RSU 73 Chromebook/Ipad Guidelines

21-22

RSU 73 Technology Department Contact Information

Tech Director	**Chris Hollingsworth**	**chollingsworth@rsu73.com**	**207.897.6722 ext 121**
Technician/Data	**Mark Bonnevie**	**mbonnevie@rsu73.com**	**207.897.4319 ext 223**
Technician	**Noah Keneborus**	**nkeneborus@rsu73.com**	**207.897.4319 ext 223**

Website: rsu73.com/technology

Technology Department Goals

1. **Make a commitment to support technology as a viable instructional strategy**
2. **Maintain a working infrastructure of technology equipmnent and software while anticipating for future needs**
3. **Be responsive to technlogy needs, interests and goals to create the best possible learning environment**
4. **Create an effective, dynamic, current, adjustable tech plan**

Laptop Take Home Safety Information

Before bringing the laptop home parents should understand the following:

- **Home internet access is not necessary for the local productivity software on the laptop to operate**
- **Home Internet access, is available (contact building administrators)**
- **Any and all after school computer use should always take place in a location where parents can monitor their child**
- **All internet browsing is monitored**

Technology Care and Use Guidelines

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

General Use of Technology Devices

1. **Devices with recording capabilities 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. **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.**
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:

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

Saving Work & Backup

All work on a Chromebook is automatically saved to the students Google Drive school account

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 to go home.**
2. **Be aware that content on Chromebooks is still 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..**

Not meeting these expectations will lead to reduced privileges or consequences

Updated 9/17/2018

NEPN/NSBA Code: IJNDB

STUDENT COMPUTER AND INTERNET USE AND INTERNET SAFETY

Spruce Mountain School District, RSU73, computers, network, and Internet access are provided to support the educational mission of the schools and to enhance the curriculum and learning opportunities for students and school staff. This policy and the accompanying rules also apply to laptops issued directly to students, whether they are used at school or off school premises.

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

Violations of this policy and Spruce Mountain School District's computer and Internet rules may also result in disciplinary action, referral to law enforcement, and/or legal action.

Spruce Mountain School District computers remain under the control, custody, and supervision of the school unit at all times. The school unit monitors all computer and Internet activity by students. Students have no

expectation of privacy in their use of school computers, whether they arused on school property or elsewhere.

INTERNET SAFETY

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

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

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

IMPLEMENTATION OF POLICY AND "ACCEPTABLE USE" RULES

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

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

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

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

STUDENT COMPUTER, INTERNET USE RULES AND INTERNET SAFETY

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

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

A. ***Acceptable Use***

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

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

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

B. ***Consequences for Violation of Computer Use Policy and Rules***

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

The building principal shall have final authority to decide whether a student's privileges will be limited, suspended or revoked based upon the

circumstances of the particular case, the student's prior disciplinary record, and any other relevant factors.

INTERNET SAFETY

Spruce Mountain School District uses filtering technology designed to block materials that are obscene or harmful to minors, and child pornography. Although Spruce Mountain School District takes precautions to supervise and monitor student use of the Internet, parents should be aware that the Spruce Mountain School District cannot reasonably prevent all instances of inappropriate computer and Internet use by students in violation of Board policies and rules, including access to objectionable materials and communication with persons outside of the school. The school unit is not responsible for the accuracy or quality of information that students obtain through the Internet. In the interest of student Internet safety, Spruce Mountain School District educates students and parents about online behavior, including interacting with other people on social networking sites and in chat rooms, the dangers of engaging in unlawful online activities, and issues surrounding "sexting" and cyberbullying awareness and response. The Superintendent /designee shall be responsible for integrating age-appropriate Internet safety training and "digital citizenship" into the curriculum and for documentation of Internet safety training,

C. *Probibited Uses*

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

1. ***Accessing or Posting Inappropriate Materials*** **- Accessing, submitting, posting, publishing, forwarding, downloading, scanning or displaying defamatory, abusive, obscene, vulgar, sexually explicit, sexually suggestive, threatening, discriminatory, harassing and/or illegal materials or engaging in "cyber bullying;"**
2. ***Illegal Activities*** **- Using the school unit's computers, networks, and Internet services for any illegal activity or in violation of any Board policy or school rules. The school unit assumes no responsibility for illegal activities of students while using school computers;**
3. **Violating Copyrights - Copying, downloading or sharing any type of copyrighted materials (including music or films) without the owner's permission (see Board policy/procedure EGAD- Copyright Compliance). The school unit assumes no responsibility for copyright violations by students;**

4. **Copying Software - Copying, transmitting, accessing or downloading software without the express authorization of the Technology Coordinator and building administrator. Unauthorized copying of software is illegal and may subject the offender to substantial civil and criminal penalties. The school unit assumes no responsibility for illegal software copying by students;**
5. **Plagiarism - Representing as one's own work any materials obtained on the Internet (such as term papers, articles, music, etc.). When Internet sources are used in student work, the author, publisher, and website must be identified;**
6. **Non-School-Related Uses - Using the school unit's computers, networks, and Internet services for any personal reasons not connected with the educational program or assignments. Examples of these but not limited to are buying, selling, advertising, spamming, mass unsolicited mail using, etc…**
7. **Misuse of Passwords/Unauthorized Access – Sharing passwords, using other users' passwords, and accessing or using other users accounts; page 2 of 5**
8. **Malicious Use/Vandalism – Any malicious use, disruption or harm to the school unit's computers, networks, and Internet services, including but not limited to hacking activities and creation/uploading of computer viruses; and**
9. **Unauthorized Access to Blogs/Chat Rooms/Social Networking Sites - Accessing blogs, chat rooms or social networking sites (or any websites) to which student access is prohibited-**

D. *No Expectation of Privacy*

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

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

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

F ***Student Security on RSU73's Networks***

A student is not allowed to reveal his/her full name, address or telephone number, social security number, or other personal information like self portraits on the Internet via the district's networks without prior permission from a teacher and a website publishing form. Students should never agree to meet people they have contacted through the Internet without parental permission. Students should inform their teacher if they access information or messages that are dangerous, inappropriate, or make them uncomfortable in any way. Internet blocking and filtering are present in all networks but are not guaranteed to prevent all intrusions.

