4526
( ) Required
(X) Local
(X) Notice

COMPUTER NETWORK ACCEPTABLE USE POLICY

The Board of Education is committed to the use of computer technology to promote student education and administrative efficiency. The Board recognizes that a computer network and the Internet are invaluable educational, administrative and research tools. The Board encourages the use of computers and computer-related technology in the District's classrooms and offices. However, 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 Superintendent of Schools shall establish regulations that govern the use and security of the District's computer network. All users of the District's computer network and equipment must comply with this policy and its regulations. Failure to comply may result in disciplinary action; suspension and/or revocation of computer access privileges; and possible legal action.

District records include all emails and other electronically-stored information when they are created in the course of District business and retained as evidence of official policies, decisions or actions. All District records must be retained in accordance with law and are subject to disclosure. Users (including students, faculty and staff) have no right to privacy or confidentiality when using or accessing the District's computer equipment and network.

The Superintendent shall designate a computer network coordinator to oversee the use of District computer resources. The computer coordinator will prepare in-service programs for the training and development of District staff in computer skills; electronic record retention policy and practices; and the incorporation of computer use into the curriculum.

The Superintendent, in conjunction with the designated purchasing agent for the District, the computer network coordinator and the instructional materials planning committee, shall be responsible for the recommendation to purchase and distribute 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. Questions about this policy should be directed to the designated computer network coordinator, records access officer or a direct supervisor.

To protect personally identifiable student information, any staff member wishing to utilize web-or cloud-based subscription services that make use of student names and/or ID numbers, must receive prior approval from the Director of Technology. The Director of Technology will determine if a formal contact is required with the supplier or if the terms of service are sufficient to address privacy and security requirements.

Ref: N.Y. Arts and Cultural Affairs Law §§57.13-57.39 "Local Government Records Law"
N.Y. Education Law §814 "Courses of Study in Internet Safety"

N.Y. Public Officers Law §§84-90, “Freedom of Information Law”
8 N.Y.C.R.R. Ch. IV, Appendix I, “Records Retention and Disposition Schedule ED-1”

Adoption date: November 10, 2009
Amended Date: May 10, 2011
Amended Date: August 25, 2015

COMPUTER NETWORK ACCEPTABLE USE REGULATION

The following Regulations shall govern acceptable use of the District's computer network and access to the Internet.

I. Administration Responsibilities

- The Superintendent of Schools shall designate a computer network coordinator to oversee the District's computer network.
- The computer network coordinator shall monitor and examine all network activities, as appropriate, to ensure proper use of the computer network.
- The computer network coordinator is responsible for disseminating the District's Policy and Regulations that govern acceptable use for all users.
- The computer network coordinator will provide employee training for proper use of the District's computer network. The coordinator will also ensure that staff-persons who supervise student use of the network will provide similar training to their students. This may include providing copies of the District's Computer Network Acceptable Use Policy and Regulations. All students in grades 2 through 12 shall be required to receive the most current "Proper and Acceptable Student Technology Use" document. This document is to be returned to the school, signed by the student and a parent or guardian, before computer access is granted.
- The computer network coordinator will ensure that school district personnel are informed of their responsibility to retain electronic records in accordance with the "Record Retention and Disposition Schedule ED-1" (ED-1) set forth by the Commissioner of Education.
- The computer network coordinator will take all reasonable steps to ensure that all programs or software loaded onto the computer network have been scanned for viruses.

II. Acceptable Use and Conduct for All Network Users

- Access to the District's computer network is provided solely for District business, education and research in accordance 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, discipline and/or possible legal action.
- Each individual in whose name an access account is issued is responsible at all times for its proper use.
- Each network user will be issued a login name and password. Each user must change this password periodically.
- Each user is expected to abide by generally accepted rules of network etiquette. This includes being polite and using only appropriate language. Abusive language, vulgarities and swear words are never appropriate.

- Each user is expected to protect the privacy and confidentiality of electronically-stored personal information, usernames and passwords on District computers.
- Any user who identifies a security problem on the District's computer network must notify an appropriate teacher, direct supervisor or the computer network coordinator. He or she may not demonstrate the problem to anyone other than the appropriate supervisor.
- Any user who is identified as a security risk or who has a history of violating the District's acceptable use requirements may be denied access to the District's network.

III. Prohibited Activity and Use for All Network Users

The following is a list of prohibited uses of the District's computer network. Any violation may result in discipline or other appropriate penalty.

