

# Acceptable Use Policy for all Digital Components and Internet Service 2019 - 2020

---

As used in this document, the term “Computer[s]” refers to any desktop, laptop, or other mobile computing device owned or issued by the Ogdensburg Borough School District to any student for school and/or home use. The term “Computer Services” refers to the School District’s network or Internet connections used to access school or Internet-based information.

All students are responsible for their actions and activities involving Computers and/or Computer Services, and for their computer files, passwords, and accounts. This document provides general guidance concerning the use of the Computers and/or Computer Services and examples of prohibited uses. The rules do not attempt to describe every possible prohibited activity. Students, parents, and school staff who have questions about whether a particular activity is prohibited are encouraged to contact the Technology Coordinator. These rules apply to all Computers and/or school Computer Services regardless of how they are accessed.

Utilization of computers, the computer system, school network, and internet is a privilege. Students are expected to use these resources responsibly and only for educational purposes that align with school curriculum.

## *Terms of Agreement*

---

**In order for a student to be allowed access to computers, the school computer system, computer network, and the Internet, parents must sign-off for this consent form by the first Friday of the School year.**

## *Acceptable Use*

---

1. **Educational Mission, Curriculum, Instruction.** Ogdensburg Borough School District’s Computers and/or Computer Services are provided solely for educational purposes and research consistent with the Ogdensburg Borough Public School’s educational mission, curriculum, and instructional goals.
2. **Board Policies.** Students must comply with all Board policies, school rules, and expectations concerning student conduct and communications when using Computers and/or Computer Services, whether on or off school property. The school’s code of conduct applies to all of a student’s online activity.  
Any gesture, written, verbal, or electronic communication on or off school grounds can be considered harassment, intimidation, or bullying and will be handled accordingly (BOE Policy 5512).
3. **Teacher Instruction.** Students must also comply with all specific instructions from all school staff when using the Computers and/or Computer Services.
4. **Assigned Computers.** Students are to use the Computer that is assigned to them. Students are expected to sign out of all online accounts, log off the computer, and plug in devices at the end of each day.
5. **Mobile Devices.** Mobile Devices include smartphones, tablets, smart watches, e-readers or any similar mobile electronic device that can access an internet connection. The use of

personal mobile devices on the School District's property is a privilege, not a right. The use of mobile devices are prohibited unless express permission is granted. Mobile devices may not be used to make calls, send text messages, surf the Internet, take photos or use any other application during the school day.

6. **Network Usage.** Network and Internet access is provided as a tool for education. The District reserves the right to monitor, inspect, copy, review, and store, at any time and without prior notice, any and all usage of the computer network and Internet access and any and all information transmitted or received in connection with such usage. All such information files shall be and remain the property of the District and no user shall have any expectation of privacy regarding such materials.
7. **Network Rules.** All users must abide by rules of Network etiquette including the following:
  - a. Use appropriate language and graphics. No swearing, vulgarities, suggestive, obscene, belligerent, or threatening language or images.
  - b. Avoid language and/or graphic representations which may be offensive to others.
  - c. Do not use network or Internet access to make, distribute, or redistribute jokes, stories, or other material which are based on slurs or stereotypes relating to race, gender, ethnicity, nationality, religion, or sexual orientation.
  - d. Do not assume that a sender of email is giving permission for you to forward or redistribute the message to third parties or to give his/her email address to third parties.
8. **Educational Purposes.** Teachers may allow individual students to use email, electronic chat rooms, instant messaging, social networking sites, and other forms of direct electronic communications for **educational purposes only** and with proper supervision.
  - a. Proper supervision shall include the teachers having the students' usernames and passwords on file and actively monitoring the all accounts. Proper supervision includes verifying that students do not use student personal email (non-school issued) accounts and personal social networking sites in the school environment. Teachers must monitor all communications. The teacher must monitor all communications. No personal addresses, personal phone numbers, or last names of students will be permitted to be given out on the Internet.
  - b. No identifiable photographs will be allowed to be published on the Internet without appropriate written consent. Concerning a student, appropriate written consent means a signature by a parent or legal guardian of the student.
  - c. A student may not attempt to access any Internet resources without the prior consent of the teacher. The Internet is an extension of the classroom and teachers are responsible for and must be aware of where his/her students go on the Internet.
9. **Student Photos/ Student Work.** Publishing student pictures and work on websites promotes learning and collaboration and provides an opportunity to share the achievements of students. Images and products of Pre-K - 8 students may be included on the website without identifying captions or names. Parents/Guardians must indicate their written consent to publish their child's photo on any school related website before the item is published to the web. Please note that under no circumstances will Pre-K - 8 student photos or work be identified with first and last name on an Ogdensburg website, including the district, school, or teacher website.
10. **Copyright.** All students and faculty must adhere to the copyright laws of the United States (P.L.94-553: <https://www.copyright.gov/history/pl94-553.pdf> ) and the Congressional Guidelines that delineate it regarding software, authorship, and copying information.

