



BAYONNE BOARD OF EDUCATION  
Administration Building  
669 Avenue A  
Bayonne, NJ 07002

John J. Niesz  
*Superintendent of Schools*

Tel. (201) 858-5817  
Fax (201) 858-6289

---

---

## **Bayonne Board of Education: Acceptable Use Policy (AUP) for Students and Staff**

### **General Principles**

The Bayonne School District ("District") provides computer equipment, computer services, and Internet access to its students and staff exclusively for educational purposes. Our goal in providing these technology resources is to **improve** learning and teaching through research, professional development, collaboration, and the dissemination and use of global communication resources.

The District maintains the right to monitor all activity on its network and computer facilities 24/7. This includes cloud-based internet content filtering and monitoring for all staff and students when using their Bayonne Board of Education user accounts and/or devices.

Given the complex connections between various government agencies and computer networks, all users must adhere to strict regulations. These regulations are provided to ensure that staff, community, students, and their parents or legal guardians are fully aware of their responsibilities. The District may modify these regulations at any time by publishing the updated version on the network and through other official channels.

Users are expected to demonstrate good behavior on computer networks and with online resources, just as they would in a classroom or on school grounds. It's important to remember that communications on computer networks and online resources are often public in nature, and all District policies and regulations governing behavior and communications apply.

Access to the District's computer networks and resources is a privilege, not a right. Each user is individually responsible for their behavior and communications. All users are required to comply with District standards and abide by the agreements they have signed. The District is not responsible for the actions of individuals who violate its policies and regulations while using the computer network or computers.

Electronic file storage areas are treated the same as other school storage facilities. District administrators may review files and communications to maintain system integrity and ensure responsible system use.

---

### **Prohibited Activity**

Users of District computers, computer networks, and Internet access are strictly prohibited from engaging in, but not limited to, the following behaviors:

- Sending or displaying offensive messages or pictures.
- Engaging in any conduct that violates any existing District policies.
- Attempting to or successfully logging into network administrative accounts, services, emails, or log files.
- Using obscene language and/or accessing visual depictions that are obscene as defined in section 1460 of Title 18, United States Code.
- Using or accessing inappropriate content, as defined in section 2256 of Title 18, United States Code.
- Using or accessing visual depictions that are harmful to minors, including any pictures, images, graphic image files, or other visual depictions that, taken as a whole and with respect to minors, are harmful.
- Harassing, demeaning, insulting, defaming, discriminating against, or attacking others.
- Sending, displaying, or receiving lewd, indecent, profane, vulgar, rude, threatening, racist, offensive, or inflammatory speech or material.
- Knowingly and recklessly posting false information.

- Engaging in activities that could materially or substantially interfere with or disrupt the operation of the District, its educational mission, or other students' rights.
- Attempting to or accessing District network administrator credentials.
- Sharing or distributing Wi-Fi access credentials.
- Attempting to or accessing staff or student usernames and/or passwords other than your own.
- Damaging computers, computer systems, or computer networks.
- Intentionally compromising the integrity of District data.
- Intentionally disrupting network traffic or crashing the network.
- Violating intellectual property laws, including, but not limited to, copyright and/or trademark infringement.
- Using District resources to commit fraud.
- Using another's password, account, or identity, or forging email messages.
- Trespassing in another's folders, work, or files.
- Intentionally wasting limited resources.
- Employing the computer network/computers for unauthorized commercial purposes.
- Obtaining and/or disclosing, without proper authorization, confidential pupil information, including but not limited to names, addresses, telephone numbers, attendance records, email addresses, building locations, and other personally identifiable information.
- Obtaining and disclosing, without proper authorization, personal information relating to staff and family members of staff and/or pupils.
- Engaging in personal business or personal communications during school hours.
- Gaining or seeking unauthorized access to the network, files of others, and any electronic District data.
- Engaging in other activities that do not advance the educational purposes for which the computer network/computers are provided.

