Internet Filtering Procedures:

As a District we place a very high importance on providing an educational environment that is focused on the safety and well-being of our students.

The Internet is such a vast and expanding repository of every conceivable topic that sifting out what is appropriate can be a daunting task. To this end the District has employed the use of an Internet Filtering Appliance. The District iBoss Internet filter is tasked with filtering in what is good and filtering out what is bad. This platform is capable of many levels of filtering over a variety of Internet services. Broad Web Categories are set for blanket filtering such as 'Adult Content', 'pornography/nudity', 'private websites', or 'gun & weapons'. There are numerous Web Categories to choose to either allow or block. We block some and allow others. For instance we allow Web Categories 'Government', 'Technology', and 'Transportation' but block 'Violence & Hate' and 'Image/Video Search'. The Web Category database is updated daily from the iBoss service. Hundreds of sites are associated with the various Categories with each update.

We also block sites according to application type. Chat, Gaming, and File Sharing applications are blocked from being used. If a website is considered a social media site it is also blocked.

There is a pre-defined list of Keywords of an adult or high-risk nature that if used in a search string or found in a search result will trigger the filter to block the content from displaying in the web page.

Our iBoss filter is very flexible and gives us the ability to unblock specific sites that may fall into one of the filtering rules even though they may contain relevant material for educational purposes. Conversely we can also block specific sites if they are found to be of no educational value or inappropriate for our students. Web filtering is a moving target and can sometimes be difficult to manage. The sheer number of sites added to the Internet each day makes it a daunting and never-ending endeavor.

We have two filtering groups, Staff and Students.

The Staff filtering group is a little less stringent on the areas that it filters. This allows our staff members to preview sites that may be blocked and recommend those they feel are appropriate for their students. They can then notify the Curriculum Department of the site. The Curriculum Department will evaluate the site and approve or disapprove the site for filtering.

The Student filtering group is configured with a tighter filtering level and is applied to all students in the District. This includes filtering above the requirements to meet the Children's Internet Protection Act (CIPA).

BOARD OF EDUCATION – SOUTH LYON COMMUNITY SCHOOLS

POLICY 7540: ACCEPTABLE USE POLICY FOR TECHNOLOGY

The South Lyon Community School District offers staff and students the opportunity to take advantage of technology in a variety of electronic formats and at the same time realizes adherence to an acceptable use policy is necessary.

South Lyon Community School District
The District manages all information technologies used for educational purposes, and accordingly has the following responsibilities and rights:

Responsibilities

1. Assign network accounts.
2. Maintain and repair electronic information system.
3. Provide training opportunities in the use and application of technology.
4. Provide resources, within the framework of the budget, that support the mission of the school.

Rights

1. Select software, including a filter which limits access to content and materials of legitimate pedagogical concerns only. Despite prudent, reasonable and best efforts, the District is unable to absolutely preclude access to materials deemed inappropriate or otherwise objectionable.
2. Define the privileges and responsibilities of members.
3. Require a signed acceptable use policy contract.
4. Review, retain, edit and/or remove any material from USER ACCOUNT if the superintendent's designee, at his/her sole discretion, believes it may be unlawful, obscene, indecent, abusive or otherwise objectionable or inappropriate.

The District is not responsible for resources accessed or actions taken by its members that are not consistent with the objectives of the district; nor is the District responsible for the loss of data due to system failure.

The District makes no warranties of any kind, whether express or implied, for the use of its educational technology, including but not limited to the loss of data resulting from delays, non-delivery or any service interruption. Furthermore, the district is not responsible for any damages to a user's hardware or software incurred from downloading a computer virus.

The policies and regulations for technology use in the District are in accordance with State laws including Public Act 212.

Network Members
The following people may be granted accounts, upon agreement to the terms stated in this policy, from the District Network:

1. Students who are currently enrolled in the district,
2. Faculty and Staff who are currently employed by the district,
3. Other requests will be granted on a case-by-case basis, depending on need and resource availability.

Privileges
Members have the privilege to use technology in a manner consistent with the educational objectives of the school district.

A user's privilege to access educational technology resources may be restricted, suspended or revoked for violation of this policy. Access may also be inhibited by certain actions, including but not limited to routine maintenance, device availability, daily schedules, course requirements, safety concerns and assignments or reassignments.

