Students Come First

Technology Task Force

One to One Policy Guide

http://www.studentscomefirst.org/

IDAHO STATE DEPARTMENT OF EDUCATION
P.O. BOX 836720
BOISE, ID 83720

Policy Guide Doc. Pg. #	Policy Area	Federal, State or Recommendation for Local Development	Task Force recommendation for policy development	Policy Examples
7.	District Technology Integration Rationale	Recommendations for Local Development	The Technology Task Force encourages Idaho districts to craft and articulate a vision for how technology will support effective instruction and increase student achievement.	Genesee SD (ID) Newton SD (TX) Crescent SD (OK)
9.	Parent involvement and Parental Use	Recommendations for Local Development	The Technology Task Force recognizes that parental involvement has a significant impact on student learning and recommends that all schools provide parent trainings (face to face, online or written format) multiple times throughout the year and that parental attendance is **required** at one training before the mobile device is allowed to be taken to the student's home. While the Technology Task Force encourages parental use of school issued devices it is important to make it clear that: • The mobile computing device is intended to support the academic growth of Idaho students • Parental involvement in student learning through technology is strongly encouraged • Use of school issued technology outside of this purpose (i.e. personal gain, activities unrelated to student learning) is prohibited	MLTI - Maine Crescent SD (OK)
10.	Take home device	Recommendations for Local Development	The Technology Task Force recommends students be permitted to take devices home after a parent training. If districts do not allow students to take devices home, then the district is responsible for ensuring the devices are properly charged. A signed Acceptable Use Policy must be submitted prior for devices to be taken home. It is also recommended that a nominal insurance fee be charged ($25-$75) for students and families interested in taking devices home from school. Fee collections can then be used for districts to self-insure, insure through a third party or to cover the cost of device repair / replacement for malicious damage or loss.	Crescent, (OK) MLTI - Maine
13.	Use outside of Idaho	Recommendations for Local Development	State issued mobile computing devices may be taken out of Idaho at the discretion of the local district. The Technology Task Force strongly recommends local districts set policy that keeps them informed when a student wishes to take the device out of Idaho for either a brief or extended period. The local district is responsible for the devices deployed to its students and is charged with balancing student access to the device and appropriate oversight.	MLTI - Maine
14.	Accounts / authorization	Recommendations for Local	***This may be a state solution. To be clarified when contract is awarded.***	

	(student, teacher, administrator)	Development		
15. 15.	Acceptable / Responsible Use Policy Internet Filtering	**State requirement** Idaho Statue 33-132 **Federal requirement** Children's Internet Protection Act	All Idaho schools are required to have an acceptable use policy that includes the responsibility of the user when the device is used outside the school environment. All users should be made aware of the local school acceptable use policy; it is recommended that the policy be posted on the school or district web site. Local districts are responsible for the devices once deployed. Policy regarding acceptable use, including network usage and internet filtering, is to be crafted at the local level and should emphasize protecting bandwidth and usage for students and staff. All (students, staff, parents, vendors, etc…) who wish to access district provided networks (including WiFi) must agree to and sign the district's Acceptable Use Policy. http://www.fcc.gov/guides/childrens-internet-protection-act	Genesee SD (ID) Newton ISD (TX) Crescent SD (OK) Canby SD (OR) Irving ISD (TX) Auburn, (AL)
38.	Personal Devices in Classroom	Recommendations for Local Development	The Technology Task Force recognizes the challenge of incorporating and monitoring student owned computers into the school one-to-one program and encourages district decision makers to discuss this policy issue with classroom teachers.	
39.	Limitation of Liability	Recommendations for Local Development	For the purposes of limiting liability, the Technology Task Force emphasizes that districts are responsible for devices once deployed.	Clackamas, (OR) William Fremd High School, (IL) Randolph Field Independent SD, (TX)
41.	Augmentation of State Solution	Recommendations for Local Development	Districts interested in supplementing the hardware and / or software of the state issued mobile computing are solely responsible for the initial, and ongoing cost, compatibility, upkeep, maintenance and disposal of supplemental items.	
42.	Parental Consent	Recommendations for Local Development	The Technology Task Force recommends that district policy pertaining to parental consent (i.e. media and library content) include digital content.	Canby, (OR) Kentucky Dept. of Education
43.	Search and Seizure (imbed in AUP – Student Handbook)	Recommendations for Local Development State statutes	The Idaho Constitution at Article I, Section 17 and Idaho Code Section 18-3302D recommendations for search and seizure	Canby (OR)
44.	Intellectual Property Rights	Recommendation for Local Development	Districts are encouraged to expand their existing intellectual property rights policy to include work created through technology and imbed in student	

			handbook.	
45.	Teacher Code of Conduct	Recommendations for Local Development	Additional information regarding teacher code of conduct can be found in the Acceptable Use Policy section of this document. The Technology Task Force recommends districts build policy in this area around the Idaho Professional Standards Commission Code of Ethics for certificated staff and incorporate the appropriate use of technology. http://www.sde.idaho.gov/site/teacher_certification/code_ethics.htm	Randolph SD (TX)
46.	Monitoring of Student Activity on Device	Recommendations for Local Development	All use of school issued electronic device shall not be considered private. Designated District staff shall be authorized to monitor all activity at any time to ensure appropriate use. All monitoring shall comply with local, state and federal laws.	
47.	Individualized Content on Device	Recommendations for Local Development	At no time does the device become the personal property of students or staff; however districts are encouraged to allow students to place individualized items the device, which are limited to music, pictures and other items that do not hinder the network or device functionality. The district should clarify that it is not liable for copyright infringement or loss of data related to individual content placed on the device.	Newton, (TX)
48.	Online Safety	State Requirement Idaho Statute 33-132	The Idaho Attorney General has developed an online safety program titled Protecteens, which addresses this issue, among others. For more information visit: http://www.ag.idaho.gov/internetSafety/protecTeens.html	Genesee SD (ID) Kim Comando Newton SD (TX)
50.	Cyberbullying	**State Requirement** Idaho Statute 18-917A Recommendations for Local Development	The Technology Task Force encourages a strong emphasis on preventing cyberbullying as section 18-917A, Idaho Code prohibits this activity.	Technology for Learning: **A Guidebook for Change**
51.	Technology Advisory Councils / Stakeholder involvement (separate category) Digital Citizenship	Recommendations for Local Development	Stakeholder involvement serves to increase collective ownership of the initiative and can aid in policy implementation and information dissemination. The Technology Task Force encourages districts / schools to: • Establish local councils, including parents and students, to inform technology integration into the learning environment. • Develop policies and practices which include language on digital citizenship and link to common sense media.org • Include reference to digital citizenship in student handbook	

52.	Device Ownership / Responsible entity	Clarification of device chain of responsibility	Similar to any resource local districts purchase with state funds, responsibility of the mobile computing devices resides at the local level. The SDE plans to purchase devices after a 4 year lease cycle at which point districts will be given the opportunity to purchase the devices from the state at a rate similar to what the state paid. Once purchased by the district, re-deployment, re-sale or disposal of technology equipment, after a 4 year life cycle, is at the discretion of the district.	

Policy Guide Background

In 2010 the Idaho state legislature and governor enacted a package of education reform laws, titled ***Students Come First***, that include a significant focus on the integration of technology in instruction including a ***one-to-one*** ratio of mobile computing devices in grades 9-12 (phased in over time), technological upgrades for every classroom and an instructional management system which will enable teachers and parents to access real time information related to the academic performance of students. Critical to the success of these reforms is clear policy and guidance related to the governance of mobile computing devices assigned to students and staff. The components of Students Come First create avenues for students to customize their learning, for teachers to expand their repertoire of resources for instruction, for administrators and school boards to have more control over district operations and for parents to access a higher level of information about student performance and district business. For more information on Students Come First visit: http://www.studentscomefirst.org/.

The Students Come First ***Technology Task Force*** was formed in part to make recommendations around the governance of these devices. This manual is a compilation of Idaho state requirements, policy recommendations and considerations to inform local decision making; the majority of policy design has been left up to local school districts. In addition to best practice policies from throughout the nation stakeholder input, captured through online surveys, was incorporated in the process of developing this guide. For more information on the Technology Task Force visit: http://www.studentscomefirst.org/technologytaskforce.htm.

Statutory Reference for One-to-One Implementation (Section 33-1627(4), Idaho Code)

"In order to assist in providing students with access to online courses, the state department of education shall contract for the provision of mobile computing devices for the students and teachers of each high school. Such devices shall be provided to all high school teachers beginning in the 2012-2013 school year, unless the teacher already has a computing device available and requests that one not be provided. Such devices for teachers shall be replaced every four (4) years.

Devices shall be provided for high school students beginning in the 2013-2014 school year. The number of devices provided to students each year shall be equal to one-third (1/3) of the high school students through the 2015-2016 school year, after which the number shall be equal to the number of ninth grade students

Each school district or public charter school shall develop a policy on student use of the mobile computing devices outside of the school day. Such policy shall be in compliance with the provisions of section 33-132, Idaho Code. *The state department of education shall develop a policy addressing the issue of damage, loss, repair and replacement of the mobile computing devices."*

District Technology Integration Rationale

***EXAMPLE*: Genesee SD (ID) Statement of Purpose:**

District-Provided Access to Electronic Information, Services, and Networks

Internet access and interconnected computer systems are available to the District's students and faculty. Electronic networks, including the Internet, are a part of the District's instructional program in order to promote educational excellence by facilitating resource sharing, innovation, and communication.

