Technology Care and Use Guidelines

Conners Emerson School

(SAVE for future reference)

We understand that we are to meet the following expectations regarding MDIRSS technology devices at school, home, and transit between:

General Use of Technology Devices

1. Devices with recording capabilities (iPads, Macbooks, Phones, etc.) are never to be taken into a locker room or school bathroom as per state law.
2. Devices will be fully charged for the beginning of each school day (either at school or home)
3. Devices must be handled with care, protected from heat and cold, and the weather.
4. Devices are to be used as an educational tool.
5. Passwords are to remain private from other students. **You will be required to provide your password to a teacher or administrator if requested.**
6. You need to report any problems with your device as soon as possible upon return to school.
7. **The school's Acceptable Use Policy is in effect at ALL times regardless of location (home or school).**
8. Food and drink will be kept away from school technology devices.
9. Cost of intentional abuse repair will be the responsibility of the parent/guardian.
10. Devices will always be kept in a safe and secure location. (For example, do not leave devices in unlocked cars, on tables in the lunchroom, on top of lockers, out on the front porch, etc.)

Home Use of Technology Devices (*as applicable*)

1. Devices will be brought to the school the next school day.
2. Devices will be brought to school fully charged. (NOTE: Do not charge devices when in the case.)
3. At home, devices are to be used in common rooms (living room, den, kitchen) by responsible family members only.
4. Devices will be stored in the case when not in use at home.
5. Parents will supervise Internet use at home.

Screen Care and Protection

Screens are often the most fragile and expensive part of technology devices. To protect them:

a. If placed in a book bag, it should be in a way that avoids placing pressure or weight on the screen.
b. Do not lean on the top of the device or its screen.
c. Keep protective covers on the device and closed when not in use.
d. Clean screens with a soft cloth only, do not use cleaners of any type.
e. Carry devices only in their *closed* cases (zip, velcro, etc.)

Saving Work & Backup

Students are responsible for storing data and backing up safely onto network resources. Devices may fail or need to be reset at anytime. All data on the device that was not properly stored or backed up will be lost.

Internet Use When Not On School Network

1. Students are allowed, with parent/guardian permission, to set up wireless networks on their school devices when devices are allowed go home.
2. *** Be aware that content on devices will not be filtered when using networks other than the school's wireless network.**

Sound

1. Sound must be muted at all times unless permission is obtained from the teacher.
2. Music is only allowed on school technology devices at the discretion of teacher.

iPads

1. Only school provided Apple ID's (username@MLTI.NET) are to be used on school device unless specifically instructed by a school administrator to use another specific Apple ID
2. Only install or use applications that do not violate federal or state laws or the school's Acceptable Use Policy.
3. Only install and use applications and use websites that are allowed by students my age.

Not meeting these expectations will lead to reduced privileges or consequences according to the Inappropriate Technology Use Discipline Rubric.

MDIRSS
Student Computer and Internet Use Rules
[Acceptable Use Policy (AUP)]

These rules implement Committee policy IJNDB – Student Computer and Internet Use. The rules are intended to provide general guidelines and examples of prohibited uses, but do not attempt to state all required or prohibited behavior by users. Failure to comply with Committee policy IJNDB and these rules may result in loss of computer and Internet access privileges, disciplinary action and/or legal action.

A. Computer Use is a Privilege, Not a Right

Student use of the school unit's computers, networks and Internet services is a privilege, not a right. Unacceptable use/activity may result in suspension or cancellation of privileges as well as additional disciplinary and/or legal action.

The building principal shall have final authority to decide whether a student's privileges will be denied or revoked.

B. Acceptable Use

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

The same rules and expectations govern student use of computers as apply to other student conduct and communications.

Students are further expected to comply with these rules and all specific instructions from the teacher or other supervising staff member/volunteer when accessing the school unit's computers, networks and Internet services.

C. Prohibited Use

The user is responsible for his/her actions and activities involving school unit computers, networks and Internet services, and for his/her computer files, passwords and accounts.

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

1. **Accessing Inappropriate Materials:** Accessing, submitting, posting, publishing, forwarding, downloading, scanning or displaying materials that are defamatory, abusive, obscene, vulgar, sexually explicit, sexually suggestive,

threatening, discriminatory, harassing and/or illegal;

2. **Illegal Activities:** Using the school unit's computers, networks and Internet services for any illegal activity or that violates other Committee policies, procedures and/or school rules;

3. **Violating Copyrights:** Copying or downloading copyrighted materials without the owner's permission;

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

5. **Copying Software:** Copying or downloading software without the express authorization of the system administrator;

6. **NonSchoolRelated Uses:** Using the school unit's computers, networks and Internet services for non-schoolrelated purposes such as private financial gain; commercial, advertising or solicitation purposes, or for any other personal use.

7. **Misuse of Passwords/Unauthorized Access:** Sharing passwords, using other users' passwords without permission and/or accessing other users' accounts;

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

9. **Unauthorized Access to Chat Rooms/News Groups:** Accessing chat rooms or news groups without specific authorization from the supervising teacher

D. No Expectation of Privacy

The school unit retains control, custody and supervision of all computers, networks and Internet services owned or leased by the school unit. The school unit reserves the right to monitor all computer and Internet activity by students. Students have no expectation of privacy in their use of school computers, including email and stored files.

