# Lansing School District
# Internet Safety Policy

I. **Filtering and Monitoring**

A. Filtering software or services will be used on student computers with access to the Internet. This will block or filter access to visual depictions that are obscene, child pornography, or harmful to minors. When adults are using the Internet, materials that are obscene and child pornography must still be filtered or blocked. Requests by faculty and staff to access filtered materials will be reviewed by the Superintendent and/or his or her designee on a case-by-case basis to determine the legitimacy of the educational and/or business reasons underlying such request.

B. Educational staff will, to the best of their ability, monitor student use of the Internet in school, take reasonable measures to prevent access by minors to inappropriate material on the Internet and World Wide Web, restrict access by minors to harmful materials, and enforce compliance with the District's Acceptable Use Policy.

II. **Safety**

A. **Expressly Prohibited Network Use.** In addition to the guidelines and rules stated in the School District's policy entitled "Acceptable Use for Technology," the following network uses are expressly prohibited:

1. No use of School District computers, software, or computer networks ("system") shall serve to disrupt the operation of the system by others; system components including hardware or software shall not be destroyed, modified without administrative permission, or abused in any way.
2. Malicious use of the system to develop programs or institute practices that harass other users or gain unauthorized access to any entity on or outside the system and/or damage the system of an entity on or outside the School District's network is prohibited.
3. Use of the system to access, store, or distribute obscene or pornographic material is prohibited.
4. Subscriptions to mailing lists, bulletin boards, chat groups, and commercial on-line services and other information services must be pre-approved by the Superintendent or his or her designee.

B. **Personal Security**. In addition to the requirements of the School District's policy entitled "Acceptable Use for Technology," the following specific security requirements shall be enforced:

1. Users shall not seek information on, obtain copies of, or modify files, other data, or passwords belonging to other users; misrepresent other users on the system; or attempt to gain unauthorized access to any entity's system.
2. Communications may not be encrypted so as to avoid security review.
3. Users should change passwords regularly and avoid easily guessed passwords, in accordance with School District administrative rules and/or procedures.
4. Personal information such as complete names, addresses, telephone numbers and identifiable photos should remain confidential when communicating on the system. Students should never reveal such

information without permission from their teacher and parent or guardian. No user may disclose, use, or disseminate any personally identifiable information regarding students without prior authorization.

5. Student should never make appointments to meet people in person whom they have contacted on the system without School District and parent permission.
6. Students should notify their teacher or other adult whenever they come across information or messages they deem dangerous or inappropriate on the web or when using electronic mail, chat rooms, and other forms of direct electronic communications (*e.g.* instant message services).

**No Student Expectation of Privacy**

School District Internet access is provided students for educational purposes, only. Accordingly, students have no privacy interest in use of the School District's system, and shall be so advised in writing. The Superintendent or his/her designee shall monitor student usage of the School District's system to ensure compliance with applicable law, regulations, and School District policies and procedures.

**Administrative Rules**

The Superintendent or his/her designee may develop specific procedures, rules, or guidelines to implement and/or enforce this policy.

**Legal References**

47 USC § 254
47 CFR § 54.500, *et seq*.

## Filtering in the District

SquidGuard, a free Internet filtering service, is used in the Lansing School District. SquidGuard was put in place in January 2003 after funding to continue the use of the WebSense subscription was not available. More information about SquidGuard can be found at:

http://www.mesd.k12.or.us/
http://squidguard.mesd.k12.or.us/
http://k12ltsp.org/