## ***Failure to Follow Acceptable Use Policy***

---

Use of the Computers, Computer Network and Internet is a privilege, not a right. A user who violates this agreement shall, at a minimum, have his or her access to the Network and Internet terminated and is subject to disciplinary action by the school administrator. The District may also take other disciplinary actions.

**Unacceptable Uses of the Network** may include:

1. Uses that cause harm to others or damage to their property. For example:
  - a. Do not engage in defamation (harming another's reputation by lies).
  - b. Do not employ another's password or some other user identifier that misleads message recipients into believing that someone other than you is communicating, using his/her access to the network or the Internet.
  - c. Do not upload any harmful form of programming or vandalism (virus, trojan, malware, spyware, bots, time bomb, etc.).
  - d. Do not participate in hacking activities or any form of unauthorized access to other computers, networks, or information systems.
2. Uses that jeopardize the security of student access and of the computer network or other networks on the Internet.
  - a. Do not disclose or share your password with others.
  - b. Do not impersonate another user.
3. Uses that are commercial transactions. Students may not use the school network to sell or buy anything over the Internet.
4. Uses whereby you give private information about yourself or others.
5. Uses that are for commercial, political, illegal, financial, or religious purposes are forbidden. These violations shall be reported to a teacher or administrator immediately.
6. Use of threatening, profane, harassing, or abusive language is forbidden.
7. Use of the network for illegal activities is prohibited. Uses that are illegal activities, including copyright or contract violations. Other illegal activities include:
  - a. Tampering with computer hardware or software,
  - b. Unauthorized entry into computers and files (hacking),
  - c. Knowledgeable vandalism or destruction of property,
  - d. Deletion of computer files; Such activity is considered a crime under state and federal law.
  - e. Any use which violates state or federal law relating to copyright, trade secrets, the distribution of obscene or pornographic materials, or which violates any other applicable law or municipal ordinance, is strictly prohibited.
8. No user is permitted to knowingly or inadvertently load or create a computer virus or load any software that destroys files and programs, confuses users, or disrupts the performance of the system. No third party software will be installed without the consent of the assigned administrator.
9. Invading the privacy of another user, using another's account, posting personal messages without the author's consent, and sending or posting anonymous messages shall be forbidden.

10. Accessing pornographic or obscene materials, or using or sending profanity in messages shall be forbidden.
11. Any subscription to bulletin boards, listservs, or online services shall be approved by the superintendent or the designee prior to any such usage.
12. The use of anonymous proxies to get around content filtering is strictly prohibited and is a direct violation of this agreement.

### ***Internet Safety***

---

1. **Parents and Users.** Despite every effort for supervision and filtering, all users and their parents/ guardians are advised that access to the electronic network may include the potential for access to materials inappropriate for school-aged students. Every user must take responsibility for his or her use of the network and Internet and avoid these sites.
2. **Personal Safety.** In using the network and Internet, users should not reveal personal information such as home address or telephone number. Users should never arrange a face-to-face meeting with someone "met" on the Internet without a parent's permission.
3. **Confidentiality of Student Information.** Personally identifiable information concerning students may not be disclosed or used in any way on the Internet without the permission of a parent or guardian. Users should never give out private or confidential information about themselves or others on the Internet.
4. **Active Restriction Measures.** The District will utilize filtering software or other technologies to prevent students from accessing visual depictions that are (1) obscene, (2) pornographic, or (3) harmful to minors. The use of anonymous proxies to get around the content filter is strictly prohibited and will be considered a violation of this policy. The school will also monitor the online activities of students, through direct observation and/or technological means.