G ***Network System Security***

The security of the school unit's computers, networks, network devices. and Internet services are a high priority. Any user who attempts to breach system security, causes a breach of system security, or fails to report a system security problem shall be subject to disciplinary and/or legal action in addition to having his/her computer privileges limited, suspended, or revoked. Any student who identifies a security problem must notify his/her teacher immediately. The student shall not demonstrate the problem to others or access unauthorized network device material..

***** IMPLEMENTATION OF POLICY AND "ACCEPTABLE USE" RULES *****

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

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

H. *Additional Rules for Laptops Issued to Students*

1. **Laptops are loaned to students as an educational tool and are only authorized for use in completing school assignments**
2. **Before a laptop is issued to a student, the student must sign the school's "acceptable use" agreement. Parents are required to attend an informational meeting before a laptop will be issued to their child. Attendance will be documented by means of a "sign in" sheet. The meeting will orient parents to the goals and workings of the laptop program, expectations for care of school-issued laptops, Internet safety, and the school unit's rules in regard to use of this technology.**
3. **Students and their parents are responsible for the proper care of laptops at all times, whether on or off school property,Loss or theft of a laptop must be reported immediately to school staff, and, if stolen, to the RSU 73 SRO authority as well.**
4. **The Board's policy and rules concerning computer and Internet use apply to use of laptops at any time or place, on or off school property. Students are responsible for obeying any additional rules concerning care of laptops issued by school staff.**
5. **Violation of policies or rules governing the use of computers, or any careless use of a laptop may result in a student's laptop being confiscated and/or a student only being allowed to use the laptop under the direct supervision of school staff. The student will also be subject to disciplinary action for any violations of Board policies or school rules.**
6. **Parents will be informed of their child's login password. Parents are responsible for supervising their child's use of the laptop and Internet access when in use at home.**
7. **The laptop may only be used by the student to whom it is assigned and by family members,**
8. **Laptops must be returned in acceptable working order at the end of the school year or whenever requested by school staff.**

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

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

Regional School Unit 73 Board of Directors	Code: IJNDB-E Page1

SUBJECT : Acceptable Use Form - Student Computer and Internet Use and Internet Safety	
DATE OF ORIGINAL POLICY:	September 2010
DATE OF NEXT REVIEW:	2018
CANCELS POLICY CODE:	None
REVISION DATE:	August 2011, Jan 24, 2013
JURISDICTION:	RSU 73 Schools

RSU #73

STUDENT AND PARENT/GUARDIAN TECHNOLOGY ACCEPTABLE USE POLICY

STATEMENT

The use of and access to technology is essential in preparing our students for the 21st century. RSU73 is pleased to offer our students and parents/guardians the opportunity to use state of Maine issued laptops in Grades 7/8. We expect that students and parents abide by the following statement and that one handles the equipment (hardware & software) with care and respect, reporting abuse and misuse as soon as possible.

When using issued IPads/Chromebook laptops, or any computer, students and parents/guardians are NEVER allowed to print, copy, upload, download, update, delete, or modify anything (software or hardware) on laptops or computers without the permission of their teacher, principal or technology team member. Students and parents /guardians should only be using the district issued IPads/Chromebook laptops for RSU73 educational and vocational purposes. We also expect ALL students and parents/guardians to use the Internet responsibly adhering to safety measures, educational goals, copyright and plagiarism rules and laws, and the principles of responsible citizenship.

Notes: Students can lose the privilege to bring the laptop home or lose the laptop for a period of time (depending on the severity of the infraction). Do not add unapproved, personalized stickers or write or scratch the laptops. Laptop misuse and/or abuse will result in consequences.

If you need any other information or have questions, please call RSU 73 and speak to Chris Hollingsworth

Student care and proper use

Student donts for IPad/Chromebooks: Practice and share responsible use! (mantra) Be a responsible and respectable digital citizen!

Don't change password and don't share passwords

Don't share or swap laptops.

Don't share or swap chargers, cords, and carrying case

Don't remove issued carrying case or laptop name tags or stickers

Don't drink or eat near Device-avoid spillage!

Don't write on Devices or scratch or add unapproved, personalized stickers, drawings, etc..

Don't leave Devices unattended

Don't use water or sprays to clean Devices

Don't try to repair any device. Report damage to staff. Report any hardware and software issues to staff.

When using the IPad/Chromebook laptops or any computer, NEVER print, copy, upload, download, update, delete, or modify anything (software or hardware) on laptops or computers without the permission. Use for educational purposes

Reminder: Students are responsible for keeping laptops charged

Intellectual Property

Respect and protect the intellectual property of others.
Do Not infringe copyrights (no making illegal copies of music, games or movies)..
Do Not plagiarize.
Communicate only in ways that are kind and respectful.
Report threatening or discomforting materials and communications to a teacher.
Do Not intentionally access, transmit, copy or create material that violates the school's code of conduct (such as messages that are pornographic, threatening, rude, discriminatory or meant to harass)
Do Not intentionally access, transmit, copy or create material that is illegal (such as obscenity, stolen materials or illegal copies of copyrighted works).