***EXAMPLE*: Newton ISO Middle School Laptop Handbook) TX**
Statement of Purpose / Rationale Language:

The District recognizes that available and developing technologies provide tools essential to the efficient and effective operation of our schools and are vital to the teaching/learning process. To ensure that all staff and students receive adequate access to appropriate technology and the training to use it effectively, the following policies shall apply:

A. The purpose of technology is to equip students and staff to become productive and resourceful life-long learners through the access to information and tools to process it;
B. All computer users shall understand and comply with existing copyright laws;
C. District staff shall be permitted to borrow hardware and software in compliance with approved building policies;
D. All hardware purchases shall meet standards to assure compatibility with existing and planned programs, and the hardware inventory shall be updated annually;
E. All software shall be previewed prior to purchase to assure compatibility with existing and planned programs, and the software inventory shall be updated and published annually;
F. The District shall provide staff development activities for all staff appropriate to their assignments;
G. The Director of Finance and Support Services shall work with the district Technology Advisory Council (TAC) to prepare a proposed budget for staff, including staff development, hardware and repair, software and updates, dues and fees, etc.;
H. District and building Technology Advisory Councils shall meet regularly under the direction of district and building technology coordinators to develop, implement, and monitor the practices to support these policies.

***EXAMPLE*: Crescent SD (OK)**
Frequently Asked Questions Language:

Why is there a laptop project?

Crescent Public Schools wants to provide our students with an opportunity to move beyond the norm. Our goal is to develop 21st century skills. Those skills include becoming a self-directed learner

that relies on critical thinking, communication, and problem solving as opposed to the traditional recalling of facts.

Laptops in education are not something one can measure in traditional education. Laptops for each student provides strong degree of equity providing each student an opportunity to participate on a level playing field.

Laptops have students more excited, more engaged, and excited about the opportunity. The laptop provides a 24/7 learning environment. There is an opportunity to work at home, after hours, and it is self-paced.

Finally, the laptop project is an exercise in collaboration. Collaboration with others next door or around the world is yet another opportunity to discover more, learn more, and reach that goal as a 21st century skilled individual.

How do computers change what happens in the classroom?

Good teaching practices are STILL good teaching practices! Knowledge acquisition by students is STILL important! However, computers provide teachers and students a learning "environment" in which teachers can provide the resources needed for students to practice the process of *critical thinking*.

Memorization of facts with little understanding of the concept involved is no longer a *major* part of the students' learning experience.

The teacher's role in the *Digital Learning Environment* is to support students as they become more effective learners. Traditional classes become Hybrid or "Blended" Classes combining the best of face-to- face interactions with the best of Virtual Learning Environments, like Moodle.

Developing a personalized curriculum for 1-to-1 Web-Based Instruction is a time-consuming process requiring teachers to learn new skills. This is the reason Crescent Public Schools uses Wednesday afternoons, from 2 pm to 4 pm, for Staff Development.

Parental Involvement

***EXAMPLE*: Maine Learning Technology Initiative**
Parental Training Requirement:

Northeast and the Island Regional Tech. in Education Consortium Maine and Henrico County expects parents to attend 90-minute training before the mobile device can go home. These sessions provide technical information about the machines as well as an explanation of the code of conduct established for the use and care of the mobile device and are offered several times throughout the day. MLTl participating middle schools and high schools are required to implement take home policies that allow students to take the laptop home.

***EXAMPLE*: Crescent SD (OK)**
Parental Use Policy Language:

The mobile computing device experience is to include parents and guardians of our students. The laptop is an opportunity for all to get involved and to be part of the educational experience.

Frequently Asked Questions

Can parents use the student's laptop?

YES! We want the laptop experience to include parents and guardians of our students. The laptop is an opportunity for all to get involved and to be part of the education experience. We want everyone to benefit.

If you are experiencing difficulty acquiring a login from your student please contact the technology director, _____, at the school and he will assist you with the Information you need.

Can parents use the computer to check their student's grades?

YES! CPS uses an online grade reporting system called Information NOW, by STI. There is a link to this system on the left side of all major District Webpages.

Each student is given a personal "login" to the system so they can stay abreast of their progress. Parents should use the same login to *regularly* check their student's progress. *This may be done from ANY computer connected to the Internet!*

If you are experiencing difficulty acquiring this login from your student please contact the technology director, _____, at the school and he will assist you with the information you need.

Take Home Device

***EXAMPLE*: Crescent, (OK)**
Frequently Asked Question Language

Can the student take the laptop home?

The student may take the laptop home *only* after the purchase of a laptop insurance policy. This policy has a yearly fee of $70.00. There is no deductible and it is a comprehensive plan that covers accidents and theft - but NOT willful misuse.

Every computer taken home MUST have its OWN insurance policy. One policy may NOT be shared by multiple computers. The District will provide an insurance payment plan for families with multiple student computers.

Is the student required to have Internet access at home?

The student is not *required* to have Internet access at home. This is entirely optional and that decision is to be made by each home. However, the school district believes that having Internet access at home *does* provide a valuable and educational opportunity for the home.

How will students get their work done if they do not have Internet access at home?

Students are given the traditional amount of time to do required work in class. In the situation to where a student needs Internet resources in order to complete an assignment, it will be the responsibility of the student to work with the instructor to gather those resources and download them to the student's laptop before leaving campus for the day. Students may access the school wireless network from school campus grounds after school hours in those situations when Internet connection is urgent.

Do I have to have wireless Internet?

Wireless Internet is not a must. Student MacBooks have both wireless and telephone modems. However, wireless Internet provides a greater freedom at school and at home. Wireless connectivity allows individuals to share the same connection from any location within range of the wireless access point.

How do I get Internet access at home?

Internet access is all about availability in your area. The District highly recommends high speed access instead of dial-up. Dialup is adequate for basic functions, like checking email, but in order to access the interactivity of the Internet and media resources, a high speed or broad band connection is recommended.

***EXAMPLE*: Maine Learning Technology Initiative**
Local Take-Home Policy

The Department wants students to be able to take the devices home to support learning. It is strongly recommended that school policies and procedures support take home and do not restrict or make onerous the process of taking the device home at night. Further, the Department strongly

recommends that school policies recognize that students are in the best position to determine when/if it is necessary to take the device home at night.

The Maine Learning Technology Foundation, in cooperation with MLTI, offers free Internet access to those students who qualify.

MLTI participating middle schools and high schools are required to implement take home policies that allow students to take the laptop home.

Care of MacBooks at School & Home

MacBooks should not go home until parents have attended a two to three hour meeting with the school to understand their role and responsibilities, and have signed appropriate policies that the school and district have adopted. Both the student and parent should sign the permission form. Computer laptop procedures and rules for home use should include clearly defined provisions for recharging and caring for the machines, and expectations for appropriate use at home. Without these rules and procedures, students should not take MacBooks off school property.

A basic overview of safe handling is below, along with cleaning information. For a more detailed description of what's on the MacBook and some basic how-to's, please click here to download a pdf version of the MacBook Care & Handling Guide.

General Handling and Care for Parents and Students to know:

- Mishandling of your MacBook could result in your losing it!
- The MacBook is fun to use, but it is not a toy! Remember that it is a computer and must be handled with care.
- The MacBooks belong to the Maine Department of Education. They are on loan to you to use as a tool for learning.
- The Brenthaven Sleeve should be used when transporting the MacBook. The sleeve may be used inside your backpack as well as carried independently. Normal precautions should be taken at all times. Even in the sleeve, you should never place a lot of weight.
- To properly put the MacBook in the sleeve, please ensure the screen (top of the machine) is facing the BACK of the sleeve and that the ports are facing up.
- Protect the computer from the weather.
- Protect it from heat or cold. Don't leave your computer in a car overnight, near a heat source, etc.
- Do not eat or drink near where you are using the computer.
- Computers should not be used in cafeterias, at dinner tables, etc while food/drink are present.
- Close the computer carefully – from the center of the screen – do not slam it shut!
- Use the MacBook on a flat stable surface …….. if it falls it may break! Do not use the laptop in your lap. The laptop should be on a flat smooth surface in order to maintain air flow around the bottom case. Placing the laptop on a pillow or on your bed will cause the MacBook to overheat.
- Do not insert things into openings (ports) of the MacBook.
- Be patient. Sometimes computers require time to do their job.
- If/when you take the MacBook home for assignments, be sure it is recharged for the next school day. Never charge the MacBook while it is in the Brenthaven Sleeve. The MacBook should be in a ventilated space while charging.

- For your own health, when using the computer, it should be kept at least 18 inches from your eyes and the screen should be at a lower level than your eyes.
- Only use standard size CDs and/or DVD discs with the optical drive. Never insert non-standard sized optical media into the drive because the media will get stuck inside the drive.
- You MAY NOT mark the computer in any way with markers, stickers etc.

Cleaning

- Wipe the surfaces lightly with a clean soft cloth.
- Do not use water or other cleaning solutions on the MacBook.
- To keep the screen clean, do not touch it with your fingers.

Cables

- When charging cable needs to be connected, be sure to line it up correctly when inserting and removing.
- If the battery is not charging, do not wiggle the power cord. Try removing it and fully reinserting it.
- Be careful not to jerk the MacBook around when cables are attached.
- Never charge the MacBook while it is in the Brenthaven Sleeve. The MacBook should be in a ventilated space while charging.

Use Outside of Idaho

***EXAMPLE*: Maine Learning Technology Initiative**
Use Outside of Maine

MLTI MacBooks may be taken out of Maine at the discretion of the local school. The Department strongly suggests that local schools set local policy that keeps the school informed when a student wishes to take the device out of Maine for either a brief or extended trip. The local school remains responsible for the devices in its deployment as reflected in the MLTI Asset Manager, although the buffer pool and MLTI Applecare warranty protection remain in place regardless of the location of the laptop.

Accounts (Students, teacher, administrator)

Details will be provided when vendor solution is identified

Acceptable Use / Availability of Access / Internet Filtering

Section 33-132, Idaho Code requires each local school district in the state to adopt and file an internet use policy with the state superintendent of public instruction. The policy, approved by the local board of trustees, shall require filtering technology that blocks internet materials that are harmful to minors, establish disciplinary measures for violators, and provide a component of internet safety to be integrated into the schools instructional program.

Section 33-132, Idaho Code brings Idaho into compliance with the federally mandated **Children's Internet Protection Act** (CIPA), which stipulates the following:

Background

The Children's Internet Protection Act (CIPA) is a federal law enacted by Congress to address concerns about access to offensive content over the Internet on school and library computers. CIPA imposes certain types of requirements on any school or library that receives funding for Internet access or internal connections from the E-rate program – a program that makes certain communications technology more affordable for eligible schools and libraries. In early 2001, the FCC issued rules implementing CIPA.