- Infringing on any copyrights or other intellectual property rights, including copying, installing, receiving, transmitting or making available any copyrighted software on the District's 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 another user's account or password.
- Attempting to read, delete, copy or modify the email of other network users.
- Deliberately interfering with the ability of other users to send, receive or save email or electronic information.
- Forging or attempting to forge email messages.
- Deleting or attempting to delete email messages that the law requires to be retained as District records.
- 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.

- Intentionally disrupting network traffic or crashing the network and connected systems
- Installing software on the District's computers and/or network without the permission of either a direct supervisor or the computer network coordinator.
- Using District's computer equipment or network resources for commercial activity, financial gain or fraud.
- Stealing data, equipment or intellectual property.
- Gaining or seeking to gain unauthorized access to any files, resources or computer or telephone networks.
- Incurring any financial obligation through the use of the District's computer network or the Internet without the express written permission of either a direct supervisor or the computer network coordinator.
- 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 manner that is inconsistent with directions from teachers, staff or generally-accepted network etiquette.

IV. Electronic Communications by District Personnel

Emails and other electronically-stored information that are created in the course of school district business and retained as evidence of official policies, decisions or actions are records, which must be retained in accordance with ED-1 and District Policy; and may be disclosed in accordance with the Freedom of Information Law (FOIL).

Examples of electronic information and email that are records include:

- Policies and directives;
- Correspondence or memoranda related to school district business;
- Work schedules and assignments;
- Agendas and minutes of meetings;
- Drafts of documents that are circulated for comment or approval;
- Documents that initiate, authorize or complete a business transaction; and
- Final reports or recommendations.

By contrast, examples of electronically stored information that are not records include:

- Extra copies of documents;
- Personal messages or telephone message notifications;
- Social event announcements; and
- Copies or summaries of documents distributed for convenience or reference.

To identify the retention period of an email or other electronically stored information, District staff shall identify the type of record the electronic information is, and under which records series it falls in ED-1. Electronic records shall be disposed of in accordance with ED-1 and the District's recordkeeping system. After electronic records are filed in the District's recordkeeping system, users shall dispose of extra copies of such records in a timely manner.

V. Electronic Communications by School Board Members

As public officers, school board members may confer by email and instant message, but may not engage in any series of electronic communications that results in a collective decision, (such as a vote taken by email).

All email and electronically stored information by and between school board members that are records (under the definition set forth above) must receive the same diligent recordkeeping treatment as all other District records in accordance with District policy.

VI. Records Retention Obligations for all District Personnel and Board Members

- All school personnel and board members are expected to file, retain and/or dispose of any email or electronically stored information that constitutes a record in accordance with ED-1 and District policy.
- All school personnel and board members are expected to regard any email or electronic record containing information that is personally identifiable to any student as a confidential student record in accordance with the Family Education Rights and Privacy Act (FERPA).
- All school personnel and board members are expected to regard any email or electronically stored information that constitutes a public record as subject to disclosure under FOIL unless they fall within a statutory exception.

VII. No Privacy Guarantee for Network Users

District personnel and students who use the District's computer network must not expect – and the District does not guarantee – privacy for any use of the District's computer network.

The District reserves the right to access and view any material that is created or accessible on the District's computer equipment or computer network.

In addition to disclosure under FOIL, and FERPA all emails and other electronically stored information may be subject to disclosure as part of discovery proceedings in legal actions.

VII. Sanctions

All users of the District's computer network and equipment are required to comply with the District's Policy and Regulations that govern acceptable use of the District's computer network. Failure to comply with the Policy or Regulations may result in disciplinary action, suspension and/or revocation of computer access privileges.

In addition, any information that pertains to or suggests illegal activity will be reported to the proper authorities for appropriate legal action. Transmission of any material in violation of any federal, state and/or local law or regulation is strictly prohibited. This includes, but is not limited to, materials that are protected by copyright, threatening or obscene material or material protected by trade secret.

VIII. District Responsibilities

The District makes no warranties of any kind, either expressed or implied, for the access being provided. The District assumes no responsibility for the quality, availability, accuracy, nature or reliability of the service and/or information available on the District's computer network or the Internet. 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 used and provided.

The District is not responsible for any damage that may be suffered by any user, including but not limited to the loss of data that may result from delays, delivery failures, unintended deliveries or service interruptions. The District is not responsible for unauthorized financial obligations that may arise through the use of or access to the District's computer network or the Internet.

The District may take precautions to regulate access and information on the District's computer equipment and network, but such methods do not provide a foolproof enforcement of the District's Acceptable Use Policy and Regulation. Ultimately, it is the responsibility of each user not to initiate access to prohibited material.

Adoption date: November 10, 2009
Amended Date: May 10, 2011
Amended Date: August 25, 2015