PERSONNEL

TECHNOLOGY USE IN INSTRUCTION/ ACCEPTABLE USE OF DISTRICT COMPUTER NETWORKS

The Board of Education is committed to optimizing student learning and teaching. The Board considers student access to current technology to be a powerful and valuable educational and research tool, and encourages the use of computers and computer-related technology in district classrooms for the purpose of advancing and promoting learning and teaching.

The computer network can provide a forum for learning various software applications and through online databases, bulletin boards and electronic mail, can significantly enhance educational experiences and provide statewide, national and global communication opportunities for staff and students.

All users of the district's computer network and the Internet must understand that use is a privilege, not a right, and that use entails responsibility. The district reserves the right to control access to the Internet for all users of its computers and network. The district may either allow or prohibit certain kinds of online activity, or access to specific websites.

The District computer network should be used only for educational purposes. Educational use of the computer networks include classroom activities, professional development and individualized student learning. Additionally, the system may be used by employees to increase communication and enhance productivity. Some computer systems which can be accessed via telecommunications contain materials that are defamatory, inaccurate, obscene, profane, threatening, bigoted, or illegal. The District does not condone the use of such materials and does not permit use of such materials in any District facilities, or on the district network.

The district will implement a centralized Internet filtering system that prevents or blocks access to certain material on the Internet. Filtering is used to prevent users from accessing inappropriate material that is deemed "child pornography, obscene or harmful to minors." The filtering system will be provided, maintained and monitored by an external agency

Regulations and handbooks, to be developed by the Superintendent, ***in consultation with the Assistant Superintendent for Curriculum and Instruction, the Assistant Superintendent for Human Resources, the Director of MIS, and the Coordinator of Instructional Technology*** will provide specific guidance as well as rules governing the use and security of the district's computer network. All users of the district's computer network and equipment, including but not limited to students and staff, shall comply with the policy and regulation. Failure to comply may result in suspension or revocation of computer access privileges and/or disciplinary action in accordance with the Code of Conduct and/or the Civil Service Law, Education Law and/or collective bargaining agreements, as applicable.

The Superintendent shall be responsible for designating a Director of MIS to oversee the use of district technology resources. The Coordinator of Instructional Technology will prepare

in-service programs for the training and development of district staff in technology skills, and for the incorporation of technology in appropriate subject areas.

With increased concern about identity theft, unwarranted invasion of privacy and the need to protect personally identifiable information, prior to students being directed by staff to use any cloud-based educational software/application, staff must get approval from the Director of MIS. The Director of MIS will determine if a formal contract is required or if the terms of service are sufficient to address privacy and security requirements, and if parental permission is needed.

The Superintendent, working in conjunction with the designated purchasing agent for the district, the Director of MIS and the Coordinator of Instructional Technology will be responsible for the purchase and distribution of computer software and hardware throughout district schools. They shall prepare and submit for the Board's approval a comprehensive multi-year technology plan, which shall be revised as necessary to reflect changing technology and/or district needs.

Parents and legal guardians of students are to be made aware of the District's policies governing use of its computer networks and the consequences for violations of these policies. The District will provide students and parents/guardians with a guide to the appropriate use of District computer networks which includes guidelines for student network safety. It is expected that parents/guardians will ensure that their children understand and adhere to the District guidelines.

Cross-ref: 5300, Code of Conduct
5695, Student Use of Personal Electronic Devices

Policy adopted: 1/11/16

CITY SCHOOL DISTRICT
City of White Plains, NY

PERSONNEL

TECHNOLOGY USE IN INSTRUCTION/ACCEPTABLE USE OF DISTRICT COMPUTER NETWORKS
RULES AND REGULATIONS

The following rules and regulations govern the use of the district's computer network system and access to the Internet.

I. Administration

- The Superintendent of Schools shall designate a Director of MIS to oversee the district's computer network.
- The Director of MIS shall monitor and examine all network activities, as appropriate, to ensure proper use of the system.
- The Director of MIS shall be responsible for disseminating and interpreting district policy and regulations governing use of the district's network at the building level with all network users.
- The Director of MIS shall provide employee training for proper use of the network and will ensure that staff supervising students using the district's network provide similar training to their students, including providing copies of district policy and regulations governing use of the district's network.
- The Director of MIS shall ensure that all disks and software loaded onto the computer network have been scanned for computer viruses.
- The Director of MIS will review staff requests to use 'cloud-based' educational software/applications to ensure that personally identifiable information (PII) is protected in accordance with district standards prior to student use.
- All student agreements to abide by district policy and regulations and parental consent forms shall be kept on file in the appropriate school building.