What CIPA Requires

- Schools and libraries 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 (for computers that are accessed by minors). Before adopting this Internet safety policy, schools and libraries must provide reasonable notice and hold at least one public hearing or meeting to address the proposal.
- Schools subject to CIPA are required to adopt and enforce a policy to monitor online activities of minors.
- Schools and libraries subject to CIPA are required to adopt and implement an Internet safety policy addressing: (a) access by minors to inappropriate matter on the Internet; (b) the safety and security of minors when using electronic mail, chat rooms and other forms of direct electronic communications; (c) unauthorized access, including so-called "hacking," and other unlawful activities by minors online; (d) unauthorized disclosure, use, and dissemination of personal information regarding minors; and (e) measures restricting minors' access to materials harmful to them.

Schools and libraries are required to certify that they have their safety policies and technology in place before receiving E-rate funding.

- CIPA does not affect E-rate funding for schools and libraries receiving discounts only for telecommunications, such as telephone service.

- An authorized person may disable the blocking or filtering measure during use by an adult to enable access for bona fide research or other lawful purposes.
- CIPA does not require the tracking of Internet use by minors or adults.

You can find out more about CIPA or apply for E-rate funding by contacting the Universal Service Administrative Company's (USAC) Schools and Libraries Division (SLD). SLD also operates a client service bureau to answer questions at 1-888-203-8100 or via email through the SLD website.

Additional Information:

For information about other telecommunications issues, visit the FCC's Consumer & Governmental Affairs Bureau website, or contact the FCC's Consumer Center by calling 1-888-CALL-FCC (1-888-225-5322) voice or 1-888-TELL-FCC (1-888-835-5322) TTY; faxing 1-866-418-0232; or writing to:

Federal Communications Commission
Consumer & Governmental Affairs Bureau
Consumer Inquiries and Complaints Division
445 12th Street, SW
Washington, D.C. 20554.
For more information on CIPA visit:
http://www.fcc.gov/guides/childrens-internet-protection-act

***EXAMPLE*: Genesee SD (ID)**
Internet Filtering Policy Language:

Internet Filtering

Filtering is only one of a number of techniques used to manage student's access to the Internet and encourage acceptable usage. It is not viewed as a foolproof approach to preventing access to material considered inappropriate or harmful to minors. Anything that falls under at least one of the categories below shall be blocked/filtered due to its inappropriate content. This list will be updated/modified as required.

- Nudity/ pornography – prevailing U.S. standards for nudity, provocative semi-nudity, sites which contain pornography or links to pornographic sites
- Sexuality – sites which contain materials, images or descriptions of sexual aids, descriptions of sexual acts or techniques, sites which contain inappropriate personal ads
- Violence – sites which promote violence, images or description of graphically violent acts, graphic autopsy or crime-scene images [The intention is to prevent access to sites that sensationalize this content. This is not intended to prevent access to educational content of controversial subjects such as the holocaust or autopsies if deemed appropriate for curriculum purposes.]
- Crime – information of performing criminal acts (e.g., drug or bomb making, computer hacking), illegal file archives (e.g., software piracy)
- Drug Use – sites which promote the use of illegal drugs, material advocating the use of illegal drugs (e.g. marijuana, LSD) or abuse of any drug. Exception: material with valid-educational use

- Tastelessness – images or descriptions of excretory acts (e.g., vomiting, urinating), graphic medical images outside of a medical context
- Language/Profanity – passages/words too coarse to be softened by the word filter, profanity within images/sounds/multimedia files, adult humor [If available, categorical filtering of sites deemed to be excessively profane will be utilized. This does not mean that the filter will parse the content every page as it is requested to search for profanity.]
- Discrimination/Intolerance – Material advocating discrimination (e.g., racial or religious intolerance), sites which promote intolerance, hate or discrimination. Exception: materials with valid educational use if needed for curriculum purposes.
- Interactive Mail/Chat – sites which contain or allow inappropriate email correspondence, sites which contain or allow inappropriate chat areas.
- Inappropriate Banners – advertisements containing inappropriate content.
- Gambling – sites which allow or promote online gambling.
- Weapons – sites which promote illegal weapons, sites which promote the use of illegal weapons. Exception: materials with valid educational use if needed for curriculum purposes.
- Body Modification – sites containing content on tattooing, branding, cutting, etc.
- Additional categories may be blocked for purposes other than objectionable content. Non-educational content, games, or sites that are bandwidth intensive are examples of content that may be blocked or filtered to keep distractions at a minimum and reduce the load on the District network and systems. Filtering should also be used in conjunction with:
- Educating students to utilize the internet in a safe and responsible manner.
- Using recognized Internet gateways as a searching tool and/or homepage for students, in order to facilitate access to appropriate material;
- Using "Acceptable Use Agreements;" Using behavior management practices for which internet access privileges can be earned or lost; and
- Appropriate supervision, either in person and/or electronically.

The technology director and/or building principal and/or instructional staff shall monitor student Internet access. Internet filtering software or other technology-based protection systems may be disabled by a supervising teacher or school administrator, as necessary, for purposes of bona fide research or other educational projects being conducted by students age 18 and older.

Review of filtering technology and software shall be done on a periodic basis and is the responsibility of the Technology Director. It shall be the responsibility of the Technology Director to bring to the Board any suggested modification of the filtering system and to address and assure that the filtering system meets the standards of Idaho Code 18-1514 and any other applicable provisions of Chapter 15, Title 18, Idaho Code.

Acceptable Use Policy Language:

Acceptable Uses

1. **Educational Purposes Only.** All use of the District's electronic network must be (1) in support of education and/or research, and in furtherance of the District's stated educational goals; or (2) for a legitimate school business purpose. Use is a privilege, not a right. Students have no expectation of privacy in any materials that are stored, transmitted, or received via the District's electronic network or District computers. The District reserves the right to monitor, inspect, copy, review and store, at

any time and without prior notice, any and all usage of the computer network and Internet access and any and all information transmitted or received in connection with such usage.

Unacceptable Uses of Network and Resources. The following are considered examples of unacceptable uses and constitute a violation of this policy. Additional unacceptable uses can occur other than those specifically listed or enumerated herein:

A. Uses that violate the law or encourage others to violate the law, including but not limited to transmitting offensive or harassing messages; offering for sale or use any substance the possession or use of which is prohibited by the District's student discipline policy; viewing, transmitting or downloading pornographic materials or materials that encourage others to violate the law; intruding into the networks or computers of others; and downloading or transmitting confidential, trade secret information, or copyrighted materials.
B. Uses that cause harm to others or damage to their property, person or reputation, including but not limited to engaging in defamation (harming another's reputation by lies); employing another's password or some other user identifier that misleads message recipients into believing that someone other than you is communicating, or otherwise using his/her access to the network or the Internet; uploading a worm, virus, other harmful form of programming or vandalism; participating in "hacking" activities or any form of unauthorized access to other computers, networks, or other information.
C. Uses that attempt to bypass District security policies and systems such as internet content filters, proxy servers, and monitoring software.
D. Uses amounting to harassment, sexual harassment, bullying or cyber-bullying. Specific District policies regarding these behaviors exist and shall be applied to such infractions.
E. Uses that jeopardize the security of student access and of the computer network or other networks on the Internet.
F. Uses that constitute the download, access, installation, or modification of software on district systems that are not expressly provided by the district and approved the by the technology director.
G. Connecting or attempting to connect equipment or devices to the district network or systems without the express consent of the technology director.
H. Uses that are commercial transactions. Students and other users may not sell or buy anything over the District provided network or internet connection without prior approval for educational purposes. Students and others should not give information to others, including credit card numbers and social security numbers.
I. Sending, receiving, viewing or downloading obscene materials, materials harmful to minors and materials that depict the sexual exploitation of minors.
J. Students are prohibited from using personal email accounts, social networking services, or chat rooms on the district network, equipment or systems. District provided email accounts or social networking services *may* be provided to students for educational purposes only. Use of such resources shall be in accordance with all other district policies regarding

***EXAMPLE*: Genesee SD (ID)**
Student Possession of Electronic Devices Policy Language:

Student possession of electronic communication devices (cell phones, beeper/pagers, PDAs, laptops or other related electronic devices) is only allowable subject to the following rules and regulations. Strict adherence to these rules and regulations is required.

Possession of an electronic communication device by a student is a privilege which may be forfeited by any student not abiding by the terms of this policy. Students shall be personally and solely responsible for the security of their electronic communication devices. The Genesee Joint School District shall not assume any responsibility for theft, loss or damage of an electronic communication device, or unauthorized use of such device.

Secondary students may use electronic communication devices before and after school, during the lunch break and in between classes as long as they do not create a distraction or disruption. Elementary students may only use electronic communication devices before or after school.

Use of electronic communication devices, except approved laptops and PDAs, at any other time is prohibited and they will be powered completely off, concealed and secured in hall lockers or vehicles during the academic day, but not locker room lockers. Electronic communications devices, with the exception of approved laptops or PDAs, are strictly prohibited in classrooms, locker rooms, restrooms and shower facilities. Students violating this allowable use provision shall be subject to discipline.

On the first violation the device will be confiscated and not returned until a parent conference has been held. Subsequent violations will be subject to suspension and expulsion. No expectation of confidentiality will exist in the use of electronic communication devices on school premises. Laptops and PDAs can be used for educational purposes such as taking notes and writing papers after obtaining prior permission of the Principal with a signed disclaimer by both parent/guardian and student. However the use of any communication functionality of the laptop or PDA is expressly prohibited. This includes, but is not limited to, wireless internet access, peer-to-peer (ad-hoc) networking, or any other method of communication with other devices or networks. In no circumstance will the device be allowed to connect to the District network.