E. Compensation for Losses, Costs and/or Damages

The student and/or the student's parent/guardian shall be responsible for compensating the school unit for any losses, costs or damages incurred by the school unit related to violations of policy IJNDB and/or these rules, including investigation of violations.

MDIRSS

Student Computer and Internet Use

[Internet Safety Policy (ISP)]

Conners Emerson School provides computers, networks and Internet access to support the educational mission of the schools and to enhance the curriculum and learning opportunities for students and school staff. The Committee believes that the resources available through the Internet are of significant value in the learning process and preparing students for future success. At the same time, the unregulated availability of information and communication on the Internet require that schools establish reasonable controls for lawful, efficient and appropriate use of this technology.

Student use of school computers, networks and Internet services is a privilege, not a right. Students are required to comply with this policy and the accompanying rules (IJNDBR). Students who violate the policy and/or rules may have their computer privileges revoked and may also be subject to further disciplinary and/or legal action.

All Conners Emerson Elementary School computers remain under the control, custody and supervision of the school unit. The school unit reserves the right to monitor all computer and Internet activity by students. Students have no expectation of privacy in their use of school computers.

While reasonable precautions will be taken to supervise student use of the Internet, Conners Emerson School cannot reasonably prevent all inappropriate uses, including access to objectionable materials and communication with persons outside of the school in violation of Committee policies/procedures and school rules. The school unit is not responsible for the accuracy or quality of information that students obtain through the Internet.

Students and parents shall be informed of this policy/procedure on an annual basis through handbooks and/or other means selected by the Superintendent/designee.

The Superintendent shall be responsible for implementing this policy and the accompanying rules, and for advising the Committee of the need for any future amendments or revisions to the policy. The Superintendent may develop additional administrative procedures/rules governing the daytoday management and operations of the school unit's computer system as long as they are consistent with the Committee's policy/rules. The Superintendent may delegate specific responsibilities to building principals and others as he/she deems appropriate.

Cross Reference: IJNDBR – Student Computer and Internet Use Rules

GCSA – Employee Computer and Internet Use

Adopted: 05/08/95

Revised: 09/03/03

F. School Unit Assumes No Responsibility for Unauthorized Charges, Costs, or Illegal Use

The school unit assumes no responsibility for any unauthorized charges made by students, including but not limited to credit card charges, long distance telephone charges, equipment and line costs, or for any illegal use of its computers such as copyright violations.

G. Student Security

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

H. System Security

The security of the school unit's computers, networks and Internet services are a high priority. Any user who identifies a security problem must notify the system administrator. The user shall not demonstrate the problem to others. Any user who attempts or causes a breach of system security shall have his/her privileges revoked and may be subject to additional disciplinary and/or legal action.

Cross Reference: IJNDB – Student Computer and Internet Use

First Reading: 06/11/03

Second Reading: 08/13/03

Adopted: 08/13/03

MDIRSS ELEMENTARY SCHOOLS: INAPPROPRIATE TECHNOLOGY USE DISCIPLINE RUBRIC

- Offenses not listed on this chart will be addressed at the discretion of the school administration
- Loss of device, Internet access, or email access will be determined on a case-by-case basis by school administration

LEVEL 1 • Carrying device carelessly • Accessing inappropriate websites • Using the Web at inappropriate times* • Gaming without express permission of supervising teacher • Downloading inappropriate materials • Plagiarism • Messaging inappropriate content or at inappropriate times • Use of another student's device • Allowing another student to use your device *NOTE: Appropriateness to be determined by the supervising teacher.	**1st Offense** 1/2 hour detention to be served with teacher in classroom where infraction occurred Detention slip given to student and returned with parent signature (copy goes to administrator) **Step 1 on Ladder**	**2nd Offense** 1 hour detention to be served with administrator School administrator sends letter or makes phone call home **Step 2 on Ladder**	**3rd Offense** 1 hour detention to be served with administrator Meeting with parent(s) Network/Internet related abuse may result in loss of Network/Internet access **Step 3 on Ladder**	**Further Infractions** Referred to school administrator for action.
LEVEL 2 • Clearing web or other history • Accessing offensive material • Bypassing or seeking ways to bypass network filters • Misuse of passwords • Neglectful handling of device such as leaving unattended in hallways, locker rooms, windowsills, cubbies etc.	**1st Offense** 1 hour detention to be served with administrator Administrator writes letter and calls home **Step 2 on Ladder**	**2nd Offense** 1 hour detention to be served with administrator Administrator writes letter home & schedules meeting with parent(s) **Step 3 on Ladder**	**Further Infractions** Referred to school administrator for action.	

• Defacing your assigned device				
LEVEL 3 • Vandalizing another's device • Harassment or bullying (involving technology) • Illegal activities	**1st Offense** Student and parents meet with meet with school administrator and/or law enforcement officials.	**Further Infractions** Referred to school administrator and/or law enforcement officials for action.		

Updated: September, 2013