

STUDENT COMPUTER/DEVICE AND INTERNET USE RULES

All students are responsible for their actions and activities involving school unit computers/devices, network and Internet services (such as Google's G-Suite for Education), 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. The 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 or the Technology Director. 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.

A. Acceptable Use

1. The school unit's 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 School Committee policies, school rules and expectations concerning student conduct and communications when using school 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.
4. Students are required to provide their passwords for any school-issued computers/devices to building administrators.

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 School Committee 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 Director. 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 School Committee policy/procedure EGAD - Copyright Compliance.*

4. **Downloading “Apps”** – Students may not download any “apps” without prior approval from and 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 others’ 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.
10. **Unauthorized Access to Blogs/Social Networking Sites, Etc.** – Students may not access blogs, social networking sites, etc., to which student access is prohibited.

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

The student and his/her parents/guardians are responsible for compensating the school unit for any losses, costs or damages incurred for violations of School Committee 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 network/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/iPads/chromebooks are loaned to students as an educational tool and may be used for purposes specifically authorized by school employees and/or the MLTI program.
2. Parents are required to attend an informational meeting before a device will be issued to their child as part of the MLTI Program. Both the student and his/her parent must sign the school's acknowledgment form.
3. 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 device. Biddeford School Department offers an insurance program for parents to cover replacement costs and/or repair costs for damages not covered by the device warranty. **Parents who choose not to purchase the plan should be aware that they are responsible for any costs associated with loss, theft, or damage to a device issued to their child.**
4. If a device is lost or stolen, this must be reported to the building principal immediately. If a device is stolen, a report should be made to the local police and the building principal immediately.
5. The School Committee's policy and rules concerning computer/device 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 employees.
6. 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 School Committee policies/procedures or school rules.

7. Parents will be informed of their child's login password. Parents are responsible for supervising their child's use of the device and Internet access when in use at home.
8. The device may only be used by the student to whom it is assigned and family members to the extent permitted by the school or the MLTI program.
9. All use of school-loaned devices by all persons must comply with the school's Student Computer/Device and Internet Use-Rules.
10. Devices must be returned in acceptable working order at the end of the school year or whenever requested by school staff.

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

1. A student who wishes to use a privately-owned computer/device in school may do so with teacher or school administrator consent.
2. The Technology Coordinator or a member of the technology department will determine whether a student's privately-owned computer/device meets the school unit's network requirements.
3. Requests may be denied if it is determined that there is not a suitable educational basis for the request and/or if the demands on the school unit's network or employees would be unreasonable.
4. The student is responsible for proper care of his/her privately-owned computer/device, including any costs of repair, replacement, or any modifications needed to use the computer/device at school.
5. The school unit is not responsible for damage, loss, or theft of any privately-owned computer/device.
6. Students are required to comply with all School Committee policies, administrative procedures and school rules while using privately-owned computers/devices at school.
7. Students have no expectations of privacy in their use of a privately-owned computer/device while at school. The school unit reserves the right to search a student's privately-owned computer/device if there is reasonable suspicion that the student has violated School Committee policies, administrative procedures or school rules, or engaged in other misconduct while using the computer/device.

8. The school unit may confiscate any privately-owned computer/device used by a student in school without authorization as required by these rules. The contents of the computer may be searched in accordance with applicable laws and policies.
9. Violation of any School Committee policies, administrative procedures, or school rules involving a student's privately-owned computer/device may result in the revocation of the privilege of using the computer at school and/or disciplinary action.

H. Google G-Suite for Education

The school unit will, at its discretion, create Google G-Suite for Education accounts for students. Accounts will be terminated when a student ceases to be a student in the school unit.

Google G-Suite features will be enabled on a user-by-user basis at the discretion of the Technology Director. Use of Google G-Suite is subject to Google's acceptable use policy (a copy of which is available upon request from the Information Technology Department). The school unit maintains the right to suspend or terminate a student's access to his or her account when it believes there has been a violation of school unit policy, procedure, rules, or of law.

Students must, at all times, take reasonable measures to protect files and information in G-Suite, including, but not limited to, not sharing passwords or other login information, logging out of accounts when not in use, never attempting to access or accessing another user's account without permission, and being careful and purposeful when deciding whether to share access to information with other students.

Cross Reference: IJNDB – Student Use of School-Issued Computers/Devices and Internet and Cyber Safety
EGAD – Copyright Compliance
EGAD-R – Copyright Compliance Guidelines
JICK – Bullying and Cyberbullying

Adopted: April 27, 1999

Revised: October 26, 2010, May 9, 2017