msba MAINE SCHOOL BOARDS ASSOCIATION
PUBLIC EDUCATION ADVOCATES

49 Community Drive, Augusta, ME 04330
Telephone: (207) 622-3473 Fax: (207) 626-2968
Website: *www.msmaweb.com*

MSSA
Maine School Superintendents Association

TESTIMONY NEITHER FOR NOR AGAINST

L.D. 1333

AN ACT TO PROTECT CHILDREN BY MODERNIZING INTERNET AND DIGITAL MEDIA FILTERING REQUIREMENTS FOR EDUCATION

Senator Rafferty, Representative Brennan and members of the Education and Cultural Affairs Committee. I am Eileen King, deputy executive director of the Maine School Management Association, testifying on behalf of the legislative committees of the Maine School Boards Association and Maine School Superintendents Association, neither for nor against L.D. 1333.

The Children's Internet Protection Act (CIPA) was enacted by Congress in 2000 to address concerns about children's access to obscene or harmful content over the Internet. CIPA imposes certain requirements on schools or libraries that receive discounts for Internet access through the E-rate program – a program that makes Internet access more affordable for schools.

Schools subject to CIPA may not receive the discounts offered by the E-rate program unless they certify that they have an Internet safety policy that includes technology protection measures. The protection measures must block or filter Internet access to pictures that are: (a) obscene; (b) child pornography; or (c) harmful to minors.

Schools subject to CIPA have two additional certification requirements: 1) their Internet safety policies must include monitoring the online activities of minors; and 2) they must educate minors about appropriate online behavior, including interacting with other individuals on social networking websites, in chat rooms, and cyberbullying awareness and response.

Schools subject to CIPA are also required to adopt and implement an Internet safety policy addressing:

- Access by minors to inappropriate matter on the Internet;
- The safety and security of minors when using electronic mail, chat rooms and other forms of direct electronic communications;
- Unauthorized access, including so-called "hacking," and other unlawful activities by minors online;
- Unauthorized disclosure, use, and dissemination of personal information regarding minors; and
- Measures restricting minors' access to materials harmful to them.

To align with CIPA requirements school districts in Maine are required to adopt policies GCSA and GCSA-R that addresses Employee Computer and Internet Use as well as policies IJNDB and IJNDB-R that address Student Computer and Internet Use and Internet Safety. These policies have been included in this testimony for your review.

Steven W. Bailey
MSBA Executive Director

Eileen E. King
MSSA Executive Director

Members of MSLN fall under the Cisco Umbrella filtering system, which is provided to schools for free. Cisco combines multiple monitoring and filtering functions that provide protection for our students on school devices. This type of filtering and monitoring system, if school districts were required to pay for it, would cost our districts thousands of dollars each year.

We support the intent of the bill: keeping our students safe online. Membership to MSLN provides the security this bill is seeking at no cost to our school districts. It is for these reasons that our organizations are neither for nor against L.D. 1333.

EMPLOYEE COMPUTER AND INTERNET USE

[School unit name] computers, network, and Internet access are provided to support the educational mission of the schools and to enhance the curriculum and learning opportunities for students and school staff. This policy and the accompanying rules also apply to laptops, I-pads, tablets and other devices issued directly to staff, whether they are used at school or off school premises.

OPTION ONE

Employees may only utilize the school unit computers, network, and Internet services for purposes related to school programs and operations and performance of their job responsibilities. School unit computers, network, and Internet services may not be used for personal purposes.

OR:

OPTION TWO

School unit computers, network, and Internet services are provided for purposes related to school programs and operations, and performance of their job responsibilities. Incidental personal use of school computers is permitted as long as such use: (1) does not interfere with the employee's job responsibilities and performance; (2) does not interfere with system operations or other system users; and (3) does not violate this policy and the accompanying rules, or any other Board policy, procedure or school rules. "Incidental personal use" is defined as use by an individual employee for occasional personal communications.

Compliance with the school unit's policies and rules concerning computer use is mandatory. An employee who violates this policy and/or any rules governing use of the school unit's computers shall be subject to disciplinary action, up to and including termination. Illegal uses of the school unit's computers will also result in referral to law enforcement.

