Book	Administrative Guideline Manual
Section	7000 Property
Title	STAFF NETWORK AND INTERNET ACCEPTABLE USE AND SAFETY
Code	ag7540.04
Status	Active
Legal	P.L. 106-554, Children's Internet Protection Act of 2000 18 U.S.C. 1460 18 U.S.C. 2246 18 U.S.C. 2256 20 U.S.C. 6777, 9134 (2003) 20 U.S.C. 6801 et seq., Part F, Elementary and Secondary Education Act of 1965, as amended (2003) 47 U.S.C. 254(h), (1), Communications Act of 1934, as amended (2003)
Adopted	September 27, 2012

7540.04 - **STAFF NETWORK AND INTERNET ACCEPTABLE USE AND SAFETY**

Staff members are encouraged to use the Board's computers/network and Internet connection for educational purposes. Use of such resources is a privilege, not a right. Staff members must conduct themselves in a responsible, efficient, ethical, and legal manner. Unauthorized or inappropriate use, including any violation of these guidelines, may result in cancellation of the privilege, disciplinary action consistent with the applicable collective bargaining agreement and Board policy, and/or civil criminal liability. Prior to accessing the Internet at school, staff members must sign the Staff Network and Internet Acceptable Use and Safety Agreement.

Smooth operation of the Board's Network relies upon users adhering to the following guidelines. The guidelines outlined below are provided so that users are aware of their responsibilities.

A. Staff members are responsible for their behavior and communication on the Internet. All use of the Network must be consistent with the educational mission and goals of the District.

B. Staff members may only access the Internet by using their assigned Internet/E-mail account. Use of another person's account/address/password is prohibited. Staff members may not allow other users to utilize their passwords. Staff members are responsible for taking steps to prevent unauthorized access to their accounts by logging off or "locking" their computers when leaving them unattended.

C. Staff members may not intentionally seek information on, obtain copies of, or modify files, data or passwords belonging to other users, or misrepresent other users on the network. Staff members may not intentionally disable any security features of the Network.

D. Staff members may not use the Internet to engage in "hacking" or other unlawful activities.

Staff members shall not use the Network to transmit material that is threatening, obscene, disruptive, or sexually explicit or that can be construed as harassment or disparagement of others based upon their race, national origin, sex, sexual orientation, age, disability, religion, or political beliefs. Sending, sharing, viewing, or possessing pictures, text messages, e-mails, or other materials of a sexual nature (i.e. sexting) in electronic or any other form, including the contents of a wireless communication device or other electronic equipment is grounds for discipline up to and including termination. Such actions will be reported to local law enforcement and child services as required by law.

E. Transmission of any material in violation of any State or Federal law or regulation, or Board policy is prohibited.

F. Any use of the Internet for commercial purposes, advertising, or political lobbying is prohibited.

G. Staff members are expected to abide by the following generally accepted rules of network etiquette:

1. Be polite, courteous, and respectful in your messages to others. Use language appropriate to school situations in any communications made through the Board's computers/network. Refrain from using obscene, profane, vulgar, sexually explicit, defamatory, or abusive language in your messages.

2. Never reveal names, addresses, phone numbers, or passwords of students while communicating on the Internet.

3. Check e-mail frequently and delete e-mail promptly from the personal mail directory to avoid excessive use of the electronic mail disk space. Nothing herein alters the staff member's responsibility to preserve e-mail and other electronically stored information that constitutes a public record, student education record, and/or a record subject to a Litigation Hold.

H. Use of the Internet to access, process, distribute, display or print child pornography and other material which is obscene, objectionable, inappropriate or harmful to minors is prohibited. As such, the following material is prohibited: material that appeals to a prurient interest in nudity, sex and excretion; material that depicts, describes or represents in a patently offensive way with respect or 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 material that lacks serious literary, artistic, political or scientific value as to minors. Offensive messages and pictures, inappropriate text files, or files dangerous to the integrity of the Board's computers/network (e.g., viruses) are also prohibited.

I. Malicious use of the Network to develop programs that harass other users or infiltrate a computer or computer system and/or damage the software components of a computer or computing system is prohibited. Staff members may not engage in vandalism or use the Network in such a way that would disrupt its use by others. Vandalism is defined as any malicious or intentional attempt to harm, steal or destroy data of another user, school networks, or technology hardware. This includes but is not limited to uploading or creation of computer viruses, installing unapproved software, changing equipment configurations, deliberately destroying or stealing hardware and its components, or seeking to circumvent or bypass Network security and/or the Board's technology protection measures. Staff members also must avoid intentionally wasting limited resources. Staff members must immediately notify the building principal, or supervisor if they identify a possible security problem. Staff members should not go looking for security problems, because this may be construed as an unlawful attempt to gain access.

J. All communications and information accessible via the Internet should be assumed to be private property (i.e, copyrighted and/or trademarked). All copyright issues regarding software, information, and attributions of authorship must be respected.

K. Downloading of information onto the Board's hard drives is prohibited; all downloads must be to floppy disk. If a staff member transfers files from information services and electronic bulletin board services, the staff member must check the file with a virus-detection program before opening the file for use. Only public domain software may be downloaded. If a staff member transfers a file or software program that infects the Network with a virus and causes damage, the staff member will be liable for any and all repair costs to make the Network once again fully operational.

L. Privacy in communication over the Internet and the Network is not guaranteed. To ensure compliance with these guidelines, the Board reserves the right to monitor, review and inspect any directories, files and/or messages residing on or sent using the Board's computers/network. Messages relating to or in support of illegal activities will be reported to the appropriate authorities.

Staff members have no right or expectation to privacy when using the Network. The District reserves the right to access and inspect any facet of the Network, including, but not limited to, computers, devices, networks or Internet connections, e-mail or other messaging or communication systems or any other electronic media within its technology systems or that otherwise constitutes its property and any data, information, e-mail, communication, transmission, upload, download, message or material of any nature or medium that may be contained therein.

A staff member's use of the Network constitutes his/her waiver of any right to privacy in anything s/he creates, stores, sends, transmits, uploads, downloads or receives on or through the Network and related storage medium and equipment. Routine maintenance and monitoring, utilizing both technical monitoring systems and staff monitoring, may lead to discovery that a staff member has violated Board policy and/or the law.

An individual search will be conducted if there is reasonable suspicion that a staff member has violated Board policy and/or law, or if requested by local, State or Federal law enforcement officials.

Staff are reminded that their communications are subject to Michigan's public records laws and FERPA.

M. Use of the Internet and any information procured from the Internet is at the staff member's own risk. The Board is not responsible for any damage a user suffers, including loss of data resulting from delays, non-deliveries, mis-deliveries, or service interruptions. The Board is not responsible for the accuracy or quality of information obtained through its services. Information (including text, graphics, audio, video, etc.) from Internet sources used in class should be cited the same as references to printed materials.

N. Disclosure, use and/or dissemination of personal identification information of minors via the Internet is prohibited, except as expressly authorized by the minor student's parent/guardian on the "Student Network and Internet Acceptable Use and Safety Agreement Form."

O. Proprietary rights in the design of web sites hosted on the Board's servers remains at all times with the Board without prior written authorization.

Staff members are reminded that personally identifiable student information is confidential and may not be disclosed without prior written parental permission.

Any individual who is aware of a violation of the Board policy or this guideline, including inappropriate on-line contact, content or conduct, such as sexting, harassment or cyberbullying, should bring it to the attention of the school principal or Superintendent immediately.