superintendent/designee.

IX. Email is Public Record

According to the Ohio Public Records Laws, electronic mail ("email") and other like electronic records are considered public records. There are limited exceptions to public disclosure of email communications, which include: emails associated with personnel actions, emails subject to the attorney-client privilege and emails containing information exempt from public disclosure pursuant to the Family Educational Rights and Privacy Act ("FERPA"); however, the vast majority of the email traffic generated within the District is a public record. The District frequently receives public records requests for employee email. When requested, all email, including personal email may be disclosed.

Employees are strongly cautioned not to make any assumption of privacy when using district email.

X. Agreement

Upon the initial use of any district system, all individuals must accept the terms of the *district Network and Communications Technology Usage Agreement,* before they may access any district system.

XI. Glossary

Authorized: Given approval to, right to do or participate in specific assignment or area.

Blog: A blog (a contraction of the term *weblog)* is a website, usually maintained by an individual with regular entries of commentary, descriptions of events, or other material such as graphics or video. Entries are commonly displayed in reverse-chronological order. "Blog" can also be used as a verb, meaning *to maintain or add content to a blog*.

Communication: A process by which information is exchanged between individuals through a common system, exchange of information.

Cyberstalking: Generally defined, stalking involves repeated harassing or threatening behavior. Today, advances in technology have created a new crime—Cyberstalking. While there is not a universally accepted definition, cyberstalking involves the use of the Internet, email or other means of electronic communication to stalk (or harass) another individual. The use of electronic technology has broadened the ways stalkers can harass their victims.

Hacking: To modify a program, often in an unauthorized manner, by changing the code itself.

Harmful to minors: Any act that can be harmful to minors as defined by the Children's Internet Protection Act and including but not limited to any picture, image, graphic image file or other visual depiction that:

- Taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex or excretion;
- 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 acts, or a lewd exhibition of the genitals; and
- Taken as a whole, lacks serious literary, artistic, political or scientific value as to minors.

Information Technology: The technology involving the development, maintenance and use of computer systems, software and networks for the processing and distribution of data.

Internet: An electronic communications network that connects computer networks and organizational computer facilities around the world.

Individual: Employee, both full and part-time; substitute teacher; student teacher; intern; volunteer; contractor; vendor; or other person granted access to use any district technology.

Intern: An advanced student or graduate usually in a professional field (as medicine or teaching) gaining supervised practical experience (as in a hospital or classroom).

Network: A system of computers, peripherals, terminals and databases connected by communication lines.

Student Teacher: College student pursing a degree in education who teaches in a classroom under the supervision of an experienced certified teacher in order to qualify for a degree in education.

Use of district network and communication technologies: Accessing district networks or applications with personal computers, telephones, smart phones or other technology.

Vendor: A company that supplies parts or services to another company (also called "supplier").

Wiki: A page or collection of Web pages designed to enable anyone who accesses it to contribute or modify content, using a simplified markup language. Wikis are often used to create collaborative websites and to power community websites.

XII. Appendix: "Netiquette" Rules (Standards of Conduct)

1. Individuals must abide by the district network etiquette ("netiquette") rules. These rules include but are not limited to the following:

2. Individuals must use appropriate language; use of profanity, vulgarities, abusive or inappropriate language will not be allowed.

3. In any electronic communication that is not used in support of district education, research and business, individuals must not reveal personal information about others, such as full name, personal address or phone numbers.

4. Individuals should release their own personal identification information with discretion, and only when such release supports a student's education or career development. The district is not responsible for any damages or injuries suffered as the result of any individual releasing personal identification information.

[Adoption Date: 10/11/04]

LEGAL REFS.: Children's Internet Protection Act, 47 U.S.C. 254(h) U.S.C.9134
Child Online Protection Act, 47 U.S.C. 231
ORC 149.43 Section (RC)