Bronx Charter Schools for Better Learning

Acceptable Technology Use Policy

Statement of Purpose

Bronx Charter Schools for Better Learning (the "School" or the "Schools") is pleased to offer our students, staff and guests access to the World Wide Web and other electronic networks. The advantages afforded by the rich, digital resources available today through the World Wide Web outweigh any disadvantage. However, it is important to remember that access is a privilege, not a right, and carries with it responsibilities for all involved.

Terms of Agreement

In order for a student to be allowed access to a School computer system, computer network, and the Internet, parents must sign and return the attached consent form each year by September 12.

In order for a staff member to be allowed access to a district computer system, computer network, and the Internet, the staff member must sign and return the attached consent form each year by September 12.

Electronics & Acceptable Technology Use Policy

Bronx Charter Schools for Better Learning (the "School" or the "Schools") must monitor the use of the Schools' information systems to ensure compliance with institutional policies, protect the security and maintain the efficiency of its systems, and discourage inappropriate use. All students, employees, and other authorized users ("Users") must use the Schools' information technology resources ("IT Resources") in ethical and acceptable ways to ensure that all members of the School community have access to reliable, robust IT Resources that are safe from unauthorized or malicious use. At any time, and for any lawful purpose, the Schools may monitor, intercept and search any communication or data transmitted or stored on the IT Resources, including any personal information.

By using the School's IT Resources, including utilizing a School issued iPad, you hereby accept and agree to comply with the terms and conditions set forth in this Electronic Information Systems Acceptable Use Policy and provide consent for any personal information input by you (your child) to be transferred to off-site servers located outside the location from which you are accessing the system, even if your access is through a personal computer, smartphone, or other portable devices.

IT Resources: The School's IT Resources include, but are not limited to, School owned iPads and computers (whether used on School property or at home), networks, servers, telephones, and other infrastructure, whether utilized on- or off-campus; laptops, tablets, disks, other physical devices or media owned or provided by the Schools, and all devices and storage media attached to the network; digital systems, websites, and other digital services utilized by the Schools, whether hosted on- or off-campus; files, folders, documents, web pages, and other digital information; e-mail, voicemail, SMS, IM, or other digital or analog communications; account names, passwords, or related information or settings; and systems, settings, and configurations.

Acceptable Use: The School's IT Resources are intended for school use, to support activities that support learning and teaching. The Schools strictly prohibit the use of the Schools' IT Resources for purposes that may be disruptive, offensive to others, or harmful to morale. Users may not send, display, access, or download messages, text, files, or images in violation of any laws. At all times, our school community expectations must be applied. The following are unacceptable uses of the School's IT Resources. This list is not exhaustive.

Harassment or Discrimination: In accordance with the Dignity for All Students Act ("DASA") and the Schools' disciplinary code, the Schools will provide an environment that is free of discrimination, bullying (including cyberbullying), and harassment. Unless required for academic or other School-related purposes, Users may not view, display, or transmit in digital or physical form any of the following: sexually explicit information or images, ethnic slurs, racial epithets or anything that may be construed as discrimination, harassment or disparagement of others based on their race, color, religion, sex, national origin, sexual orientation, age, disability, marital status, or any other category protected by federal, state and local law. The Schools' policies against harassment, discrimination, and bullying all apply fully to use of the Schools' IT Resources.

All reports of violations to this policy will be investigated, documented, and may result in loss of technology and/or Internet privileges as well as further disciplinary consequences, in accordance with the Schools' Discipline Policy. The administration of the Schools reserve the right to monitor any and all activity generated by student use of technology equipment.

Unauthorized Use of Intellectual Property: Users may not violate the rights of any person or company protected by copyright, trade secret, patent, or other intellectual property, or other proprietary rights. Users may not conduct academic dishonesty or plagiarism, illegal or fraudulent activity, or any other activity prohibited by the Schools' policies.

Misuse of the Schools' Network, Software, and Computers: Users may not intentionally introduce malicious programs into Schools' computers, tablets, networks, servers, or hosted services; inappropriately use or share School-authorized IT privileges or resources with anyone outside the Schools; bypass the Schools' firewall; host or access file-sharing services for any illegal or inappropriate purposes; play, stream, or download games, video, multimedia, or other large files for non-academic purposes; modify another User's password, files, or permissions; copy or download software from School IT Resources without permission; install software on lab and/or office computers without permission; or use the Schools' IT Resources for any private purpose for personal gain, commercial enterprise, or non-Schools'-related fundraising.