[School unit name] computers remain under the control, custody, and supervision of the school unit at all times. The school unit reserves the right to monitor all computer and Internet activity by employees. Employees have no expectation of privacy in their use of school computers.

Employees shall be informed of this policy and the accompanying rules through handbooks, the school website, computer start-up page and/or other means selected by the Superintendent. **[Note: This paragraph can be modified to reflect the practice of the local school unit.]**

The Superintendent is responsible for implementing this policy and the accompanying rules. Additional administrative procedures or school rules governing the day-to-day management and operations of the school unit's computer system may be implemented, consistent with Board policies and rules. The Superintendent may delegate specific responsibilities to the Technology Coordinator and others as he/she deems appropriate.

Cross Reference: EGAD – Copyright Compliance
GCSA-R – Employee Computer and Internet Use Rules
IJNDB – Student Computer and Internet Use

EMPLOYEE COMPUTER AND INTERNET USE RULES

These rules implement Board policy GCSA (Employee Computer and Internet Use). Each employee is responsible for his/her actions and activities involving school unit computers, networks, and Internet services, and for his/her computer files, passwords, and accounts. These rules provide general guidance concerning the use of the school unit's computers and examples of prohibited uses. The rules do not attempt to describe every possible prohibited activity by employees. Employees who have questions about whether a particular activity or use is prohibited are encouraged to contact a building administrator or the Technology Coordinator.

A. Consequences for Violation of Computer Use Policy and Rules

Failure to comply with Board policy GCSA, these rules, and/or other procedures or rules governing computer use may result in disciplinary action, up to and including termination. Illegal use of the school unit's computers will also result in referral to law enforcement.

B. Access to School Computers, Networks, and Internet Services

The level of employee access to school unit computers, networks, and Internet services is based upon specific job requirements and needs. Unauthorized access to secure areas of the school unit's computers and networks is strictly prohibited.

C. Acceptable Use

[School unit name] computers, networks, and Internet services are provided to employees for administrative, educational, communication, and research purposes consistent with the school unit's educational mission, curriculum, and instructional goals. All Board policies, school rules, and expectations for professional conduct and communication apply when employees are using the school unit's computers, networks, and Internet services.

D. **Personal Use**

OPTION ONE

Employees may only utilize school unit computers, networks, and Internet services for purposes related to schools programs and operations, and performance of job responsibilities. School unit computers, network, and Internet services may not be used for personal purposes.

OR

OPTION TWO

School unit computers, network, and Internet services are provided for purposes related to school programs and operations, and performance of their job responsibilities. Incidental personal use of school computers is permitted as long as such use: 1) does not interfere with the employee's job responsibilities and performance; 2) does not interfere with system operations or other system users; and 3) does not violate this policy and the accompanying rules, or any other Board policy, procedure, or school rules. "Incidental personal use" is defined as use by an individual employee for occasional personal communications.

E. **Prohibited Uses**

Examples of unacceptable uses that are expressly prohibited include, but are not limited to, the following:

1. Any use that is illegal or which violates other Board policies, procedures, or school rules, including harassing, discriminatory or threatening communications and behavior, violations of copyright laws, etc. The school unit assumes no responsibility for illegal activities of employees while using school computers.

2. Any use involving materials that are obscene, pornographic, sexually explicit or sexually suggestive;

3. Any inappropriate communications with students or minors;

4. Any use for private financial gain, or commercial, advertising, or solicitation purposes;

5. Any use as a forum for communicating by email or any other medium with other school users or outside parties to solicit, proselytize, advocate or communicate the views of an individual or non-school-sponsored organization; to solicit membership in or support of any non-school-sponsored organization; or to raise funds for any non-school-sponsored purpose, whether profit or not-for-profit. No employee shall knowingly provide school e-mail addresses to outside parties whose intent is to communicate with school employees, students, and/or their families for non-school purposes. Employees who are uncertain as to whether particular activities are acceptable should seek further guidance from the building principal or other appropriate administrator.