### **Internet Usage**

District staff shall supervise student use of the Internet. Students are required to immediately notify a staff member if anyone attempts to initiate any inappropriate personal contact with them while using the District's Internet access.

### **Electronic Communication Between Staff and Students**

#### **1. Email**

In accordance with District Policies 3283 and 4283, staff are required to maintain their District email accounts as the primary means of communication with administration, staff, parents, and other educational contacts. At no time should staff and students communicate via personal email accounts. All communication must be conducted through the District email system. If a staff member receives an email from a student's personal email account, the staff member must respond with their District email and inform the student that all future communication should occur through their District email.

#### **2. Cellular Telephone**

In accordance with District Policies 3283 and 4283, personal cellular telephone communication is prohibited between staff and students, unless the teaching staff member has prior approval from their building administration to use their personal cellular telephones for communication directly related to professional responsibilities. Any approved communication shall not extend beyond the approved activity.

#### **3. Text Messaging**

In accordance with District Policies 3283 and 4283, text messaging and/or website messaging communication is prohibited between staff and students, unless the teaching staff member has prior approval from their building administration to use text messaging and/or website messaging for communication directly related to professional responsibilities. Any approved communication shall not extend beyond the approved activity.

---

## **Social Media**

### **1. Professional Social Media**

In accordance with District Policies 3283 and 4283, teaching staff may engage in professional social media activities (e.g., platforms dedicated to homework, study guides, reminders, activities, teams, and clubs) after securing proper approvals. Staff members who engage in professional social media activities should maintain separate professional and personal email addresses. They should not use their personal email addresses for professional social media activities; instead, their professional social media presence should utilize their District email address. The teacher must also have signed parental consent when using any of the above types of application with students. (See Electric Communication Form)

Staff should treat professional social media spaces and communication like a classroom and/or professional workplace. The same standards expected in the District's professional settings are expected on professional social media sites. If a particular type of behavior is inappropriate in the classroom, that behavior is also inappropriate on the social media site.

Staff should exercise caution, sound judgment, and common sense when using professional social media sites. They should use privacy settings to control access to their professional social media sites to ensure communications reach only the intended audience. However, staff should be aware of limitations to privacy settings and that communications can easily become public. Staff have an individualized responsibility to understand the rules of the social media site being used.

Professional social media communication must adhere to District policies, rules, and regulations, as well as applicable laws, including but not limited to prohibitions on the disclosure of confidential information and prohibitions on the use of harassing, obscene, discriminatory, defamatory, or threatening language. No personally identifiable student information, including student photographs, may be posted by staff on social media websites without the express consent of the students' parents. (BBOED Media-Release Form). Students who participate in professional social media sites may not be permitted to post photographs featuring other students.

### **2. Personal Social Media**

In accordance with District Policies 3283 and 4283, staff will not communicate ("friend," "follow," "comment," etc.) with students who are currently enrolled in District schools via personal social media sites or websites. Communication between staff and students through personal social networking websites is only permitted under two specific circumstances:

- (a) Familial Relationship: When both the staff member and the parent of the child provide written notification to their building administration confirming that the staff member and child are relatives and that communication through social media websites is allowed.
- (b) Emergency Situation: If an emergency situation requires such communication, in which case the staff member must notify his/her building administration of the contact as soon as possible.

Staff utilizing personal social media websites must represent themselves professionally. They are encouraged to use appropriate privacy settings to control access to their personal social media sites. However, staff should be aware of limitations to privacy settings and that communications can easily become public. Staff have an individualized responsibility to understand the rules of the social media site being used.

## **Personal Devices**

Staff are permitted to use their personal devices for instructional purposes only during the school day. Staff are expected to silence all handheld devices and put them away during instructional time unless they are being used for educational purposes. The Bayonne Board of Education is not responsible for the damage, vandalism, loss, or theft of any personal devices brought onto school grounds.

Students must keep all cellphones and other handheld devices silenced and put away during school hours, unless instructed by staff to use them for educational purposes. The Bayonne Board of Education is not responsible for the damage, vandalism, loss, or theft of any personal devices brought onto school grounds.

