

The School Board recognizes that technological resources can enhance student performance by offering effective tools to assist in providing a quality instructional program, facilitating communications with parents/guardians, staff, and the community, supporting District and school operations, and improving access to and exchange of information. The Board expects all students to learn to use the available technological resources that will assist them in the performance of their education. As needed, students shall receive lessons and instruction in the appropriate use of these resources.

Students shall be responsible for the appropriate use of technology and shall use the District's technological resources primarily for purposes related to their education. Students are hereby notified that there is no expectation of privacy on district computers, computer files, email, internet usage logs, and other electronic data.

The Superintendent or designee shall ensure that all District computers with Internet access have a technology protection measure to prevent access to visual depictions that are obscene or pornographic and that the operation of such measures is enforced.

The Superintendent shall establish administrative regulations and a Responsible Use Agreement that outlines student obligations and responsibilities related to the use of District technology. The Superintendent also may establish guidelines and limits on the use of technological resources. Inappropriate use may result in a cancellation of the student's user privileges, disciplinary action, and/or legal action in accordance with law, Board policy, and administrative regulations.

The Superintendent or designee shall provide copies of related policies, regulations, and guidelines to all students and parents.

Law Reference:

- RSA 194:3-d, School District Computer Networks
- 47 U.S.C. §254, Requirements For Certain Schools – Internet Safety
- 20 U.S.C. §6777, Enhancing Education Through Technology – Internet Safety

Appendix Reference: JICL-R

Date Adopted: March 21, 2023

Responsible Computer, Network and Internet Use

Overview:

The Portsmouth School Department provides its students and staff access to a multitude of technology resources. These resources provide opportunities to enhance learning and improve communication within our community and with the global community beyond our campus. The advantages of having access to these resources are far greater than any potential downside. However, with the privilege of access is the responsibility of students, teachers, staff, and the public to exercise appropriate personal responsibility in their use of these resources. The School Department policies are intended to promote the most effective, safe, productive, and instructionally sound uses of networked information and communication tools. The School Department also makes a good faith effort to protect its students from exposure to Internet materials that are harmful or explicit. The School Department maintains a system of Internet content filtering devices and software controls that meet federal standards established in the Children's Internet Protection Act (CIPA) for on-site use of the technology resources of the School Department.

Digital Citizen:

The Portsmouth School Department uses information and technology in safe, legal, and responsible ways. A responsible digital citizen is one who:

- Respects One's Self- Users will select online names that are appropriate and will consider the information and images that are posted online.
- Respects Others- Users will refrain from using technologies to bully, tease, or harass other people.
- Protects One's Self and Others- Users will protect themselves and others by reporting abuse and not forwarding inappropriate materials or communications.
- Respects Intellectual Property- Users will suitably cite any and all use of websites, books, media, etc.
- Protects Intellectual Property- Users will request to use the software and media others produce.

Expectations:

Responsible use of the School Department's technology resources is expected to be ethical, respectful, academically honest, and supportive of the school's mission. Each computer user has the responsibility to respect every other person in our community and on the Internet. Digital storage and electronic devices used for school purposes will be treated as extensions of the physical school space. Administrators, or their designees, may review files and communications (including electronic mail) to ensure that users are using the system in accordance with School Department policy. Users should not expect that files stored on servers or disks will be private. Users also should understand that school servers regularly record Internet activity in log files that are available to the public under RSA 91-A: Access to Public Records and Meetings.

Some activities are expressly prohibited by law. Users are expected to abide by the generally accepted rules of network etiquette. The following guidelines are intended to clarify expectations for conduct, but they should not be construed as all-inclusive.