6. Any communication that represents personal views as those of the school unit or that could be misinterpreted as such;

7. Downloading or loading software or applications without permission from the system administrator. Unauthorized copying of software is illegal and may subject the copier to substantial civil and criminal penalties. The school unit assumes no responsibility for illegal software copying by employees.

8. Sending mass emails to school users or outside parties for school or non-school purposes without the permission of the Technology Coordinator or building administrator.

9. Any malicious use or disruption of the school unit's computers, networks, and Internet services; any breach of security features; or misuse of computer passwords or accounts (the employee's or those of other users);

10. Any misuse or damage to the school unit's computer equipment, including opening or forwarding email attachments (executable files) from unknown sources and/or that may contain viruses;

11. Any attempt to access unauthorized sites or any attempt to disable or circumvent the school unit's filtering/blocking technology;

12. Failing to report a breach of computer security to the system administrator;

13. Using school computers, networks, and Internet services after such access has been denied or revoked; and

14. Any attempt to delete, erase, or otherwise conceal any information stored on a school computer that violates these rules or other Board policies or school rules, or refusing to return computer equipment issued to the employee upon request.

F. No Expectation of Privacy

[School unit name] computers remain under the control, custody, and supervision of the school unit at all times. The school unit reserves the right to monitor all computer and Internet activity by employees and other system users. Employees have no expectation of privacy in their use of school computers, including email messages and stored files, and Internet access logs.

G. Disclosure of Confidential Information

Employees are expected to use appropriate judgment and caution in communications concerning students and staff to ensure that personally identifiable information remains confidential.

H. Employee/Volunteer Responsibility to Supervise Student Computer Use

Employees and volunteers who use school computers with students for instructional purposes have a duty of care to supervise such use. Teachers, staff members, and volunteers are expected to be familiar with the school unit's policies and rules concerning student computer and Internet use and to enforce them. When, in the course of their duties, employees or volunteers become aware of a student violation, they are expected to stop the activity and inform the building principal.

I. Compensation for Losses, Costs and/or Damages

The employee is responsible for compensating the school unit for any losses, costs, or damages incurred by the school unit for violations of Board policies and school rules while the employee is using school unit computers, including the cost of investigating such violations. The school unit assumes

no responsibility for any unauthorized charges or costs incurred by an employee while using school unit computers.

Cross Reference: GCSA - Employee Computer and Internet Use

Adopted: _____

STUDENT COMPUTER AND INTERNET USE AND INTERNET SAFETY

[School unit name] computers, network, and Internet access are provided to support the educational mission of the schools and to enhance the curriculum and learning opportunities for students and school staff. This policy and the accompanying rules also apply to laptops, I-pads, tablets and other devices issued directly to students, whether they are used at school or off school premises.

Compliance with **[School unit name]**'s policies and rules concerning computer and Internet use is mandatory. Students who violate these policies and rules may have their computer privileges limited, suspended, or revoked. The building principal is authorized to determine, after considering the circumstances involved, whether and for how long a student's computer privileges will be altered. The building principal's decision shall be final **[OR: may be appealed to the Superintendent]**.

Violations of this policy and **[School unit name]**'s computer and Internet rules may also result in disciplinary action, referral to law enforcement, and/or legal action.

[School unit name] computers remain under the control, custody, and supervision of the school unit at all times. The school unit monitors all computer and Internet activity by students. Students have no expectation of privacy in their use of school computers, whether they are used on school property or elsewhere.

INTERNET SAFETY

[School unit name] uses filtering technology designed to block materials that are obscene or harmful to minors, and child pornography. Although **[School unit name]** takes precautions to supervise and monitor student use of the Internet, parents should be aware that the **[School unit name]** cannot reasonably prevent all instances of inappropriate computer and Internet use by students in violation of Board policies and rules, including access to objectionable materials and communication with persons outside of the school. The school unit is not responsible for the accuracy or quality of information that students obtain through the Internet.