Responsibilities
Members are responsible for:

1. Adhering to the terms stated in this policy.
2. Demonstrating appropriate use and care of educational technology and refraining from using any technology for which they have not received training.
3. Notifying the proper authority promptly after identifying or experiencing a problem. Examples of problems that require notification (list should not be considered exhaustive):
    - Damaged equipment
    - Equipment that does not work properly
    - Software that does not work properly
    - Disruption of the network by others
    - Disruption of the system's performance
    - Degrading, demeaning, obscene, indecent or inappropriate information you discover in the system
    - Another user accessing the system through your account and/or Password
    - Programs that infiltrate a computer or system and harass others or cause damage
4. Observing generally accepted rules of network etiquette. Network etiquette includes but is not limited to the following:
    - Be Polite. Do not send defamatory, inaccurate, abusive, obscene, indecent, profane, threatening or illegal material.
    - Use Appropriate Language. Do not swear or use vulgarities or any other inappropriate language.
    - Maintain Privacy. Do not reveal the home address or phone number of yourself or any other person.
    - Avoid Disrupting the Network. Do not use the network in such a way that you disrupt the use of the network by others.

5. Maintaining the integrity of the Network system. Users are expected to utilize systems and services to facilitate learning and enhance educational information exchange. The school District's telecommunications network is intended for District business and educational purposes. As a monitored telecommunications network, no stated or implied guarantee is made regarding the privacy of electronic mail (e-mail) folders, files or documents or any other telecommunications transmitted or received over this network.
6. Adhering to appropriate copyright, trademark, trade secrets and licensing agreements.
7. Receiving permission from the proper authority before using a disk, video or other sources that might endanger the integrity of the network.

Prohibited Use

Use of the school district's education technology is intended for legitimate education purposes which support and enhance school curriculum and business and which are consistent with the school district's mission statement. With the universal acceptance of electronic communication, the District recognizes that usage may extend beyond the intended purpose. However, the District expects this use to be responsible and limited in scope. Users are expected to utilize systems and services in such a fashion as to not disrupt or interfere with the user's responsibilities and the business of the District. The following uses are strictly prohibited and may subject the offender to restriction, suspension or termination of educational technology privileges and to appropriate disciplinary sanctions, such conduct to include, but not be limited to:

1. Using the technology for profit or commercial purposes.
2. Maliciously using technology to harass, intimidate or discriminate against others.
3. Use of the Network to engage in cyberbullying is prohibited. "Cyberbullying" is defined as the use of information and communication technologies (such as e-mail, cell phone and pager text messages, instant messaging (IM), defamatory personal websites, and defamatory online personal polling websites); to support deliberate, repeated, and hostile behavior by an individual or group, that is intended to harm others." [Bill Belsey (http://www.cyberbullying.ca/)

   Cyberbullying includes, but is not limited to the following:
   a. Posting slurs or rumors or other disparaging remarks about a student or a staff member on a website or on weblog;
   b. Sending e-mail or instant messages that are mean or threatening, or so numerous as to be perceived to be harassing in nature;
   c. Using a camera phone to take and send embarrassing and/or sexually explicit photographs/recordings of a student or staff member;
   d. Posting degrading caricatures, misleading or fake photographs of students or staff members on websites.

4. Deliberately damaging any technology component.
5. Unauthorized entry into a file, whether to use, read, change or for any other purpose.
6. Unauthorized transfer, deletion or duplication of a file.
7. Unauthorized use of another individual's identification or password.
8. Unauthorized access to telecommunications files or facilities.
9. Use of computing facilities that interfere with the work of another student, faculty member or school official.
10. Use of computing facilities to draft, send or receive inappropriate communications including, but not limited to, communications which are indecent, obscene, profane, vulgar, threatening, defamatory or otherwise prohibited by law.
11. Use of computing facilities, including telecommunications facilities, to interfere with the operation of the school district's computing system.
12. Violation of copyright, trademark, trade secrets or licensing agreement.
13. Use of computing facilities for the purchase, sale and/or advertisement of goods or services.
14. Use of computing facilities to access chat rooms or student maintained e-mail accounts or any other telecommunications that are of an unsupervised nature.
15. Using technology for political lobbying that does not support the District's mission and does not benefit students and/or the District.
16. Using technology for individual political campaigning.

Consequences of Prohibited Use

Consequences may include any or all of the following:

1. Any member who fails to comply with the terms of this agreement will have his/her privilege revoked for a period of time.
2. Repeated or severe infractions of this policy may result in permanent termination of privileges.
3. The superintendent or his/her designee will determine what is acceptable use based upon this policy. His/her decision is final.
4. Members violating the terms of this policy may face additional disciplinary action deemed appropriate in keeping with the disciplinary policies and guidelines of the school.
5. Users will be required to make restitution for any intentional damages to educational technology or unauthorized expenses incurred through the misuse of educational technology.

Revised January 17, 2011