- Use of electronic devices should be consistent with the School Department's educational objectives, mission, and curriculum.
- Transmission of any material in violation of any local, federal, and state laws is prohibited. This includes, but is not limited to: copyrighted material, licensed material, and threatening or obscene material.
- Intentional or unintentional use of computing resources to access or process, proxy sites, pornographic material, explicit text or files, or files dangerous to the integrity of the network is strictly prohibited.
- Software and/or services may not be installed or downloaded on school devices without prior approval of the Superintendent or designee.
- Use of computing resources for commercial activities, product advertisement, religious, or political lobbying is prohibited.
- Users may be held personally and financially responsible for malicious or intentional damage done to network software, data, user accounts, hardware, and/or unauthorized costs incurred.
- Files stored on district-managed networks are the property of the school district and, as such, may be inspected at any time and should not be considered private.
- Materials published for electronic publication must be for educational purposes. School administrators, teachers, and staff may monitor these materials to ensure compliance with content standards.

Policy Violations:

The school reserves the right to refuse access to the Internet to anyone. Violating any portion of this policy may result in disciplinary action, including temporary or permanent ban on computer or Internet use, suspension or dismissal from school, and/or legal action. The School Department may cooperate with law enforcement officers in investigations related to illegal activities conducted through its network. Law Reference: RSA 194:3-d, 47U.S.C. Section 254, Children's Internet Protection Act.

Legal References:

RSA 194:3-d, School District Computer Networks

Pub. L. No. 106-554, Children's Internet Protection Act (www.ifea.net/cipa.html)

OYSTER RIVER COOPERATIVE SCHOOL BOARD	Policy Code: JICL
Date of Adoption: August 20, 2008 Previously: IJNDB Adopted Code Change to SB: October 6, 2010 Policy Committee: January 7, 2015 School Board First Read: January 7, 2015 School Board Second Read/Adoption: January 21, 2015 Re-review to Policy Committee: 2/8/17 & 12/12/18 School Board First Read: December 19, 2018 School Board Second Read/Adoption: January 2, 2019	Page 1 of 1 Category: Priority

STUDENT COMPUTER AND INTERNET USE

Oyster River School District's computers, networks 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.

Student use of school computers, networks and Internet services is a privilege, not a right. Compliance with the District's policies and rules concerning computer use is mandatory. Students who violate these policies and rules may 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 Oyster River School District computers remain under the control, custody and supervision of the school District at all times. The District monitors all computers and Internet activity by students. Students have no expectation of privacy in their use of District computers.

High School Students are allowed to use their personal computer at school with prior authorization, provided that they comply with this policy and the accompanying rules.

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

It is further understood that students will not do anything that compromises or disrupts the integrity of the Oyster River Cooperative School District's network.

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

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

Legal Reference: RSA 194:3-d

Cross Reference:

JICL-R – Student Computer/Device and Internet Use Rules

JICK – Bullying and Cyberbullying Pupil Safety and Violence Prevention

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.*

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 2 of 4

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.

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 3 of 4

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.

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 4 of 4

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

JICL - SCHOOL DISTRICT INTERNET ACCESS FOR STUDENTS

The School Board recognizes that Internet access can enhance student performance by providing access to all types of up-to-date information. The Board expects all students to learn to use the internet to assist them in the performance of their learning. Students shall receive lessons and instruction in the appropriate use of the internet.

Students shall be responsible for the appropriate use of the internet and shall use the internet primarily for purposes related to their education. Students are hereby notified that there is no expectation of privacy on district devices, computer files, email, and other electronic data.

The Superintendent or designee shall ensure that all District devices with Internet access have a protection measure that prevents access to inappropriate content. The Superintendent or designee may disable the technology protection measure, either selectively or globally, if requested of an adult to enable access to bona fide research, educational or other lawful purpose.

The Superintendent shall establish administrative regulations and an Acceptable Use Agreement that outlines student obligations and responsibilities related to the use of the internet. He/she also may establish guidelines and limits on the use of the internet. Inappropriate use may result in a cancellation of the student's privileges, disciplinary action, and/or legal action in accordance with law, Board policy, and administrative regulations.

The Superintendent or designee shall provide copies of related policies, regulations, and guidelines to all students. Students shall be required to acknowledge in writing that they have read and understand the District's Acceptable Use Agreement.