While the use of electronic communication devices by students is allowed subject to these rules, the capability of some devices to take, store or transmit pictures is strictly prohibited. It is the District's position that this use poses a threat to freedoms of privacy. Additionally, these devices can be used to exploit personal information and compromise the integrity of educational programs. Accordingly, the use of the camera function of any electronic communication device is strictly prohibited on school premises at all times. Students who violate this provision of the policy will have their electronic communication device confiscated and held until the end of the school year.

Electronic communication device usage by students while riding to and from school on the bus, or on the bus during school-sponsored activities is at the discretion of the bus driver.

Distracting behavior that creates an unsafe environment will not be tolerated.

***EXAMPLE*: Newton ISD (TX)**
Availability of Access Policy Language:

The Superintendent or designee shall implement, monitor, and evaluate electronic media resources for instructional and administrative purposes.

Access to the District's electronic communications system, including the Internet, shall be made available to students and employees primarily for instructional and administrative purposes and in accordance with administrative regulations. Limited personal use of the system shall be permitted if the use:

I. Imposes no tangible cost on the District;
2. Does not unduly burden the District's computer or network resources; and
3. Has no adverse effect on an employee's job performance or on a student's academic performance.

Use by Members of the Public Policy Language:

Access to the District's electronic communications system, including the Internet, shall be made available to members of the public, in accordance with administrative regulations. Such use shall be permitted so long as the use:

1. Imposes no tangible cost on the District; and
2. Does not unduly burden the District's computer or network resources.

Student Guidelines for Acceptable Use of Technology Resources

These guidelines are provided here so that students and parents are aware of the responsibilities students accept when they use district owned computer hardware, operating system software, application software, stored text, data files, electronic mail, local databases, CDROMs, digitized information, communications technologies and internet access. In general, this requires efficient, ethical and legal utilization of all technology resources.

1. Expectations

a) Student use of computers, other technology hardware, software and computer networks including the internet is only allowed when supervised or granted permission by a staff member.
b) All users are expected to follow existing copyright laws. Copyright guidelines are posted and/or available in the media center of each campus as well as posted in the campus library.
c) Although the District has an Internet safety plan in place, students are expected to notify a staff member whenever they come across information or messages that are inappropriate, dangerous, threatening, or make them feel uncomfortable.
d) Students who identify or know about a security problem are expected to convey the details to their teacher without discussing it with other students.

2. Unacceptable conduct includes, but is not limited to the following:

a) Using the network for illegal activities, including copyright, license or contract violations, downloading inappropriate materials, viruses, and/or software, such as but not limited to hacking and host file sharing software.

b) Using the network for financial or commercial gain, advertising, or political lobbying.
c) Accessing or exploring on-line locations or materials that do not support the curriculum and/or are inappropriate for school assignments, such as but not limited to pornographic sites.
d) Vandalizing and/or tampering with equipment, programs, files, software, system performance or other components of the network. Use or possession of hacking software is strictly prohibited.
e) Causing congestion on the network or interfering with the work of others, e.g., chain letters or broadcast messages to lists or individuals.
f) Intentionally wasting finite resources, i.e., on-line time, real time music. No streaming videos/music.
g) Gaining unauthorized access anywhere on the network.
h) Revealing the home address or phone number of one's self or another person.
i) Invading the privacy of other individuals.
j) Using another user's account, password, or 10 card or allowing another user to access your account, password, or 10.
k) Coaching, helping, observing or joining any unauthorized activity on the network.
I) Forwarding/distributing E-mail messages without permission from the author.
m) Posting anonymous messages or unlawful information on the system.
n) Engaging in sexual harassment or using objectionable language in public or private messages, e.g., racist, terroristic, abusive, sexually explicit, threatening, stalking, demeaning or slanderous.
o) Falsifying permission, authorization or identification documents.
p) Obtain copies of, or modify files, data or passwords belonging to other users on the network.
q) Knowingly placing a computer virus on a computer or network.

Student Code of Conduct - Misbehaviors & Consequences
Computer Resources

District resources have been invested in computer technology to broaden instruction and to prepare students for an increasingly computerized society. Use of these resources is restricted to students working under a teacher's supervision and to approved purposes only. Students and parents will be asked to sign a user agreement regarding appropriate use of these resources; violations of this agreement may prompt termination of privileges and other disciplinary action.

Level II Misbehaviors

Level II misbehaviors are more severe and/or more persistent than Level l misbehaviors. The student's conduct infringes upon the rights of other students or adults. The student's conduct negatively impacts the educational efficiency of other students and the staff. The administrator who is working with the student shall invite the parents to participate in a conference in order to review Level I procedures that have been attempted, to solicit their cooperation in changing the student's behavior, and to inform them of the serious consequences of persistent Level II misbehaviors:

- Engaging in conduct that contains the element of breaching computer security under Section 33.02(b)(1) of the Texas Penal Code.
- Violation of the Guideline for acceptable use of Technology Resources as outlined on pages 8-11 , unless specified as a Level II Misbehavior.

Level II Consequences

Consequences of Level II misbehaviors include, but are not limited to, the following:

1. Any Level l consequence or combination of consequence
2. In-school suspension
3. Suspension
4. Notification of outside agency and/or police with filing of charges when appropriate
5. Behavior contract
6. Behavior improvement parent involvement program
7. Voluntary enrollment in a residential rehabilitation/treatment program
8. Assignment to an alternative education program from four to six weeks and notification of placement sent to the juvenile justice system

Level Ill Misbehaviors

Level Ill misbehaviors are such that the student has disrupted or threatens to disrupt the school's efficiency to such a degree that his/her presence is not acceptable. Common signs of Levell II misbehaviors include, but are not limited to, the following offenses committed on school property or within 300 feet of school property, or while attending a school sponsored or school related activity except as noted:

- Engages in conduct that contains the element of breaching computer security under Section 33.02(b)(2-5) of the Texas Penal Code.
- Use or possession of hacking software or any other software capable of causing harm.

Level Ill Consequences

Consequences of Level Ill misbehaviors include, but are not limited to, any of the following:

1. The consequences of Level II misbehaviors 1-8 shall be assignment to an alternative education program from four to six weeks and notification of placement sent to the juvenile justice system.
2. Notification of police, with filing of charges when appropriate.
3. Permanent removal from the class of the teacher reporting the offense.
4. Voluntary enrollment in a residential rehabilitation/treatment program.
5. Withdrawal of various privileges (computer access).

***EXAMPLE*: Crescent SD (OK)**
Network Access Policy Language:

Students are not *required* to have Internet access at home. This is entirely optional and that decision is to be made by each home. However, the school district believes that having Internet access at home *does* provide a valuable and educational opportunity for the home. Students may access the school wireless network from school grounds after school hours in those situations when Internet connection is urgent.

***EXAMPLE*: Canby SD (OR)**
Acceptable Use Policy Language:

1. The Superintendent, or his/her designee, will serve as the coordinator to oversee the District system and will work with the Clackamas ESD Superintendent, or his/her designee, and other state and local organizations, as necessary.
2. The building principal, or his/her designee, will serve as the building-level coordinators for the system, will approve building-level activities, ensure teachers receive proper training in the use of the system and the requirements of this policy, establish a system to ensure adequate supervision of students using the system, maintain executed user agreements, and be responsible for interpreting the Administrative Procedures at the building level.

3. Designated staff will develop procedures for the use of the Network that are in accord with this policy statement, the Clackamas ESD policy, and other District policies and procedures, including the student code of conduct. These procedures can include, but are not limited to:
    a. Policies and procedures for students, staff and Board members, and guests.
    b. The level of access that will be provided at various grade levels.
    c. A district Web procedure.
    d. Agreements for students, employees and guests, and informational material for parents.
4. System Security:
    a. Users are responsible for the use of their individual account and should take all reasonable precautions to prevent others from being able to use their account. Under no conditions should a user provide his or her password to another person.
    b. Users will immediately notify an appropriate school employee if they have identified a possible security problem. Users will not go looking for security problems, because this may be construed as an illegal attempt to gain access.
    c. Users will avoid the inadvertent spread of computer viruses by following the standard virus protection procedures if they download software.
5. Inappropriate Language
    a. Restrictions against inappropriate language apply to public messages, private messages, and material posted on Web pages.
    b. Users will not use obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful language.
    c. Users will not post information that, if acted upon, could cause damage or a danger of disruption.
    d. Users will not engage in personal attacks, including prejudicial or discriminatory attacks.
    e. Users will not harass another person. Harassment is persistently acting in a manner that distresses or annoys another person. If a user is told by a person to stop sending them messages, they must stop.
    f. Users will not knowingly or recklessly post false or defamatory information about a person or organization.
6. Respecting Resource Limits
    a. Users will use the system only for educational and professional or career development activities, and limited, high-quality, personal research.
    b. Users will not download large files unless absolutely necessary. If necessary, users will download the file at a time when the system is not being heavily used and immediately remove the file from the system computer to their personal computer or diskette.

c. Users will not post chain letters or engage in "spamming". (Spamming is sending an annoying or unnecessary message to a large number of people.)
d. Users will check their E-mail frequently, delete unwanted messages promptly, and stay within their E-mail quota.
e. Users will subscribe only to discussion group mail lists that are relevant to their education or professional/career development. Students may subscribe with the approval of their instructor and must unsubscribe at the end of the school year unless special arrangements are made.

7. Plagiarism and Copyright Infringement
    a. Users will not plagiarize works that they find on the Internet. Plagiarism is taking the ideas or writings of others and presenting them as if they were original to the user. The user should follow the expressed requirements. If the user is unsure whether or not they can use a work, they should request permission from the copyright owner.
    b. Users will respect the rights of copyright owners. Copyright infringement occurs when an individual inappropriately reproduces a work that is protected by a copyright. If a work contains language that specifies acceptable use of that work, the user should follow the expressed requirements. If the user is unsure whether or not they can use a work, they should request permission from the copyright owner.
8. Inappropriate Access to Material
    a. Users will not use the District system to access material that is profane or advocates violence or discrimination towards other people (hate literature). For students, a special exception may be made if the purpose is to conduct research and access is approved by both the teacher and the parent. District employees may access the above material only in the context of legitimate research.
    b. If a user inadvertently accesses such information, they should immediately disclose the inadvertent access in a manner specified by their school. This will protect users against an allegation that they have intentionally violated the policies and procedures.