In the interest of student Internet safety, **[School unit name]** also educates students **[OR: students and parents]** about online behavior, including interacting with other people on social networking sites and in chat rooms, the dangers of engaging in "hacking" and other unlawful online activities. and issues surrounding "sexting" and cyberbullying awareness and response.

The Superintendent /designee shall be responsible for integrating age-appropriate Internet safety training and "digital citizenship" into the curriculum and for documentation of Internet safety training.

IMPLEMENTATION OF POLICY AND "ACCEPTABLE USE" RULES

The Superintendent/designee shall be responsible for implementation of this policy and the accompanying "acceptable use" rules. Superintendent/designee may implement additional administrative procedures or school rules consistent with Board policy to govern Internet access and the day-to-day management, security and operations of the school unit's computer and network systems and to prevent the unauthorized disclosure, use and dissemination of personal information regarding minors.

Students and parents shall be informed of this policy and the accompanying rules through student handbooks, the school website, and/or other means selected by the Superintendent.

Legal Reference: 20 USC § 677 (Enhancing Education through Technology Act)
47 USC § 254(h)(5) (Children's Internet Protection Act)
47 CFR § 54.52 (Children's Internet Protection Act Certifications)
Federal Communications Commission Order and Report 11-125, (August 10, 2011)

Cross Reference: EGAD - Copyright Compliance
GCSA - Employee Computer and Internet Use
IJNDB-R - Student Computer and Internet Use Rules
IJND – Distance Learning Program

STUDENT COMPUTER AND INTERNET USE RULES

These rules accompany Board policy IJNDB (Student Computer and Internet Use). Each student is responsible for his/her actions and activities involving school unit computers (including I-Pads, tablets, laptops and other devices issued to students), networks, and Internet services, and for his/her computer files, passwords, and accounts.

These rules provide general guidance concerning the use of the school unit's computers and examples of prohibited uses. The rules do not attempt to describe every possible prohibited activity by students. Students, parents, and school staff who have questions about whether a particular activity is prohibited are encouraged to contact the building principal or the Technology Coordinator.

A. Acceptable Use

The school unit's computers, networks, and Internet services are provided for educational purposes and research consistent with the school unit's educational mission, curriculum, and instructional goals.

All Board policies, school rules, and expectations concerning student conduct and communications apply when students are using computers, whether the use is on or off school property.

Students are also expected to comply with all specific instructions from school administrators, school staff or volunteers when using the school unit's computers.

B. Consequences for Violation of Computer Use Policy and Rules

Compliance with the school unit's policies and rules concerning computer use is mandatory. Students who violate these policies and rules may, after having been given the opportunity to respond to an alleged violation, have their computer privileges limited, suspended, or revoked. Such violations may also result in disciplinary action, referral to law enforcement, and or legal action.

The building principal shall have final authority to decide whether a student's privileges will be limited, suspended or revoked based upon the circumstances of the particular case, the student's prior disciplinary record, and any other relevant factors.

C. **Prohibited Uses**

Examples of unacceptable uses of school unit computers that are expressly prohibited include, but are not limited to, the following:

1. **Accessing or Posting Inappropriate Materials** – Accessing, submitting, posting, publishing, forwarding, downloading, scanning or displaying defamatory, abusive, obscene, vulgar, sexually explicit, sexually suggestive, threatening, discriminatory, harassing and/or illegal materials or engaging in "cyber bullying;"

2. **Illegal Activities** – Using the school unit's computers, networks, and Internet services for any illegal activity or in violation of any Board policy or school rules. The school unit assumes no responsibility for illegal activities of students while using school computers;

3. **Violating Copyrights** – Copying, downloading or sharing any type of copyrighted materials (including music or films) without the owner's permission (see Board policy/procedure EGAD – Copyright Compliance). The school unit assumes no responsibility for copyright violations by students;

4. **Copying Software** – Copying or downloading software without the express authorization of the Technology Coordinator. Unauthorized copying of software is illegal and may subject the copier to substantial civil and criminal penalties. The school unit assumes no responsibility for illegal software copying by students;

