OYSTER RIVER COOPERATIVE SCHOOL BOARD	Policy Code: JICL-R
Draft to Policy Committee: February 8, 2017 Policy Committee: December 12, 2018 School Board Review: January 2, 2019	Page 1 of 4

STUDENT COMPUTER/DEVICE AND INTERNET USE RULES

All Oyster River students are responsible for their actions and activities involving school unit computers/devices, network and Internet services, and for their computer files, passwords and accounts. These rules provide general guidance concerning the use of the school unit's computers/devices, networks, and Internet services, and examples of prohibited uses. Due to the ever-changing resources, available on the Internet these rules do not attempt to describe every possible prohibited activity by students. Students, parents and school employees who have questions about whether a particular activity is prohibited are encouraged to contact a building administrator These rules apply to all school computers/devices wherever used, and all uses of school servers, Internet access and networks regardless of how they are accessed. Notwithstanding FERPA and other related laws, students have no expectation of privacy regarding their use on the school district computer network. Oyster River Cooperative School District recognizes that electronic communication/social media/texting is not a replacement for meaningful dialogue between students to students or students to staff. When practical, the district encourages face to face communication.

A. Acceptable Use

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

2. Students must comply with all Board policies, school rules and expectations concerning student conduct and communications when using school computers/devices and/or personal computers/devices, whether on or off school property.

3. Students also must comply with all specific instructions from school employees and volunteers when using the school unit's computers/devices and/or personal computers/devices.

B. Prohibited Uses

Unacceptable uses of school unit computers/devices include, but are not limited to, the following:

1. **Accessing or Communicating Inappropriate Materials –** Students may not access, submit, post, publish, forward, download, scan or display defamatory, abusive, obscene, vulgar, sexually explicit, sexually suggestive, threatening, discriminatory, harassing, bullying/cyberbullying and/or illegal materials or messages.

2. **Illegal Activities –** Students may not use the school unit's computers/devices, network and Internet services for any illegal activity or in violation of any Board policy/procedure or school rules. The school unit assumes no responsibility for illegal activities of students while using school computers/devices.

3. **Violating Copyrights or Software Licenses –** Students may not copy, download or share any type of copyrighted materials (including music or films) without the owner's permission; or copy or download software without the express authorization of the Technology Coordinator. Unauthorized copying of software is illegal and may subject the copier to substantial civil and criminal penalties. The school unit assumes no responsibility for copyright or licensing violations by students. *See Board policy/procedure EGAD – Copyright Compliance.*

4. **Downloading "Apps" or Installing Software** – Students may not download any "apps" or install software without prior approval from an authorized school employee.

5. **Plagiarism –** Students may not represent as their 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 web site must be identified.

6. **Use for Non-School-Related Purposes -** Using the school unit's computers/devices, network and Internet services for any personal reasons not connected with the educational program or school assignments.

7. **Misuse of Passwords/Unauthorized Access –** Students may not share passwords (except with authorized school employees); use other users' passwords; access or use other users' accounts; or attempt to circumvent network security systems.

8. **Malicious Use/Vandalism –** Students may not engage in any malicious use, disruption or harm to the school unit's computers/devices, network and Internet services, including but not limited to hacking activities and creation/uploading of computer viruses.

9. **Avoiding School Filters –** Students may not attempt to or use any software, utilities or other means to access Internet sites or content blocked by the school filters. If a student believes filtering should be less restrictive on a temporary basis for specific, bona fide research purposes, he/she should discuss the matter with his/her teacher.

C. 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 for violations of Board policies/procedures and school rules while the student is using school unit computers/devices, networks, and/or Internet services, 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/devices, networks, and/or Internet services.

D. Student Security

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

E. System Security

The security of the school unit's computers/devices, network and Internet services is a high priority. Any student who identifies a security problem must notify his/her teacher or building administrator immediately. The student shall not demonstrate the problem to others or access unauthorized material.

F. Additional Rules for Devices Issued to Students

1. Laptops are loaned to students as an educational tool and may be used for purposes specifically authorized by school employees.

2. Students and their families are responsible for the proper care of devices at all times, whether on or off school property, including costs associated with repairing or replacing the devices

3. If a device is lost or stolen, this must be reported to a building administrator immediately. If a device is stolen, a report should be made to the local police and a building administrator immediately.

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

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

6. All use of school-loaned devices by all persons must comply with the school's Student Computer/Device and Internet Use Rules.

7. Devices must be returned in acceptable working order whenever requested by school staff.

G. Additional Rules for Use of Privately-Owned Computers/Devices by

High School Students are permitted to use privately-owned computers/electronic devices at the high school. Electronic Devices include but are not limited to laptops, smart phones, tablets, calculators, gaming devices, wearables, and monitoring devices for medical conditions. Additionally, the following expectations of students are established:

1. The use of privately-owned computers/electronic devices is at the discretion of school administrators, classroom teachers, coaches, bus drivers, or employees chaperoning trips.

    a. After review by principals, teachers will annually post their rules related to the use of electronic devices.

2. The use of cameras or the camera/video/sound recording functions on any electronic device is strictly prohibited in locker rooms and restrooms. In other school locations, students are required to obtain permission before photographing, taking videos or recording any individual. Students are also required to obtain prior permission before posting any photos, videos or sound recordings of individuals taken at school or during school activities on social media or elsewhere.

3. The student is responsible for proper care of his/her privately-owned computer/device, including maintaining security updates provided by the manufacturer or software vendor, any costs of repair, replacement or modifications needed to use the device at school.

4. Oyster River Cooperative School District is not responsible for damage, loss or theft of any privately-owned computer/electronic device.

5. Care must be taken to use such devices in a manner that does not interrupt the activities of others. Students are required to comply with all Board policies, administrative procedures and school rules while using privately-owned computers/electronic devices at school.

6. Students have no expectation of privacy in their use of privately-owned computer/electronic device while at school. Such devices may be subject to search if there is reasonable suspicion that a student is violating Board policies, procedures, or school rules, or engaging in other misconduct. School administrators may confiscate such devices for as long as necessary to complete their investigation.

7. Students violating these rules will be subject to discipline, which may include:
   a. Exclusion of the device from school for an extended period;
   b. Sanctions ranging from detention to suspension from school depending upon the nature of the offense and the student's disciplinary record.

Cross Reference:

JICJ-Student Use of Computer/Electronic Devices at School
JICK – Bullying and Cyberbullying Pupil Safety and Violence Prevention