### ***Use of Web Tools***

---

Online communication is critical to our students' learning skills needed in their future. Skills and tools such as blogging and podcasting offer an authentic, real-world vehicle for student expression. As educators, our primary responsibility to students is their safety. Hence, expectations for classroom blogging, student protected e-mail, podcasting, or other web interactive use must follow all established Internet safety guidelines.

#### **Blogging/ Podcasting Terms and Conditions**

1. The use of blogs, podcasts or other web tools are considered an extension of your classroom. Therefore, any speech that is considered inappropriate in the classroom is also inappropriate in all uses of blogs, podcasts, or other web tools. This includes but is not limited to profanity, racist, sexist, or discriminatory remarks.
2. Students using blogs, podcasts or other web tools are expected to act safely by keeping ALL personal information out of their posts. Students using such tools agree to not share their username or password with anyone besides their teachers and parents and treat blogspaces as classroom spaces. A student should NEVER post personal information on the web (including but not limited to last names, personal details including address or phone numbers, or

photographs). Do not, under any circumstances, agree to meet someone you have met over the Internet. Speech that is inappropriate for class is also inappropriate for a blogspace.

3. Any personal blog a student creates in class is directly linked to the class blog which is typically linked to the student profile, and therefore must follow these blogging guidelines. In addition to following the parameters of this document, students need to realize that anywhere they use that login it links back to the class blog. Therefore, anywhere that login is used (posting to a separate personal blog, commenting on someone else's blog, etc) the account should be treated the same as a school blog and follow these guidelines. Comments made on blogs should be monitored and, if they are inappropriate, deleted.
4. Never link to web sites from your blog or blog comment without reading the entire article to make sure it is appropriate for a school setting.
5. Students who do not abide by these terms and conditions may lose their opportunity to take part in the project and he/she may be subject to consequences appropriate to misuse.

### **Consequences**

The particular consequences for violations of Acceptable Use Policies shall be determined by the school Administration. The Superintendent or designee and the Board shall determine when school expulsion and/or legal action(s) are the appropriate course of action.

Individuals violating the Policies shall be subject to appropriate discipline, which includes but is not limited to:

1. Use of computer.network only under direct supervision
2. Suspension of network privileges
3. Revocation of network privileges
4. Suspension of computer privileges
5. Revocation of computer privileges
6. Suspension from school
7. Expulsion from school, and/or
8. Legal action and prosecution by the authorities.

### **Social Networking Sites**

1. Examples include sites similar in nature to *Facebook, Pinterest, Instagram*.
2. Students may only use social networking sites if directed by a teacher.
3. Video conferencing or chatting online with classmates during class occurs only if directed by the teacher.

### ***Teacher Responsibilities***

---

The teacher will:

1. Provide developmentally appropriate guidance and monitoring to students as they make use of telecommunications and electronic information resources to conduct research and other studies related to the district's curricula.
2. Inform all students of their rights and responsibilities as users of the district network prior to gaining access to that network, either as an individual user or as a member of a class or group.
3. Use all networked resources in support of educational goals.
4. Treat student infractions of the Acceptable Use Policy according to the school discipline policy.

5. Provide alternate activities for students who do not have permission to use the Internet.

### ***Principal Responsibilities***

---

The Principal will:

1. Include the Acceptable Use Policy in family handbook.
2. Be sure handbooks are available to all students.
3. Treat student infractions of the Acceptable Use Policy according to the school discipline policy.
4. Keep permission forms on file for one year.
5. Identify students without permission slips for internet use to the teaching staff.

### ***District Responsibilities***

---

The District will:

1. Ensure that filtering software is in use to block access to materials that are inappropriate, offensive, obscene, or contain pornography.
2. Have the Acceptable Use Policy reviewed every year and approved by the Board.