Statutory/Regulatory/Policy/Handbook Cross References

ESD Policy JICL-R (Acceptable Internet Use Procedures – Students) RSA 194:3-d
(School District Computer Networks) 47 U.S.C. §254 (Requirements For Certain
Schools – Internet Safety) 20 U.S.C. §6777 (Enhancing Education Through Technology
– Internet Safety) Handbook (Referenced in Student and Personnel Handbooks)

APPROVED/REVISED: June 2, 2011, September 18, 2014, August 4, 2016, September 19, 2019

PREVIOUS POLICY: August 17, 2006 “Acceptable Computer, Network, E-Mail and Internet Use

JICL-R - ACCEPTABLE INTERNET USE PROCEDURES AND AGREEMENT - STUDENTS

The purpose of the Acceptable Use Procedures and Agreement is to provide the procedures, rules, guidelines, and the code of conduct for the use of technology and the Internet.

Definition The definition of "information networks" is any configuration of hardware and software, which connects users. The network includes, but is not limited to, all of the computer hardware, operating system software, application software, stored text and data files. This includes electronic mail, local databases, externally accessed databases, recorded magnetic or optical media, clip art, digital images, digitized information, communications technologies, and new technologies as they become available. Stand-alone workstations are also governed by this acceptable use procedure.

The School District Services The School District provides resources for teaching and learning, communication services, and business data services by maintaining access to local, regional, national, and international sources of information. The School District information resources will be used by members of the school community with respect for the public trust through which they have been provided and in accordance with policy and regulations established by the School District. These procedures do not attempt to articulate all required or proscribed behavior by its users.

Successful operation of the network requires that all users conduct themselves in a responsible, decent, ethical and polite manner while using the network. The user is ultimately responsible for his/her actions in accessing network services.

Guidelines

1. Access to the networks and to the information technology environment within the District is a privilege and must be treated as such by all users of the network and its associated systems.
2. Information networks will be used for the purposes of research, education, and school related business and operations.
3. Any system which requires password access or for which the District requires an account, such as the Internet, will only be used by the authorized user. Account owners are ultimately responsible for all activity under their accounts.
4. The resources of the District are limited. All users must exercise prudence in the shared use of this resource.

Unacceptable Use

The District has the right to take disciplinary action, remove device and networking privileges and/or take legal action, for any activity characterized as unethical and unacceptable. Unacceptable use activities constitute, but are not limited to, any activity through which any user:

1. Violates such matters as institutional or third-party copyright, license agreements or other contracts. The unauthorized use of and/or copying of software is illegal.
2. Interferes with or disrupts other network users, services or equipment. Disruptions include, but are not limited to: distribution of unsolicited advertising, propagation of computer worms or viruses, distributing quantities of information that overwhelm the system, and/or using a District network to make unauthorized entry into any other resource accessible via the network.
3. Seeks to gain or gains unauthorized access from a proxy site, VPN or other.
4. Uses or knowingly allows another to use any device or computer system to devise or execute a scheme to defraud or to obtain money, property, services, or other things of value by false pretenses, promises, or representations.
5. Destroys, alters, dismantles or otherwise interferes with the integrity of device based information and/or information resources.
6. Invades the privacy of individuals or entities.
7. Uses the network for commercial or political activity.
8. Installs unauthorized software for use on District devices.
9. Uses a network to access inappropriate materials.
10. Submits, publishes or displays any defamatory, inaccurate, racially offensive, abusive, obscene, profane, sexually oriented, or threatening materials or messages either publicly or privately.
11. Uses a District network for illegal harassing, vandalizing, inappropriate or obscene purposes, or in support of such activities.

School District Rights

The District reserves the right to:

1. Monitor all activity. Notwithstanding FERPA and other related laws, students have no expectation of privacy regarding their use on the school district device network.
2. Make determinations on whether specific uses of a network are consistent with these acceptable use procedures.