***EXAMPLE*: Irving ISD (TX)**
Acceptable Use Policy Language:

Guidelines for Acceptable Use of Technology Resources

These guidelines are provided here so that employees are aware of the responsibilities they accept when they use district-owned computer hardware, operating system software, application software, stored text, data files, electronic mail, local databases, CD-ROMS, digitized information, communication technologies, and internet access. In general, this requires efficient, ethical, and legal utilization of all technology resources.

1 . Expectations

a. Use of computers, other technical hardware, computer networks and software is only allowed when granted permission by the employee's supervisor.
b. All users are expected to follow existing copyright laws. Copyright guidelines are posted and/or available in the media center of each campus as well as posted on the district website.

c. Although the District has an Internet safety plan in place, employees are expected to notify their supervisor or the Executive Director of Technology whenever they come across information or messages that are inappropriate, dangerous, threatening, or make them feel uncomfortable.
d. Employees who identify or know about a security problem are expected to convey the details to their supervisor or the Executive Director of Technology without discussing it with others.
e. Employees are responsible for securing technology devices when not in use and for returning them in good working condition.
f. Employees shall be held to the same professional standards in their public use of electronic media as they are for any other public conduct. If am employee's use of electronic media violates state or federal law or District policy, or interferes with the employee's ability to effectively perform his or her job duties, the employee is subject to disciplinary action, up to and including termination of employment.

2. Unacceptable Conduct (includes the following, but is not limited to)

a. Using the network for illegal activities, including copyright or contract violations, downloading inappropriate materials, viruses, and/or software, to hacking and host file sharing software.
b. Using the network for financial or commercial gain, advertising, proselytizing, or political lobbying.
c. Accessing or exploring on-line locations or materials that do not support the curriculum and/or are inappropriate for school assignments, such as but not limited to pornographic sites.
d. Vandalizing and/or tampering with equipment, programs, files, software, system performance or other components of the network. Use or possession of hacking software is strictly prohibited.
e. Causing congestion on the network or interfering with the work of others, e.g., chain letters or broadcast messages to lists or individuals.
f. Wasting finite resources, i.e., downloading movies or music for non-educational purposes.
g. Gaining unauthorized access anywhere on the network.
h. Revealing the home address or phone number of one's self or another person.
i. Invading the privacy of other individuals.
j. Using another user's account, password, or ID card or allowing another user access to your account, password, or 10.
k. Coaching, helping, observing or joining any unauthorized activity on the network.
I. Posting anonymous messages or unlawful information on the system.
m. Engaging in sexual harassment or using objectionable language in public or private messages, e.g., racist, terroristic, abusive, sexually explicit, threatening, stalking, demeaning, slanderous.
n. Falsifying permission, authorization of identification documents.
o. Obtain copies of, or modify files, data or passwords belonging to other users on the network.
p. Knowingly placing a computer virus on a computer or network.
q. Using personal computing devices on the District network, except mobile devices for district approved programs

3. **Acceptable Use Guidelines**

a. General Guidelines:

1. All employees will have access to all available forms of electronic media and communication which is in support of education and research and in support of the educational goals and objectives of the Irving Independent School District.
2. Employees are responsible for their ethical and educational use of the computer on-line services at the Irving Independent School District.
3. All policies and restrictions of the District's computer on-line services must be followed.
4. Access to the District's computer on-line services is a privilege and not a right. Each employee will be required to sign the Acceptable Use Policy Agreement Sheet and adhere to the Acceptable Use Guidelines in order to be granted access to District computer on-line services.
5. The use of any District computer on-line services at the Irving Independent School District must be in support of education and research and in support of the educational goals and objectives of the Irving Independent School District.
6. When placing, removing, or restricting access to specific databases or other District computer on-line services, school officials shall apply the same criteria of educational suitability used for other education resources.
7. Transmission of any material which is in violation of any federal or state law is prohibited. This includes, but is not limited to: student or other confidential information, copyrighted material, threatening or obscene material, and computer viruses.
8. Any attempt to alter data, the configuration of a computer, or the files of another user, without the consent of the individual campus administrator or technology administrator will be considered an act of vandalism and subject to disciplinary action in accordance with Board Policy.

b. Network Etiquette

1. Be polite.
2. Use appropriate language.
3. Do not reveal personal data (home address, phone number, and phone numbers of other people).
4. Remember that the other users of District computer on-line services and other networks are human beings whose culture, language, and humor have different points of reference from your own.
5. Users should be polite when forwarding email. The intent of forwarding email should be on a need to know basis.

c. E-Mail

(1) E-mail should be used primarily for educational or administrative purposes.
(2) E-mail transmissions, stored data, transmitted data, or any other use of District computer on-line services by students, employees or other user shall not be considered confidential and may be monitored at any time by designated staff to ensure appropriate use.
(3) All e-mail and all contents are property of the District.

4. Consequences

The student in whose name a system account and/or computer hardware issued will be responsible at all times for its appropriate use. Noncompliance with the guidelines published here in the Student Code of Conduct and in Board Policy CQ may result in suspension or termination of technology privileges and disciplinary actions. Use or possession of hacking software is strictly prohibited and violators will be subject to Phase Ill consequence of the Code of Conduct. Violation of applicable state or federal law, including the Texas Penal Code, Computer Crimes, Chapter 33 will result in criminal prosecution or disciplinary action by the district. Electronic mail, network usage, and all stored files shall

not be considered confidential and may be monitored at any time by designated district staff to ensure appropriate use.

The district cooperates fully with local, state or federal officials in any investigation concerning or relating to violations of computer crime laws. Contents of email and network communications are governed by the Texas Open Records Act; proper authorities will be given access to their content.

Irving ISD Acceptable Use Agreement

Student Section

_____

Student name (print) Grade

_____

School

I have read the Student Acceptable Use Guidelines. I agree to follow the rules contained in this policy. If I violate the rules I may lose my access privilege to the District's computer online services and may face disciplinary action.

_____

Student signature Date

Parent Section

I have read the Student Acceptable Use Guidelines. I understand that the Internet is a worldwide group of hundreds of thousands of computer networks. I agree that the Irving Independent School District does not control the content of these Internet networks. I understand if my child violates the Acceptable Use Guidelines, his/her access privilege to the District's computer online services may be revoked and may be subject to disciplinary action. The Irving Independent School District has my permission to give network and Internet access to my child. I understand that my child will maintain this privilege as long as the procedures described in the District Acceptable Use Guidelines are followed.

I also grant permission for examples of my child's schoolwork to be published on the World Wide Web as an extension of classroom studies, provided that the home address, home phone number, student's last name or a close-up photograph is not included.

Note: While the District will use filtering technology to restrict objectionable material, it is not possible to absolutely prevent such access. It will be your responsibility to follow the rules for appropriate use. Parents who do not want their child to have Internet access and/or have their schoolwork published on the web, should submit this request in writing annually to their child's principal. While the district will attempt to restrict access, it is ultimately the responsibility of the parent to ensure their child does not violate this request.

_____/_____/_____

Parent or Guardian signature Date

_____

Parent name (print)

_____ _____

Home address Phone

***EXAMPLE*: Auburn, (AL)**
Acceptable Use Policy

Resources

These guidelines are provided, so that students and parents are aware of the responsibilities students accept when they use district owned computer hardware, operating system software, application software, stored text, data files, electronic mail, local databases, CD-ROMs, digitized information, communications technologies and Internet access. In general, this requires efficient, ethical and legal utilization of all technology resources.

1. Expectations:

a. Students are expected to use computers, other technology hardware, software and computer networks including the Internet as defined by the *Student/Parent Laptop Agreement*.
b. All users are expected to follow existing copyright laws. Copyright guidelines are posted and/or available in the media center of each campus as well as posted on the district website.
c. Although the district has an Internet safety plan in place, students are expected to notify a staff member whenever they come across information or messages that are inappropriate, dangerous, threatening, or make them feel uncomfortable.
d. Students who identify or know about a security problem are expected to convey the details to their teacher without discussing it with other students.

2. Acceptable Use Guidelines – Auburn City Schools District Network Services

a. General Guidelines

1. Access to the Auburn City Schools network is a privilege and not a right. Each employee, student and/or parent will be required to sign the Acceptable Use Policy Agreement Sheet and adhere to the Acceptable Use Guidelines in order to be granted access to the network.
2. Students are responsible for their ethical and educational use of the computer network resources and on-line services.
3. All policies and restrictions of the acceptable use policy for computer network resources and online services must be followed.
4. The use of any network services at the Auburn City School District must be in support of education and research and in support of the educational goals and objectives of the Auburn City School District.
5. When placing, removing, or restricting access to specific databases or other network resources, school officials shall apply the same criteria of educational suitability used for other education resources.
6. Transmission of any material which is in violation of any federal or state law is prohibited. This includes, but is not limited to: confidential information, copyrighted material, threatening or obscene material, and computer viruses.
7. Any attempt to alter data, the configuration of a computer, or the files of another user, without the consent of the individual, campus administrator, or technology administrator, will be considered an act of vandalism and subject to disciplinary action in accordance with the Auburn City Schools Student Pupil Progression Plan.

8. Parents concerned with the network services at their child's school should refer to the Pupil Progression Plan handbook and follow the stated procedure.
9. Any parent wishing to restrict their child's access to any network services will provide this restriction request in writing to school principal. Parents will assume responsibility for imposing restrictions only on their own children.
10. Parents, who do not want their child to have Internet access and/or have their schoolwork published on the web, should submit this request in writing annually to their child's principal. While Auburn City Schools attempts to restrict Internet access, it is ultimately the responsibility of the parent to ensure the child does not violate this request.

b. Network Etiquette

1. Be polite.
2. Use appropriate language.
3. Do not reveal personal data/information (home address, phone number, phone numbers of other people), including photographs and videos.
4. Remember that the other users of the network services and other networks are human beings whose culture, language, and humor have different points of reference from your own.