II. Internet Access

- Students will be provided Internet access during the school day.
- Students will be provided with individual access accounts after an agreement has been signed by the student and their parent and the student has attended an acceptable use orientation session. At that time, students may be granted internet and e-mail access through a classroom account. Parents or guardians may specifically request that their child not be provided access through the classroom account by notifying the district in writing.
- Students may have Internet access for educational purposes only.

- Student Internet access may be restricted depending on the grade level.
- All users will be prohibited from: accessing social networking sites and playing online games, except where it is connected with the instructional program.
- All users will be prohibited from watching videos online except where it is connected with the instructional program.
- Students are not to participate in chat rooms, except where it is connected with the instructional program.
- Students may not construct their own web pages using district computer resources, except where it is connected with the instructional program.
- A staff member will be required to monitor all of the above activities by student.
- All employees will have access to the Internet and electronic mail through the district network. Certain training requirements may be established by the administration as necessary
- Guests may receive an individual account with the approval of a district administrator if there is a specific, district-related purpose requiring such access. Use of the system by a guest must be specifically limited to the district-related purpose. An agreement will be required and parental signature will be required if the guest is a minor.

III. Acceptable Use and Conduct

- Access to the district's computer network is provided only for educational purposes and research consistent with the district's mission and goals.
- Use of the district's computer network is a privilege, not a right. Inappropriate use may result in the suspension or revocation of that privilege, as well as disciplinary sanctions, as appropriate.
- Each individual in whose name an access account is issued is responsible at all times for its proper use.
- All network users will be issued a login name and password. Passwords must be changed periodically.
- Only those network users with written permission from the principal or computer network coordinator may access the district's system from off-site (e.g., from home).
- All network users are expected to abide by the generally accepted rules of network etiquette. This includes being polite and using only appropriate language. Abusive or sexual language or images, vulgarities and swear words are all inappropriate.
- Network users identifying a security problem on the district's network must notify the appropriate teacher, administrator or computer network

coordinator. Under no circumstance should the user demonstrate the problem to anyone other than to the district official or employee being notified.

- Any network user identified as a security risk or having a history of violations of district computer use guidelines may be denied access to the district's network.

IV. Prohibited Activity and Uses

The following is a list of prohibited activity concerning use of the district's computer network. Violation of any of these prohibitions may result in suspension or revocation of a user's access to the network, as well as disciplinary sanctions, as appropriate

- Using the network for commercial activity, including advertising.
- Infringing on any copyrights or other intellectual property rights, including copying, installing, receiving, transmitting or making available any copyrighted software on the district computer network.
- Using the network to receive, transmit or make available to others obscene, offensive, or sexually explicit material.
- Using the network to receive, transmit or make available to others messages that are racist, sexist, abusive or harassing to others.
- Using the network to harass, bully, threaten, discriminate against, defame or abuse others
- Using another user's account or password.
- Attempting to read, delete, copy or modify the electronic mail (e-mail) of other system users and deliberately interfering with the ability of other system users to send and/or receive e-mail.
- Forging or attempting to forge e-mail messages.
- Engaging in vandalism. Vandalism is defined as any malicious attempt to harm or destroy district equipment or materials, data of another user of the district's network or of any of the entities or other networks that are connected to the Internet. This includes, but is not limited to, creating and/or placing a computer virus on the network.
- Using the network to send anonymous messages or files.
- Using the network to receive, transmit or make available to others a message that is inconsistent with the district's Code of Conduct.
- Revealing the personal address, telephone number or other personal information of oneself or another person.
- Using the network for sending and/or receiving personal messages, except where connected with the instructional program
- Intentionally disrupting network traffic or crashing the network and connected systems.

- Installing personal software or using personal disks on the district's computers and/or network without the permission of the appropriate district official or employee.
- Using district computing resources for commercial or financial gain or fraud.
- Stealing data, equipment or intellectual property
- Gaining or seeking to gain unauthorized access to any files, resources, or computer or phone systems, in or outside of the district's network, or vandalizing the data of another user.
- Wastefully using finite district resources.
- Changing or exceeding resource quotas as set by the district without the permission of the appropriate district official or employee.
- Using the network while access privileges are suspended or revoked.
- Using the network in a fashion inconsistent with directions from teachers and other staff and generally accepted network etiquette.
- Using the network to perform any act that constitutes a crime

V. No Reasonable Expectation of Privacy

No users of the district's computer network, including but not limited to students and/or employees shall have a reasonable expectation of privacy in electronic mail (e-mail) or in any use of the district's computer network or equipment. The district reserves the right to monitor, access and/or view any emails/files/materials stored on district equipment or any material used in conjunction with the district's computer network at any time for any reason.