5. **Plagiarism** – Representing as one's own work any materials obtained on the Internet (such as term papers, articles, music, etc.). When Internet sources are used in student work, the author, publisher, and website must be identified;

6. **Non-School-Related Uses** – Using the school unit's computers, networks, and Internet services for any personal reasons not connected with the educational program or assignments;

7. **Misuse of Passwords/Unauthorized Access** – Sharing passwords, using other users' passwords, and accessing or using other users' accounts;

8. **Malicious Use/Vandalism** – Any malicious use, disruption or harm to the school unit's computers, networks, and Internet services, including but not limited to hacking activities and creation/uploading of computer viruses; and

9. **Unauthorized Access to Blogs/Chat Rooms/Social Networking Sites** – Accessing blogs, chat rooms or social networking sites to which student access is prohibited. **[NOTE: Schools that allow such use should modify this paragraph to reflect local decisions.]**

D. **No Expectation of Privacy**

[School unit name] computers remain under the control, custody, and supervision of the school unit at all times. Students have no expectation of privacy in their use of school computers, including email, stored files, and Internet access logs.

E. **Compensation for Losses, Costs, and/or Damages**

The student and his/her parents are responsible for compensating the school unit for any losses, costs, or damages incurred by the school unit for violations of Board policies and rules while the student is using school unit computers, including the cost of investigating such violations. The school unit assumes no responsibility for any unauthorized charges or costs incurred by a student while using school unit computers.

F. **Student Security**

A student is not allowed to reveal his/her full name, address or telephone number, social security number, or other personal information on the Internet without prior permission from a teacher. Students should never agree to meet people they have contacted through the Internet without parental permission. Students should inform their teacher if they access information or messages that are dangerous, inappropriate, or make them uncomfortable in any way.

G. **System Security**

The security of the school unit's computers, networks, and Internet services is a high priority. Any student who identifies a security problem must notify his/her teacher immediately. The student shall not demonstrate the

problem to others or access unauthorized material. Any user who attempts to breach system security, causes a breach of system security, or fails to report a system security problem shall be subject to disciplinary and/or legal action in addition to having his/her computer privileges limited, suspended, or revoked.

H. **Additional Rules for Laptops Issued to Students**

1. Laptops are loaned to students as an educational tool and are only authorized for use in completing school assignments.

2. Before a laptop is issued to a student, the student must sign the school's "acceptable use" agreement. Parents are required to attend an informational meeting before a laptop will be issued to their child. Attendance will be documented by means of a "sign in" sheet. The meeting will orient parents to the goals and workings of the laptop program, expectations for care of school-issued laptops, Internet safety, and the school unit's rules in regard to use of this technology.

3. Students and their parents are responsible for the proper care of laptops at all times, whether on or off school property, including costs associated with repairing or replacing the laptop. **[School unit name]** offers an insurance program for parents to cover replacement costs and/or repair costs for damages not covered by the laptop warranty. Parents who choose not to purchase insurance should be aware that they are responsible for any costs associated with loss, theft, or damage to a laptop issued to their child.

4. Loss or theft of a laptop must be reported immediately to **[insert appropriate school personnel]**, and, if stolen, to the local law enforcement authority as well.

5. The Board's policy and rules concerning computer and Internet use apply to use of laptops at any time or place, on or off school property. Students are responsible for obeying any additional rules concerning care of laptops issued by school staff.

6. Violation of policies or rules governing the use of computers, or any careless use of a laptop may result in a student's laptop being confiscated and/or a student only being allowed to use the laptop under the direct supervision of school staff. The student will also be subject to disciplinary action for any violations of Board policies or school rules.

7. Parents will be informed of their child's login password. Parents are responsible for supervising their child's use of the laptop and Internet access when in use at home.

8. The laptop may only be used by the student to whom it is assigned and by family members, to the extent permitted by Maine's laptop program.

9. Laptops must be returned in acceptable working order at the end of the school year or whenever requested by school staff.

Cross Reference: EGAD – Copyright Compliance
IJNDB – Student Computer and Internet Use