3. Unacceptable conduct includes, but is not limited to the following:

a. Using the network for illegal activities, including copyright, license or contract violations, downloading inappropriate materials, viruses, and/or software, such as but not limited to hacking and host file sharing software.
b. Using the network for financial or commercial gain, advertising, or political lobbying.
c. Accessing or exploring on-line locations or materials that do not support the curriculum and/or are inappropriate for school assignments, such as but not limited to pornographic sites.
d. Vandalizing and/or tampering with equipment, programs, files, software, system performance or other components of the network.
e. Using or possessing hacking software.
f. Causing congestion on the network or interfering with the work of others, e.g., chain letters or broadcast messages to lists or individuals.
g. Intentionally wasting resources, i.e., on-line time, real-time music.
h. Gaining unauthorized access anywhere on the network.
i. Revealing the home address or phone number of oneself or another person.
j. Invading the privacy of other individuals.
k. Using another user's account, password, or ID card or allowing another user to access your account, password, or ID.
l. Coaching, helping, observing or joining any unauthorized activity on the network.
m. Forwarding/distributing e-mail messages without permission from the author.
n. Posting anonymous messages or unlawful information on the system
o. Engaging in sexual harassment or using objectionable language in public or private messages, e.g., racist, terroristic, abusive, sexually explicit, threatening, stalking, demeaning or slanderous.
p. Falsifying permission, authorization or identification documents.
q. Obtain copies of, or modify files, data or passwords belonging to other users on the network.

r. Knowingly placing a computer virus on a computer or network.

Pupil Progression Plan – Misbehaviors & Consequences

(The following is an excerpt from the Auburn City Schools Pupil Progression Plan.)

Type I Misbehaviors

Consequences of Type I misbehaviors include, but are not limited to, the following:

1. Minor disruption in the classroom or during school activities
2. Verbal abuse of another person
3. Non-directed use of profane or obscene communication (verbal, written, gestures)
4. Unauthorized fund raising
5. Chronic failure to bring supplies to class
6. Inappropriate affectionate behavior

Type I Consequences

Consequences of Type I misbehaviors include, but are not limited to, the following:

1. Parent/Guardian Contact
2. Counseling
3. Detention
4. Saturday School Program
5. In-School Suspension (ISS)
6. Suspension
7. Juvenile Authorities

Type II Misbehaviors

Type II misbehaviors are more severe and/or more persistent than Type I misbehaviors. The student's conduct infringes upon the rights of other students or adults. The student's conduct negatively impacts the educational efficiency of other students and the staff. The administrator who is working with the student shall invite the parents to participate in a conference in order to review Type II procedures that have been attempted, to solicit their cooperation in changing the student's behavior, and to inform them of the serious consequences of persistent Type II misbehaviors:

1. Engaging in conduct that contains the element of breaching computer security under Section 13A-8-100 Alabama Computer Crime Act.

2. Violation of the Guideline for acceptable use of Technology Resources as outlined on pages 8-11, unless specified as a Type II Misbehavior.

Type II Consequences

Consequences of Type II misbehaviors include, but are not limited to, the following:

1. Any Type I consequence or combination of consequence
2. Parent/guardian contact
3. Counseling
4. Detention
5. Suspension from riding all buses
6. Suspension
7. Saturday School Program
8. In-School Suspension [ISS]
9. Alternative School
10. Juvenile authorities
11. Law enforcement officials
12. Restitution

Type III Misbehaviors

Type III misbehaviors are such that the student has disrupted or threatens to disrupt the school's efficiency to such a degree that his/her presence is not acceptable. Common signs of Type III misbehaviors include, but are not limited to, the following offenses committed on school property or within 300 feet of school property, using school equipment, or while attending a school sponsored or school related activity except as noted:

1. Engages in conduct that contains the element of breaching computer security under Section 13A-8-100 Alabama Computer Crime Act.
2. Use or possession of hacking software or any other software capable of causing harm.

Type III Consequences

Consequences of Type III misbehaviors include, but are not limited to, any of the following:

1. The consequences of Type II misbehaviors 1-10 shall be assignment to an alternative education program from four to six weeks and notification of placement sent to the juvenile justice system.

Consequences for Type III misbehaviors may also include the following:

1. Any Type I or Type II consequence or combination of consequence
2. Counseling
3. Suspension
4. In-school suspension [ISS]
5. Alternative school
6. Indefinite suspension
7. Expulsion from school
8. Juvenile authorities
9. Law enforcement officials (Alabama lists all of the laws that pertain to these misbehaviors and what the punishments are for each offense)

***EXAMPLE*: Maine Learning Technology Initiative**

Acceptable Use Policy (AUP)

All schools are required to maintain an Acceptable Use Policy. All users should be made aware of the local school AUP. Schools should determine if the district/school's AUP requires additional policies related to MLTI, particularly responsibilities of the user when the device is used outside the school environment.

All participating schools must post their AUP on the school or district's web site. The URL to the AUP should be on file with the MLTI Project Office, http://www.maine.gov/mlti/aup/. (See Example Below) Schools should email the URL to their AUP to mlti.project@maine.gov.

EXAMPLE: Waterville Junior High School (ME)

ELECTRONIC INFORMATION - K-12/ADULT-ED ACCEPTABLE USE POLICY

1. **Guidelines on the Acceptable Use of Electronic Information Resources**

Information resources offer access to computers and people throughout the world. Students and staff will have access to electronic mail, college and university libraries, information and news from a variety of sources and research institutions, software of all types, discussion groups on a wide variety of topics, and much more.

The following guidelines are intended to be helpful and provide a base from which district and school policies can be tailored. While the emphasis here is on appropriate use, there is no intent to diminish the vital nature of electronic information services.

While electronic information resources offer tremendous opportunities of educational value, they also offer persons with illegal or inappropriate purposes avenues for reaching students, teachers, and others including parents.

The following represent some of the illegal and inappropriate uses that may occur:

- Using the network for commercial advertising
- Using any non-school supported email program, instant messaging programs or chat rooms
- Using copyrighted material in reports without permission
- Using the network to lobby for votes
- Using the network to access a file that contains pornographic pictures
- Using the network to send/receive messages that are racist
- Using the network to send/receive inflammatory messages
- Creating a computer virus and placing it on the network
- Using the network to send/receive a message with someone else's name on it
- Using the network to send/receive a message that is inconsistent with the school's code of conduct and mission statement
- Using the network to send/receive messages that are sexist and/or contain obscenities
- Using the network to provide addresses or other personal information that others may use inappropriately
- Using the network for sending and receiving a large number of personal messages
- Malicious or intentional damage to school- or state-owned equipment

**All users should be aware that the inappropriate use of electronic information resources can be a violation of local, state, and federal laws. Violations can lead to prosecution*.

1. **Protection of users:**

Waterville Public schools will make every attempt to protect the users from inappropriate material available on the Internet or World Wide Web. To this end Waterville Public Schools will employ filtering technology to prohibit inappropriate material from entering the school network. In addition, to ensure the safety of both students and staff, the use of any non-school supported email program, instant messaging program, or chat rooms is forbidden.

2. **Electronic Information Resource Contract**

We are pleased to announce that Internet, Maine-Net, e-mail and other school - or state-owned electronic information services are now available to students and teachers in the Waterville Public School System. The Waterville Public School System strongly believes in the educational value of such electronic services and recognizes the potential of such to support our curriculum and student learning in our school system. Our goal in providing this service is to promote educational excellence by facilitating resource sharing, innovation, and communication. The Waterville Public School System will make every effort to protect students and teachers from any misuses or abuses as a result of their

experiences with an information service. All users must be continuously on guard to avoid inappropriate and illegal interaction with the information service.

Listed below are the provisions of this contract. If any user violates these provisions, access to the information service may be denied and you may be subject to disciplinary action.

Terms and Conditions of this Contract

1. Personal Responsibility

As a representative of this school, I will accept personal responsibility for reporting any misuse of the network or school, or state-owned equipment to the system administrator. Misuse can come in many forms, but is commonly viewed as vandalism or any message(s) sent or received that indicate or suggest pornography, unethical or illegal solicitation, racism, sexism, inappropriate language, and other issues described in this document.

2. Acceptable Use

The use of my assigned account and school - or state-owned equipment must be in support of education and research and with the educational mission of the Waterville Public School System. I am personally responsible for this provision at all times when using the electronic information service.

A. Use of other organization's networks or computing resources must comply with rules appropriate to that network.

B. Transmission of any material in violation of any United States or other state organizations law is prohibited. This includes, all but is not limited to: copyrighted material, threatening or obscene material, or material protected by trade secret.

C. Use of product advertisement or political lobbying is also prohibited.

3. Privileges

The use of the information system is a privilege not a right, and inappropriate use of school - or state owned-equipment may result in the cancellation of those privileges. The Waterville Public School System Technology Committee (operating under the aegis of the school board and the central office) will decide what is appropriate use, and their decision is final. The system administrator(s) may close an account at any time deemed necessary. The administration, staff, or faculty of the Waterville Public School System may request that the system administrator deny, revoke, or suspend specific user accounts and/or the use of school - or state-owned equipment. The school administration reserves the right to remove any messages or files that are deemed to be inappropriate.

4. Network Etiquette and Privacy

You are expected to abide by the generally accepted rules of network etiquette. These rules include (but are not limited to) the following:

a) BE POLITE! Never send, or encourage others to send, abusive messages.

b) Use APPROPRIATE LANGUAGE. Remember that you are a representative of our school and our school system on a non-private system. You may be alone with your computer, but what you say and do can be viewed globally! Never swear, use vulgarities, or any other kind of inappropriate language. Illegal activities of any kind are strictly forbidden.

c) PRIVACY. Do not reveal your home address or personal phone number or the addresses of students or colleagues.

d) ELECTRONIC FILES. Electronic mail and files stored or transmitted, using school resources are not guaranteed to be private. The Network Administrator has access to all electronic information for the purposes of backups, records retention, and routine system monitoring. Messages relating to or in support of illegal activities must be reported to the authorities.
e) DISRUPTIONS. Do not use the network in any way that would disrupt the use of the network by others.