Misuse of Websites: The Schools' websites may only be used for School-related academic purposes. Use of the Schools' websites, including http://www.bronxbetterlearning.org are subject to this policy as well as any User Agreement posted on the website.

Misuse of Email: Users may not send unsolicited email messages, spam, chain letters, or advertising materials; impersonate others' e-mail address, internet address, electronic signature, or other personal identifying information; or use e-mail in any way that would cause disruption, harassment, or harm. E-mail is not a secure method of information transmission, so Users must take reasonable precautions to protect privacy and security. Home addresses, telephone numbers, passwords, and other personal information should not be included in email signatures. Students' personal or identifying information must never be shared outside the Schools' domain without permission.

Social Media: When used inappropriately, social media can transform from a powerful educational tool that allows students to connect, communicate, and access a wealth of informational resources into the source of serious long-term consequences. College admissions officers and prospective employers will not hesitate to use any social media missteps — even those made when a student is quite young — when considering an individual's candidacy for admission or employment. Social Media as defined in this policy includes any and all web-based technologies used to broadcast messages and participate in dialogues. Examples include Facebook, Twitter, LinkedIn, Snapchat, Instagram, YouTube, emails, texting, blogs, message boards, personal websites, chat rooms, group discussions, etc.

According to this Policy, the Schools expect that their resources are used only for teaching and learning. The Schools have the right (and exercise the right) to monitor users' electronic usage, without further notification than set forth in this policy. This policy extends the right to monitor your use of social media sites if you use any electronic equipment, servers or services provided to you by the Schools. In our ever-expanding world of technology, students may run into staff members' personal pages on sites like Facebook and Instagram. In the same way that certain lines should not be crossed between students and school employees in real life, they also should not be crossed in the virtual world. Please note that no employees at our Schools may accept or initiate friend requests with current students and should exercise caution and careful judgment about former students or alumni.

Students are responsible for their own behavior when communicating with social media and will be held accountable for the content of the communications that they transmit or post. Students are responsible for complying with the Schools' conduct requirements. What would be considered inappropriate in the Schools or classrooms is inappropriate online. Examples of inappropriate conduct include, but are not limited to:

- Posting or publishing any insensitive or inappropriate information or content on any social media and from viewing any insensitive or inappropriate social media content.
- Communicating with teachers or administrators via personal social media. *The only permissible electronic method of email communication with a teacher is through emailing the teacher or administrator at his or her School email account.*
- Impersonating or assuming the identity of any other individual while using social media.
- Posting or publishing any information about themselves or another individual that is confidential or of a private nature. This includes posting information such as last names, school names, addresses, email addresses, phone numbers, other contact information, or any other information a student might reasonably expect another individual to want to keep private.
- Using any device capable of capturing video, pictures, or audio to record or take pictures of any other individual without their express consent and permission. In addition, use of such recording devices on School grounds is strictly prohibited. Moreover, no such recordings or pictures shall be posted on social media unless they are educationally related. Also, students are not allowed to "tag" an individual in a picture or recording without their express consent and permission.

Students must immediately comply with any request that infringing materials be removed from any social media platform. Students should always be mindful of the fact that material posted or published online will be public for a very long time and may perhaps become a permanent part of their record. Students should be sensitive of others, should avoid posting or publishing anything distasteful, and should not post or publish anything they would not be willing to say to an individual in person.

This social media policy applies any time students are on school grounds, using school property, under the supervision of school authority, or using social media in a manner that endangers a student's or staff member's physical or emotional safety, security or well-being and materially and substantially interferes with the requirements of appropriate discipline in the operation of the Schools.

Student Personal Technology: With continued introduction of internet capable devices, it is important for the Schools to articulate clear expectations about their use. Please note that:

Classroom/School Building

Students are prohibited using any unauthorized electronic devices while in school. This includes cell phones, gaming devices or any other communication/entertainment devices. Devices will be confiscated and held by the Principals. Parents/guardians may make arrangements to pick up the device. Devices that should not be brought to school include, but are not limited to:

- Cell phones
- Smart watches
- iPods and MP3 Players
- iPads or any other tablet or eReader
- Laptops
- Cameras
- Headphones or headsets
- Any device capable of taking pictures or recording video content

This prohibition does not apply if the student has received an accommodation from the Committee on Special Education (CSE) or the Pupil Assistance Team (PAT).

Exams

Personal technology devices, with the exception of approved calculators in appropriate moments of an exam, are never to be used during exams.

Access to Information and Privacy: Users of the Schools' IT Resources may access only the confidential or proprietary information for which they are authorized and may use that information only for the purposes for which it is intended. Users are responsible for knowing and following School policies regarding use of confidential information.