No student or staff member can expect privacy in any content stored or accessed through the District network. District email and all computer hardware and subscriptions are the property of the District. All users are hereby notified that any

and all content stored on the District network or computers is subject to review and inspection, including emails and personal and/or professional files. All users are advised that all Internet activity, including email and websites visited, is monitored and archived.

The District makes no warranties of any kind, neither expressed nor implied, for the computer resources and Internet access that it provides. The District will not be responsible for any damages users may suffer, including but not limited to loss of data resulting from delays or interruptions in service. The District will not be responsible for the accuracy, nature, or quality of information gathered from District-provided Internet access. The District will not be responsible for personal property used to access District computers or networks, or for District-provided Internet access. The District will not be responsible for unauthorized financial obligations resulting from District-provided Internet access. The District reserves the right to limit the use of personal electronic devices that disrupt the educational environment for students and/or staff.

### **Artificial Intelligence (AI) Use and Academic Integrity**

The Bayonne School District acknowledges that Artificial Intelligence (AI) tools are becoming increasingly prevalent and can be valuable resources for learning and creativity. However, the use of AI must align with the District's commitment to academic integrity and ethical conduct and adhere to District Policies 2365 & 5701.

In accordance with District Policies 2365 & 5701, any use of AI tools that compromises academic integrity is strictly prohibited and will be considered academic dishonesty. Student

- **Submitting AI-Generated Content as Original Work:** Presenting work generated entirely or substantially by an AI tool (e.g., an essay, report, code, or artwork) as your own original thought, research, or creation without proper attribution and explicit permission from the instructor. For instance, turning in an essay written by ChatGPT without any personal input or citation is a direct violation.
- **Using AI to Cheat on Assessments:** Employing AI tools during exams, quizzes, or other assessments where the use of such tools is not explicitly permitted. This includes using AI to answer questions, solve problems, or generate responses that are meant to demonstrate individual knowledge or skills.
- **Plagiarism through AI:** Copying and pasting content from an AI tool without proper citation or integration into your original work. Just like content from any other source, AI-generated text or ideas must be attributed if used in academic submissions.
- **Circumventing Learning Objectives:** Using AI tools to bypass the intended learning process or to avoid developing required skills. For example, if an assignment is designed to teach critical thinking and research skills, using AI to provide pre-digested answers would undermine the educational objective.
- **Misrepresenting AI's Role:** Falsely claiming that AI had no role in the creation of a submission when it did, or exaggerating the extent of AI's involvement to misleadingly enhance the perceived quality of one's work.

### **Consequences of Misuse**

Violating any part of this Acceptable Use Policy (AUP) will lead to disciplinary action, aligning with the District's existing policies on student and staff conduct, including those addressing academic dishonesty. Such consequences for misuse or violation may include, but are not limited to, the loss of online privileges, the loss of access to District-issued devices, failing grades on assignments, suspension, or other disciplinary measures as outlined in the student handbook or student/staff agreements and policies.

*Please sign and return this portion*

---



**Bayonne Board of Education:**



**Staff & Student Acceptable Use Policy**

All students and staff within the Bayonne School District will adhere to the rules, regulations, and procedures of the Acceptable Use Policy as they pertain to the various technologies outlined below, as well as the District Board Policies #2360, 2361, 2365 3282, 3283, 4282, 4283, 5701, 7523, 7523 and the District Internet Safety Plan. All forms can be found at: <https://www.bboed.org/Page/486>

***By signing below, I acknowledge that I understand and accept the Acceptable Use Policy.***

Full Name of Student or Staff Member:

\_\_\_\_\_

Signature of Student or Staff Member: \_\_\_\_\_

Date: \_\_\_\_\_

**STUDENT ONLY**

Parent Signature: \_\_\_\_\_

Date: \_\_\_\_\_

School/House: \_\_\_\_\_

Homeroom Teacher: \_\_\_\_\_ HR #: \_\_\_\_\_