5. Services

The Waterville Public School System makes no warranties of any kind, whether expressed or implied, for the service it is providing. Waterville Public Schools will not be responsible for any damages suffered while on this system. These damages include loss of data as a result of delays, non-deliveries, miss-deliveries, or service interruptions caused by the system or your errors or omissions. Use of any information via the information system is at your own risk. Waterville Public Schools specifically disclaims any responsibility for the accuracy of information obtained through its services.

6. Security

Security on any computer system is a high priority because there are so many users. If you identify a security problem, notify the system administrator at once. Never demonstrate the problem to other users. Never use another person's account without written permission from that person. All use of the system must be under your own account. Any user identified as a security risk will be denied access to the information system.

7. Vandalism

Vandalism is defined as any malicious attempt to harm or destroy school - or state-owned equipment or the data of another user or any other agencies or networks that are connected to the system. This includes, but is not limited to physical damage and the uploading or creation of computer viruses. Any vandalism will result in the loss of computer services, disciplinary action, reimbursement of costs of malicious or intentional damages, and legal referral.

8. Updating

The information service may occasionally require new registration and account information from you to continue the service. You must notify the information system of any changes in your account information.

ADOPTED: June 17, 2002; REVISED: 7/21/03; REVISED: 4/7/08
LEGAL REFERENCE:
SOURCE: Board Policy

***EXAMPLE*: Auburn, AL**
AJHS Handbook – Terms of the Computer Agreement

Terms of the Computer Agreement Terms:

Non-refundable user fees of $50, annually, must be paid prior to taking possession of the property. You will comply at all times with the Auburn City Schools district's *Student/Parent Laptop Agreement*. Any failure to comply ends your right of possession effective immediately.

If this fee creates a financial hardship on the student or parent from obtaining a laptop, please contact the school administration about payment options. Upon proof of financial hardship, the administration may elect to create a payment plan for the student to pay out fees over time.

Title:

Legal title to the property is with the district and shall at all times remain in the district. Your right of possession and use is limited to and conditioned on your full and complete compliance with the *Student/Parent Laptop Agreement*. The student in whose name a system account and/or computer hardware are issued will be responsible at all times for its appropriate care and use.

Liability:

- The permission granted to the student ceases on the last calendar day for the current school year (unless terminated earlier by ACS). Failure to return the said laptop on or before this date to the campus principal or his/her designee may result in criminal charges being sought against the student and/or the person who has the laptop. Auburn City Schools reserves the right at any time to demand return of the laptop forthwith.
- In case of theft, vandalism, and other criminal acts, a police report MUST be filed by the student or parent within 48 hours of the occurrence. Incidents happening off campus must be reported to the police by the parent and a copy of the report be brought to the school.
- If laptop is stolen and student reports the theft (by the next school day) and police filed a report, then the student will not be charged for the cost of the unit.
- Student will be charged the Fair Market Value of the laptop if deliberately damaged or vandalized. (see Fair Market Value chart below).

Fair Market Value
Original cost to the District is currently $1450
Age of Laptop Value
1 year or less 50% of FMV
2 years 45% of FMV
3 years 35% of FMV
4 years 30% of FMV

- Students/Parents are responsible for reasonable cost of repair for deliberately damaged laptops (see Repair Pricing chart below). The costs of any other parts needed for repairs will be based on manufacturer's current price list.

Table of Estimated Repair Pricing
Deliberate Damage or Neglect
Broken Screen (LCD) $300
Keyboard $25
Power Adapter + Cord $60
Battery $60
Re-image of Hard Drive due to violation of Acceptable Use Policy $15

Repossession:

If you do not timely and fully comply with all terms of this agreement and the *Student/Parent Laptop Agreement*, we have the right to notify the authorities to come to your place of residence to pick up the property.

Use of Computers and Laptops on the Network

Auburn City Schools is committed to the importance of a student being able to continue with his work when his laptop is experiencing problems. To assist with this problem the district is providing the following:

Network Student Drives

Student logins will provide access to a network drive, which can only be accessed at school. Students can save important items on this network drive, keeping a backup that they can access from anywhere on the network.

Classroom Computers

The district has desktop computers in the classroom. Students can use these computers if they do not have their laptop. They will be able to access their saved work on their network drive. No loaning or borrowing Laptops. Do not loan laptops to other students/people inside or outside of the school district. Do not borrow a laptop from another student. Do not share password or usernames with others.

Student Guidelines for Acceptable Use of Technology Resources

These guidelines are provided, so that students and parents are aware of the responsibilities students accept when they use district owned computer hardware, operating system software, application software, stored text, data files, electronic mail, local databases, CD-ROMs, digitized information, communications technologies and Internet access. In general, this requires efficient, ethical and legal utilization of all technology resources.

1. **Expectations:**

a. Students are expected to use computers, other technology hardware, software and computer networks including the Internet as defined by the *Student/Parent Laptop Agreement*.

b. All users are expected to follow existing copyright laws. Copyright guidelines are posted and/or available in the media center of each campus as well as posted on the district website.

c. Although the district has an Internet safety plan in place, students are expected to notify a staff member whenever they come across information or messages that are inappropriate, dangerous, threatening, or make them feel uncomfortable.

d. Students who identify or know about a security problem are expected to convey the details to their teacher without discussing it with other students.

2. Acceptable Use Guidelines – Auburn City Schools District Network Services

a. General Guidelines

1. Access to the Auburn City Schools network is a privilege and not a right. Each employee, student and/or parent will be required to sign the Acceptable Use Policy Agreement Sheet and adhere to the Acceptable Use Guidelines in order to be granted access to the network.

2. Students are responsible for their ethical and educational use of the computer network resources and on-line services.

3. All policies and restrictions of the acceptable use policy for computer network resources and online services must be followed.

Personal Devices in Classroom

The Technology Task Force recognizes the challenge of incorporating and monitoring student owned computers into the school one-to-one program and encourages district decision makers to discuss this policy issue with classroom teachers.

Limitation of Liability

***EXAMPLE*: Clackamas Education Service District (OR)**
Limitation of Liability Language:

The District and Clackamas ESD makes no warranties of any kind, either express or implied, that the functions or the services provided by or through the District system will be error-free or without defect. The District will not be responsible for any damage users may suffer, including but not limited to, loss of data or interruptions of service. The District is not responsible for the accuracy or quality of the information obtained through or stored on the system. The District will not be responsible for financial obligations arising through the unauthorized use of the system. Users will indemnify and hold the ESD and District harmless from any losses sustained as the result of intentional misuse of the system by user.

MONITORED USE

Electronic mail transmissions and other use of the electronic communications system by students and employees shall not be considered private. Designated District staff shall be authorized to monitor such communication at any time to ensure appropriate use.

***EXAMPLE*: William Fremd High School, IL**
Disclaimer

District 211 makes no warranties of any kind, expressed or implied, for the opinions, advice, services, merchandise, or other information provided by system users, information providers, service providers, or other third parties on the Network. District 211 is not responsible for any damages suffered by users including, but not limited to, loss of data resulting from unacceptable use, delays, non- or mis-delivery of information, or service interruptions of any kind or for any reason. Use of information or services provided on the Network is at the user's own risk. District 211 specifically disclaims any responsibility for the accuracy of information or materials of any sort obtained through the use of the Network. District 211 provides no assurance of privacy for information transmitted via the Network or contained in District-owned storage media including, but not limited to, electronic mail. District 211 reserves the right to search and examine, any District-owned storage media or storage media owned by others used with District-owned equipment. Users deemed a security risk may be denied access to the Network.

***EXAMPLE*: Randolph Field Independent SD, (TX)**
RFISD Acceptable Use Guidelines
Disclaimer

The Randolph Field Independent School District's system is provided on an "as is, as available" basis. The District does not make any warranties, whether express or implied, including, without limitation, those of merchantability and fitness for a particular purpose with respect to any services provided by the system and any information or software contained therein. The District does not warrant that the functions or services performed by, or that the information or software contained on the system will meet the system user's requirements, or that the system will be uninterrupted or error-free, or that defects will be corrected.

Opinions, advice, services, and all other information expressed by system users, information providers, service providers, or other third party individuals in the system are those of the providers and not the District.

Augmentation of State Solution

Districts interested in supplementing the hardware and / or software of the state issued mobile computing are solely responsible for the initial, and ongoing cost, compatibility, upkeep, maintenance and disposal of supplemental items.

Parental Consent

***EXAMPLE*: Canby, (OR)**
ACADEMIC FREEDOM, FREE SPEECH, & SELECTION OF MATERIAL

1. Board policies on Academic Freedom and Free Speech will govern the use of the Internet.
2. When using the Internet for class activities, teachers will:
    a. Select material that is appropriate in light of the age of the students and what is relevant to the course objectives.
    b. Preview the materials and sites they require for students access to determine the appropriateness of the material contained on, or accessed through, the site.
    c. Provide guidelines and lists of resources to assist their students in channeling their research activities effectively and properly.
    d. Help their students develop the skills to ascertain the truthfulness of information, distinguish fact from opinion, and engage in discussions about controversial issues while demonstrating tolerance and respect for those who hold divergent views.

***EXAMPLE*: Kentucky Department of Education**
Live@EDU AUP Requirements

Federal law requires that any child age 13 and under have parental consent to access online services, such as the Microsoft Live@EDU offering. Districts must include in their respective local AUPs the language provided below:

The Outlook Live e-mail solution is provided to your child by the district as part of the Live@edu service from Microsoft. By signing this form, you hereby accept and agree that your child's rights to use the Outlook Live e-mail service, and other Live@EDU services as the Kentucky Department of Education may provide over time, are subject to the terms and conditions set forth in district policy/procedure as provided and that the data stored in such Live@EDU services, including the Outlook Live e-mail service, are managed by the district pursuant to policy 08.2323 and accompanying procedures. You also understand that the Windows Live ID provided to your child also can be used to access other electronic services that provide features such as online storage and instant messaging. Use of those Microsoft services is subject to Microsoft's standard consumer terms of use (the Windows Live Service Agreement), and data stored in those systems are managed pursuant to the Windows Live Service Agreement and the Microsoft Online Privacy Statement. Before your child can use those Microsoft services, he/she must accept the Windows Live Service Agreement and, in certain cases, obtain your consent.