VI. Sanctions

All users of the district's computer network and equipment are required to comply with the district's policy and regulations governing the district's computer network. Failure to comply with the policy or regulation may result in suspension and/or revocation of computer access privileges as well as disciplinary action in accordance with the Code of Conduct and/or Civil Service, Education Law and/or collective bargaining agreements, as applicable. .

In addition, illegal activities are strictly prohibited. Any information pertaining to or implicating illegal activity will be reported to the proper authorities. Transmission of any material in violation of any federal, state and/or local law or regulation is prohibited. This includes, but is not limited to materials protected by copyright, threatening or obscene material or material protected by trade secret. Users must respect all intellectual and property rights and laws.

VII. District Responsibilities

The district makes no warranties of any kind, either expressed or implied, for the access being provided. Further, the district assumes no responsibility for the quality, availability, accuracy, nature or reliability of the service and/or information provided. Users of the district's computer network and the Internet use information at their own risk. Each user is responsible for verifying the integrity and authenticity of the information that is used and provided.

The district will not be responsible for any damages suffered by any user, including, but not limited to, loss of data resulting from delays, non-deliveries, mis-deliveries, or service interruptions caused by its own negligence or the errors or omissions of any user. The district also will not be responsible for unauthorized financial obligations resulting from the use of or access to the district's computer network or the Internet.

Further, even though the district may use technical or manual means to regulate access and information, these methods do not provide a foolproof means of enforcing the provisions of the district policy and regulations.

Regulations adopted: 1/11/16

CITY SCHOOL DISTRICT
City of White Plains, NY

PERSONNEL

Internet Safety

The Board of Education is committed to undertaking efforts that serve to make safe for children the use of district computers for access to the Internet and World Wide Web. To this end, although unable to guarantee that any selected filtering and blocking technology will work perfectly, the Board directs the Superintendent of Schools to procure and implement the use of technology protection measures that block or filter Internet access by:

- Adults to visual depictions that are obscene or child pornography, and
- Minors to visual depictions that are obscene, child pornography, or harmful to minors, as defined in the Children's Internet Protection Act.

Subject to staff supervision, however, any such measures may be disabled or relaxed for adults conducting bona fide research or other lawful purposes, in accordance with criteria established by the Superintendent or his or her designee.

The Superintendent or his or her designee also shall develop and implement procedures that provide for the safety and security of students using electronic mail, chat rooms, and other forms of direct electronic communications; monitoring the online activities of students using district computers; and restricting student access to materials that are harmful to minors.

In addition, the Board prohibits the unauthorized disclosure, use and dissemination of personal information regarding students; unauthorized online access by students, including hacking and other unlawful activities; and access by students to inappropriate matter on the Internet and World Wide Web. The Superintendent or his or her designee shall establish and implement procedures that enforce these restrictions.

The Director of Management Information Systems (MIS) designated under the district's policy on the acceptable use of district computers (policy 4526) shall monitor and examine all district computer network activities to ensure compliance with this policy and accompanying regulations. He or she also shall be responsible for ensuring that staff and students receive training on their requirements.

All users of the district's computer network, including access to the Internet and World Wide Web, must understand that use is a privilege, not a right and that any such use entails responsibility. They must comply with the requirements of this policy and accompanying regulation, in addition to generally accepted rules of network etiquette, and the district's policy on the acceptable use of computers and the internet (policy 4526). Failure to comply may result in disciplinary action including, but not limited to, the revocation of computer access privileges.

PERSONNEL

As part of this policy, and the district's policy on acceptable use of district computers (policy 4526), the district shall also provide age-appropriate instruction regarding appropriate online behavior, including:

1. interacting with other individuals on social networking sites and in chat rooms, and
2. cyberbullying awareness and response.

Instruction will be provided even if the district prohibits students from accessing social networking sites or chat rooms on district computers.

