



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

The Bayonne School District (“District”) provides computer equipment, computer services, and Internet access to its students and staff for educational purposes only. The purpose of providing the technology resources is to improve learning and teaching through research, teacher training, collaboration, and the dissemination and the use of global communication resources. The District reserves the right to monitor all activity on network/computer facilities/computers. 24/7 cloud based internet content filtering and monitoring is in place for staff and students while using their Bayonne Board of Education user account.

Because of the complex association between so many government agencies and computer networks/computers, the end user of these computer networks/computers must adhere to strict regulations. Regulations are provided here so that staff, community, and student users, as well as the parent(s) or legal guardian(s) of students, are aware of their responsibilities. The District may modify these regulations at any time by publishing modified regulations on the network and elsewhere.

Students and staff are responsible for good behavior on computer networks/computers just as they are in a classroom or on other school grounds. Communications on the computer network/computers/online resources are often public in nature. Policies and regulations governing behavior and communications apply. The District’s networks, Internet access and computers are provided to students and staff for educational purposes only. Access to the District’s computer networks/computers is a privilege, not a right. Individual users of the District’s computer network/computers are responsible for their behavior and communications over the computer network/computers/online resources. Users will be required to comply with District standards and will abide by the agreements they have signed.

The District is not responsible for the actions of individuals utilizing the computer network/computers who violate the District’s policies and regulations.

Electronic file storage areas shall be treated in the same manner as other school storage facilities. District administrators may review files and communications to maintain system integrity and to ensure that users are using the system responsibly.

Prohibited Activity

Users of District computers/computer networks/internet access are prohibited from engaging in behavior including, but not limited to, the following:

1. Sending or displaying offensive messages or pictures;
2. Engaging in any conduct which violates existing District policy;
3. Attempt to or successfully log into network administrative accounts, services, emails, log files, etc;
4. Using obscene language and/or accessing visual depictions that are obscene as defined in section 1460 of Title 18, United States Code;
5. Using or accessing inappropriate content, as defined in section 2256 of Title 18, United States Code;
6. 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;
7. Harassing, demeaning, insulting, defaming, discriminating against or attacking others;
8. Sending, displaying or receiving lewd, indecent, profane, vulgar, rude, threatening, racist, offensive or inflammatory speech or material;
9. Knowingly and recklessly posting false information;
10. Engaging in activities that could materially or substantially interfere or disrupt the operation of the District, the District’s educational mission or other students’ rights;
11. Attempting to or accessing District network admin credentials;
12. Sharing or distributing WIFI access credentials;
13. Attempting to or accessing staff or student username and/or passwords other than your own;

14. Damaging computers, computer systems or computer networks;
15. Intentionally compromising the integrity of District data;
16. Intentionally disrupting network traffic or crashing the network;
17. Violating intellectual property laws, including, but not limited to, copyright and or trademark infringement;
18. Using District resources to commit fraud;
19. Using another's password, account or identity, or forging email messages;
20. Trespassing in another's folders, work or files;
21. Intentionally wasting limited resources;
22. Employing the computer network/computers for unauthorized commercial purposes;
23. 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;
24. Obtaining and disclosing, without proper authorization, personal information relating to staff and family members of staff and or pupils.
25. Engaging in personal business or personal communications during school hours;
26. Accessing or using personal email accounts during school hours, unless said conduct is being done in connection with, or in the furtherance of, an educational purpose;
27. Gaining or seeking unauthorized access to the network, files of others and any electronic District data; and
28. Engaging in other activities that do not advance the educational purposes for which the computer network/computers are provided.

Internet

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

Electronic Communication Between Staff and Students

1. **Email:** In accordance to District Policy 3283 and 4283 staff is required to maintain their District email accounts as a 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 should be done through the District email. If a teacher receives an email from a student's personal email account, the staff member is to respond with their District email and inform the student that all communication moving forward should be done through district email.
2. **Cellular Telephone:** In accordance to District Policy 3283 and 4283 personal cellular telephone communication is prohibited between staff and students, unless the teaching staff member has approval from their building administration to use their personal cellular telephones to communicate directly related to professional responsibilities. Any approved communication shall not extend beyond the approved activity.
3. **Text Messaging:** In accordance to District policy 3283 and 4283 text messaging and or website messaging communication is prohibited between staff and students, unless the teaching staff member has approval from their building administration to use text messaging and or website messaging to communicate directly related to professional responsibilities. Any approved communication shall not extend beyond the approved activity.

Professional Social Media

In accordance to District policy 3283 and 4283 teaching staff may engage in professional social media activities – such as those dedicated to homework, study guides, activities, teams and clubs – after securing proper approvals. Staff members who decide to engage in professional social media activities should maintain separate professional and personal email addresses. As such, staff should not use their personal email addresses for professional social media activities. The professional social media presence should utilize their District email address.

Staff should treat professional social media space and communication like a classroom and/ or professional workplace. The same standards expected in the District's professional settings are expected on professional 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. Staff should use privacy settings to control access to their professional social media sites to ensure that the communications reach only

the intended audience. However, staff should be aware of limitations to privacy settings and that communications can easily become public. Staff has an individualized responsibility to understand the rules of the social media site being used.

Professional social media communication should be in accordance with District policies, rules and regulations, as well as with 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 may be posted by staff on social media websites, including student photographs, without the consent of the students' parents. Students who participate in professional social media sites may not be permitted to post photographs featuring other students.

Personal Social Media

In accordance with District policy 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 (a) when both the staff member and the parent of the child put in writing to their building administration that the staff member and child are relatives and communication through social media websites is allowed; and (b) if an emergency situation requires such communication, in which case the staff member should 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 has an individualized responsibility to understand the rules of the social media site being used.

Personal Devices

Staff is allowed to use their personal devices for instruction purposes only during the school day. Staff is expected to silence all hand held devices and put away during instructional time unless using for educational purposes. The Bayonne Board of Education is not responsible for the damage, vandalism, loss, or theft of any personal devices brought on school grounds.

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

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, 3282, 3283, 4282, 4283, 7522, 7523 and the District Internet Safety Plan. All forms can be found at: <https://www.bboed.org/domain/35>

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 #: _____