A sample written agreement form that includes this provision is available from KSBA (Dara. Bass@ksba.org or 1-800-372-2962, ext. 1220).

Search and Seizure

The Idaho Constitution at Article I, Section 17, states:

> The rights of the people to be secure in their persons, houses, papers and effects against unreasonable searches and seizures shall not be violated; and no warrant shall issue without probable cause shown by affidavit, particularly describing the place to be searched and the person or thing to be seized.

Relating to the presence of weapons at school, Idaho Code Section 18-3302D(3) states:

> Right to search students or minors. *For purposes of enforcing the provisions of this section, employees of a school district* shall have the right to search all students or minors, including their belongings and lockers, *that are reasonably believed to be in violation of the provisions of this section, or applicable school rule or district policy, regarding the possessing of a firearm or other deadly or dangerous weapon.* (Emphasis added.)

***EXAMPLE*: Canby (OR)**
ACADEMIC FREEDOM, FREE SPEECH, & SELECTION OF MATERIAL

1. System users have a limited privacy expectation in the contents of their personal files and records of their on line activity while on the District system.
2. Routine maintenance and monitoring of the system may lead to discovery that the user has or is violating the District policies and procedures, the student disciplinary code, or state and federal law.
3. An individual search will be conducted if there is reasonable suspicion that a user has violated the law or the student disciplinary code. The nature of the investigation will be reasonable and in the context of the nature of the alleged violation.
4. District employees should be aware that their personal files may be discoverable under ORS 192.410, the state public records laws.

Intellectual Property Rights (reference in student handbook)

***EXAMPLE*: Randolph Field Independent SD, (TX)**
RFISD Acceptable Use Guidelines

No Right To Privacy

Users of Randolph Field ISD electronic communication devices and networking infrastructure have no right to privacy. Any communications or data transmitted on Randolph Field IsD systems, regardless of medium, is subject to being monitored, intercepted, and archived. Users of Randolph Field ISD networking and electronic communications infrastructure agree to surrender any school assets and media as directed by either the Superintendent, Director of Technology, Principal, Associate Principal, Vice Principal, or designee. Personal assets, media and electronic equipment designed to interface with any Randolph Field ISD networking or electronic infrastructure equipment requires approval of the Director of Technology for use and network interface.

Teacher Code of Conduct

***EXAMPLE*: Randolph Field Independent SD, (TX)**
RFISD Acceptable Use Guidelines

General Teacher and Administration Guidelines

1. The individual in whose name a system account is issued will be responsible at all times for its proper use.
2. Teachers and administrators will lock their workstations when not in use.
3. Students are strictly prohibited from accessing any network or data resource intended for teacher or administration use only.
4. Systems may not be used for illegal purposes, in support of illegal activities or in any activity prohibited by District Policy.
5. System users may not use another person's account or password.
6. No teacher may use another teacher's classroom account unless cleared through the technology department.
7. System users must purge electronic files and mail in accordance with established retention guidelines.

Monitoring of Student Activity on Device

All use of school issued electronic device shall not be considered private. Designated District staff shall be authorized to monitor all activity at any time to ensure appropriate use. All monitoring shall comply with local, state and federal laws.

Individualized Content on Device

At no time does the device become the personal property of students or staff; however districts are encouraged to allow students to place individualized items the device, which are limited to music, pictures and other items that do not hinder the network or device functionality. The district should clarify that it is not liable for copyright infringement or loss of data related to individual content placed on the device.

***EXAMPLE*: Newton, (TX)**
Newton ISO Middle School Laptop

Music, Games, or Pictures

- All software loaded on the system must be District approved.
- Illegal downloading and distribution of copyrighted works are serious offenses that carry with them the risk of substantial monetary damages and, in some cases, criminal prosecution.
- Copyright infringement also violates the District's Internet Service Provider's terms of service and could lead to limitation or suspension of the District's Internet service.
- Students found with illegal tiles on their computer, will have their laptop confiscated and reimaged.

Online Safety

The Idaho Attorney General has developed an online safety program titled Protecteens, which addresses this issue among others. For more information visit:
http://www.ag.idaho.gov/internetSafety/protecTeens.html

Idaho's one to one initiative provides an opportunity to explore digital citizenship among high school students. Information and lesson plans can be found at:
http://www.commonsensemedia.org/about-us/our-mission

***EXAMPLE*: Genesee SD (ID)**
Online Safety Statement of Purpose:

In accordance with this policy and the Board's philosophy to ensure the safety of all students, the District shall provide an appropriate planned instructional component for internet safety which shall be integrated into the District's regular instructional program. The purpose of the program is to increase students' knowledge of safe practices for internet use.

This instructional component shall include all required components of the Protecting Children in the 21st Century Act. In addition to the existing CIPA certifications required of schools in section 254(h)(5) of the Act, the Protecting Children in the 21st Century Act requires the school, school board, local educational agency, or other authority with responsibility for administration of the school to certify that it "as part of its Internet safety policy is educating minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response."

***EXAMPLE*: Kim Comando**, who writes the CyberSpeak column in *USA Today,* compiled instructions that districts commonly use. These include:

1. *Never* give out personal information without parents'/caregivers' permission.
2. Anyone can post anything to a Web site. Review Web sites carefully. Teachers must help students with this process.
3. It is important to cite sources when copying information from a Web site or other electronic resources. When you copy information from a Web site or other electronic resources, you *must* cite the source, or it is plagiarizing. If you do copy and paste information, put it in quotations marks and list the source from which you obtained it.
4. When you copy pictures, video, or sound clips, you must also cite the source from which you obtained them.
5. Do not play games, send instant messages, or access inappropriate Web sites during school. Remember that the laptop is a tool for learning. If you choose to do any of these things, you are jeopardizing the laptop program and your integrity. There will be consequences as established by the Walled Lake Schools Student Code of Conduct.

6. The district has a filter to prevent you from accessing inappropriate Web sites. People who post pornographic images or who are involved in hate groups often find ways to get around filters. If you accidentally stumble upon an inappropriate Web site, quickly exit, close your lid, and tell your teacher. *Do not show* your classmates what happened or discuss it with them. Be sure to follow this procedure.
7. Do not use file-sharing services. These sites allow strangers from all over the world to share files. They can be used to download movies, TV shows, music, software, and more. File sharing can cause serious problems. First of all, it is illegal to download copyrighted materials, and you could end up in a lawsuit. Second, you are opening up your computer to all users of the file-sharing service! File-sharing services work by installing shared folders on your computer; any files stored in the shared folder are open for others to view, download, and save. Virus creators love file-sharing services; it is easy for them to hide a virus in a song (or any other file) and save it to millions of share folders. When the song is opened, you get a special present….a virus. If you have a file-sharing program, remove it. Parents, check to see if your son/daughter has access to them, go to the control panel and select Add or Remove Programs. Highlight the program and then click the Remove button.

***EXAMPLE*: Newton SD (TX)**
Internet Safety Planning:

The Superintendent or designee shall develop and implement an Internet safety plan to:
I. Control students' access to inappropriate materials, as well as to materials that are harmful to minors;
2. Ensure student safety and security when using electronic communications;
3. Prevent unauthorized access, including hacking and other unlawful activities; and
4. Restrict unauthorized disclosure, use and dissemination of personally identifiable information regarding students.

Cyberbullying

Reference materials: Technology for Learning: **A Guidebook for Change**

Educating parents, students, and teachers about cyberbullying is crucial. Students must understand the consequences of engaging in cyberbullying. For example, district leaders may decide that students would lose their Internet or instant-messaging accounts. Teaching them to respect others and to take a stand against bullying of all kinds makes a difference in creating an overarching school culture of anti-harassment and respect.

Motives for cyberbullying differ, and so must responses and solutions. Unfortunately, no one-size-fits-all recommended response to or solution for cyberbullying exists. Cyberbullies are similar to traditional schoolyard bullies but often cloak their activities in anonymity. Schools walk a fine line in handling cyberbullying that occurs off campus outside the school day. When schools reach beyond the district's boundaries to address cyberbullying after hours, parents can bring lawsuits claiming that the actions exceed the school's authority and violate students' right to free speech.

School personnel can be very effective brokers in working with the parents/caregivers to stop cyberbullying. They can teach students cyberethics and the related law. There are creative situations in which schools can work around the claim that their actions exceed the scope of their authority. An effective plan is to add a cyberbullying provision to the school's acceptable-use policy, reserving the right to discipline the student for off-campus activities if they are meant to have an effect on another student or they adversely affect the safety and well-being of a student while he or she is in school. This then becomes a contractual, not a constitutional, issue.

Parents and caregivers must be the trusted adults to whom students can turn when things go wrong online and offline. Young people don't always turn to parents and caregivers, because they are concerned that the adults will overreact. Children tend to believe that telling someone about cyberbullying incidents will make matters worse.
They worry that parents/caregivers will call others or the school, assign blame, and/or remove Internet privileges. School personnel can educate parents/caregivers about steps to take in response to their children's being cyberbullied. A formal dissemination of symptoms, how to recognize cyberbullying, etc., is a productive step.

Technology Advisory Councils

The Technology Task Force encourages districts / schools to establish local councils, including parents and students, to inform technology integration into the learning environment. Stakeholder involvement serves to increase collective ownership of the initiative and can aid in policy implementation and information dissemination.

Device Ownership

Similar to any resource local districts purchase with state funds, responsibility of the mobile computing devices resides at the local level. The SDE plans to purchase devices after a 4 year lease cycle at which point districts will be given the opportunity to purchase the devices from the state at a rate similar to what the state paid. Once purchased by the district, re-deployment, re-sale or disposal of technology equipment, after a 4 year life cycle, is at the discretion of the district.