3. Determine appropriate use.
4. Remove a user's access to the network at any time it is determined that the user engaged in unauthorized activity or violated these acceptable use procedures. 6. Cooperate fully with any investigation concerning or relating to the District's network Activity.

School District Internet Code of Conduct

Use of the Internet by students and staff of the District shall be in support of education and research that is consistent with the mission of the District. Internet use is limited to those persons who have been issued District-approved accounts. Use will be in accordance with the District's Acceptable Use Procedures and this Code of Conduct. Users are expected to abide by the following terms and conditions:

1. Protect the integrity of your accounts.
2. Respect the privacy of other users. Do not use other users' passwords.
3. Be ethical and courteous. Do not send hate, harassing or obscene mail, discriminatory remarks, or demonstrate other antisocial behaviors.
4. Maintain the integrity of files and data. Do not modify or copy files/data of other users without their consent.
5. Treat information created by others as the intellectual property and creative rights of the creator. Respect copyrights.
6. Use any network in a way that does not disrupt its use by others.
7. Do not destroy, modify or abuse the hardware or software in any way.
8. Do not develop or pass on programs that harass other users or infiltrate a computer or computing system and/or damage the software components of a computer or computing system, such as viruses, worms, "chain" messages, etc.
9. Do not use the Internet to access or process pornographic or otherwise inappropriate material.
10. Do not use the Internet for commercial purposes.

The District reserves the right to remove a user's account if it is determined that the user is engaged in unauthorized activity or is violating this code of conduct.

School District Internet Access Release Form and Acceptable Use Agreement

As a condition of my right to use the School District network resources, including access to the Internet, students understand and agree to the following:

1. To abide by the District Acceptable Use Procedures and Code of Conduct.

JICL-R3

2. That District administrators and designated staff have the right to review any material stored on District devices in files and to edit or remove any material which they, in their sole discretion, believe may be unlawful, obscene, abusive, or otherwise objectionable and students hereby waive any right of privacy which I may otherwise have to such material.
3. That the School District will not be liable for any direct or indirect, incidental, or consequential damages due to information gained and/or obtained via use of the District's network resources.
4. That the School District does not warrant that the functions of any District network, or any network accessible through District resources, will meet any specific requirements you may have, or that the network resources will be error-free or uninterrupted.
5. That the School District shall not be liable for any direct or indirect, incidental, or consequential damages (including lost data or information) sustained or incurred in connection with the use, operation, or inability to use District networks and resources.
6. That the use of the District network(s), including access to public networks, is a privilege which may be revoked by network administrators at any time for violation of the Acceptable Use Procedures and Code of Conduct. The School District will be the sole arbiter(s) of what constitutes violation of the Acceptable Use Procedures or Code of Conduct.
7. In consideration for the privilege of using the School District network resources and in consideration for having access to the public networks, I hereby release the School District, its operators, and any institutions with which they are affiliated from any and all claims and damages of any nature arising from my use, or inability to use, the District network resources.

THIS FORM MAY BE SIGNED USING THE EPPING SCHOOL DISTRICT INFO SNAP PROGRAM.

Name of User/Student:

Home phone:

School of Attendance:

I hereby certify that I have read the Acceptable Use Policy and Procedures; that I fully understand their terms and conditions; and that I will abide by the terms conditions set forth in those documents.

Signature of User/Student:

Date:

Signature of Parent:

Date:

Statutory/Regulatory/Policy/Handbook Cross References

ESD Policy JICL (School District Internet Access for Students) RSA 194:3-d (School District Computer Networks) 47 U.S.C. §254 (Requirements For Certain Schools – Internet Safety) 20 U.S.C. §6777 (Enhancing Education Through Technology – Internet Safety) Handbook (Referenced in Student and Personnel Handbooks)

APPROVED/REVISED: June 2, 2011, September 18, 2014, August 25, 2016

PREVIOUS POLICY: August 17, 2006 “Acceptable Computer, Network, E-Mail and Internet Use