The Schools reserve the right to review and disclose all digital information, including word processing documents, spreadsheets, databases, email, voicemail, instant messages, and any other electronic documents or communication, including any documents and messages that do not pertain to School business, that are stored or processed on the Schools' IT Resources.

Authorized representatives of the Schools and their delegates may review such information for any purpose required by the Schools, at any time, without notice to the User. These purposes may include, but are not limited to, retrieving School information, maintenance of the Schools' IT Resources, troubleshooting hardware or software problems, preventing system misuse, School investigations, health and safety emergencies, compliance with legal and regulatory requests for information, or compliance with local, state, and federal laws.

The Schools, therefore, do not guarantee the privacy of any electronic information stored or processed on School IT Resources, even if password protected. The Schools reserve the right to retrieve, examine, and remove files or logs from School IT Resources without the User's consent. Users of the Schools' IT Resources waive any right to privacy with regard to any use of the Schools' equipment and systems.

User Security: Users are responsible for the security of computer system passwords, personal account passwords, and personal identification numbers and will be held accountable for any violations of acceptable use that are traced to their accounts or use of School IT Resources.

Users must employ security practices established by the School. Users must follow School policies established for maintaining and managing passwords. Users have had unique passwords created for their use on School-issued devices and must create secure passwords on non-School-issued devices that access School IT Resources. Passwords should be changed frequently and should never be written down or told to anyone.

Users should password-protect computers when leaving their desk or room and should ensure the physical security of IT Resources by storing computers and other devices in locked locations. Effective security practice includes a prompt and appropriate response to a security breach. Users must immediately report incidents in which they believe computer or network security has been jeopardized.

Use of Likeness and School Work: The Schools may, with a User's prior consent, make use of photographs of the User or other likenesses and of such User's work (written, artistic, etc.) on the Schools' website and in other promotional materials. Each User must ensure that he or she has obtained the necessary permissions before publishing any names or photographs of students or student work. Under no circumstances are Users allowed to publish student photographs accompanied by students' full names. In case of any uncertainty whether permissions would be required for publication of student information, Users should consult the Building Principal. Users must receive prior approval from the Building Principal before posting material or publishing links.

Liability: The Schools' IT Resources are provided "as is" and "as available." The Schools disclaim all representations and warranties, express or implied, of any kind with respect to the IT Resources and the content including warranties of, merchantability, fitness for a particular purpose and non-infringement of intellectual property and proprietary rights. Without limiting the general disclaimer, the Schools do not warrant the availability, accuracy, completeness, timeliness, functionality, reliability, sequencing, or speed of delivery of the Schools' IT Resources.

Enforcement: Any User who becomes aware of a misuse of the Schools' IT Resources should immediately report the matter to the Building Principal. Violations of this Policy will be investigated, documented, and may result in suspension or revocation of computer, network, or service access; discipline, up to and including suspension, expulsion, or termination of employment; and/or legal prosecution, in accordance with School Policy and the law. The administration of the Schools reserve the right to monitor any and all activity generated by student use of technology.

AUP Summary

This is a summary of the Electronics & Acceptable Technology Use Policy Guidelines. All students and parents are encouraged to read the full Administrative Guidelines before signing this Statement of Understanding. All students and parents as well as staff must sign the Statement of Understanding before using the Schools' technology.

1. All use of the Schools' technology must be in support of education and used in ethical and acceptable ways.

2. Anyone using BBL technology is responsible for the preservation and care of that technology.

3. Accounts are to be used only by the owner. The sharing of login and password information is prohibited, unless special permission is given by administrator/teacher.

4. Personal information must not be shared over the Internet.

5. Users are not permitted to bypass BBL filters for any reason, unless special permission is given by administrator/teacher.

6. All BBL Network usage may be monitored and archived.

7. Cyber bullying is not tolerated.

8. Any violations of the use of technology should be reported to an administrator/teacher. Violations of the AUP will be subject to disciplinary action as outlined in the AUP.

By using the School’s IT Resources, including utilizing a school issued iPad, you hereby accept and agree to comply with the terms and conditions set forth in this Electronic Information Systems Acceptable Use Policy.

I have read & understand this Acceptable Use Policy and agree to abide by it:

____ ____________________

(Student or Staff Signature)   (Date)

____ _____________________

(Student or Staff Printed Name)   (Graduation Year if applicable))

To be completed annually by Parents/Legal Guardians of all students:

I have read and discussed this Acceptable Use Policy with my child:

____ ____________________

(Parent Signature)