Cross-ref: 4526, Technology Use in Instruction/Acceptable Use of District Computer Networks

Ref: Children's Internet Protection Act, Public Law No. 106-554
Broadband Data Services Improvement Act/Protecting Children in the 21st Century Act, Public Law No. 110-385
47USC 254
20USC 6777

Policy adopted: 1/11/16

CITY SCHOOL DISTRICT
City of White Plains, NY

PERSONNEL

INTERNET SAFETY REGULATIONS

The following rules and regulations implement the Internet Safety Policy adopted by the Board of Education to make safe for children the use of district computers for access to the Internet and World Wide Web.

I. Definitions

In accordance with the Children's Internet Protection Act,

- Child pornography refers to any visual depiction, including any photograph, film video, picture or computer or computer generated image or picture, whether made of produced by electronic, mechanical, or other means, of sexually explicit conduct, where the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct. It also includes any such visual depiction that (a) is, or appears to be, of a minor engaging in sexually explicit conduct; or (b) has been created, adapted or modified to appear that an identifiable minor is engaging in sexually explicit conduct; or (c) is advertised, promoted, presented, described, or distributed in such a manner that conveys the impression that the material is or contains a visual depiction of a minor engaging in sexually explicit conduct.
- Harmful to minors means any picture, image, graphic image file, or other visual depiction that (a) taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion; (b) depicts, describes or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or lewd exhibition of the genitals; and (c) taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

II. Blocking and Filtering Measures

- The Superintendent or his or her designee shall secure information about, and ensure the purchase or provision of, a technology protection measure that blocks access from all district computers to visual depictions on the Internet and World Wide Web that are obscene, child pornography or harmful to minors.
- The district's Director of MIS shall be responsible for ensuring the installation and proper use of any Internet blocking and filtering technology protection measures obtained by the district.
- The Director of MIS or his or her designee may disable or relax the district's Internet blocking and filtering technology measure only for adult

staff members conducting research related to the discharge of their official responsibilities.

- The Director of MIS shall monitor the online activities of adult staff members for whom the blocking and filtering technology measure has been disabled or relaxed to ensure there is not access to visual depictions that are obscene or child pornography.

III. Monitoring of Online Activities

- The district's Director of MIS shall be responsible for monitoring to ensure that the online activities of staff and students are consistent with the district's Internet Safety Policy and this regulation. He or she may inspect, copy, review, and store at any time, and without prior notice, any and all usage of the district's computer network for accessing the Internet and World Wide Web and direct electronic communications, as well as any and all information transmitted or received during such use. All users of the district's computer network shall have no expectation of privacy regarding any such materials.
- "Students may only use the district's Computer Network, resources and applications to access the Internet and World Wide Web for purposes related to their course work. All use, whether during the school day and/or from home, must conform to the district's code of conduct
  Staff supervising students using district computers shall help to monitor student online activities to ensure students access the Internet and World Wide Web, and/or participate in authorized forms of direct electronic communications in accordance with the district's Internet Safety Policy and this regulation.
- The district's Director of MIS shall monitor student online activities to ensure students are not engaging in hacking (gaining or attempting to gain unauthorized access to other computers or computer systems), and other unlawful activities.

IV. Training

- The district's Director of MIS and Coordinator of Instructional Technology shall provide training to staff and students on the requirements of the Internet Safety Policy and this regulation at the beginning of each school year.
- The training of staff and students shall highlight the various activities prohibited by the Internet Safety Policy, and the responsibility of staff to monitor student online activities to ensure compliance therewith.
- The district shall provide age-appropriate instruction to students regarding appropriate online behavior. Such instructions shall include, but not be limited to: Positive interactions with others online, including on social

networking sites and in chat rooms; proper online social etiquette; protection from online predators and personal safety; and hot to recognize and respond to cyber bullying and other threats.

- Students shall be directed to consult with their classroom teacher if they are unsure whether their contemplated activities when accessing the Internet or Worldwide Web are directly related to their course work.
- Staff and students will be advised to not disclose, use and disseminate personal information about students when accessing the Internet or engaging in authorized forms of direct electronic communications.
- Staff and students will also be informed of the range of possible consequences attendant to a violation of the Internet Safety Policy and this regulation.

V. Reporting of Violations

- Violations of the Internet Safety Policy and this regulation by students and staff shall be reported to the Building Principal, and the Direct Supervisor of any staff member.
- The Principal and Staff Supervisor shall take appropriate corrective action in accordance with authorized disciplinary procedures.
- Penalties may include, but are not limited to, the revocation of computer access privileges, as well as school suspension in the case of students and disciplinary charges in the case of staff.

Regulations adopted: 1/11/16

CITY SCHOOL DISTRICT
City of White Plains, NY